DAVID MOISÉS TERÁN PÉREZ

ADMINISTRACIÓN Y SEGURIDAD

EN REDES DE COMPUTADORAS

Alfaomega

DAVID MOISÉS TERÁN PÉREZ

ADMINISTRACIÓN Y SEGURIDAD
EN REDES DE COMPUTADORAS

Alfaomega

Director Editorial
Marcelo Grillo Giannetto
mgrillo@alfaomega.com.mx

Jefe de Ediciones
Francisco Javier Rodríguez Cruz
jrodriguez@alfaomega.com.mx

Datos catalográficos
Terán Pérez, David Moisés
Administración y seguridad en redes de computadoras
Primera Edición
Alfaomega Grupo Editor, S.A. de C.V. México
ISBN: 978-607-538-097-1
Formato: 17 x 23 cm Páginas 460

Administración y seguridad en redes de computadoras

Primera edición: Alfaomega Grupo Editor, México, enero 2018

Dr. Isidoro Olvera (Eje 2 sur) No. 74, Col. Doctores, C.P. 06720, Cuauhtémoc, Ciudad de México

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Pág. Web: **http://www.alfaomega.com.co**
E-mail: **cliente@alfaomegacolombiana.com**

ISBN: 978-958-778-407-7

Impreso en Colombia. Printed in Colombia.

Empresas del grupo:

México: Alfaomega Grupo Editor, S.A. de C.V. – Dr. Isidoro Olvera No. 74, Col. Doctores, C.P. 06720, Cuauhtémoc, Cd. de Méx.
Tel.: (52-55) 5575-5022 – Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396
E-mail: atencionalcliente@alfaomega.com.mx

Colombia: Alfaomega Colombiana S.A. – Calle 62 No. 20-46, Barrio San Luis, Bogotá, Colombia
Tels.: (57-1) 746 0102 / 210 0122 – E-mail: cliente@alfaomegacolombiana.com

Chile: Alfaomega Grupo Editor, S.A. – Av. Providencia 1443. Oficina 24, Santiago, Chile
Tel.: (56-2) 2235-4248 – Fax: (56-2) 2235-5786 – E-mail: agechile@alfaomega.cl

Argentina: Alfaomega Grupo Editor Argentino S.A. - Av. Córdoba 1215 Piso 10 - C.P. 1055
Ciudad Autónoma de Buenos Aires, Argentina
Tel/Fax: (54-11) 4811-0887 – E-mail: ventas@alfaomegaeditor.com.ar
www.alfaomegaeditor.com.ar

Acerca del autor

David Moisés Terán Pérez

Es ingeniero mecánico electricista con especialidad en sistemas eléctricos de potencia, egresado de la Universidad Nacional Autónoma de México (UNAM); maestro en Microelectrónica por la Universidad de La Sorbona (París, Francia), maestro en ciencias de la educación por la Universidad del Valle de México (UVM); y doctor en educación por la Universidad Pedagógica Nacional (UPN). Cuenta con 27 años de experiencia como docente en educación superior como la Universidad Nacional Autónoma de México (UNAM), el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM), la Universidad del Pedregal, la Universidad Tecnológica de México (UNITEC), la Universidad ICEL, la Escuela Bancaria Comercial (EBC), entre muchas otras.

A Diana, Emanuel y David

Mensaje del Editor

Una de las convicciones fundamentales de Alfaomega es que los conocimientos son esenciales en el desempeño profesional, ya que sin ellos es imposible adquirir las habilidades para competir laboralmente. El avance de la ciencia y de la técnica hace necesario actualizar continuamente esos conocimientos, y de acuerdo con esto Alfaomega publica obras actualizadas, con alto rigor científico y técnico, y escritas por los especialistas del área respectiva más destacados.

Consciente del alto nivel competitivo que debe de adquirir el estudiante durante su formación profesional, Alfaomega aporta un fondo editorial que se destaca por sus lineamientos pedagógicos que coadyuvan a desarrollar las competencias requeridas en cada profesión específica.

De acuerdo con esta misión, con el fin de facilitar la comprensión y apropiación del contenido de esta obra, cada capítulo inicia con el planteamiento de los objetivos del mismo y con una introducción en la que se plantean los antecedentes y una descripción de la estructura lógica de los temas expuestos; asimismo, a lo largo de la exposición se presentan ejemplos desarrollados con todo detalle y cada capítulo finaliza con unas conclusiones y algunos cuentan con una serie de prácticas.

Los libros de Alfaomega están diseñados para ser utilizados en los procesos de enseñanza aprendizaje, y pueden ser usados como textos en diversos cursos o como apoyo para reforzar el desarrollo profesional; de esta forma, Alfaomega espera contribuir a la formación y al desarrollo de profesionales exitosos para beneficio de la sociedad, y espera ser su compañera profesional en este viaje de por vida por el mundo del conocimiento.

Contenido

Capítulo 7

Introducción

Administración y seguridad en Redes de Computadoras presenta herramientas teóricas y prácticas que permiten a los ingenieros prepararse para las certificaciones de CISCO, las cuales evalúan los conocimientos y las habilidades que se tienen sobre del diseño y soporte de redes. Para ello se muestran una serie de prácticas y bancos de preguntas que simulan las que aplica CISCO.

La obra, como su título lo anuncia, aborda dos temas: la administración de redes de computadoras y su seguridad. En el primero, se plantea cómo configurar la red para que no existan fallas y que ésta sea funcional, dependiendo de la cantidad de usuarios que la utilizan. En la seguridad informática se desarrollan los principios y fundamentos de la teoría de la seguridad informática, además de los objetivos, políticas, procedimientos y arquitectura de la seguridad.

El libro está dividido en siete capítulos, cuenta con dos secciones de prácticas y dos de bancos de preguntas para la certificación de CISCO.

Generalidades sobre la administración de una red de computadoras

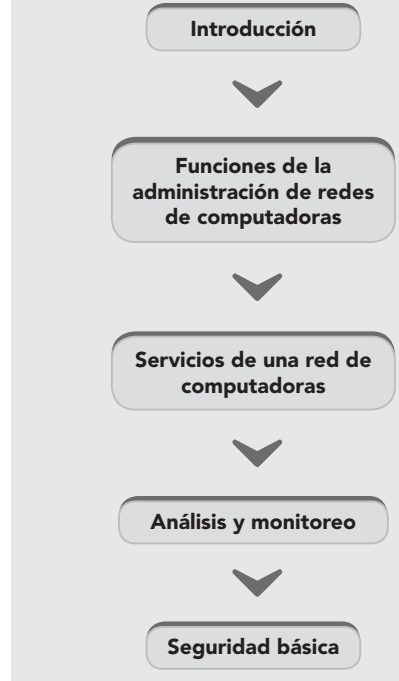
La diferencia entre la genialidad y la estupidez humana: es que la genialidad, sí tiene sus límites.

Albert Einstein

Después de estudiar este capítulo, el lector será capaz de:

- Entender qué es la administración de una red de computadoras.
- Comprender la importancia de la administración de una red de computadoras.
- Establecer en qué consiste la administración de una red de computadoras.

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:



1.1 Introducción

La evolución en las técnicas de gestión de una red de computadoras se dirige siempre con los avances en las tecnologías, lo que ha conducido al progreso de las redes de transmisión de datos en las organizaciones, en las cuales se asientan los diversos sistemas de administración, que se caracterizan por recursos en constante incremento del número, complejidad y heterogeneidad.

En este sentido, las redes de transmisión de datos surgieron como el medio de interconectar diferentes equipos que, instalados de forma remota unos con otros, han ofrecido capacidades de acceso a distintos servicios: diversas capacidades de procesamiento, bases de datos, conocimientos internacionales, compartición de grandes recursos, edición y almacenamiento de información, etcétera (Terán Pérez, 2014).

La administración de redes convergentes de computadoras abarca en general el tratamiento de datos estadísticos e información sobre el estado de distintas partes de la red, y se llevan a cabo las acciones necesarias para ocuparse de fallas y otros cambios. La técnica más primitiva para la monitorización de éstas es hacer *pinging*[1] entre los servidores críticos, método basado en un datagrama de eco (*echo*), el cual produce una réplica inmediata cuando llega al destino (Terán Pérez, 2010).

La mayoría de las implementaciones TCP/IPv4[2] (o en un futuro, el TCP/IPv6) incluyen el *ping*, por medio del cual se sabrá qué ocurre en la red: si se recibe una réplica, significa que el servidor se encuentra activo; en caso contrario, se sabrá que hay algún error. Si los *ping* a todos los servidores de una red no dan respuesta, es lógico concluir que la conexión a dicha red, o esta misma, no funciona; si solamente uno de los servidores no responde, es razonable concluir que sólo un servidor tiene algún problema (Kurose y Keith, 2005). También hay un enfoque oficial TCP/IP para llevar a cabo la monitorización: en la primera fase se usa un conjunto de protocolos SGMP (*Simple Gateway Monitoring Protocol*) y SNMP (*Simple Network Management Protocol*) ambos diseñados para recoger información y cambiar los parámetros de la configuración y otras entidades de la red. El primero se encuentra disponible para varias pasarelas (*gateways*) comerciales, así como para sistemas UNIX; además, tiene mecanismos para añadir informaciones que varían de un dispositivo a otro. Cualquier implementación SGMP necesita que se proporcione un conjunto de datos para que empiece a funcionar (Black, 1997).

Por su parte, el protocolo SNMP apareció a finales de 1988, es ligeramente más complejo y, por ende, requiere mayor información para trabajar, razón por la que usa el llamado MIB (*Management Information Base*), que es resultado de numerosas reuniones de comités formados por vendedores y usuarios. También se espera la elaboración de un equivalente de TCP/IP de CMIS (*Content Management Interoperability Services*), el servicio ISO de monitorización de redes; sin embargo, CMIS y sus protocolos CMIP (*Common Management Information Protocol*) todavía no son estándares oficiales ISO, pero se encuentran en fase experimental.

[1] El mecanismo del comando *ping* es similar al usado en el sonar, puesto que permite observar si hay conectividad entre dos computadoras y registra el tiempo que tardan en llegar los paquetes con relación en la tardanza de la respuesta.

[2] El modelo TCP/IP se utiliza para comunicaciones en red. Éste proporciona conectividad de extremo a extremo especificando la manera en la cual deben ser transmitidos, direcciones, formateados y enrutados los datos para el destinatario.

En términos generales, todos los protocolos persiguen el mismo objetivo, que es recoger información crítica de una forma estandarizada; para ello se ordena la emisión de datagramas UDP (*User Datagram Protocol*) desde un programa de administración de redes que se ejecuta en alguno de los servidores. Por lo regular, la interacción es bastante simple, se realiza con el intercambio de un par de datagramas básicos: una orden y una respuesta. El mecanismo de seguridad también es muy sencillo porque permite que se incluyan contraseñas en las órdenes (en SGMP se conoce como una sesión de nombre —*session name*—, en lugar de una contraseña). También existen métodos de seguridad más elaborados basados en la criptografía, los cuales se abordarán más adelante (Boggs, Mogul y Kent, 1988).

La existencia de dispositivos de comunicaciones dispersos que implementan e interconectan entre sí todas estas redes, obliga a disponer de sistemas de gestión para la configuración, supervisión, diagnóstico y mantenimiento de los dispositivos. Los enlaces de comunicaciones para el acceso a servicios avanzados de telecomunicaciones han permitido que los más avanzados gestionen las redes para un mejor aprovechamiento. Si bien en un principio la administración de una red significaba atención más o menos individualizada a los elementos, en la actualidad se busca una gestión única de la red (Stallings, 2010).

La gestión de redes y de sistemas comprende las aplicaciones específicas que incorporan la posibilidad de gestión e interacción en parámetros asociados al rendimiento, así como de las plataformas web, las bases de datos y, en definitiva, los sistemas que componen la arquitectura de una organización; es decir, los servidores. Aunque por lo regular se identifican con un determinado *hardware* (incluyendo componentes, garantías y actividades de reparación) y un *software* de base estáticos, se requiere realizar actividades continuas de gestión de los mismos para así mejorar la disponibilidad, la seguridad, la integración con el resto de los elementos, la confiabilidad, el rendimiento, etcétera (Terán Pérez, 2010).

Los principales problemas relacionados con la expansión de las redes de computadoras son la administración del correcto funcionamiento día a día y la planificación estratégica de su crecimiento; de hecho, se estima que más del 70% del costo total de una red corporativa se atribuye a estos. Por todo ello, la gestión de red integrada como conjunto de actividades dedicadas al control y vigilancia de los recursos de telecomunicación, se ha convertido en un aspecto de enorme importancia en el mundo de las comunicaciones (Millán Tejedor, 2009).

1.2 Funciones de la administración de redes de computadoras

La administración de redes es una profesión muy demandada. La proliferación de las redes informáticas y las consecuencias en el uso y abuso, ha hecho que la administración de redes, se convierta en una tarea imprescindible para las organizaciones (empresas, industrias, corporativos, dependencias o instituciones). La administración de redes informáticas se vinculada con la tecnología de la información (TI). Esta última se relaciona con el diseño, el desarrollo, la implementación, el soporte y la administración de *hardware*, *software*, y los sistemas informáticos en red. Los profesionales de TI poseen un amplio conocimiento sobre sistemas de computación y sistemas operativos; además gozan de las capacidades necesarias para llevar a cabo la administración de la red.

El concepto de la administración de las redes informáticas define las diversas tareas que desarrollan los profesionales de TI en una red informática con el objetivo de brindar de forma efectiva numerosos servicios de red, garantizando la disponibilidad y la calidad que espera el usuario final. La administración de red involucra personas, *software* y *hardware*. Los administradores de redes son los profesionales de TI que garantizan el servicio continuo al usuario. El conjunto de herramientas de gestión de redes forman parte del *software* que participa en la tarea de administración. Y por ende, el *hardware* se relaciona de forma directa con los dispositivos de red usados para administrar dicha red.

En las empresas y en los centros de datos, la administración de redes de computadoras es más compleja con mayor volumen de trabajo en comparación a la administración de redes domésticas, debido al cúmulo de información que se almacena y a la infraestructura de dichas redes. La administración de redes de computadoras empresariales, se orienta a garantizar con éxito el mantenimiento y funcionamiento adecuado de los servicios de correo electrónico, la administración y la seguridad de las bases de datos y del sitio web empresarial; que por consecuencia contribuye a la satisfacción del cliente.

1.2.1 Configuración y administración

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red, las cuales incluyen

- Servicios de soporte técnico (configuraciones).
- Asegurarse que la red sea utilizada con eficiencia.
- Verificar que los objetivos de calidad del servicio sean alcanzados.

Un administrador de red sirve a los usuarios de distintas formas, crea espacios de comunicación, atiende sugerencias, mantiene a tiempo y en buena forma las herramientas requeridas, vigila el adecuado funcionamiento del *hardware* y *software* de las computadoras y redes a su cargo, también se ocupa de la documentación que describe la red; respeta la privacidad de los usuarios y promueve el buen uso de los recursos (Bertsekas y Gallager, 1992). A cambio de tantas responsabilidades, la recompensa es el buen funcionamiento de la red como un medio que vincula a las personas a través del uso de las computadoras y los programas como herramientas para agilizar algunas labores que dan tiempo y eficiencia para la productividad personal.

De igual forma, el administrador de red debe conocer las reglas de *root* (en sistemas operativos del tipo UNIX, es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos —mono o multiusuario—), que también es llamado súper-usuario o la cuenta del administrador. El *root* puede hacer muchas cosas que un usuario común no puede, como cambiar el dueño o los permisos de los archivos y enlazar a puertos de numeración pequeña. No es recomendable utilizar el usuario *root* para una simple sesión de uso habitual porque se pone en riesgo el sistema al garantizar acceso privilegiado a cada programa en ejecución; por ello, es preferible usar una cuenta normal y el comando su para acceder a los privilegios de *root* de las máquinas que se administra, dado que puede configurar servicios y establecer políticas que afectarán a los usuarios de la red. Algunas de las labores que sólo pueden hacerse desde la cuenta del administrador son:

- Cambiar el nombre de la cuenta que permite gestionar un sistema Linux.
- Configurar los programas que se inician junto con el sistema.
- Administrar las cuentas de usuarios; así como los programas y la documentación instalada.
- Configurar los programas y dispositivos.
- Ajustar la zona geográfica, fecha hora.
- Supervisar el espacio en discos y mantener las copias de respaldo.
- Precisar los servicios que funcionarán en la red.
- Solucionar problemas con dispositivos o programas.

Finalmente, en este contexto, el término "monitoreo" describe el uso de un sistema que revisa constantemente una red de computadoras en busca de componentes defectuosos o lentos para luego informar cuál la problemática y dar solución a la misma (Bhatti y Crowcroft, 2000). La administración de redes es un subconjunto de funciones: mientras que un sistema de detección de intrusos monitorea una red por amenazas externas, otro monitorea en busca de problemas causados por la sobrecarga en la infraestructura y fallas en los servidores, figura 1.1.

Figura. 1.1 Administración de una red de computadoras en la práctica

Para determinar el estatus de un servidor web, un *software* de monitoreo envía con periodicidad peticiones del protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*) con el objetivo de obtener páginas para un servidor de correo electrónico y después enviar mensajes mediante el protocolo SMTP, los cuales posteriormente serán retirados mediante IMAP (*Internet Message Access Protocol*) o POP3 (*Protocolo Post Office*). Por lo general, los datos evaluados son tiempo de respuesta y disponibilidad (*uptime*), aunque también se obtienen estadísticas con consistencia y fiabilidad que han ganado popularidad.

La generalizada instalación de dispositivos de optimización para redes de áreas extensas (WAN, *Wide Area Network*) tiene un efecto adverso en la mayoría del *software* de monitoreo, en especial al intentar medir de manera precisa el tiempo de respuesta de punto a punto, dado el límite de visibilidad de ida y vuelta. Las fallas de peticiones de estado producen ciertas acciones variables desde del sistema de monitoreo. Por ejemplo, una alarma puede ser enviada al administrador como una ejecución automática de mecanismos de controles de fallas (Held, 2010).

La monitorización del servidor puede ser interna (por ejemplo, se comprueba su *software*) o externa (revisión manual); en ambas se verifican características como el uso del procesador y la memoria, el rendimiento de la red, el espacio libre en disco y las aplicaciones instaladas. A lo largo de este proceso se comprueban también los códigos HTTP enviados del servidor (definidos en la especificación HTTP RFC[3] 2 616) que son la forma más rápida de comprobar el funcionamiento. A continuación, se dan ejemplos de las herramientas de monitoreo más utilizadas:

Tcpdump. Permite monitorear a través de comandos de la consola de LINUX, todos los paquetes que atraviesan la interfaz indicada. A la par de los múltiples filtros, parámetros y opciones, *tcpdump* ofrece infinidad de combinaciones para monitorear, como el tráfico que ingresa de una IP, un servidor o una página determinada; se puede solicitar el tráfico de un puerto específico o pedirle que muestre todos los paquetes cuyo destino sea una dirección MAC determinada.

Wireshark: *sniffer.*[4] Captura las tramas y paquetes que pasan a través de una red. Cuenta con todas las características estándar de un analizador de protocolos y posee una interfaz gráfica fácil de manejar. Se usa con frecuencia en Ethernet, aunque es compatible con otras redes.

Hyperic. Aplicación que posibilita administrar infraestructuras virtuales, físicas y en la nube. Este programa autodetecta muchas tecnologías y cuenta con dos versiones: una *open source* y una comercial. Algunas de sus características son la optimización para ambientes virtuales que integran *vCenter* y *vSphere*, también cuenta con capacidad para funcionar en 75 componentes comunes como bases de datos en dispositivos y servidores de red y detecta de forma automática los componentes de cualquier aplicación virtual.

Nagios. Sistema de monitoreo que concede a cualquier empresa identificar y resolver errores críticos antes de que afecten los procesos de negocio. En caso de un error, la aplicación se encarga de alertar al grupo técnico para que rápidamente sea resuelto sin afectar a los usuarios finales.

[3] Los RFC o *Request for Comments* son publicaciones de cierto grupo de trabajo de ingeniería de Internet que describen distintos aspectos del funcionamiento de éste en protocolos y redes de computadoras.

[4] El programa informático que registra la información enviada por los periféricos, así como la actividad en una computadora.

La evolución y tendencias de las herramientas de monitoreo de redes establecen retos a los ejecutivos de la Tecnología de la Información (TI) como mostrar los datos de su operación para que los ejecutivos de la organización dispongan de elementos suficientes para reconocer y fomentar la importancia de la tecnología como un componente habilitador del negocio (Held, 2010). Dicha evolución se ha alimentado mediante la llegada de protocolos más avanzados de visualización de tráfico como Netflow, Jflow, Cflow, Sflow, IPFIX o Netstream; el propósito hoy en día es tener una perspectiva global del "todo" para categorizar adecuadamente los eventos que afectan el desempeño de un servicio o del proceso de negocio involucrado (Held, 2010). De hecho, a medida que han avanzado las tecnologías, se ha atravesado por diferentes etapas en el monitoreo de redes, las cuales se enumeran a continuación:

Primera generación. Aplicaciones propietarias para monitorear dispositivos activos o inactivos. La industria ha desarrollado un sinfín de herramientas para tratar de presentar los recursos de una forma amable y en tiempo real, éstas presentan los elementos a través de un código universal de colores:

Verde: todo funciona en orden.

Amarillo: detección de algún problema temporal que no afecta la disponibilidad; sin embargo, se deben realizar ajustes para no perder la comunicación.

Anaranjado: el problema se ha hecho persistente y requiere pronta atención para evitar afectaciones a la disponibilidad.

Rojo: el dispositivo se encuentra fuera de servicio en ese momento y requiere acciones inmediatas para su restablecimiento.

Segunda generación. Aplicaciones de análisis de parámetros de operación a profundidad; por medio de estos, las herramientas realizan un análisis detallado con el fin de evaluar los estados de los componentes dentro de los dispositivos (microprocesador, memoria, espacio de almacenamiento, paquetes enviados y recibidos, *broadcast*, *unicast*, *multicast*, etcétera); de manera que es posible ajustar los parámetros y establecer los niveles de servicio del dispositivo. Este tipo de aplicaciones se apoyan en *sniffers* y en elementos físicos distribuidos conocidos como probadores (*probes*), cuya función es, exclusivamente, colectar estadísticas del tráfico, controladas desde una consola central.

Tercera generación. Aplicaciones de análisis punta a punta con enfoque al servicio. Con mayores niveles de información sobre los dispositivos se tienen elementos adicionales de análisis, pero aún no existen suficientes parámetros para tomar decisiones. Esta generación de aplicaciones con enfoque transaccional captura flujos de tráfico e identifica cuellos de botella y latencias a lo largo de las conexiones que existen entre los componentes de un servicio, entregando información acerca de "la salud" de éste; además logra conectar todas las partes de manera más eficiente; en dicho caso, cada dispositivo sabe cuándo se debe informar a otro sin afectarlo en sus tareas, esto para no generar una sobrecarga de información, lo cual significa que existe una toma de decisiones con enfoque de repercusión, generada en los negocios.

Cuarta generación. La personalización de indicadores de desempeño de los procesos de negocio llevando el crecimiento de las soluciones tecnológicas a los requerimientos de las organizaciones actuales dentro de las cuales están aquellas que monitorean el Desempeño de Aplicaciones (APM, *Application*

Performance Management), donde convergen elementos de tecnología (*Backend*) con los sistemas de los que forman parte para llevar a cabo las transacciones que impulsan los procesos de negocio (*Frontend*); en otras palabras, es un análisis de "punta a punta". El potencial de estas herramientas permite tener información simultánea de:

- Predicciones del desempeño.
- Modelado de escenarios (simulación y emulación).
- Análisis y planeación de capacidades.
- Funcionalidades de ajustes a las configuraciones.
- Mediciones de impacto al negocio (calidad, salud y riesgos en los servicios prestados).
- Experiencia del usuario.

En resumen, el término "configuración" tiene un significado diferente dependiendo del contexto en que sea utilizado, aun dentro del diseño y la operación de las redes de computadoras (Held, 2010). Una configuración puede ser:

- Una descripción de un sistema distribuido basado en la ubicación física y geográfica de los recursos, la cual incluye la manera en que se encuentran interconectados además de la información sobre las relaciones lógicas. Ésta puede basarse en diferentes puntos de vista (organizacional, administrativo, etcétera) o en aspectos relacionados con la seguridad.
- Un proceso para manipular la estructura del sistema distribuido donde se establecen o modifican parámetros que controlan la operación y ajustan el ambiente requerido para su funcionamiento normal.
- El resultado de un proceso de ordenamiento donde el sistema generará un conjunto de ciertos valores de los parámetros característicos para la operación normal del recurso.

La configuración, como el proceso de adaptación de los sistemas a un ambiente operativo, implica instalar nuevo *software*, actualizar el viejo, conectar dispositivos y hacer cambios en la topología de la red o en su tráfico (Day y Zimmermann, 1983); aunque ésta se acompaña de técnicas para hacer cambios e instalaciones físicas, se considera intensiva en procesos controlados por *software* y ajuste de parámetros, que incluyen, entre otros, selección de funciones, autorización, protocolos (longitud de los mensajes, tamaños de ventanas, timers, prioridades), de conexión (tipo y clases de dispositivo, velocidad de transmisión, paridad); en entradas en las tablas de enrutamiento, en servidores de nombres; en directorios; en parámetros de filtraje para cortafuegos (*firewalls*) y encaminadores (*routers*); para el algoritmo de STP (*Spanning Tree Protocol*),[5] para los enlaces conectados a los encaminadores (interfaces, ancho de banda), para máxima cuota de los usuarios, etcétera.

Los siguientes aspectos se presentan en relación con el proceso de la configuración, donde las herramientas que ayudan a disponer los componentes son:

[5] STP es un protocolo de red, nivel 2 del Modelo OSI (capa de enlace de datos); gestiona la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones), además, permite a los dispositivos de interconexión activar o desactivar en automático los enlaces de conexión de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones del usuario.

Lugar. Una configuración puede hacerse en el mismo dispositivo o realizarse de forma remota; por ejemplo, por medio de un servidor DHCP. El sistema que se configura no siempre es compatible desde el equipo (servidor remoto) a configurar, esto puede deberse a razones técnicas, de organización o seguridad.

Almacenamiento. La configuración puede almacenarse en NVRAM (*Non-Volatile Random Access Memory*), en discos duros, en un *boot server* para ser "invocada" a través de los protocolos adecuados o, incluso, es posible que se recargue a través de la red.

Validez. Una configuración estática es aquella donde cada reconfiguración implica interrumpir la operación del componente (apagar y prender o reiniciar el sistema). Una dinámica, por otra parte, permite hacer cambios mientras el componente opera.

Interfaz de usuario del configurador. La calidad de la interfaz de usuario depende de la magnitud de los parámetros que pueden ser modificados con rapidez o aplicados al mismo tiempo a varios dispositivos. El sistema de configuración y la documentación de ésta deben estar protegidos de uso no autorizado (con contraseñas, en áreas físicas restringidas, con seguridad del protocolo de configuración, etcétera).

La administración de la configuración implica establecer parámetros, definir valores de umbral (*threshold*), determinar filtros, asignar nombres a los objetos administrados, proveer la documentación necesaria y cambiar las configuraciones cuando sea necesario (figura 1.2).

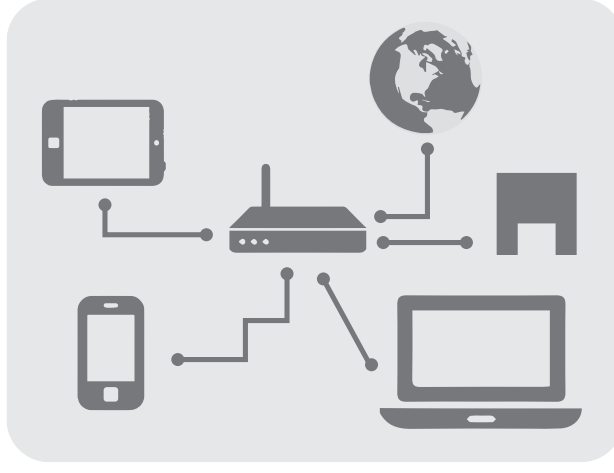


Figura. 1.2 Administración de la configuración para el uso de equipos en una red de computadoras

Las herramientas para la administración de la configuración deberían cubrir:

- Autotopología y autodescubrimiento de los componentes de red permitiendo extrapolar una descripción de la configuración a partir de un ambiente real.

- Sistemas para describir la documentación de las configuraciones o bases de datos maestras.
- Elementos para generar mapas de la configuración de una red. Es decir, el uso de MRTG (*Multi Router Traffic Grapher*) que en la práctica es un recopilador de datos del tráfico de la red, para supervisar la red. O también, el uso de Nagios que es un sistema de monitorización de redes.
- Herramientas para activar sistemas de respaldo (*back-up*).
- Instrumentos para establecer e invocar parámetros de configuración y estados del sistema.
- Materiales para distribuir *software* y controlar el uso de licencias.
- Componentes para supervisar y controlar la autorización.

1.2.2 Fallas

La administración de las fallas se relaciona con la detección, aislamiento y eliminación de comportamientos anormales del sistema (figura 1.3). La identificación y seguimiento de éstas es un problema operacional importante en todos los sistemas de procesamiento de datos (Lin y Costello, 2004). En comparación con sistemas no conectados a una red, la administración de fallas en redes de computadoras y sistemas distribuidos es más difícil por una diversidad de razones que incluyen, entre otras, el mayor número de componentes involucrados, la amplia distribución física de los recursos, la heterogeneidad de los componentes de *hardware* y *software*, así como las diferentes unidades de la organización involucradas.

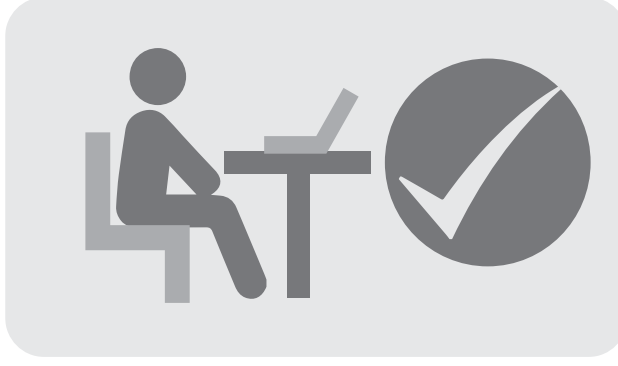


Figura 1.3 Correcta administración de las fallas en una red de computadoras

Una falla puede ser definida como una desviación de las metas operacionales establecidas con respecto en las funciones del sistema o los servicios. Los mensajes sobre las fallas son dados a conocer por el mismo componente o por los usuarios del sistema. Algunas de las fuentes más frecuentes de errores son:

- Los elementos que conforman los enlaces (cables UTP o de fibra óptica, líneas dedicadas, canales virtuales, entre otros).

- El sistema de transmisión (*transceivers*, *concentradores*, *switches*, servidores de acceso, encaminadores).
- Sistemas finales (clientes o servidores).
- El *software* de los componentes.
- La operación incorrecta por parte de los usuarios y los operadores.

La función de la administración de las fallas es detectar y corregir con rapidez los errores para asegurar un alto nivel de disponibilidad de un sistema distribuido y los servicios que éste presta; por otro lado, las tareas son:

- Monitoreo del sistema y la red.
- Respuesta y atención a alarmas.
- Diagnóstico de las causas de la falla.
- Establecer la propagación de errores.
- Presentar y evaluar medidas para recuperarse de los errores.
- Operación de sistemas de etiquetación de problemas (TTS, *Trouble Tickets Systems*)
- Proporcionar asistencia a usuarios *(Help Desk*).

Además, las siguientes capacidades técnicas pueden ayudar en el análisis de fallas:

- Autoidentificación de los componentes del sistema.
- Realización de pruebas, por separado, con los componentes del sistema.
- Facilidades de seguimiento (*tracing*).
- Disposición de una bitácora (*log*) de errores.
- Hacer eco de los mensajes en todas las capas del protocolo.
- Posibilidad de revisar los vaciados (*dumps*) de memoria.
- Métodos para generar errores a propósito en ambientes predefinidos para el sistema.
- Posibilidad de iniciar rutinas de autoverificación y transmisión de datos de prueba a puertos específicos (*test de loops*, *test remotos*), al igual que pruebas de asequibilidad con paquetes ICMP (*ping* o *traceroute*).
- Establecer opciones para valores de umbral.
- Activación de reinicios planificados (dirigidos a puertos, grupos de puertos o componentes específicos).
- Disponibilidad de sistemas para realizar tests especiales (osciloscopios, reflectómetros, probadores de interfaces, analizadores de protocolos, monitoreadores de *hardware* para supervisión de líneas).
- Soporte de mecanismos de filtraje para mensajes de fallas o alarmas y correlación de eventos para reducir el número de eventos relevantes y para análisis de las causas de los problemas.
- Interfaces de herramientas de administración de fallas a sistemas de etiquetación de problemas y soporte técnico o ayuda al usuario (*help desk*); es decir, propagación automática de notificaciones y correcciones de fallas.

1.2.3 Contabilidad (administración de los usuarios)

La administración de los usuarios comprende tareas como la gestión de los nombres y las direcciones, servicios relacionados con directorios y permisos para el uso de los recursos, así como de contabilidad (figura 1.4), pues existen costos asociados al proporcionar servicios de comunicaciones que deben ser informados a los usuarios (cargos de acceso y de utilización).

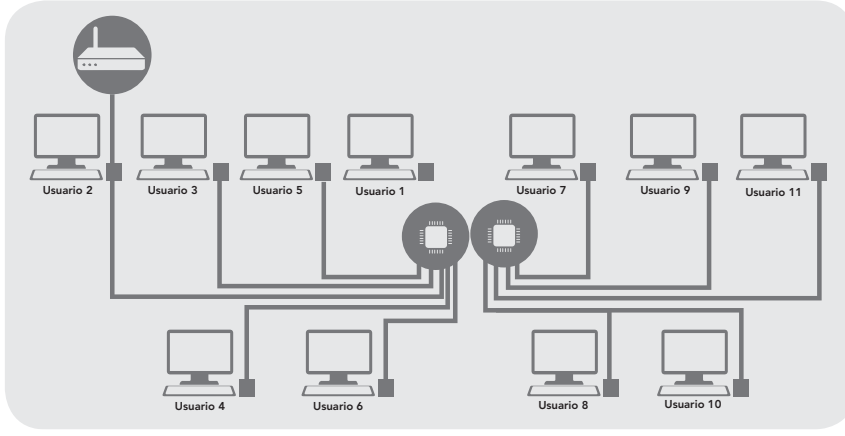


Figura 1.4 Representación de la administración de los usuarios en una red de computadoras.

Las estrategias y procedimientos para la asignación de costos no pueden ni deben ser establecidos rígidamente por un sistema de contabilidad; además, es importante que su administración sea capaz de ajustarse a los lineamientos de una política dada (Chen y Nahrstedt, 1998).

La administración de la contabilidad también incluye la recopilación y cuidado de estadísticas de uso, definición de unidades de contabilización, asignación de cuentas y costos, mantenimiento de bitácoras de contabilidad, establecimiento y monitoreo de las cuotas concedidas y, finalmente, definición de políticas de contabilidad y tarifas que permitirán generar facturas y cargos a los usuarios. Si varios proveedores están involucrados en la prestación de los servicios, las reglas de conciliación también pertenecen a la administración de la contabilidad. Este proceso puede realizarse repartiendo ingresos mediante una tarifa plana o con un precio para cierta unidad de tráfico.

Cómo se implemente el sistema de contabilidad, qué enfoque se utilizará para recopilar los parámetros de contabilidad y cómo serán distribuidos los costos, es una decisión administrativa que puede ser influenciada por políticas de la organización. Entre más sutil sea el enfoque, más complicado e intensivo en costos es el procedimiento de contabilidad.

Los parámetros "de uso" utilizados para calcular los costos incluyen la cantidad de paquetes o *bytes* transmitidos, la duración de la conexión, el ancho de banda, la calidad del servicio o Q_OS (*Quality of Service*), la conexión, la localización de los participantes en la comunicación, los costos para servicios de conversión de protocolos vía una pasarela (*gateway*), el uso de recursos en los servidores y el de productos de *software* (control de licencias). Además de los costos variables, también se tienen en cuenta los fijos (espacio de oficina, mantenimiento, depreciación de muebles y equipos, etcétera).

1.2.4 Desempeño

En términos de los objetivos (muy concretos y específicos), la administración del desempeño se entiende como una continuación sistemática de la administración de fallas: mientras que ésta última es la responsable de asegurar que una red de comunicaciones o un sistema distribuido solamente opere, la segunda busca que el sistema, como un todo, se comporte bien; es decir, se enfoca en la calidad del servicio (figura 1.5) (Clark, Shenker y Zhang, 1992).

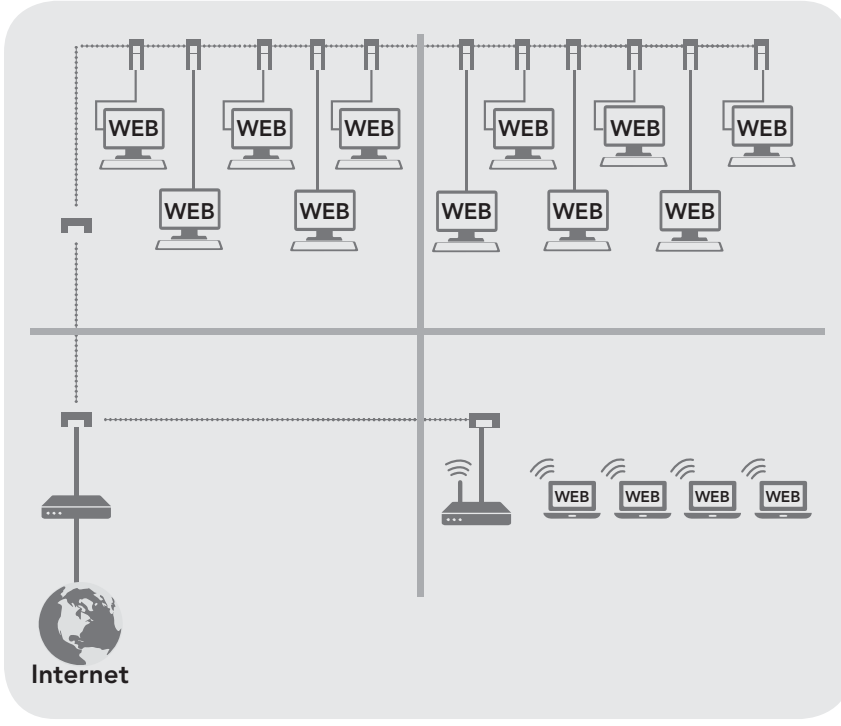


Figura 1.5 Administración del desempeño de una red de computadoras

La calidad del servicio (Q_OS) es un mecanismo para establecer una interfaz que permita "negociar" entre el proveedor y el cliente. Su importancia se incrementa a medida de que más relaciones entre estos se involucran en la implementación de redes corporativas o de sistemas distribuidos (Tompros y Denazis, 2007). Entonces, la interfaz de servicios es definida por las siguientes características:

- Especificación del servicio y del tipo de éste (determinístico, estadístico, el mejor posible).
- Definición de los parámetros de Q_OS relevantes con valores cuantificables incluyendo los de uso, promedio y límite; entre muchos otros.
- Establecimiento de las operaciones de monitoreo.
- Descripción de reacciones a cambios de los parámetros de Q_OS.

Sin embargo, es difícil y no siempre posible proporcionar una definición completa de una interfaz de servicios sobre la base de lo escrito antes (Salazar *et al.*, 2002) que tienden a aparecer las siguientes situaciones:

Problemas en el mapeo vertical de Q_OS. Gracias a que los sistemas de comunicación son sistemas por capas, los parámetros de Q_OS específicos a la capa N tienen que ser mapeados de dicha manera: (N+1) o (N-1). Por ejemplo, un parámetro de la Q_OS orientada a la aplicación (en este caso, calidad de transmisión de voz), se debe mapear a la Q_OS dependiente de la red (*jitter*). Las jerarquías de Q_OS aún no están definidas por completo para todos los protocolos o servicios. Esta situación se exacerba cuando los servicios de diferentes capas se proveen por distintos proveedores (*carriers*).

Problemas en el mapeo horizontal de Q_OS. Si más de un proveedor participa en una red corporativa, el resultado puede ser la concatenación de diferentes subredes o secciones de troncales, que son utilizadas para proveer un servicio con una calidad uniforme entre dos usuarios. Se asume que cada *carrier* tiene implementadas las mismas características de calidad de servicio o, al menos, utiliza protocolos de negociación de Q_OS, de reservación de recursos o administración estandarizados. Cuanto más complejo sea el servicio, menos probable es que se reúnan estos requerimientos.

Métodos de medición. La forma óptima para calcular la Q_OS sería aplicar métodos de medida basados en cantidades visibles en la interfaz de servicio antes que utilizar un análisis de la tecnología suministrada por el proveedor, pues ésta puede cambiar rápidamente y, además, las cantidades medidas no son de interés del cliente; por ello, para él deben ser convertidas a los parámetros de Q_OS.

En resumen, la administración del desempeño incorpora todas las medidas requeridas para asegurar que la calidad del servicio (Q_OS) cumpla con un contrato de nivel de servicios (Bhatti y Crowcroft, 2000), esto incluye:

- Establecer métricas y parámetros de calidad de servicio.
- Monitorear todos los recursos para detectar posibles y reales "cuellos de botella" en el desempeño, así como traspasos de los umbrales.
- Realizar medidas y análisis de tendencias para predecir fallas que puedan ocurrir.
- Evaluar bitácoras históricas (*logs*).
- Procesar los datos medidos y elaborar reportes de desempeño.
- Llevar a cabo planificación de desempeño y de capacidad (*capacity planning*), lo cual implica proporcionar modelos de predicción, simulados o analíticos, utilizados para verificar los resultados de nuevas aplicaciones, mensajes de afinamiento y cambios de configuración.

1.2.5 Seguridad

La seguridad se relaciona con los sistemas distribuidos y los recursos de la compañía que "vale la pena" proteger como la información, la infraestructura de tecnologías de la información (ITI) y los servicios, los cuales se encuentran expuestos a amenazas o al uso inadecuado (Berghel, 2001). Las medidas de seguridad son necesarias para prevenir

daños y pérdidas, así como para establecer acciones que busquen "enfrentar" las amenazas y riesgos obtenidos como resultado de los análisis de seguridad del sistema en red (Anderson, 2008); los cuales, por lo regular, derivan de:

Ataques pasivos. Robo de información llevado a cabo de forma oculta y a través del análisis de tráfico de la red.

Ataques activos. Accesos no autorizados por medio de elementos como virus, tras lo que se lleva a cabo, por ejemplo, suplantación de usuarios, traducida en una manipulación de secuencias de mensajes, manejo de los recursos al recargar su uso, reconfiguración no autorizada, reprogramación de sistemas, etcétera.

Mal funcionamiento de los recursos.

Comportam**iento inapropiado o deficiente y respuestas de operación incorrectas.**

Las metas y los requerimientos de seguridad se establecen a partir de análisis de amenazas y de los valores que necesitan protección (Berghel, 2001). Las políticas de seguridad definidas podrán identificar los requerimientos de seguridad; algunos ejemplos son:

- Las contraseñas (*passwords*) deben ser cambiadas cada tres semanas.
- Sólo los gerentes de segunda línea tienen acceso a los datos del personal.
- Todos los ataques que afecten la seguridad del sistema serán registrados y se les hará un seguimiento.

Dichas políticas sirven como marco de referencia para los servicios de seguridad necesarios y su implementación; por ello, la administración de seguridad comprende los siguientes puntos:

- Realizar un análisis de las posibles y probables amenazas.
- Definir e implementar políticas reales de seguridad.
- Verificación de la identidad (autenticación basada en firmas digitales y en la certificación).
- Establecer e implementar controles de acceso.
- Garantizar la confidencialidad (encriptación).
- Asegurar la integridad de los datos (autenticación de mensajes).
- Monitoreo de los sistemas para prevenir amenazas de seguridad.
- Elaborar reportes sobre el estado de la seguridad y su vulneración o de sus intentos.

Podría asumirse que un conjunto de procedimientos de seguridad reconocidos, cuya mayor parte está disponible como software de dominio público, ya existe en el área de administración de seguridad. El principal problema es encontrar la forma correcta de incorporarlos a una arquitectura de la administración y de controlarlos de una manera uniforme dentro del marco de las políticas de seguridad.

1.3 Servicios de una red de computadoras

La finalidad de los servicios de una red de computadoras, es que los usuarios de los sistemas informáticos de una organización, puedan hacer un mejor uso de los mismos, enriqueciendo de este modo el rendimiento global de la organización. Así, las organizaciones obtienen una serie de ventajas del uso de las redes en los entornos de trabajo como son:

- Mayor facilidad de comunicación.
- Mejora de la competitividad.
- Mejora de la dinámica de grupo.
- Reducción del presupuesto para el procesamiento de los datos, y convertirlos en información útil, para apoyar la toma de decisiones. Así como, para convertirse en conocimiento.
- Reducción de los costos de proceso por usuario.
- Mejoras en la administración de los paquetes y de los programas.
- Mejoras en la integridad de los datos.
- Mejora en los tiempos de respuesta.
- Flexibilidad en el proceso de datos.
- Mayor variedad en el uso de paquetes y de programas.
- Mayor facilidad de uso.
- Mejor y mayor seguridad.

Para que todo esto sea posible, la red debe prestar una serie de servicios fundamentales a los usuarios como:

- Acceso
- Ficheros
- Impresión
- Correo
- Información
- Otros (a especificar)

Para la prestación de los servicios de la red, se requiere que existan sistemas en la red con capacidad para actuar como servidores. Los servidores y los servicios de red, se basan en los sistemas operativos de la red (los cuales pueden ser centralizados o distribuidos). Un sistema operativo de red, es un conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios. Estos programas interceptan las peticiones de servicio de los usuarios, y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red, le permite a ésta, ofrecer capacidades de multiproceso y multiusuario.

1.3.1 DHCP

El protocolo de configuración dinámica de *host* o DHCP (*Dynamic Host Configuration Protocol*) permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor que por lo regular el servidor posee una lista de direcciones IP dinámicas que se asignan a los clientes, sabiendo en todo momento quién ha estado en posesión de cada una, cuánto tiempo la ha tenido y a quién ha sido concedida después. DHCP se estableció como una extensión del protocolo *Bootstrap* (BOOTP), el cual fue extendido porque se requería intervención manual para completar la información de configuración en cada cliente sin proporcionar un mecanismo para la recuperación de las direcciones IP en desuso. En la actualidad, éste se mantiene como el estándar para redes IPv4.

En octubre de 1993, este protocolo se publicó por primera y su implementación actual se encuentra en el estándar RFC 2 131, aunque de forma original, se definió bajo 1 531; para DHCPv6 se publica el estándar RFC 3 315 (figura 1.6), aunque 3 633 le añadió un mecanismo de delegación de prefijo (Joel, 2002).

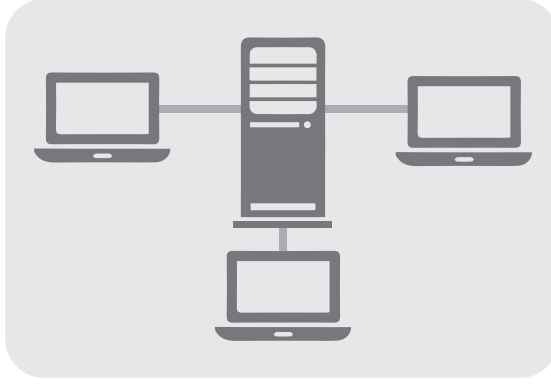


Figura 1.6 Importancia de integrar un servidor DHCP en una red de computadoras

DHCPv6 se amplió aún más para proporcionar información a los clientes con la configuración automática de direcciones sin estado en el RFC 3 736. El protocolo BOOTP, a su vez, fue definido por primera vez en el 951 como un reemplazo para la resolución de direcciones inversa o RARP (*Reverse Address Resolution Protocol*). La principal motivación para dicha sustitución fue que este último era un protocolo de la capa de enlace de datos, lo cual hizo más difícil su aplicación en muchas plataformas de servidores y requería uno presente en cada enlace de red individual.

BOOTP introdujo la innovación de un agente de retransmisión, lo que permitió el envío de paquetes BOOTP fuera de la red local utilizando enrutamiento IP estándar, por lo que un servidor central podría servir de anfitrión en muchas subredes IP (Croft, 2005).

El DHCP permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias, así como asignar y enviar en automático una nueva, si el dispositivo es conectado en un lugar diferente de la red (Perkins, 2002). El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

Asignación manual o estática. Se proporciona una dirección IP a una máquina determinada; suele utilizarse cuando se quiere controlar la asignación de dirección IP a cada cliente y, a la par, evitar que se conecten clientes no identificados.

Asignación automática. Determina una dirección IP a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se utiliza cuando el número de clientes no varía demasiado.

Asignación dinámica. Es el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de éstas y cada dispositivo conectado a la red está configurado para solicitar la suya al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable; esto facilita la instalación de nuevas máquinas-clientes a la red.

Algunas implementaciones de DHCP pueden actualizar el sistema de nombres de dominio o DNS (*Domain Name System*), asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2 136 (versión en inglés). Dichas opciones configurables están definidas en RFC 2 132 (versión en inglés) y se presentan a continuación:

- Dirección del servidor y nombre DNS.
- Puerta de enlace de la dirección IP.
- Dirección de publicación masiva (*broadcast address*).
- Máscara de subred.
- Tiempo máximo de espera del protocolo de resolución de direcciones o ARP (*Adress Resolution Protocol*).
- Unidad de transferencia máxima o MTU (*Maximum Transmission Unit*) para la interfaz.
- Dominios y servidores de servicio de información de red o NIS (*Network Information Service*).
- Servidores de protocolo de tiempo de red o NTP (*Network Time Protocol*).
- Servidor SMTP.
- Servidor TFTP.
- Nombre del servidor WINS (*Windows Internet Naming Service*).

1.3.2 DNS

Al explicar las características del DNS, se debe establecer que un nombre de dominio consiste en dos o más partes, técnicamente etiquetas, separadas por puntos cuando son escritas en forma de texto. Por ejemplo, el punto final separa la etiqueta de la raíz de la jerarquía, aunque por lo general, se omite por ser puramente formal. Una muestra de nombre de dominio correcto o FQDN *(Fully Qualified Domain Name*) es "www.ejemplo.com", figura 1.7.

Figura 1.7 Símbolo universal de DNS

A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior (TLD, *Top Level Domain*), como ".com" en www.ejemplo.com u ".org" en es.wikipedia.org. Cada etiqueta

a la izquierda especifica una subdivisión o subdominio.[6] Finalmente, la parte más a la izquierda expresa el nombre de la máquina (*hostname*); el resto sólo determina la manera de crear una ruta lógica a la información requerida. Por ejemplo, el dominio es.wikipedia.org tendría el nombre de la máquina "es", aunque en este caso no se refiere a una máquina física en particular. En teoría, esta subdivisión puede tener hasta 127 niveles, y es posible que cada etiqueta contenga hasta 63 caracteres restringidos para que la longitud total del nombre del dominio no exceda los 255, aunque en la práctica los dominios son casi siempre cortos; estos deben comenzar con una letra[7] y tienen "-" como único símbolo permitido.

Una vez establecido esto, cabe mencionar que el sistema de nombres de dominio (DNS, *Domain Name System*) nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet, pues la empresa estadounidense SRI International (antes sólo SRI o *Stanford Research Institute*) alojaba un archivo llamado hosts, que contenía todos los nombres de dominio conocidos, el crecimiento explosivo de la red causó que esto no resultara práctico, por lo que en 1983, Paul V. Mockapetris publicó los RFC 882 y 883 definiendo lo que hoy en día ha evolucionado hacia el DNS moderno.

El DNS se asocia a información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red y enfocado el propósito de localizarlos y direccionarlos a todo el mundo (Anderson, 2008). Otro de sus usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada uno. Por ejemplo, si la dirección IP del sitio FTP (*File Transfer Protocol*) de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando *ftp.prox.mx* y no la IP, pues, además de ser más fácil de recordar, es más fiable; sin embargo, la dirección numérica podría cambiar por muchas razones, sin que tenga que modificarse el nombre.

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

Clientes fase 1. Programa cliente que se ejecuta en la computadora del usuario y que genera peticiones de resolución de nombres a un servidor DNS.

Servidores DNS. contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

Zonas de autoridad. porciones del espacio de nombres raros de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y sus subdominios.

En el mundo real el DNS funciona de la siguiente forma: los usuarios, por lo general, no se comunican de manera directa con el servidor, sino que la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras usadas en Internet).

La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por su proveedor de Internet, donde la dirección de servidores puede ser ajustada de forma manual o automática mediante DHCP. En otros casos, los administradores de red tienen configurados sus propios servidores DNS. En cualquiera de las dos situaciones los servidores DNS que reciben la petición buscan en primer lugar verificar si disponen de la

[6] El "subdominio" expresa dependencia relativa, no dependencia absoluta.

[7] Véase la RFC 1 035, sección 2.3.1 *Preferencia nombre de la sintaxis*.

respuesta en la memoria caché, pues de ser así, la sirven; en caso contrario, iniciarían la búsqueda de manera recursiva. Una vez encontrada la respuesta, el servidor DNS guardará el resultado en su memoria caché para futuros usos y devuelve el resultado.

1.3.3 Telnet

Telnet (*Telecommunication Network*) es el nombre de un protocolo de red que permite viajar a otra máquina para manejarla de manera remota como si se estuviera sentado delante de ella; también se trata del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se accede debe tener un programa especial que reciba y gestione las conexiones (Braden, 1989). El puerto que se utiliza de manera común es 2,3 (figura 1.8).

Figura 1.8 Funcionamiento de Telnet

Telnet sólo sirve para acceder en modo terminal; es decir, sin gráficos, pero es una herramienta muy útil para arreglar fallas a distancia y para consultar datos personales en máquinas accesibles por la red. Además, se ha utilizado (y aún hoy se puede ocupar en su variante SSH) para abrir una sesión con una máquina UNIX, de modo que múltiples usuarios se conecten, abran sesión y puedan trabajar a través de ésta.

A pesar de sus beneficios, el mayor problema de Telnet es la seguridad porque todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano, lo cual facilita que cualquiera que espíe el tráfico pueda obtener dichos datos; por esta razón, dejó de usarse Telnet hace unos años cuando apareció y se popularizó el SSH. Algunos clientes de Telnet son mTelnet, NetRunner, Putty o Zoc.

Hoy en día, este protocolo también se usa para llegar al sistema de tablón de anuncios o BBS (*Bulletin Board System*) que al principio era accesible con sólo un módem a través de la línea telefónica. Para acceder a un BBS mediante Telnet es necesario un cliente que proporcione soporte a gráficos ANSI y los protocolos de transferencia de ficheros.[8]

[8] El protocolo de transferencia de ficheros más común con mejor funcionamiento es llamado ZModem.

En 1969 se desarrolló Telnet, la mayoría de los usuarios de computadoras en la red estaban en los servicios informáticos de instituciones académicas o en grandes instalaciones de investigación privadas y de gobierno. En este ambiente, la seguridad no fue una preocupación hasta después de la explosión del ancho de banda de los años 90 del siglo XX, pues con la subida exponencial del número de gente con acceso a Internet y, por ende, el aumento en usuarios que procuran ingresar maliciosamente a los servidores de otras personas, Telnet dejó de ser recomendado en redes con conectividad a Internet. En resumen, se hace necesario destacar tres razones principales por las cuales Telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

- Los dominios de uso general de Telnet tienen varias vulnerabilidades descubiertas a lo largo de los años y varias más que aún podrían existir.
- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones con utilidades comunes como *Tcpdump* y *Wireshark*, dando como resultado el uso de la información para propósitos maliciosos.
- Telnet carece de un esquema de autentificación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados y no interceptada entre ellos.

Estos defectos han causado el abandono y depreciación del protocolo Telnet rápidamente a favor de uno más seguro y funcional como SSH lanzado en 1995. Éste proporciona toda la utilidad presente en Telnet, pero agregó el cifrado fuerte para evitar que los datos sensibles sean interceptados y la autentificación mediante llave pública para asegurar que el equipo remoto sea realmente el autorizado. Con base en esto, los expertos en seguridad computacional como el Instituto SANS (*SysAdmin Audit, Networking and Security Institute*) y los miembros del *newsgroup* de *comp.os.linux.security* recomiendan que el uso de Telnet para las conexiones remotas sea descontinuado bajo cualquier circunstancia normal (Braden, 1989).

1.3.4 SSH

SSH (*Secure Shell*) o intérprete de órdenes seguro, es el nombre de un protocolo y del programa que lo implementa, el cual sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, así como redirigir el tráfico de "X" para ejecutar programas gráficos si se tiene un servidor "Y" corriendo en sistemas Unix y Windows.

Además, SSH permite copiar datos de forma segura, como simular sesiones FTP cifradas y gestionar claves RSA[9] (*Rivest, Shamir and Adleman*). Es el primero y más utilizado algoritmo de este tipo, válido tanto para cifrar como para firmar digitalmente.

La seguridad de éste radica en el problema de la factorización de números enteros, pues los mensajes enviados se representan mediante números y el funcionamiento se basa en el producto conocido de dos números primos grandes elegidos al azar y mantenidos en secreto para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH (figura 1.9). En la actualidad, estos primos son del orden de 10^{200} y se prevé que dicho tamaño crezca con el aumento de la capacidad de cálculo de las computadoras.

[9] Sistema criptográfico de clave pública desarrollado en 1977.

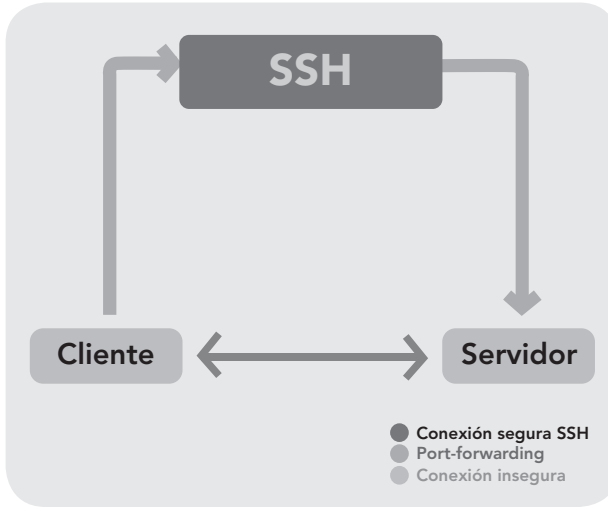


Figura 1.9 Funcionamiento de SSH

Al principio, sólo existían los *r-commands*, que se basaban en el programa *rlogin*, el cual funciona de forma similar a Telnet. La primera versión del protocolo y el programa eran libres y los creó un finlandés llamado Tatu Ylönen, pero su licencia fue cambiando y terminó apareciendo la compañía *SSH Communications Security,* que lo ofrecía de manera gratuita para uso doméstico y académico, pero exigía el pago a otras empresas. En 1997, (dos años después de que se creara la primera versión), se propuso como borrador en la IETF (*Internet Engineering Task Force*), en español llamada Grupo de Trabajo de Ingeniería Abierta (Abransom, 2000).

Por otro lado, a principios de 1999, se empezó a escribir una versión que se convertiría en la implementación libre por excelencia llamada OpenSSH de OpenBSD. En la actualidad existen dos versiones de SSH: la primera utiliza muchos algoritmos de cifrado patentados y es vulnerable a un agujero de seguridad que potencialmente permite a un intruso insertar datos en la corriente de comunicación. La segunda versión suite OpenSSH, bajo Red Hat Enterprise Linux que tiene un algoritmo de intercambio de claves mejorado que no es vulnerable al agujero de seguridad de la versión 1; sin embargo, ésta también soporta las conexiones de la primera.

1.3.5 FTP y TFTP

FTP (*File Transfer Protocol*) es un protocolo de red de transferencia de archivos entre sistemas conectados a una red TCP (*Transmission Control Protocol*) basado en la arquitectura cliente-servidor, independiente al sistema operativo utilizado en cada equipo. El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando los puertos de red 20 y 21.

Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad porque todo el intercambio de información (desde el *login* y el password del usuario en el servidor hasta la transferencia de cualquier archivo) se realiza en texto plano sin ningún tipo de cifrado con lo que un posible atacante

puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos. Para solucionar dicha situación son de gran utilidad aplicaciones como SCP y SFTP incluidas en el servicio SSH y que permiten transferir archivos cifrando toda la actividad. En el modelo, el intérprete de protocolo de usuario inicia la conexión de control en el puerto 21 (Tanenbaum, 2006). La figura 1.10 muestra la operación de FTP.

Figura 1.10 Operación de FTP

El funcionamiento de FTP es el siguiente: las órdenes estándar las genera la IP de usuario y se transmiten al proceso del servidor a través de la conexión de control. Después, las respuestas estándar se envían desde la IP del servidor al usuario por la conexión de control como respuesta a las órdenes, las cuales especifican parámetros como puerto, modo de transferencia, tipo de representación y estructura; así como la naturaleza de la operación sobre el sistema de archivos como almacenar, recuperar, añadir, borrar, etcétera.

El proceso de transferencia de datos (DTP, *Dynamic Trunking Protocol*) de usuario, u otro en su lugar, debe esperar a que el servidor inicie la conexión al puerto de datos especificado para transferirlos en función de los parámetros determinados.

También hay que destacar que la conexión de datos es bidireccional; es decir, que se puede usar simultáneamente para enviar y recibir. Ésta al principio tenía un problema: la localización de los servidores en la red; es decir, el usuario que quería descargar algún archivo mediante FTP debía conocer en qué máquina estaba ubicado. En ese momento, la única herramienta de búsqueda de información que existía era *Gopher* (o sea, literalmente, "lanzarse sobre" la información) con todas sus limitaciones: se trata de un servicio cuyo objetivo es la localización de archivos a partir del título, el cual consiste en un conjunto de menús de recursos ubicados en diferentes máquinas intercomunicadas. Cada una sirve un área de información, pero la organización interna permite que todas ellas funcionen como si se tratase de una sola. De acuerdo con esto, el usuario navega a través de los menús hasta localizar la información buscada y desconoce exactamente de qué máquina se está descargando. Con la llegada de Internet, los potentes motores de búsqueda como *Google* dejaron de lado el servicio *Gopher* y la localización de los servidores FTP pasó a ser un problema olvidado.

Algunos clientes de FTP básicos en modo consola vienen integrados en los sistemas operativos incluyendo Microsoft Windows, DOS, GNU/Linux y Unix; sin embargo, hay clientes disponibles con opciones añadidas e interfaz gráfica que más confiables a la hora de conectarse con servidores FTP no anónimos (Balacheff *et al.*, 2003), pues los anónimos

ofrecen sus servicios libremente a todos los usuarios y permiten acceder a sus archivos sin necesidad de tener un nombre de usuario o una cuenta, aunque se tendrá que introducir una contraseña momentánea (que es la dirección de correo electrónico propia); empero, la conexión se realiza con menos privilegios que un usuario normal: sólo se podrán leer y copiar los archivos públicos, así indicados por el administrador. Por otro lado, se utiliza un servidor FTP anónimo para depositar grandes archivos que no tienen utilidad y se reservan los servidores de páginas web para almacenar información textual destinada a la lectura en línea.

Si se desea tener privilegios como acceso a cualquier parte del sistema de archivos, modificación de los existentes y la posibilidad de subir los propios, por lo general se realiza mediante una cuenta de usuario: en el servidor se guarda la información de las distintas cuentas que pueden acceder a él, de forma que para iniciar una sesión FTP se debe introducir una autentificación (*login*) y una contraseña (*password*) que identifica al cliente/usuario unívocamente.

Por otro lado, al disponer de un cliente FTP basado en web se puede acceder al servidor FTP remoto como si se estuviera realizando cualquier otro tipo de navegación web: se podrán crear, copiar, renombrar y eliminar directorios; igualmente, existirá la posibilidad de cambiar permisos, editar, ver, subir y descargar archivos, así como cualquier otra función del protocolo FTP que el servidor remoto permita. Sin embargo, la entrada sin restricciones que proporcionan las cuentas de usuario implica problemas de seguridad, lo que ha dado lugar a un tercer tipo de acceso FTP denominado invitado (*guest*), que se puede considerar como la mezcla de los dos anteriores (McConell, 1996). La idea de este mecanismo es la siguiente: se trata de permitir que cada usuario se conecte a la máquina mediante su *login* y *password*, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo; de esta forma, llegará a un entorno restringido, algo muy similar a lo que sucede en los accesos anónimos, pero teniendo más privilegios.

FTP admite dos modos de conexión del cliente denominados activo o estándar (envía comandos tipo "PORT" al servidor por el canal de control al establecer la conexión) y pasivo (envía comandos tipo "PASV"). En ambos modos, el cliente lleva a cabo una conexión con el servidor mediante el puerto 21, que establece el canal de control. Pero en modo activo, el servidor siempre crea el canal de datos en el puerto 20, mientras que en el lado del cliente el canal de datos se asocia a un puerto aleatorio mayor que 1 024. Para ello, el cliente manda un comando "PORT" al servidor por el canal de control indicándole el número de puerto, de manera que aquél pueda abrirle una conexión de datos por donde se transferirán los archivos y los listados en el puerto especificado (Stallings, 2005).

Lo anterior presente una grave problemática de seguridad y es que la máquina cliente debe estar dispuesta a aceptar cualquier conexión de entrada en un puerto superior al 1 024, con los problemas que ello implica si se tiene el equipo conectado a una red insegura como Internet. De hecho, los cortafuegos que se instalen en el equipo para evitar ataques seguramente rechazarán esas conexiones aleatorias; para solucionar el problema anterior, se desarrolló el modo pasivo: cuando el cliente envía un comando "PASV" sobre el canal de control, el servidor FTP indica el puerto al que debe conectarse el cliente (mayor al 1 023; por ejemplo, 2 040); éste inicia una conexión desde el puerto que le sigue al puerto de control (por ejemplo, 1 036) hacia el del servidor especificado anteriormente (2 040).

Antes de cada nueva transferencia, tanto en el modo activo como en el pasivo, el cliente debe enviar otra vez un comando de control, tras lo que el servidor recibirá esa conexión de datos en un nuevo puerto aleatorio (si está en modo pasivo) o por el puerto 20 (si está en modo activo).

Por otro lado, en el protocolo FTP existen dos tipos de transferencia: en ASCII y binarios. Es muy importante conocer estos, pues si no se utilizan las opciones adecuadas, se puede destruir la información del archivo. Por ello, al ejecutar la aplicación FTP se debe utilizar uno de estos comandos (o poner la correspondiente opción en un programa con interfaz gráfica).

Tipo ASCII. Adecuado para transferir archivos que sólo contengan caracteres imprimibles (los archivos ASCII no son archivos resultantes de un procesador de texto); por ejemplo, páginas HTML (*HyperText Markup Language*), pero sin las imágenes que puedan contener.

Tipo binario. Usado cuando se trata de archivos comprimidos, ejecutables para computadoras personales, imágenes y archivos de audio, entre otras aplicaciones.

Por otro lado, TFTP son las siglas en inglés de *Trivial File Transfer Protocol*, que significa protocolo de transferencia de archivos trivial; el cual consiste en una versión básica de FTP. Sin embargo, TFTP a menudo se utiliza para enviar pequeños archivos entre computadoras en una red, algunas de sus características son:

- Utiliza UDP (en el puerto 69) como protocolo de transporte.
- No puede listar el contenido de los directorios.
- No existen mecanismos de autenticación o cifrado.
- Se utiliza para leer o escribir archivos de un servidor remoto.
- Soporta tres modos diferentes de transferencia: netascii, octet y mail, donde los dos primeros corresponden a los modos ASCII e imagen (binario) del protocolo FTP.

Puesto que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor, aunque se considera servidor a aquel que abre el puerto, y cliente a quien se conecta; sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, en el cual existe una relación cliente-servidor informal: la máquina A, que inicia la comunicación, envía un paquete de petición de lectura (RRQ, *Read Request*) o de escritura (WRQ, *Write Request*) a la máquina B con el nombre del archivo y el modo de transferencia; posteriormente, esta última responde con un paquete de confirmación (ACK, *Acknowledgement*), que también sirve para informar acerca del puerto al que tendrá que enviar los paquetes restantes la B. La máquina origen envía todos los datos numerados a la de destino, excepto el último, que contiene 512 bytes de datos; entonces, ésta responde con paquetes ACK numerados para todos los paquetes de datos, donde el último debe contener menos de 512 bytes de datos. Si el tamaño del archivo transferido es un múltiplo exacto de este valor, obtiene como respuesta del origen el envío de un paquete final que contiene 0 bytes de datos.

1.3.6 WWW: HTTP y HTTPS

WWW

En informática, la red informática mundial (WWW, *World Wide Web*), comúnmente conocida como web, es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet (figura 1.11). Con un navegador web, un usuario visualiza sitios compuestos de páginas que pueden contener texto, imágenes, videos u otros contenidos multimedia; además, puede navegar a través de estos usando hiperenlaces.

Entre marzo de 1989 y diciembre de 1990, el británico Tim Berners-Lee con la ayuda del belga Robert Cailliau desarrollaron la web por mientras trabajaban en el Centro Europeo de Investigaciones Nucleares (CERN) en Ginebra, Suiza; y se publicó el 7 de agosto de 1991. Berners y Cailliau propusieron utilizar el hipertexto "para vincular y acceder a información de diversos tipos como una red de nodos en que el usuario puede navegar a voluntad."

Figura 1.11 Símbolo de la web

El funcionamiento de la WWW es el siguiente: el primer paso consiste en traducir la parte del nombre del servidor de la URL en una dirección IP usando DNS. Lo siguiente es enviar una petición HTTP al servidor web solicitando el recurso. En el caso de una página web típica, primero se solicita el texto HTML, que de inmediato es analizado por el navegador, el cual hace otras peticiones para los gráficos y otros ficheros que formen parte de la página: al recibir desde el servidor web lo que se ha solicitado, el navegador busca y establece la página y cómo se describe en el código HTML, el CSS y otros lenguajes web. Al final, se incorporan las imágenes y otros recursos para producir la página completa que el usuario despliega en la pantalla (Berners-Lee; Cailliau; Loutonen; Nielsen y Secret, 1994).

Por otro lado, la web como se conoce hoy en día, ha permitido un flujo de comunicación global a una escala sin precedentes en la historia humana. Las personas separadas en el tiempo y el espacio pueden usarla para intercambiar o desarrollar sus pensamientos más íntimos o, de manera alternativa sus actividades y deseos cotidianos. Todo puede ser compartido y diseminado digitalmente con el menor esfuerzo posible, haciéndolo llegar casi de forma inmediata a cualquier otro punto del Planeta.

Desde 2007, Berners-Lee dirige el *World Wide Web Consortium* (W3C), el cual desarrolla y mantiene los siguientes y otros estándares que permiten a las computadoras de la web almacenar y comunicar con eficacia los diferentes tipos de información (Berners-Lee, 2009).

- El identificador de recurso uniforme (URI, *Uniform Resource Identifier*), que es un sistema universal para referenciar recursos como páginas web.
- El protocolo de transferencia de hipertexto (HTTP), que especifica cómo se comunican el navegador y el servidor entre ellos.
- El lenguaje de marcas de hipertexto (HTML), usado para definir la estructura y contenido de documentos de este tipo.
- El lenguaje de marcado extensible (XML, *eXtensible Markup Language*), usado para describir la estructura de los documentos de texto.

Aunque la existencia y uso de la web se basa en tecnología material que tiene a su vez algunas desventajas, esta información no utiliza recursos físicos como las bibliotecas o la prensa escrita, razón por la cual su propagación vía Internet no está limitada por el movimiento de volúmenes físicos o por copias manuales o materiales de datos. Gracias a su carácter virtual puede ser buscada fácil, eficaz y más rápido de lo que una persona podría recabarla por sí misma a través de un viaje, correo, teléfono, telégrafo o cualquier otro medio de comunicación.

La web es el medio de mayor difusión de intercambio personal aparecido en la historia de la humanidad, muy por delante de la imprenta (Berners- Lee; Bray; Connolly; Cotton; Fielding; Jeckle; Lilley; Mendelsohn; Orchard; Walsh y Williams, 2004). Como bien se ha descrito en este apartado, el alcance de la red en la actualidad es difícil de cuantificar. En

total, según las estimaciones de 2010, el número total de páginas web (bien de acceso directo mediante URL, o bien a través de enlace) era más de 27 000 millones en ese año; es decir, aproximadamente tres páginas por cada persona viva en el Planeta.

A su vez, la difusión del contenido es que en poco más de 10 años se han codificado medio billón de versiones de la historia colectiva y se han puesto frente a 1 900 millones de personas. Es en definitiva la consecución de una de las mayores ambiciones del hombre: desde la antigua Mongolia, pasando por la Biblioteca de Alejandría o la mismísima Enciclopedia de Rousseau y Diderot, el hombre ha tratado de recopilar en un mismo tiempo y lugar todo el saber acumulado desde sus inicios hasta ese momento; sueño que se ha hecho posible gracias al hipertexto. Además de todo lo reseñado, la red ha propiciado otro logro sin precedentes en la comunicación, como es la adopción de una lengua franca: el inglés, vehículo a través del cual se hace posible el intercambio de información.

HTTP

En cuanto al protocolo de transferencia de hipertexto (HTTP, *Hypertext Transfer Protocol*), se habla del elemento usado en cada transacción de la WWW; éste fue desarrollado por el W3C y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, donde el más importante es 2 616 que especifica la versión 1.1 (Fielding, Gettys, Mogul, Frystyk, Masinter y Berners-Lee, 1999). Es decir, HTTP define la sintaxis y la semántica que utilizan los elementos de *software* de la arquitectura web (clientes, servidores, *proxies*) para comunicarse. Este protocolo se orienta a transacciones y sigue el esquema petición–respuesta entre un cliente y un servidor, donde al cliente que efectúa la petición (un navegador web o un *spider*) se le conoce como user agent (agente del usuario). Por otra parte, a la información transmitida se la llama recurso y se le identifica mediante un localizador uniforme de recursos (URL, *Uniform Resource Locator*) que pueden ser archivos, el resultado de la ejecución de un programa, la consulta a una base de datos, la traducción automática de un documento, etcétera. La figura 1.12 muestra el símbolo del HTTP.

Figura 1.12 Símbolo del hipertexto HTTP

HTTP es un protocolo sin estado; es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de las aplicaciones web necesita con frecuencia mantener un estado, para ello se usan las *cookies*, que consiste en la información que un servidor puede almacenar en el sistema cliente por tiempo indeterminado; esto le permite a las aplicaciones web instituir la noción de "sesión" y rastrear usuarios.

Una transacción HTTP está formada por un encabezado seguido, opcionalmente, por una línea en blanco y algún dato. El encabezado es un bloque de datos que precede a la información propiamente dicha, por lo que muchas veces se hace referencia a él como *metadato*. Éste especificará cosas como la acción requerida del servidor, el tipo de dato retornado o el código de estado; su uso le proporciona gran flexibilidad al protocolo, permite que se envíe información descriptiva en la transacción, posibilitando la autenticación, cifrado e identificación de usuario. Si se reciben líneas de encabezado del cliente, el servidor las coloca en las variables de entorno de CGI con el prefijo HTTP_ seguido del nombre, donde un carácter guion (-) se convierte a "_". El servidor puede excluir cualquier encabezado que ya esté procesado, como *Authorization, Content-Type y Content-Length*, aparte de excluir alguno o todos los encabezados si se excede algún límite del entorno de sistema. Ejemplos de esto son las siguientes variables:

HTTP_ACCEPT. Tipos MIME (*Multipurpose Internet Mail Extensions*) que el cliente aceptará, dados los encabezados HTTP; otros protocolos quizás necesiten obtener esta información de otro lugar. Los elementos de esta lista deben estar separados por una coma, como se dice en la especificación HTTP: Tipo, tipo.

HTTP_USER_AGENT. Navegador que utiliza el cliente para realizar la petición. El formato general para esta variable es *software*/versión biblioteca/versión.

Por su parte, el servidor envía al cliente:

- Un código de estado que indica si la petición fue correcta o no: los códigos de error típicos indican que el archivo solicitado no se encontró, que la petición no se realizó de forma adecuada o que se requiere autenticación para acceder al archivo.
- La información propiamente dicha. Como HTTP permite enviar documentos de todo tipo y formato, es ideal para transmitir multimedia como gráficos, audio y video; una de sus mayores ventajas.
- Información sobre el objeto que retorna.

Hay que tener en cuenta que la lista anterior no incluye todos los campos de encabezado y que algunos de ellos sólo tienen sentido en una dirección. Finalmente, HTTP define ocho métodos (algunas veces referidos como "verbos") que indican la acción que se desea efectuar sobre el recurso identificado, el cual a menudo corresponde a un archivo o a la salida de un ejecutable que reside en el servidor como:

HEAD. Pide una respuesta idéntica a la que correspondería a una petición GET, pero sin el cuerpo. Esto es útil para recuperar metainformación escrita en los encabezados de respuesta sin tener que transportar todo el contenido.

GET. Pide una representación del recurso especificado. Por seguridad no debería ser usado por aplicaciones que causen efectos porque transmite información a través de la URI (*Uniform Resource Identifier*) agregando parámetros a la URL. Ejemplo: GET/images/logo.png, donde HTTP/1.1 obtiene un recurso llamado logo.png. Una muestra con parámetros es /index.php?page=main&lang=es.

POST. Envía los datos para que sean procesados por el recurso identificado. Los datos se incluirán en el cuerpo de la petición, lo cual puede resultar en la creación de nuevos recursos, de las actualizaciones de estos o ambas cosas.

PUT. Realiza un *upload* (o carga) de un recurso especificado. Es el camino más eficiente para subir archivos a un servidor; esto porque en POST se utiliza un mensaje multiparte que es decodificado por el servidor. En contraste, el método PUT permite escribir un archivo en una conexión *socket* establecida con el servidor. Su desventaja es que los servidores de *hosting* compartido no lo tienen habilitado. Un ejemplo es PUT/path/filename.html HTTP/1.1.

DELETE. Borra el recurso especificado.

TRACE. Este método solicita al servidor que envíe de vuelta en la sección del cuerpo de entidad de un mensaje de respuesta todos los datos que éste reciba como solicitud. Se utiliza con fines de comprobación y diagnóstico.

OPTIONS. Devuelve los métodos HTTP que el servidor soporta para un URL específico. Esto puede ser utilizado para comprobar la funcionalidad de un servidor web mediante petición en lugar de un recurso determinado.

CONNECT. Se utiliza para saber si se tiene acceso a un *host*, aunque la petición no llega necesariamente al servidor. Este método se utiliza para saber si un *proxy* da acceso a un host bajo condiciones especiales como, por ejemplo, "corrientes" de datos bidireccionales encriptadas (como lo requiere SSL).

HTTPS

El protocolo seguro de transferencia de hipertexto (HTTPS, *Hypertext Transfer Protocol Secure*) se trata de la versión segura de HTTP, que es utilizada principalmente por entidades bancarias, tiendas en línea y cualquier tipo de servicio que requiera el envío de datos personales, contraseñas y realización de operaciones financieras.

El sistema HTTPS utiliza un cifrado basado en SSL/TLS[10] para crear un canal codificado apropiado para el tráfico de información más sensible que el protocolo HTTP, cuyo nivel de encriptación depende del servidor remoto y navegador utilizado por el cliente. De este modo, se consigue que la información sensible (usuario y claves de paso) no puedan ser usadas por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, pues lo único que obtendrá será un flujo de información cifrada que le resultará imposible decodificar. El puerto estándar para este protocolo es 443.

El nivel de protección depende de la exactitud de la implementación del navegador web, del *software* del servidor y de los algoritmos de cifrado actualmente soportados; esto significa que HTTPS es vulnerable cuando se aplica a contenido estático de publicación disponible. El sitio entero puede ser indexado usando una araña web y es posible que la URI del recurso cifrado sea adivinada conociendo sólo el tamaño de la petición/respuesta. Esto permite a un atacante tener acceso al contenido estático de publicación y a la versión cifrada, facilitando un ataque criptográfico. Debido a que SSL opera bajo HTTP y no tiene conocimiento de protocolos de nivel más alto, sus servidores solamente pueden presentar estrictamente un certificado para una combinación de puerto/IP en particular. Esto quiere decir que en la mayoría de los casos no es recomendable usar un *hosting virtual* (*name-based*) con HTTPS.

Figura 1.13 Símbolo del protocolo de hipertexto HTTPS

Existe una solución llamada *Server Name Indication* (SNI) que envía el host-name al servidor antes de que la conexión sea cifrada; sin embargo, muchos navegadores antiguos no soportan esta extensión, aunque para las versiones más actualizadas la opción está incluida de origen.[11] La figura 1.13 muestra el símbolo de hipertexto seguro HTTPS.

1.3.7 NFS

El sistema de archivos de red (NFS, *Network File System*) es un protocolo a nivel de aplicación, según el Modelo OSI, que se utiliza para sistemas de archivos distribuidos en un entorno de red de computadoras de área local. Éste posibilita que distintos sistemas

[10] *Secure Sockets/Transport Layer Security* o capa de puertos seguros/seguridad de la capa de transporte.

[11] El soporte para SNI está disponible desde Firefox 2, Opera 8 e Internet Explorer 7 sobre Windows Vista.

conectados a una misma red accedan a ficheros remotos como si se tratara de locales (Huerta Villalón, s/a). En 1984, se desarrolló por *Sun Microsystems* con el objetivo de que fuera independiente de la máquina, el sistema operativo y el protocolo de transporte, lo cual fue posible gracias a que se implementó sobre los protocolos XDR (presentación) y ONC RPC (sesión). La figura 1.14 muestra la operación de NFS.

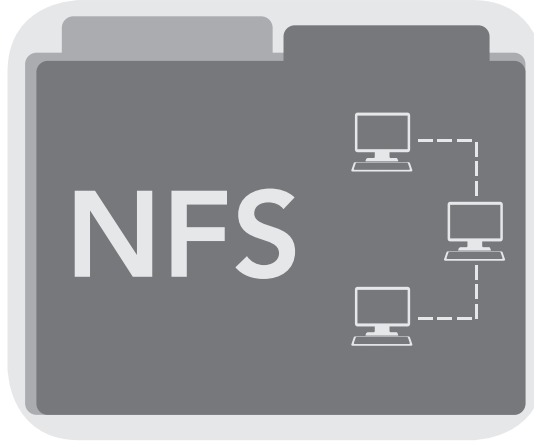


Figura 1.14 Operación de NFS

El protocolo NFS está incluido por defecto en los sistemas operativos UNIX y en la mayoría de distribuciones Linux. Las características más importantes son las siguientes:

- Está dividido al menos en dos partes principales: un servidor y uno o más clientes, donde estos últimos acceden de forma remota a los datos que se encuentran almacenados en el primero.
- Las estaciones de trabajo locales utilizan menos espacio de disco debido a que los datos se encuentran centralizados en un lugar único, pero pueden ser accedidos y modificados por varios usuarios, de forma que no es necesario replicar la información.
- Los usuarios no necesitan disponer de un directorio *home* en cada una de las máquinas de la organización, pues estos pueden crearse en el servidor de NFS para posteriormente acceder a ellos desde cualquier máquina a través de la infraestructura de red.
- También se pueden compartir a través de la red dispositivos de almacenamiento como CD-ROM y unidades ZIP; lo cual puede reducir la inversión en dichos dispositivos y mejorar el aprovechamiento del *hardware* existente en la organización.

Todas las operaciones sobre ficheros son síncronas; lo cual significa que retornan cuando el servidor ha completado todo el trabajo. En caso de una solicitud de escritura, el servidor plasmará físicamente los datos en el disco y, si es necesario, actualizará la estructura de directorios antes de devolver una respuesta al cliente, lo que garantiza la integridad de los ficheros. Al principio NFS soportaba 18 procedimientos para todas las operaciones básicas de E/S. Por su parte, los comandos de la versión 2 del protocolo son los siguientes:

NULL. Sirve para hacer *ping* al servidor y medir tiempos.

CREAT. Crea un nuevo archivo.

LOOKUP. Busca un fichero en el directorio actual y, si lo encuentra, devuelve un descriptor con más información sobre sus atributos.

READ y WRITE. Instrucciones básicas para acceder al fichero.

RENAME. Renombra un fichero.

REMOVE. Borra un fichero.

MKDIR y RMDIR. Creación y borrado de subdirectorios.

READDIR. Lee la lista de directorios.

GETATTR y SETATTR. Devuelve conjuntos de atributos de ficheros.

LINK. Crea un archivo como enlace a otro en un directorio especificado.

SYMLINK y READLINK. Llevan a cabo la creación y lectura, respectivamente, de enlaces simbólicos (en un *string*) a un archivo en un directorio.

STATFS. Devuelve información del sistema de archivos.

ROOT. Sirve para ir a la raíz (obsoleto en la versión 2).

WRITECACHE. Reservado para un uso futuro.

En la versión 3 del protocolo se eliminan los comandos "STATFS", "ROOT" y "WRITECACHE" y se agregaron los siguientes:

ACCESS. Verifica permisos de acceso.

MKNOD. Crea un dispositivo especial.

READDIRPLUS. Versión mejorada de "READDIR".

FSSTAT. Devuelve información del sistema de archivos en forma dinámica.

FSINFO. Retorna información del sistema de archivos en forma estática.

PATHCONF. Recupera información POSIX.

COMMIT. Envía datos de caché sobre un servidor con un sistema de almacenamiento estable.

Dichos comandos se corresponden con la mayoría de primitivas de E/S usadas en el sistema operativo local para acceder a ficheros locales. De hecho, una vez que se ha montado el directorio remoto, el sistema operativo local tiene que "reencaminar" las primitivas de E/S al *host* remoto; esto hace que todas sus operaciones sobre ficheros tengan el mismo aspecto, sin importar si es local o remoto.

El usuario puede trabajar con los comandos y programas habituales en ambos tipos de ficheros, ya que el protocolo NFS es completamente transparente al usuario. La versión 4 fue publicada en abril de 2003, no es compatible con las versiones anteriores y soporta 41 comandos.[12]

[12] NULL, COMPOUND, ACCESS, CLOSE, COMMIT, CREATE, DELEGPURGE, DELEGRETURN, GETATTR, GETFH, LINK, LOCK, LOCKT, LOCKU, LOOKUP, LOOKUPP, NVERIFY, OPEN, OPENATTR, OPEN_CONFIRM, OPEN_DOWNGRADE, PUTFH, PUTPUBFH, PUTROOTFH, READ, READDIR, READLINK, REMOVE, RENAME, RENEW, RESTOREFH, SAVEFH, SECINFO, SETATTR, SETCLIENTID, SETCLIENTID_CONFIRM, VERIFY, WRITE, RELEASE_LOCKOWNER, ILLEGAL.

En resumen, en la actualidad hay tres versiones de NFS en uso:

- La versión 2 (NFSv2), que es la más antigua y está ampliamente soportada por muchos sistemas operativos.
- La versión 3 (NFSv3) tiene más características, incluyendo manejo de archivos de tamaño variable y mejores facilidades de informes de errores, pero no es completamente compatible con los clientes NFSv2.
- NFS versión 4 (NFSv4) incluye seguridad *Kerberos*, trabaja con cortafuegos, permite ACL y utiliza operaciones con descripción del estado (Neuman y Ts´O, 1994).

1.3.8 CIFS

Server Message Block (SMB) es un protocolo de red que pertenece a la capa de aplicación en el Modelo OSI, el cual permite compartir archivos, impresoras y otros elementos entre nodos de una red. Es utilizado en computadores con Microsoft Windows y DOS. La figura 1.15 muestra un diagrama general del uso de CIFS.

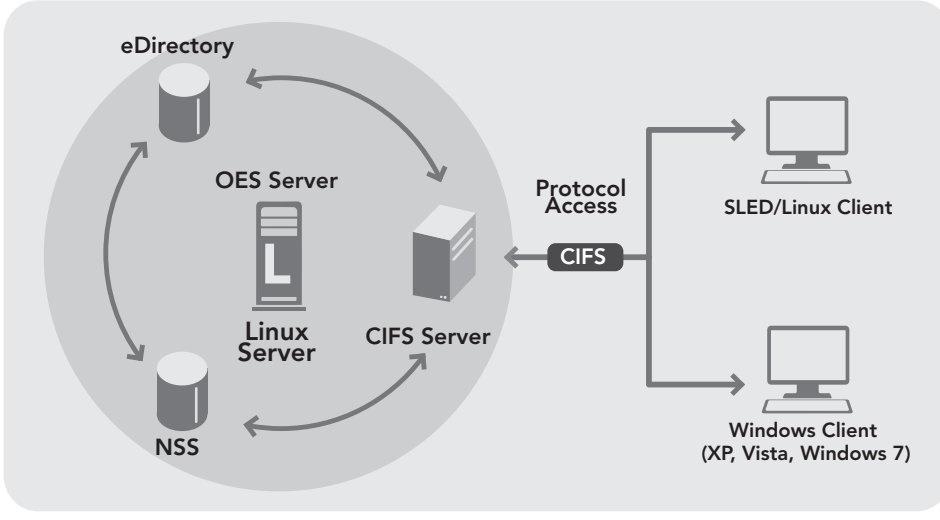


Figura 1.15 Uso de CIFS

Los servicios de impresión y el SMB para compartir archivos se han transformado en el pilar de las redes de Microsoft: en las versiones antiguas de sus productos los servicios de SMB utilizaron un protocolo que no es TCP/IP para implementar la resolución de nombres de dominio; luego, a partir de Windows 2000, se comenzó a utilizar la denominación DNS, la cual permite a los protocolos TCP/IP compartir recursos SMB (inventados por IBM), aunque la versión más común hoy en día es la modificada por Microsoft en 1998, que renombró como *Common Internet File System* (CIFS) a la cual se le añadieron características que incluyen soporte para enlaces simbólicos, enlaces duros (*hard links*) y mayores tamaños de archivo.

También existe Samba, que es una implementación libre del protocolo SMB con las extensiones de Microsoft, la cual funciona sobre sistemas operativos GNU/Linux y en UNIX.

1.3.9 *E-mail*: SMTP, POP, IMAP y SASL

El correo electrónico (en inglés: *e-mail*) es un servicio de red que permite a los usuarios enviar y recibir mensajes o cartas mediante sistemas de comunicación electrónicos. Se usa este nombre para denominar al sistema que provee dicho servicio en Internet a través del protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías (Stallings, 2010). Por medio de mensajes de correo electrónico se puede enviar no solamente texto, sino todo tipo de documentos digitales, dependiendo del sistema utilizado. La eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al ordinario para muchos usos habituales.

El correo electrónico antecede a Internet y, en realidad, fue una herramienta crucial para que dicho recurso fuera creado: en 1961 durante una demostración del MIT (*Massachusetts Institute of Technology*), se exhibió un sistema que permitía a varios usuarios ingresar a una IBM 7094 desde terminales remotas y guardar archivos en el disco, lo cual hizo posible nuevas formas de compartir información. Después en 1965, el correo electrónico comenzó a utilizarse en una supercomputadora de tiempo compartido y para 1966 se había extendido con rapidez a las redes computacionales.

El nombre correo electrónico proviene de la analogía con el correo postal: ambos sirven para enviar y recibir mensajes, y se utilizan buzones intermedios (servidores) en donde estos se guardan de manera temporal antes de dirigirse a su destino y que el destinatario los revise. Para que una persona pueda enviar un correo a otra, ambas requieren una dirección específica, la cual es proporcionada por un proveedor determinado; además, se necesita de un divisor entre el usuario y la computadora en la que se aloja el correo, que fue incorporado en 1971 por Ray Tomlinson como un signo llamado arroba (@), el cual fue elegido porque no existía en ningún nombre ni apellido. Hay dos tipos de servicio de correo electrónico:

> **Gratuitos.** Son los más usados, aunque incluyen algo de publicidad. La mayoría sólo permiten ver el correo desde un sitio web propio del proveedor para asegurarse de que los usuarios reciben la publicidad que se encuentra ahí. En cambio, otros permiten también usar un programa de correo configurado para que se descarguen los mensajes de forma automática. Una desventaja de estos correos es que en cada dirección se muestra el nombre del proveedor; por ejemplo, gapa@correo-gratuito.net.
>
> **Pagados.** Por lo regular ofrecen todos los servicios disponibles. Es el tipo de correo que un proveedor de Internet proporciona cuando se contrata la conexión. También es muy común que una empresa registradora de dominios venda, junto con el dominio y varias cuentas de correo.

Por otro lado, el correo web y el cliente de correo cuentan con ciertas diferencias. A continuación, se especifican las características de cada uno:

> **Correo web.** Casi todos los proveedores de correo dan el servicio de correo web, que permite enviar y recibir mensajes mediante un sitio diseñado para ello y, por lo tanto, usando sólo un navegador web. Es cómodo para mucha gente porque permite ver y almacenar los mensajes desde cualquier sitio en un servidor remoto en vez de en una computadora personal concreta. Como desventaja, es difícil de ampliar con otras funcionalidades, pues el sitio ofrece un conjunto de servicios predeterminados y no es posible cambiarlos; además es más lento que un programa de correo, ya que se requiere estar continuamente conectado a sitios web y leer los correos de uno en uno.

Cliente de correo. Son programas para gestionar los mensajes recibidos y poder escribir nuevos. Estos incorporan muchas más funcionalidades que el correo web, ya que todo el control del correo se encuentra en la computadora del usuario. Por ejemplo, algunos incorporan potentes filtros anti-correo no deseado (*spam*). Entre los datos necesarios para su configuración están el tipo de conexión (POP o IMAP), la dirección del servidor de correo, el nombre de usuario y la contraseña. Algunos ejemplos de programas que realizan las funciones de cliente de correo electrónico son Mozilla Thunderbird, Outlook Express y Eudora.

El funcionamiento de un programa de correo es muy diferente al de un correo web, ya que el primero descarga de golpe todos los mensajes que se tienen disponibles y luego pueden ser leídos sin estar conectados a Internet (además, se quedan grabados en la computadora). En cambio, en el segundo se leen de uno en uno y con conexión permanente a la red.

SMTP

El protocolo para la transferencia simple de correo electrónico (SMTP, *Simple Mail Transfer Protocol*) es utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. Se definió en el RFC 2 821 y es un estándar oficial de Internet.

El funcionamiento se da en línea operando en los servicios de correo electrónico; sin embargo, este protocolo posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino. Como alternativa a dicha situación se asocia ste protocolo con otros como el POP o IMAP, otorgando a SMTP la tarea específica de enviar correo y recibirlo (figura 1.16).

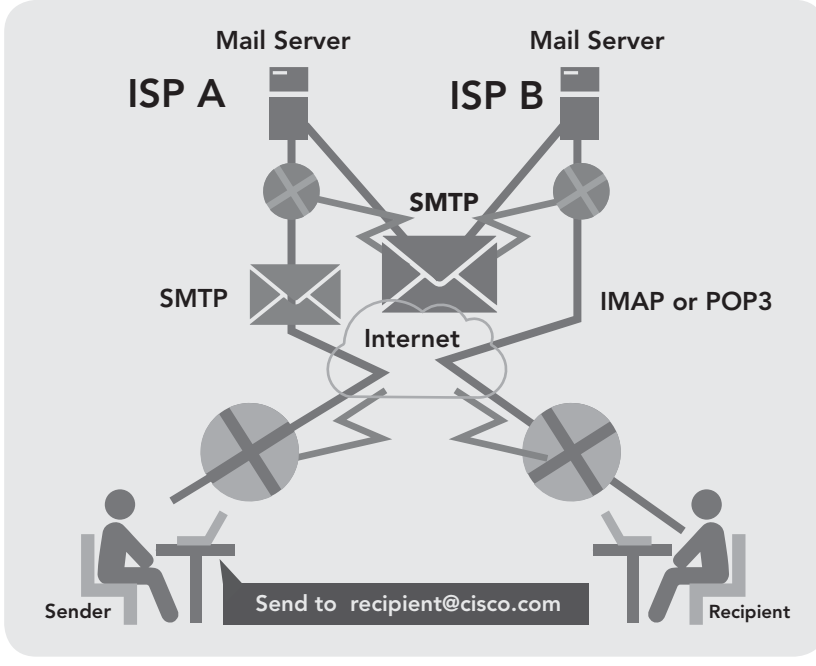


Figura 1.16 Operación de SMTP

En resumen, SMTP es un protocolo orientado a la conexión, basado en texto, en el que un remitente de correo se comunica con un receptor de correo electrónico mediante la emisión de secuencias de comandos y el suministro de los datos necesarios en un canal de flujo de datos ordenado y fiable, por lo regular TCP *(Transmission Control Protocol*). Una sesión SMTP consiste en comandos originados por un cliente (el agente de inicio, emisor o transmisor) que recibe las respuestas correspondientes del servidor (el agente de escucha o receptor) para que aquélla se abra y se intercambien los parámetros establecidos; dicha sesión puede incluir cero o más transacciones SMTP y se compone de tres secuencias de comando/respuesta, que son:

MAIL. Establece la dirección de retorno, también conocido como *Return-Path*, remitente o sobre. Ésta es la dirección para mensajes de despedida.

RCPT. Determina el destinatario del mensaje. Este mandato puede emitirse varias veces, una para cada receptor. Las direcciones son también parte de la envolvente.

DATA. Envía el contenido del mensaje texto en lugar de su envoltura. Se compone de una cabecera de mensaje y su cuerpo, separados por una línea en blanco. DATA es en realidad un grupo de comandos y el servidor responde dos veces, una para el comando de datos adecuado para reconocer que está listo para recibir el texto y la segunda, después de la secuencia final de los datos para aceptar o rechazar todo el mensaje.

Una de las limitaciones del SMTP original es que no facilita métodos de autenticación a los emisores, así que se definió la extensión SMTP-AUTH en RFC 2 554. Por otro lado, el spam es aún el mayor problema, pues no se cree que las extensiones sean una forma práctica para prevenirlo; algunos remedios pueden ser Internet Mail 2000, DKIM, *Sender Policy Framework* (SPF) y desde 2012 *Domain-Based Message Authentication, Reporting and Conformance* (DMARC).

POP

En informática, se utiliza el protocolo de oficina de correo (POP, *Post Office Protocol*) de nivel de aplicación en el Modelo OSI utilizado para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

Las versiones de este protocolo POP, informalmente conocido como POP1 y POP2, se han quedado obsoletas debido a las últimas de POP3. En general, cuando se hace referencia al término POP, se refiere directamente al POP3 dentro del contexto de protocolos de correo electrónico (figura 1.17).

Por otro lado, POP3 está diseñado para recibir correo, no para enviarlo, lo que permite a los usuarios con conexiones intermitentes o muy lentas (como aquellas por módem) descargar su correo electrónico mientras tengan conexión para revisarlo posteriormente, incluso estando desconectados. Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, por lo que un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y, finalmente, se desconecta.

La mayoría de las órdenes de POP3 identifican los mensajes dependiendo de su número ordinal en el servidor de correo. Esto genera problemas cuando un cliente pretende dejar los mensajes en el servidor, pues los que tienen un número cambian de una conexión de servidor a otra. Por ejemplo, si un buzón de correo contenía cinco mensajes en la última conexión, después otro cliente elimina el mensaje número tres si se vuelve a iniciar otra, por lo que el número que tiene el mensaje cuatro pasará a ser el tres y el cinco, el cuatro; tras lo que cambiará la dirección de estos mensajes.

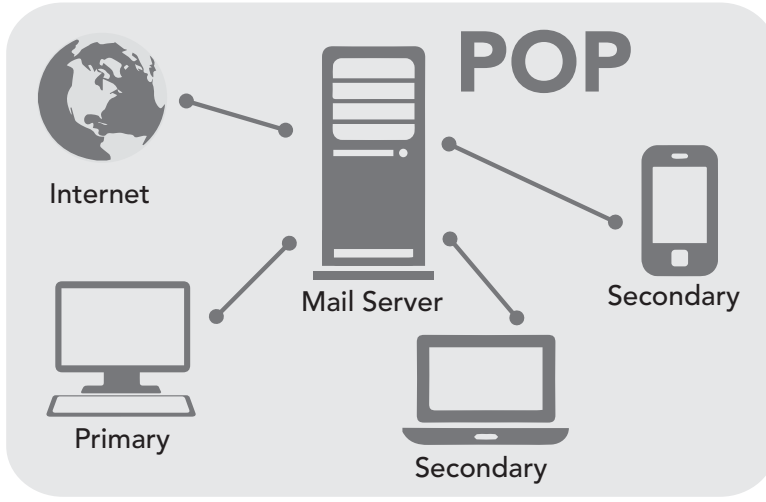


Figura 1.17 Operación de POP

Los clientes que utilizan la opción de dejar mensajes en el servidor por lo general utilizan UIDL (*Unique Identification Listing*), el cual proporciona un mecanismo que evita los problemas de numeración: el servidor le asigna una cadena de caracteres única y permanente al mensaje; cuando un cliente de correo compatible con POP3 se conecta al servidor utiliza la orden UIDL para obtener el mapeo del identificador de mensaje. De esta manera, el cliente puede utilizar ese mapeo para determinar qué mensajes se deben descargar y cuáles guardar al momento de la descarga. Al igual que otros viejos protocolos de Internet, POP3 utilizaba un mecanismo de firmado sin cifrado. La transmisión de contraseñas de POP3 en texto plano aún se da.

En la actualidad, POP3 cuenta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios. Uno de estos es APOP, el cual utiliza funciones MD5 para evitar los ataques de contraseñas. Mozilla, Eudora, Novell Evolution, así como Mozilla Thunderbird, implementan funciones APOP.

IMAP

IMAP (*Internet Message Access Protocol*) es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor. Mediante éste se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

IMAP tiene varias ventajas sobre POP como especificar carpetas del lado del servidor, visualizar los mensajes de manera remota sin descargarlos y permitir los modos de operación "conectado" y "desconectado". Los clientes de correo electrónico que utilizan IMAP dejan los mensajes en el servidor hasta que el usuario los elimine, de forma directa. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo (figura 1.18).

La versión 4 revisión 1 (IMAP4rev1) está definida por el RFC 3 501; es decir, en 1986 IMAP fue diseñado por Mark Crispin como una alternativa moderna a POP .

Todos los servidores y clientes de correo electrónico están virtualmente soportados por IMAP y POP3, aunque en algunos casos hay interfaces específicas del fabricante.

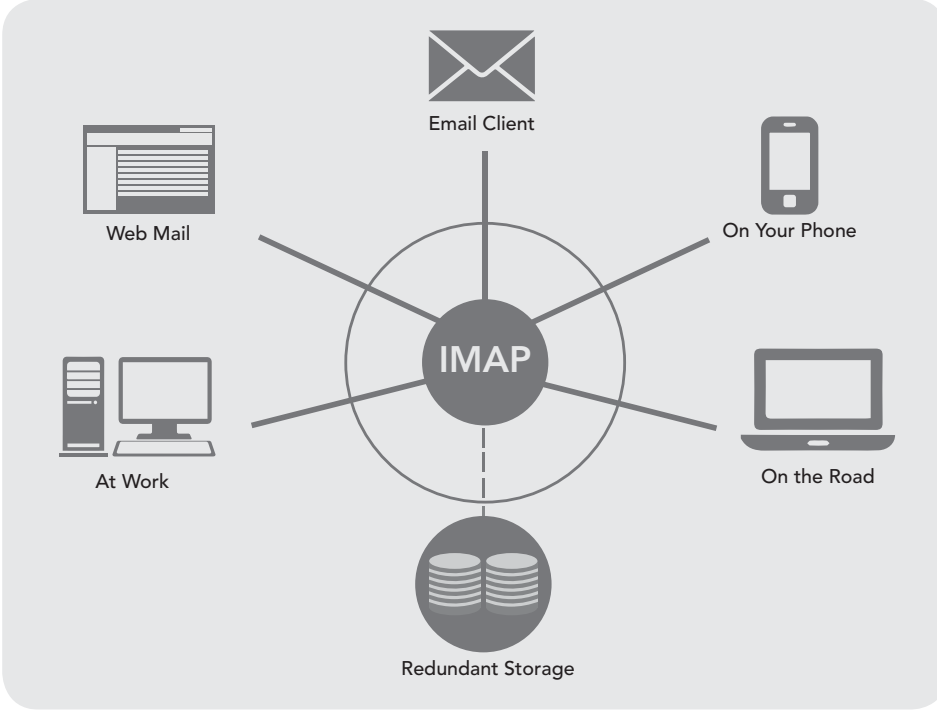


Figura 1.18 Funcionamiento de IMAP

A manera de ampliación, algunas de las características importantes que diferencian a IMAP y POP3 son:

Soporte para la conexión de múltiples clientes simultáneos a un mismo destinatario. El protocolo POP3 supone que el cliente conectado es el único dueño de una cuenta de correo. En contraste, el protocolo IMAP4 permite accesos simultáneos a múltiples clientes y les proporciona ciertos mecanismos para que se detecten los cambios hechos a un buzón de correo por usuarios concurrentemente conectados.

Soporte para acceso a partes MIME de los mensajes y obtención parcial. Casi todo el correo electrónico de Internet es transmitido en formato MIME. El protocolo IMAP4 permite a los clientes obtener por separado cualquier parte MIME individual, así como conseguir porciones de las partes individuales o los mensajes completos, lo cual es más seguro.

Soporte para que la información de estado del mensaje se mantenga en el servidor. A través de la utilización de señales definidas en el protocolo IMAP4 de los clientes, se puede vigilar el estado del mensaje; por ejemplo, si éste ha sido o no leído, respondido o eliminado. Las señales se almacenan en el servidor, de manera que varios clientes conectados al mismo correo en diferente tiempo pueden detectar los cambios hechos por otros clientes. Cabe recordar que la navegación de POP3 es un poco más lenta. El soporte para múltiples buzones de correo también le permite al servidor proporcionar acceso a los directorios públicos y compartidos.

Soporte para búsquedas de parte del servidor. IMAP4 proporciona un mecanismo para que los clientes pidan al servidor que busque mensajes de acuerdo con cierta variedad de criterios. Este mecanismo evita que se descarguen todos los mensajes de su buzón, agilizando las búsquedas.

Soporte para un mecanismo de extensión definido. Como reflejo de la experiencia en versiones anteriores de los protocolos de Internet, IMAP define un mecanismo explícito mediante el cual puede ser extendido.

Se han propuesto muchas extensiones de IMAP4 de uso común. Un ejemplo es el IMAP IDLE, que permite al servidor avise al cliente cuando ha llegado un nuevo mensaje de correo y éstos se sincronicen. Para realizar la misma tarea sin dicha extensión el cliente deberá contactar periódicamente al servidor para revisar si hay mensajes nuevos.

SASL

Finalmente, SASL (*Simple Authentication and Security Layer*), que en español se define como la capa de seguridad y autenticación simple, es un *framework* para autenticación y autorización en protocolos de Internet (figura 1.19); éste los separa de la aplicación permitiendo, en teoría, usar el soportado por cualquier aplicación que utilice SASL. A pesar de que sólo maneja la autenticación (y se requieren otros mecanismos como TLS (*Transport Layer Security*) para cifrar el contenido que se transfiere), SASL proporciona medios para un uso negociado del mecanismo elegido. Las especificaciones originales fueron editadas por John Meyers en el RFC 2 222, pero quedó obsoleto por el 4 422, editado por Alexey Melnikov y Kurt Zeilenga.

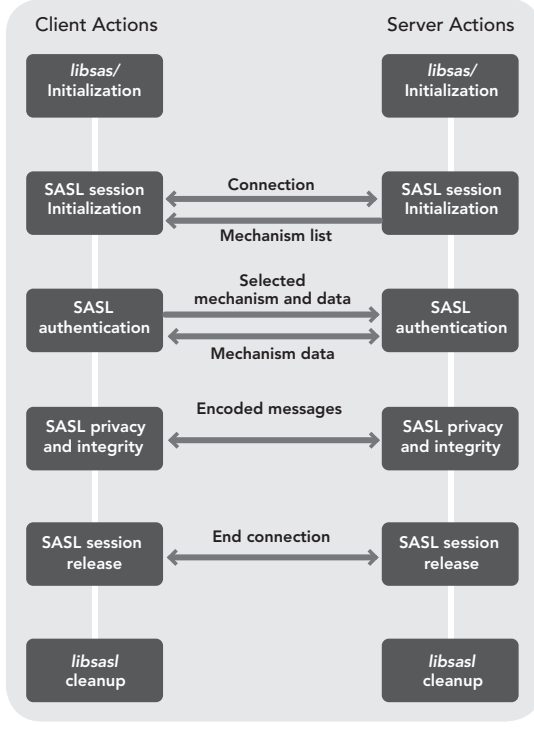


Figura 1.19 Operación de SASL

Los mencionados mecanismos se modelan como una sucesión de retos y respuestas; estos incluyen:

EXTERNAL. La autenticación está implícita en el contexto (por ejemplo, para protocolos que usan IPsec o TLS).

ANONYMOUS. Para el acceso de invitados sin autentificar.

PLAIN. Un mecanismo de contraseña simple en texto plano.

OTP. Para el sistema que evolucionó de S/KEY y se encuentra definido en RFC 2 289.

NTLM. En una red de Windows, NT LAN Manager (NTLM), es un conjunto de protocolos de seguridad de Microsoft que proporciona: autenticación, integridad y confidencialidad a los usuarios. NTLM es el sucesor del protocolo de autenticación en Microsoft LAN Manager (LANMAN), un producto anterior de Microsoft.

La suite de protocolos NTLM se implementa en un Proveedor de Soporte de Seguridad, que combina el protocolo de autenticación de LAN Manager, los protocolos NTLMv1, NTLMv2 y NTLM2 Session en un solo paquete. Si estos protocolos se utilizan o se pueden usar en un sistema que se rige por la configuración de Directiva de grupo. Para las diferentes versiones de Windows tienen diferentes configuraciones predeterminadas. Las contraseñas de NTLM se consideran débiles porque pueden ser violentadas y forzadas con hardware moderno.

Entre los protocolos que ahora mismo usan SASL se incluyen IMAP, LDAP, POP3, SMTP, XMPP y algunos servidores IRC, como Freenode.

1.4 Análisis y monitoreo

El objetivo principal de toda red es posibilitar el intercambio de información y el acceso a recursos por parte del personal que labora en una organización. Es aquí donde los sistemas de monitoreo de redes juegan un papel importante ayudando a saber qué está fluyendo a través de ellas, permitiéndose dar un servicio continuo o tomar las medidas respectivas en caso de anomalías y buscando minimizar el impacto en las operaciones normales de la organización (Terán Pérez, 2010).

En la actualidad, se ha dado un gran interés por hacer que los grandes sistemas organizacionales sean más robustos, lo cual implica también el buen diseño de *hardware* y *software*. Por ello, una rápida recuperación en situaciones de falla es fundamental, sobre todo si se dan costos intangibles, como en caso de pérdida de energía en sistemas de altas prestaciones.

Cuando las grandes organizaciones cuentan con sucursales que se interconectan a través de una red en diferentes partes del mundo, la disponibilidad de ésta y su tráfico son tan importantes como tener un sistema de tolerancia a fallas; pues al no estar disponibles provocan que los datos transmitidos no alcancen su destino, por lo que no se podrá acceder a ella. Por esta razón, al realizar el debido monitoreo de tráfico de red se estará posibilitando una mejora en la disponibilidad de los servicios que ofrece la organización porque se podría limitar su tráfico solamente a aquéllos para los cuales está destinada con el objetivo de evitar posibles usos indebidos por parte del personal administrativo. Por consiguiente, la organización podría maximizar el uso de los servicios que ofrece pronosticando hasta cierta medida si sería necesario aumentar *hardware* o restringir a ciertas aplicaciones el tráfico a través de la red interna o externa. Al tener esta información, se puede proporcionar a la gerencia del negocio las razones por las cuales se debería incrementar, y cuánto más, el ancho de banda de la red de la organización, dado que se evaluaría dicha información mediante un análisis costo–beneficio de disponibilidad.

Entonces, debido a la gran importancia que hoy tienen las redes de datos LAN/WAN en la productividad y eficiencia de las empresas es indispensable contar con una plataforma de conectividad y comunicaciones que asegure un acceso rápido a las bases de datos mejorando el desempeño de las aplicaciones para así brindar seguridad con base en sistemas de respaldo y un plan de contingencia ante catástrofes (Clark, Shenker y Zhang, 1992).

Por las razones expuestas en las organizaciones se ofrece el servicio de análisis y monitoreo de redes, orientado a prevenir y plantear soluciones concretas ante nuevos problemas o requerimientos para asegurar la estabilidad, operabilidad y flexibilidad en el tiempo del sistema en general. Éste se encuentra basado en tecnología que diagnostica y propone soluciones. Además, permite establecer estadísticas generales como niveles de utilización de la red, distribución de protocolos, estaciones más utilizadas, etcétera.

Para brindar un mejor servicio en el control y la manutención de la red y tener un apoyo real en la incorporación de las soluciones tecnológicas, se propone un plan de asesoría donde se considera desarrollar el análisis del equipamiento de conectividad y los protocolos de comunicación; además de un levantamiento de la red que se realizará con el fin de obtener la información necesaria para documentar, definir los procedimientos y planificación de las mediciones, así como las posteriores observaciones, en las cuales se establecerán los siguientes puntos:

- Protocolos de trabajo al interior de la red central: de enlace y red.
- Distribución lógica del flujo de la información: por medio de este dato es más simple identificar los puntos de congestión al interior de la red.
- Topologías: Ethernet y Fast Ethernet.
- Medios físicos de transporte: UTP, Wireless, fibra óptica, etcétera.
- Cantidad de estaciones de trabajo que componen la red en sus diferentes aplicaciones.
- Componentes activos: routers, gateways, switches, etcétera.
- Componentes pasivos: transceivers, terminadores, etcétera.
- Diagrama esquemático de la red: organización de la documentación.

Análisis del tráfico LAN

El servicio de análisis y diagnóstico de redes consiste en la instalación de un analizador por un periodo definido, el cual captura y examina en línea el tráfico y los paquetes de red de los protocolos involucrados (Halsall, 1988). El equipamiento utilizado dispone de un analizador experto que entrega información relacionada con los eventos, efectuando diagnósticos y mediciones estadísticas durante el periodo de medición. La información recolectada permitirá informar sobre el estado de diferentes parámetros relevantes del enlace como el nivel de utilización, las estaciones conectadas, los protocolos en uso, los diagnósticos de mal funcionamiento y las recomendaciones. Entre otros beneficios, permite descubrir las causas de problemas y de lentitud de las redes, ayudando realmente a sintonizar y expandir las topologías. Las características del análisis son, entre otras:

- Identificación de problemas de la red en tiempo real y en protocolos de las siete capas del Modelo OSI.
- Mediciones de estadísticas por nodo y conexión, así como de protocolos.
- Comentarios y decodificación por protocolo.
- Habilitación de reportes en planillas estándares.

Para realizar un análisis completo de la situación actual de la red se planifican mediciones en todos los segmentos implementados en ésta o en aquellos más demandados desde el punto de vista de los servicios entregados. Las variables a considerar en el estudio contemplan los siguientes puntos:

- Prestaciones (*performance*) de la red, que se refieren al porcentaje de utilización del ancho de banda de la red en sus niveles promedio, máximos y mínimos, los cuales se comparan con valores recomendados por normas, tanto nacionales como internacionales.
- Número de paquetes por segundo en función de los protocolos utilizados por las diferentes aplicaciones de comunicación.
- Distribución de los paquetes por tamaño y protocolos.
- Paquetes corruptos o con errores, que son de tipo *hardware* y *software* detectados en los servidores o las estaciones conectadas en la red.
- Anomalías detectadas en la estructura del cableado.

El objetivo principal de este análisis es determinar el ancho de banda real que es utilizado; así como los diferentes errores producidos. También se indican, por oficina, los valores referidos a la congestión, el valor de pico de tráfico, los errores en general, el porcentaje de

utilización por DLCI (*Data Link Connection Identifier*), el largo de los paquetes, etcétera (García, 2001). Los resultados de las mediciones antes descritas serán comparados con aquellos valores estándares esperados, lo cual permitirá establecer la real condición del sistema y proponer soluciones mediante un diseño lógico en etapas migratorias.

Algunos de los procedimientos a seguir después de obtenidos los datos, son los siguientes:

Análisis del equipamiento de conectividad. Conocidos los resultados de las mediciones de tráfico, es tarea fundamental analizar la eficiencia de los dispositivos que conforman la red para prevenir eventuales degradaciones en las prestaciones del sistema en general como aquellos equipos de conectividad empleados para la comunicación central y remota; por ejemplo, *switches*, *routers* y *hubs*. El objetivo es determinar la capacidad de procesamiento de estos, la operabilidad, las anomalías del *hardware* o *software*, puertas defectuosas, niveles de administración central y remota, manejo *broadcast*, paquetes, etcétera. En otras palabras, se debe recomendar los protocolos a utilizar en las aplicaciones y la factibilidad de ser implementados.

Recolección y análisis de datos. Una vez concluidas las mediciones, se procederá a recolectar los datos obtenidos y se efectuará un ordenamiento de ellos, su interpretación y análisis con el objeto de establecer el comportamiento actual de la red y definir procedimientos, medidas y soluciones concretas.

Confección del informe. Consiste en la recopilación de la información y la presentación ordenada en la forma de tablas, gráficos, junto a un diagnóstico y recomendaciones.

1.4.1 Protocolo de administración de red (SNMP)

El protocolo simple de administración de red (SNMP, *Simple Network Management Protocol*) facilita el intercambio de información de gestión entre dispositivos y permite supervisar el funcionamiento de la red, buscar y resolver sus problemas y planear su crecimiento. Las versiones de SNMP más utilizadas son la 1 (SNMPv1) y la 2 (SNMPv2). El SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad; sin embargo, no ha sido por completo aceptado en la industria (figura 1.20).

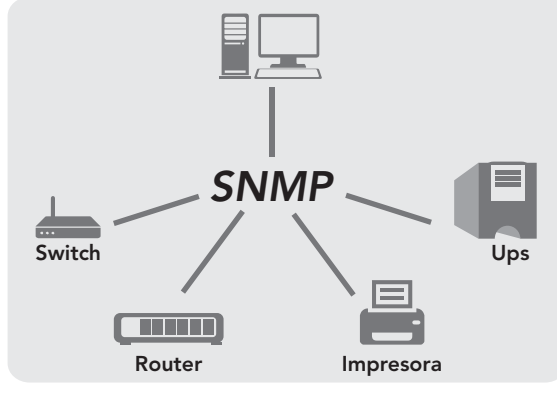


Figura 1.20 Funcionamiento de SNMP

Una red administrada a través de SNMP se compone de tres elementos claves:

Dispositivos administrados. Se encargan de recoger y almacenar información, la cual es puesta a disposición de los sistemas administradores de red (NMS, *Network Managment Station*) usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser *routers*, servidores de acceso, *switches*, puentes, concentradores, computadoras o impresoras.

Agentes. Los módulos de *software* de administración de red poseen un conocimiento local de información (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Sistemas administradores de red (NMS, *Network Management Station*). Ejecutan aplicaciones que supervisan y controlan los dispositivos administrados. Los NMS proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red; uno o más deben existir en cualquier red administrada.

Por su parte, los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos:

Comando de lectura. Usado para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

Comando de escritura. Se utiliza para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

Comando de notificación: Sirve para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía un aviso.

Operaciones transversales. Se usan para determinar qué variables soporta un dispositivo administrado y para recoger en secuencia información, como una tabla de rutas.

1.4.2 Analizadores de protocolos

Un analizador de protocolos es una herramienta que sirve para desarrollar y depurar los protocolos y las aplicaciones de red. Éste permite a la computadora capturar diversas tramas de red para analizarlas, ya sea en tiempo real o después de haberlas capturado. Lo cual significa que se puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP) y que se muestra al usuario la información decodificada (Bertsekas y Gallager, 1992). De esta forma, el usuario puede ver todo aquello que en un momento concreto está circulando por la red analizada (figura 1.21).

Además de ser de utilidad para los programadores, estos analizadores son muy provechosos para todos aquellos que quieren experimentar o comprobar cómo funcionan ciertos protocolos de red a pesar de que su estudio puede resultar poco ameno, sobre todo si se limita a la estructura y funcionalidad de las unidades de datos que se intercambian.

También, gracias a estos analizadores, se puede ver la relación que hay entre diferentes protocolos para así comprender mejor el funcionamiento. Los analizadores de protocolos se usan en diversas arquitecturas de red como redes LAN (10/100/1000 Ethernet;

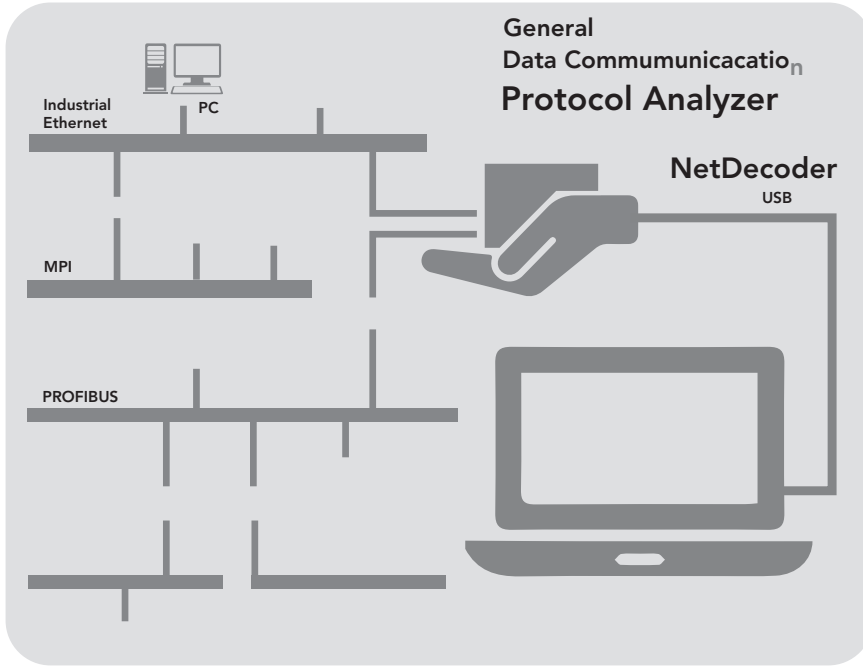


Figura 1.21 Representación de un analizador de protocolos

Token Ring; FDDI o fibra óptica), inalámbricas (*Wireless*) y WAN. Otros usos de los analizadores de protocolos son:

- Examinar y soportar demandas de nuevas aplicaciones (como VoIP).
- Obtener mayor efectividad de la red al analizar todo lo que pasa por ella y detectar problemas concretos.
- Verificar redes remotas sin necesidad de realizar largos viajes.
- Observar y monitorear varias redes a la vez.

Hay diversos tipos de analizadores de protocolos disponibles en el mercado, pero en general, son productos bastante caros. El precio depende de la capacidad de análisis, de la tecnología de red soportada y de si se trata de *software* o *hardware*. Algunos ejemplos de analizadores de protocolos son:

Appsniffing. Cuenta con una poderosa interfaz gráfica que permite diagnosticar rápidamente problemas y anormalidades en la red. Se caracteriza porque la captura puede ser efectuada tanto en el disco como en la memoria, además de que el análisis de datos y uso de filtros puede ser efectuado en tiempo real y porque permite estadísticas globales, así como un análisis TCP.

Productos Observer (Expert Observer, Observer Suite, Observer Probes, etcétera). Sirven para Ethernet, inalámbricos 802.11b y 802.11a, Token Ring y FDDI. Observer mide, captura y predice tendencias de sus redes; se ejecuta en el ambiente Windows y monitorea y sirve como herramienta para resolver problemas que se presentan en las redes.

Super Agent. Solución número uno para realizar la monitorización, establecer las tendencias y solucionar los problemas del rendimiento de aplicaciones. Permite ver con precisión y detalle los tiempos de respuesta del usuario final por toda la empresa y de todas las aplicaciones de TCP sin la necesidad de usar extremos ni sondas distribuidas.

Reporter Analyzer. Analizador pasivo del lado del servidor que rastrea y mide rápidamente las interfaces de WAN.

OptiView Console. Consola de funcionamiento centralizado de Optiview con función de acceso remoto que detecta rápidamente y supervisa de forma continua los dispositivos de red, al mismo tiempo que documenta su conectividad.

OptiView Protocol Expert. Aplicación basada en Windows que ofrece análisis de protocolos autónomos para paquetes capturados de *Workgroup Analyzer, Link Analyzer e Integrated Network Analyzer* de Optiview.

1.4.3 Planificadores

El planificador (*scheduler*) es un componente funcional muy importante de los sistemas operativos multitarea y multiproceso que es esencial en los sistemas operativos de tiempo real (figura 1.22). La función del planificador consiste en repartir el tiempo disponible de un microprocesador entre todos los procesos disponibles para su ejecución (Bournoure, *et. al.*, 2006).

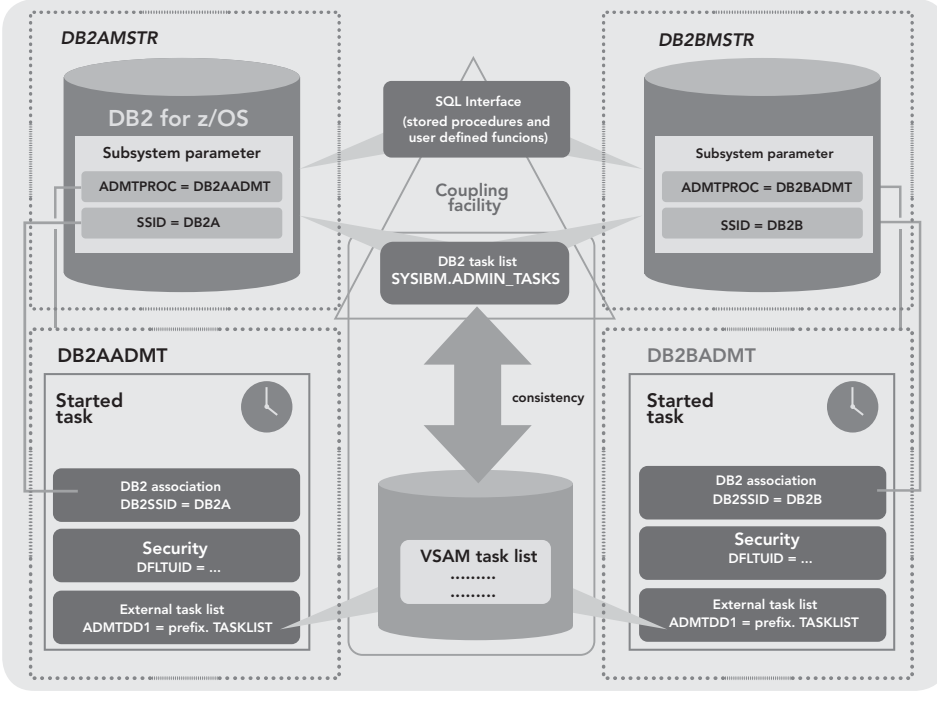


Figura 1.22 Representación de un planificador

Todo sistema operativo gestiona los programas mediante el concepto de proceso. De ahí la necesidad de que una parte del sistema operativo gestione, de una manera equitativa, cuál debe ejecutarse en cada momento para hacer un uso eficiente del procesador. Por ejemplo, si una computadora contiene un único microprocesador, éste solamente podrá ejecutar un programa en cada instante de tiempo porque nunca dejarán de trabajar por sí mismos. De manera que, en principio, cualquier programa monopoliza el microprocesador impidiendo que otros se ejecuten; por ello, la primera misión de un planificador es expulsar el programa en ejecución cuando decida que es pertinente. Esto se consigue de dos maneras, siempre con ayuda del propio *hardware*:

- Cuando expira un temporizador, que se activa a intervalos regulares de tiempo. En intervalos muy cortos, generalmente cada 250 milisegundos.
- Cuando el programa solicita una operación de entrada/salida, dado que éste no puede continuar hasta que aquélla termine, momento ideal para ejecutar otro.

En ambos casos, el control del microprocesador pasa a manos del planificador gracias a que el *hardware* genera una interrupción. En este proceso de expulsión se guarda el estado de ejecución del programa, llamado contexto. Todo esto apenas dura unos pocos milisegundos (Bournoure *et al.*, 2006).

Gracias a que el tiempo del microprocesador se reparte entre todos los procesos en intervalos muy cortos, la computadora ofrece la sensación de que estos se encuentran ejecutándose a la vez (ejecución concurrente). Cuando una computadora tiene varios microprocesadores, este esquema se repite para cada microprocesador.

Los niveles de planificación están basados en la frecuencia con la que se realiza cada uno. En los sistemas operativos de propósito general, existen tres tipos de planificadores:

Planificador a corto plazo. Es el más importante, que en inglés se denomina *dispatcher* o *short term scheduler*.

Planificador a mediano plazo. En inglés, *midterm scheduler* relacionado con aquellos procesos que no se encuentran en la memoria principal. Su misión es mover procesos entre memoria principal y disco (lo que se conoce como *swapping*).

Planificador a largo plazo. En inglés, *long term scheduler*, que es el encargado de ingresar nuevos procesos al sistema y también de finalizarlos.

Por otro lado, existen dos tipos de algoritmos de calendarización o políticas de planificación:

Expropiativos. Asignan tiempo de ejecución a cada proceso después del cual se calendariza otro hasta que cada uno acabe el trabajo. También expulsan un proceso en ejecución, si llega otro de mayor prioridad que necesita ejecutarse.

No expropiativos. Permiten que se ejecute el proceso hasta que acabe el trabajo; es decir, una vez que les llega el turno, no dejarán libre al procesador hasta que terminen o se bloqueen.

1.4.4 Análisis de desempeño de la red: tráfico y servicios

La arquitectura de rendimiento de una red describe la forma en que los usuarios, aplicaciones, dispositivos y redes logran cumplir con los requerimientos de rendimiento que fueron establecidos en el momento en que se planificó la red. Por otra parte, dentro de los niveles de análisis y diseño de redes se encuentra la arquitectura de rendimiento (Hallivuori, 2000).

En una red es de suma importancia mantener niveles óptimos en estos componentes, ya que los diferentes flujos de información generados por los usuarios, dispositivos o aplicaciones pueden verse muy afectados en sus actividades debido a variaciones de los niveles de rendimiento.[13]

Se entiende entonces por arquitectura de rendimiento, el conjunto de mecanismos que se utilizan para configurar, operar, gestionar, disponer y enlistar los recursos en la red que soportan los tráficos de flujo de información. La capacidad se puede definir, genéricamente, como la habilidad que tiene el sistema para lograr la transferencia de información a través de la red. Al término de capacidad se le liga con otros como:

Ancho de banda. Capacidad que tiene una red para transmitir datos; por lo regular, se refiere a la cantidad de estos que se pueden transferir en determinado momento a través de la red, medidos en bits por segundo (bit/s) o en sus múltiplos.

Throughput. Se refiere a la tasa promedio de datos o de mensajes que han sido transferidos con éxito y sin errores en la red de un nodo a otro.

Goodpu. Cantidad de bits de información utilizables que se envían en la red a un destino determinado por unidad de tiempo.

Retardo.[14] Cantidad de tiempo que se toma la transferencia de una unidad de información a través del sistema, desde un origen hasta un destino. Los usuarios que utilizan aplicaciones que corren en tiempo real o interactivas, esperan que el retardo en la red sea mínimo.

[13] El rendimiento en una red está compuesto por los niveles de capacidad, retardo y RMA (*Reliability, Maintainability, Availability*); esto último en español se traduce como: confiabilidad (indicador de la frecuencia de fallas que ocurren en la red y componentes, el cual representa las interrupciones no programadas de los servicios), mantenibilidad (medición estadística del tiempo que se tarda la red para volver en óptimas condiciones después de una interrupción en las funciones de manera inesperada) y disponibilidad (relación que existe entre la cantidad de fallas que sufren las misiones críticas en el sistema y la cantidad de tiempo que toma a éste recuperarse y trabajar de manera adecuada).

[14] El término utilizado cuando se dan variaciones en el retardo es conocido como *jitter*, que se refiere a las alteraciones provocadas en transmisiones de voz y de video. El retardo es crucial para los enlaces satelitales y las conexiones con cables muy largos.

1.5 Seguridad básica

La seguridad a nivel informática significa que el sistema está libre de peligro, daño o riesgo (Kaufman; Perlman y Speciner, 2002). El objetivo de establecer la seguridad básica en una red de computadoras es mantener la integridad, disponibilidad y confidencialidad de la información dentro de la red para que la organización mantenga la continuidad en sus procesos.

Cuando se habla de integridad, se quiere decir que los objetos del sistema sólo pueden ser modificados por personas autorizadas y en forma controlada. Por otro lado, la disponibilidad significa que los objetos del sistema deben permanecer accesibles a dichas personas. Por último, la confidencialidad en el sistema se presenta cuando la información contenida en éste no es brindada a entidades externas. Para alcanzar este último objetivo se debe plantear y definir lo siguiente: ¿qué recursos se quieren proteger dentro de una red?, ¿de qué?, ¿en qué grado?, ¿qué medidas y herramientas se deben implantar para alcanzar un óptimo nivel de seguridad sin perder de vista la relación costo–beneficio?

Una vez definidos estos puntos, pueden diseñarse las políticas de seguridad adecuadas para implementar en la organización y crear un perímetro de defensa que permita proteger las fuentes de información. Las normas de control interno que conforman las medidas de seguridad para sistemas interactivos y procesos en redes privadas se dividen en seguridad lógica y física, donde los recursos que se han de proteger básicamente son *hardware*, *software* y datos.

Para los tres elementos a proteger existen cuatro tipos de amenazas:

Interrupción. Cuando un objeto del sistema se pierde y queda inutilizable o no disponible.

Intercepción. Cuando un elemento no autorizado consigue un acceso a un determinado objeto del sistema.

Modificación. Cuando se altera algún objeto del sistema una vez adentro de éste.

Fabricación. Cuando se cambia algún objeto del sistema por otro de aspecto igual pero con un objetivo distinto.

Sin embargo, se debe tener en cuenta que cuando se hace referencia a seguridad en redes, el bien más preciado a proteger es la información que circula por ellas.

1.5.1 Los elementos de seguridad

Dentro de las medidas de seguridad con relación en los equipos se pueden establecer los que se describirán a continuación:

Cortafuegos (*firewall*)

Sistema de defensa lógico y físico basado en el hecho de que todo el tráfico de entrada o salida a la red debe pasar sin excepción por un sistema de seguridad capaz de autorizar, denegar y tomar nota de aquello que ocurre. El concepto de cortafuegos (*firewall*) genera controversias, por lo que se define junto con todas las normas, los procedimientos y las

herramientas que se utilizan con el objetivo de mantener la integridad, la operatividad y la privacidad de la información manejada por las computadoras (Terán Pérez, 2010). En un sistema que se interrelaciona tanto con usuarios, proveedores y entidades financieras es conveniente la utilización de un grupo de sistemas que tienden a dar seguridad a los datos de una red privada (figura 1.23); entonces, es necesario definir qué servicios pueden ser utilizados, quiénes pueden acceder a ellos y ejecutar esos servicios, así como qué mensajes y datos se deben filtrar.

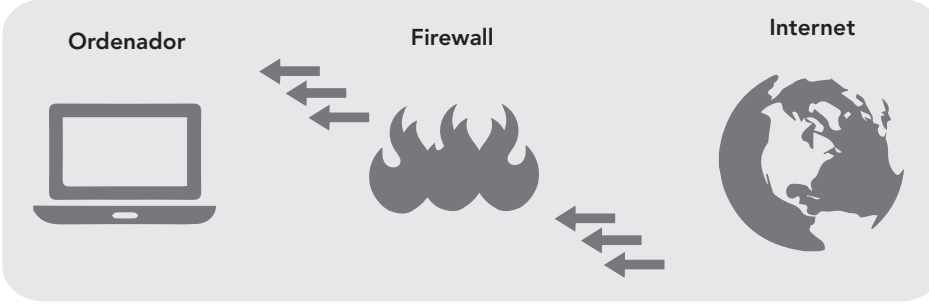


Figura 1.23 Operación de un cortafuegos

El cortafuegos tiene que detectar puntos débiles y monitorear en lapsos de tiempo cortos el estado y seguridad de la red, generando informes en tiempo real. El responsable de diseñar e implementar las políticas de seguridad para una red privada debe ser un integrador, o sea, el administrador de los recursos informáticos de la empresa quien requiere los datos y valor para considerar los puntos planteados a continuación:

- Quiénes deben acceder sólo para consultas sin actualizar ni modificar datos.
- Quiénes pueden consultar y actualizar datos.
- Quiénes pueden realizar ciertos procesos.
- Qué se debe filtrar.
- Definir las condiciones de validación por *software* y *hardware* a la par de que controla los accesos y la salida de datos de la red al exterior.
- Determinar las condiciones complementarias de seguridad para los nombres y claves; por ejemplo, preguntas, tarjetas magnéticas, contraseñas, etcétera.
- Establecer las formas de encaminar los datos que se agregan en las consultas para los usuarios que están del otro lado del cortafuegos.
- Saber qué cortafuegos es virtual.
- Control de los vínculos físicos.

A pesar de las múltiples ventajas de un cortafuegos, éste también tiene algunas debilidades como:

- No puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
- No es posible protegerse de las amenazas a que se somete por traidores o por usuarios inconscientes.

- No puede prohibir que los espías corporativos copien datos sensitivos en discos, en memorias USB o tarjetas PCMCIA y los sustraigan del edificio.
- No puede garantizar protección contra ataques de ingeniería social.
- No puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y de *software* obtenidos desde Internet, pues al momento de querer comprimir o descomprimir archivos binarios el cortafuegos de Internet no puede contar con un sistema preciso de verificación para cada tipo de virus que se puedan presentar.
- Finalmente, el cortafuegos de Internet no puede proteger contra los ataques posibles en la transferencia de datos. Estos ocurren cuando datos inocuos son enviados o copiados a un servidor interno y son ejecutados facilitando un ataque.

Proxy o servidor de defensa

El *proxy* es un *software* que se instala en una computadora personal conectada a una red local, de preferencia exclusiva para este uso, la cual se busca que funcione como una puerta lógica. Al servidor *proxy* pueden acceder los clientes, los posibles clientes o clientes virtuales, los proveedores o las instituciones financieras, siempre y cuando esté protegido en cuanto a la ubicación de los datos alojados, pues es necesario monitorear la red y su desarrollo para que no lleguen a los elementos protegidos.

Por lo regular, se trata de un programa que trabaja con servicios externos en nombre de clientes internos: estos se comunican con los servidores que a su vez trasmiten las solicitudes aprobadas a cada uno de ellos para después enviar las respuestas al servidor y de éste a los clientes. El *proxy* guarda en una unidad de disco o en una memoria las páginas consultadas para que la próxima vez que alguien lo haga entre más rápido; esto sirve para que accedan a Internet muchas personas a través de una sola conexión.

El *proxy* hace posible que desde cualquier puesto de trabajo de una red local se pueda compartir una línea telefónica conmutada común y un único módem para el uso de Internet; además de recibir y enviar correo electrónico con y sin denominación interna o subcuentas de un usuario y conectarse a servidores específicos.

El uso principal es como servidor de consulta porque muestra una copia de los archivos para que no sean afectados los originales y como ocultador o *anonimizador* de los archivos.

Pasarelas (*gateways*) a nivel de aplicación

El *gateway* se caracteriza por ser un dispositivo que filtra datos (Terán Pérez, 2010), como los puentes (*bridges*) o *routers*.

Las pasarelas en el nivel de aplicación permiten al administrador de red la implementación de una política de seguridad estricta, pues se instala un servicio *proxy* para cada aplicación deseada. Si el administrador de la red no instala el código *proxy* para una aplicación particular, el servicio no es soportado y no será posible desplazarse a través del cortafuegos, aun cuando el código *proxy* puede ser configurado para soportar únicamente las características específicas de una aplicación que el administrador de red considere aceptable, mientras que niega todas las otras. Un aumento de seguridad de este tipo incrementa los costos en términos del tipo de cortafuegos seleccionado, los servicios de aplicaciones del *proxy*, el tiempo y los conocimientos requeridos para configurar el cortafuegos; y un decrecimiento en el nivel de los servicios que podrán obtener los usuarios, dando como resultado un sistema carente de transparencia en un

ambiente amigable. Como en todos los casos, el administrador de redes debe balancear las necesidades propias en seguridad de la organización con la demanda de facilidad de usos de la comunidad.

Es importante notar que los usuarios tienen acceso por un servidor *proxy*; pero ellos jamás podrán configurar el *gateway* a nivel-aplicación; pues de ser así la seguridad se vería amenazada, puesto que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema. Por ejemplo, el intruso podría obtener el acceso de *root* e instalar un troyano[15] para recolectar las contraseñas y modificar la configuración de los archivos de seguridad.

Encaminador (*router*) filtra-paquetes

El *router* toma las decisiones de negar o permitir el paso de cada uno de los paquetes de datos que son recibidos; éste examina cada datagrama para determinar si corresponde a uno de sus paquetes filtrados y si ha sido aprobado por sus reglas; de ser así, se permite el paso del paquete, el cual será desplazado de acuerdo con la información de la tabla de ruteo. En cambio, si las reglas niegan el paso, el paquete es descartado.

El *router* de filtrado es, por lo general, transparente a los usuarios finales y a las aplicaciones, por lo que no se requiere de entrenamiento o *software* especializado que necesite ser instalado en cada uno de los servidores (Terán Pérez, 2010).

1.5.2 Medidas de seguridad lógica con relación al usuario

Existen ciertas medidas de control de identificación y autenticación de los usuarios, entre las que destacan las siguientes:

Contraseña (*password*)

La confidencialidad de una información puede verse afectada si acceden a ella personas que no están autorizadas para hacerlo. Con el objetivo de evitar esto se utilizan mecanismos que restringen el acceso de los usuarios a determinadas computadoras y ciertos sectores de la información de la empresa; estos, por lo general, son programas que habilitan el acceso de una persona a una computadora y a un sector de información luego de haberla identificado para saber qué nivel de entrada tiene al sistema. El método de identificación más utilizado es una contraseña, aunque tiene un grado de seguridad bajo si no se utiliza correctamente. Con respecto a la misma, se puede establecer que:

- Todos los usuarios deben validar su password acompañado del nombre o identificador de usuario (*username*) para acceder a la red, que debe respetar los estándares de seguridad.
- La contraseña no debe ser una palabra corta ni conocida, debe contener alternativamente letras mayúsculas, minúsculas, números y caracteres especiales.
- Debe ser secreta.
- Debe ser conocida sólo por el usuario.
- No se debe anotar con exhibición pública.
- Debe ser única para cada usuario.
- Debe modificarse periódicamente por el usuario.
- Debe contener un mínimo de seis u ocho caracteres.

[15] Programa para ejecutar aplicaciones en forma remota.

Ante la menor sospecha de que alguien pudo haber accedido indebidamente al sistema, se deberá cambiar la totalidad de las claves. Por otro lado, como medida preventiva recomendada ante el ingreso incorrecto por segunda vez de una contraseña, el sistema debería:

- Avisar con una leyenda que solamente se tiene una oportunidad más de ingresar la contraseña correcta.
- Brindar acceso por un lapso de tiempo determinado.
- En caso de insistencia, bloquear el teclado hasta que alguien lo autorice desde otro equipo con el debido control.

Existen diferentes categorías de contraseñas que autorizan posibilidades distintas, por ejemplo, claves por un periodo de tiempo dado y que caducan luego de cumplido el plazo, con accesos en horas limitadas, para ser usadas por única vez, para utilizarse un número limitado de veces y con acceso a ciertas operaciones.

Identificación de usuarios

El objetivo de esto es autenticar que la persona que desea acceder al sistema sea quien dice ser realmente; para ello, existen distintos métodos que se dividen en tres categorías:

Algo que el usuario sepa. Dentro de la primera categoría se encuentra el método de contraseñas, el cual se ha descrito anteriormente. En resumen, cuando una de las partes desea autenticarse ante la otra, se limita a mostrarle su conocimiento de una clave en común y, si es correcta, se otorga el acceso al recurso solicitado.

Algo que éste posee. Dentro de la segunda categoría, se encuentra el sistema de tarjetas inteligentes. Se trata de un dispositivo de seguridad resistente a cualquier tipo de adulteración y que ofrece funciones para un almacenamiento relativamente seguro de la información incluido su procesamiento. El método funciona de la siguiente manera: se debe introducir la tarjeta en el lector; los dos dispositivos se identifican entre sí con un protocolo a dos bandas, en el que es necesario que ambos conozcan la misma clave, lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía; además, la contraseña puede utilizarse para asegurar la comunicación entre la tarjeta y el dispositivo lector.

Tras reconocerse las dos partes, se lee la identificación personal de la tarjeta (PID *controller*) y el usuario teclea su PIN; se inicia entonces un protocolo desafío–respuesta: se envía el PID a la máquina y ésta reta a la tarjeta, que responde utilizando una clave personal del usuario. Si la respuesta es correcta, el host ha identificado la tarjeta y el usuario obtiene acceso al recurso pretendido.

Una ventaja de uso es que pueden ser utilizadas para controles físicos y lógicos; por otro lado, el método también tiene desventajas como el costo elevado, tanto para implementación como para remplazo de dichas tarjetas en caso de pérdidas o hurtos.

Una característica física del usuario (autenticación biométrica). Por último, en la tercera categoría se encuentran los sistemas de autenticación biométrica, basados en características físicas del usuario a identificar, los cuales se ejemplificarán de forma amplia más adelante. Este tipo de técnicas cuentan con dos puntos importantes a favor: el primero son más amigables para el

usuario y el segundo son las dificultades que poseen para ser vulneradas. El proceso de autenticación es similar para todos los métodos biométricos, que están compuestos por cuatro pasos:

- Captura o lectura de los datos del usuario a validar.
- Extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar).
- Comparación de las características con las guardadas en una base de datos.
- Elección entre usuarios válidos e inválidos.

Criptografía

El método de seguridad que sirve para resguardar archivos, comunicaciones, identificaciones y claves. Todos los documentos básicos o maestros de la red, así como toda trasferencia de datos, deben estar encriptados. La idea es transformar el texto normal a un texto cifrado, con lo cual el enemigo lee este último, no el original (Lockhart, 2007). Para acceder al verdadero es necesario una clave que solamente conocen el emisor y el receptor. Hay dos conceptos que deben tomarse en cuenta:

- Criptoanálisis: arte de descifrar.
- Criptología: arte de diseñar cifrados y de descifrarlos.

En las organizaciones, hay información confidencial a la que pueden tener acceso solamente las personas autorizadas. Para ello se comenzaron a utilizar técnicas de criptografía; lo cual nace a partir de la problemática de las empresas de mandar información importante a través de un canal de comunicación poco seguro como es el caso de Internet. A esto se le llama sistema de encriptación, que utiliza una clave denominada llave, necesaria para acceder a la información auténtica. Hay dos tipos de cifrados:

Por sustitución. Cada letra o grupo de letras se reemplaza por otra o por un grupo de éstas para disfrazarla.

Por transposición. Cuando se reordenan las letras, pero no se disfrazan.

También existen dos principios criptográficos:

- Todos los mensajes deben contener redundancia para evitar que los intrusos activos engañen al receptor y lo hagan actuar ante un mensaje falso.
- Deben tomarse algunas medidas para evitar que intrusos activos reproduzcan mensajes viejos.

La criptografía de clave pública requiere que cada usuario tenga dos contraseñas: una pública, usada para cifrar mensajes destinados a un usuario, y una privada, utilizada sólo por el usuario para descifrar mensajes. Existen dos tipos de claves de encriptación:

Claves simétricas. Son las mismas que los algoritmos o claves de encriptación y desencriptación.

Claves asimétricas. Utilizan una clave o algoritmo para grabar o trasmitir y otra para leer o recibir e interpretar el mensaje. Los sistemas de clave asimétrica son los que se están imponiendo, ya que ofrecen un mayor grado de seguridad; sobre todo, porque no hace falta que la clave sea conocida por más de una persona.

Firmas digitales

Bloques de datos que han sido codificados con una clave secreta y una pública. Es un sistema mediante el cual el emisor envía un mensaje firmado al receptor y de esta forma se evitan algunas situaciones como las siguientes:

- Que el transmisor no pueda repudiar el contenido del mensaje.
- Que el receptor no pueda confeccionar por sí mismo el mensaje.
- Otras medidas lógicas de seguridad.

Resguardo de archivos

Se realiza con el objetivo de recuperar la información ante cualquier catástrofe producida; esto implica que incluso ante una pérdida total de las computadoras se podrá volver a operar si se cuenta con un respaldo actualizado. La frecuencia y el tipo se determina de acuerdo con las características de la organización.

Como norma de seguridad complementaria deberán tenerse una o más copias de la versión más actualizada en un lugar físicamente alejado del sistema. Hay que diferenciar de manera tácita entre las técnicas de resguardo de archivos y los de soporte para estos métodos, que pueden ser:

- Abuela, madre e hija (ciclos de retención).
- Grabación incremental en bases de datos.
- Base de datos con objetivos de auditoría.

A continuación, se establecen los dos tipos más frecuentes de resguardo de archivos en la práctica:

> **Mirror (espejo).** Se usan dos discos que graban la información de forma simultánea y en paralelo. Un disco es la copia exacta del otro; esto asegura que ante la caída de uno, el sistema seguirá funcionando con el otro.
>
> **RAID (*Redundant Array of Independent Disk*)**. Técnica de grabación simultánea y paralela de discos, pero a diferencia del *Mirror*, el RAID distribuye los datos en bloques entre diferentes discos físicos. Esta técnica puede tener varios niveles, según la cantidad de discos entre los cuales se distribuyan los bloques de datos. El nivel más utilizado es el RAID 5, donde la información se reparte entre todos los discos asignados, por lo que si algo falla o sucede con un disco o en los otros, es posible reconstruirlos. El otro nivel es el RAID 6, que se diferencia con el cinco en que éste sí puede reconstruir dos discos.

Por más que la utilización de RAID o de *Mirror* provoque redundancia, no se deben dejar de lado.

Redundancia

Consiste en tener un equipo disponible, una red o un enlace por si falla otro. La misma está dada por la cantidad y no por la duplicidad. Con esto se quiere decir que los sustitutos no tienen por qué ser iguales, pero sí parecidos para que puedan realizar las funciones que llevaban a cabo los anteriores. Existe redundancia en equipos, redes, discos (RAID o *Mirror*), fuentes de alimentación y terminales.

Antivirus

Un virus informático en la práctica es un programa de computadoras de tipo dañino que se propaga de un sistema a otro por medio de la generación de copias idénticas de sí mismo. Estos producen mayor cantidad de daños a la información y pérdidas económicas en los grandes sistemas que tienen un entorno basado en el sistema operativo Windows, así como en las computadoras caseras. Dichos daños están generados por características diferentes a su código y son de dos tipos:

- Aquellos que producen un programa que funciona en una computadora y que el usuario ignora, aunque se denotan como ciertas anomalías: caídas del sistema, pérdidas de datos por operaciones mal realizadas, entre muchas otras.
- Aquellos que están programados para causar daños de manera directa.

La función de un programa antivirus es detectar la presencia o el accionar de un virus informático en una computadora, detener el trabajo y tomar las medidas necesarias suficientes para acotar un buen porcentaje de los daños posibles. Todo usuario de computadoras debería implementar una estrategia de seguridad antivirus, no sólo para proteger su propia información, sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados.

Un antivirus es sólo una herramienta que no es eficaz en el ciento por ciento de los casos. Por lo tanto, la única forma de que constituya a un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos, los cuales tienden a controlar la entrada de archivos al disco rígido de la computadora; esto se logra revisando con el antivirus todos los medios de almacenamiento y archivos; por supuesto, disminuyendo por completo todo tipo de tráfico. Además, una forma bastante eficaz de proteger los ejecutables es utilizar un programa verificador de integridad para que estos no sean modificados; es decir, que mantengan su estructura; de esta manera, antes de que puedan ser infectados por un virus convencional, el antivirus impediría su accionar.

1.5.3 Medidas de seguridad física para el control de acceso a las redes

Siempre que exista un dispositivo físico que complemente al *software* para dotar al sistema de redes para una mayor seguridad existirán medidas de seguridad física (Terán Pérez, 2010); algunos ejemplos de autenticaciones que pueden ser llevadas a cabo con elementos físicos agregados son las biométricas.

Verificación de la voz

Método que consiste en identificar una serie de sonidos y características para validar al usuario. Para que sea eficaz, debe haber ausencia de ruidos. Este sistema cuenta con algunas desventajas que lo hacen vulnerable ante los ataques; por ejemplo, el modelo de simulación en que el atacante reproduce las frases o palabras que el usuario legítimo pronuncia para acceder al sistema, o el tiempo que pierde el usuario hablando con el analizador más el que se necesita para autenticar al mismo. En el mercado hay dos tipos de sistemas de verificación de voz: los que se basan en textos preestablecidos y los fundamentados en textos independientes.

Verificación de escritura

El objetivo de este método es autenticar basándose en ciertos rasgos de la rúbrica. En este método se verifican las siguientes propiedades: la forma de firmar, las características dinámicas, el tiempo utilizado y el ángulo con que se realiza el trazo.

Verificación de huellas

Sistema que determina en forma unívoca la identidad de las personas porque se sabe que no hay dos que posean las mismas huellas dactilares. Este método tiene algunas desventajas, como la incapacidad de validación en caso de que el dedo esté lastimado, sucio o cuando la piel se encuentra en un estado distinto al normal.

Verificación de patrones oculares

Este modelo de autenticación biométrica se divide en dos: por un lado se analizan patrones retinales y, por otro, el iris. El primer modelo analiza la vasculatura retinal, el cual es un elemento característico de cada individuo. Con respecto al segundo, es preciso decir que se analiza una estructura única de cada individuo que forma un sistema muy complejo e inalterable durante toda la vida de la persona.

Ambos sistemas tienen algunas desventajas; por ejemplo, la escasa aceptación entre los usuarios, la falta de confianza por parte de estos y el elevado precio.

Verificación de la geometría de la mano

Este método es uno de los más rápidos dentro de los sistemas biométricos y cuenta con una probabilidad de error aceptable, en un segundo es capaz de determinar si una persona es válida o no. La ventaja de este sistema es que al mismo tiempo que autentica al usuario actualiza su base de datos ante la posibilidad de cambios, sin olvidar la gran aceptación que tiene por parte del público.

Otras medidas

Además de las descritas, es recomendable tener presentes las siguientes medidas:

- Colocar en el equipo una llave tipo *yale* o *trabex* para que corte la alimentación eléctrica a la fuente de poder; con ello, se garantiza que solamente puedan utilizarlo las personas poseedoras de la llave física.
- Eliminar los discos de las computadoras personales en red e incluso en las autónomas cuando se justifique; con ello, se trata de evitar que cualquier empleado pueda tomar un archivo que afecte la privacidad de la empresa; y además es una defensa infranqueable para el probable ingreso de virus que puedan poseer los dispositivos que se inserten en los equipos.
- Colocar un dispositivo lector o lectograbador de tarjetas magnéticas; lo que permitirá entregarle a cada usuario una tarjeta magnetizada con los datos para validar la identificación y autenticidad, además de la clave que también debe ingresar por escrito.
- Instalar una cámara de video para grabar la imagen de quien esté frente al monitor y teclado, programada para accionarse cada n minutos.
- El uso de la tarjeta inteligente con un circuito integrado (con la unidad lectora conectada a la computadora personal), más el resultado de un cálculo algorítmico, donde se graba en la tarjeta y en la base de datos cada vez que termina un acceso y luego se comparará al volver a acceder al sistema.

Existen otros elementos de identificación, siempre y cuando sí puedan ser procesados por un dispositivo contable a la computadora o la terminal.

1.5.4 Tipos de riesgos

Primero, se debe definir qué se quiere proteger y, con base en ello, identificar cuáles son los riesgos para la seguridad del sistema (Terán Pérez, 2010). La siguiente es una clasificación básica de riesgos:

Riesgos de origen físico

Dentro de este tipo de riesgos encontramos dos clases:

- Desastres naturales, donde se hallan los terremotos, las tormentas eléctricas, las inundaciones y la humedad.
- Desastres del entorno; en esta categoría están el sistema eléctrico, el ruido eléctrico, los incendios y el humo.

Personas

Son el factor de riesgo más importante a tener en cuenta porque pueden causar enormes pérdidas. Hay dos tipos de atacantes: los pasivos que entran en el sistema, pero no destruyen y los activos, que sí lo modifican.

Los posibles atacantes son:

Personal. Se trata de cualquier empleado de la organización que por error o desconocimiento efectúe algún tipo de accidente.

Exempleados. Personas interesadas en atacar el sistema, en especial si fueron despedidos. Hay que recordar que conocen el sistema, saben cuáles son las debilidades de éste y que, por donde, pueden ingresar virus, troyanos o demás amenazas lógicas.

Crackers. Tienen como objetivo los entornos de seguridad para curiosear o utilizarlas como enlace hacia otras redes, para probar nuevas formas de ataques o por diversión. Puede tratarse de personas con distintos grados de conocimiento.

Terroristas. Se trata de cualquier persona que ataca al sistema para causar algún tipo de daño.

Intrusos remunerados. Es el grupo de atacantes más peligroso porque son piratas con gran experiencia en problemas de seguridad y con un amplio conocimiento del sistema; estos son contratados por un tercero para robar secretos o para destruir la imagen de la empresa.

Amenazas lógicas

Conjunto de programas creados para dañar los sistemas informáticos. Entre ellos se encuentran los siguientes:

***Software* incorrecto.** Errores cometidos por los programadores en forma involuntaria, los cuales se denominan *bugs*. Los programas que se aprovechan de estos e ingresan en el sistema se les llama *exploits*.

Herramientas de seguridad. Armas de doble filo, ya que de la misma forma que el administrador las utiliza para detectar y solucionar fallas en sus sistemas o en la sub-red completa, un potencial intruso las puede usar para atacar.

Puertas traseras. También denominadas atajos son colocadas en los programas para tener mayor velocidad en la detección y depuración de fallas.

Bombas lógicas. Partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; a partir de ese momento tienen una función que es dañina.

Canales encubiertos. Canales de comunicación que permiten transferir información violando las políticas de seguridad del sistema.

Virus. Como se mencionó, un virus es programa desarrollado intencionalmente para instalarse en las computadoras de un usuario sin su consentimiento.

Gusanos. Programas capaces de ejecutarse y propagarse por sí mismos a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas para dañarlos. Estos tienen la característica de que son muy difíciles de programar y pueden causar mucho daño.

Caballos de Troya o troyanos. Instrucciones escondidas en un programa para que parezca que realiza las tareas correspondientes, pero en realidad ejecutan funciones ocultas sin el conocimiento del usuario.

Programas conejo o bacterias: Poseen la función es reproducirse hasta que el número de copias acaba con los recursos del sistema, produciendo una negación de servicio.

Técnicas salami. Se trata del robo automatizado de pequeñas cantidades de bienes de una gran cantidad de origen, lo cual hace dificultosa su detección.

En la actualidad, se asiste a un incremento cada vez mayor del acceso de los ciudadanos a los sistemas que ofrecen las llamadas sociedad de la información y del conocimiento. En concreto para Internet, que es ya una realidad para millones de ciudadanos. Gracias a este recurso se puede hablar de un mundo globalizado donde las fronteras no constituyen límite alguno, pero esta imagen tan positiva se ve ensombrecida por los casos de ciberdelincuencia que cada día salen a la luz.

En la práctica, toda red presenta problemas, estos, se quiera o no, siempre tendrán que ver con un individuo. Sea cual sea la causa, los parámetros a considerar son normalmente los mismos. Las redes corporativas presentan problemáticas que sí pueden ser resueltas a través de estudios y de herramientas de organización, de control y seguimiento que permiten que la funcionalidad permanezca lo más estable posible dentro de los parámetros que su seguridad lo permita (Terán Pérez, 2014).

En concordancia con lo expuesto, se puede concluir que las personas son el recurso de mayor importancia al evaluar los riesgos en una red, puesto que la seguridad de ésta comienza y termina con ellas. Para empezar, lo mejor siempre es organizar la red (y por supuesto a las personas que la incluyen) en grupos de trabajo. Por ejemplo, en un edificio de oficinas lo correcto sería dividir la red por pisos y por departamentos; luego, individualizar los sujetos y, por último, establecer los niveles de responsabilidad de cada uno de acuerdo con su función y ocupación. Se hace especial hincapié en este punto debido a que las cifras avalan esta posición: 80% de los problemas generados en una red son básicamente responsabilidad de sus integrantes, y sólo 20% se debe a factores externos

de una corporación. Los tres factores que alimentan esta estadística son ignorancia, haraganería y malicia:

- La ignorancia como factor puede ser fácilmente solucionado mediante seminarios de seguridad internos; publicidad en las ventanas de inicio de una sesión, folletos, publicaciones en murales, etc., y por medio de exámenes periódicos de las habilidades de cada usuario.
- La haraganería o flojera es un factor muy común y frecuente en las grandes corporaciones, en las cuales, las principales brechas de seguridad se deben a la incompetencia de sus integrantes al no apagar su equipo cuando se retiran de su lugar de trabajo, olvidan cerrar su sesión o, simplemente, dejan encendida su terminal sin protección alguna hacia otros individuos que buscan dañar su posición.
- En cuanto a la malicia, en ningún lado las personas se encuentran libres de las emociones de sus pares, en especial cuando se trata con personas que trabajan en conjunto y buscan o anhelan ascender de cualquier manera en los niveles de una organización. Basta decir que evitar ambientes de rivalidad y de competencia desleal e incentivar el respeto entre los compañeros de una organización logra solucionar este tipo de problemas.

La participación condicionada también ayuda a incrementar la seguridad de una organización al preguntar y escuchar los diversos problemas que las personas tienen con los equipos conectados a red; esto permite ver las cosas desde el enfoque de aquellos que participan en ella. Sin embargo, el punto que quizá más problemáticas genera al poner en marcha un plan de seguridad es, por supuesto, la misma puesta en marcha. La mayoría de los usuarios tienen problemas para "aclimatarse" con las nuevas disposiciones de seguridad y tienden a desconfiar, cometer errores y, obviamente, reclamar por los problemas acaecidos. La solución, por lo general, es dar un periodo de marcha blanca, en el cual la red tiene que ser monitoreada de manera frecuente para solucionar las diferentes problemáticas imprevistas en el plan de seguridad y, además, para evitar posibles ataques externos que se aprovechen de la vulnerabilidad del sistema (Terán Pérez, 2014).

No todos los recursos en una red poseen el mismo nivel de riesgo. Asimismo, si se considera que el factor humano tiende a ser el mayor peligro, la manipulación de un determinado recurso entrega un nivel diferente de riesgo que otro. De esta manera, el daño físico a un recurso no siempre generará una consecuencia mayor que el que puede hacerse mediante un *software* o un determinado recurso de la red; por ejemplo, no se podría decir que el daño provocado por un desperfecto en un cable puede ser mayor a la filtración de cierta información confidencial.

A partir del análisis de aquello que se necesita proteger, de quién y cómo, es posible realizar estimaciones del riesgo de la pérdida de un determinado recurso (*R*) (a todo nivel) contra su importancia (*I*). Si se le asigna un valor numérico a cada una de las dos variables anteriores, por ejemplo de cero a diez, se tendrá entonces que para (*R*), cero muestra que no existe riesgo y diez se expresa como el nivel más alto; para (*i*) cero indicará un recurso sin importancia, mientras que el valor de 10 hará referencia al recurso más importante de la red. Estos valores tienden a ser subjetivos a nivel global, pero si se consideran dentro del marco de funcionalidad de una red, se puede ver, por ejemplo, que será muy difícil encontrar un recurso sin importancia o que no existe riesgo de pérdida. Así también, probablemente tan sólo uno o dos alcanzarán los valores máximos en ambas escalas o, quizá, la funcionalidad de la red depende de todos. Como sea, la evaluación total del riesgo (*W*) estará determinada por el producto de ambos factores, dando así:

$$W_i = R_i{}^* E_i$$

Donde,
W_i = importancia del riesgo de pérdida de un determinado recurso
R_i = riesgo de pérdida del recurso
E_i = importancia del recurso
$_i$ = número del recurso evaluado

1.5.5 Tipos de ataques y vulnerabilidades

Existen varios tipos de problemáticas que pueden dañar el buen funcionamiento de las redes, algunas de éstas son:

Negación de servicio (*denial of service*). Tipo de ataque cuyo propósito es negar el acceso de un determinado recurso o de varios. Esto puede traer como consecuencia la pérdida de tiempo valioso para realizar una determinada operación, incomunicación o, finalmente, la inoperancia de uno o de varios recursos de la red. Existen tres tipos de ataques básicos para negar un servicio: consumo de recursos escasos, limitados o no renovables; destrucción o alteración de información de configuración; y eliminación o perturbación física de los componentes de la red.

Obtención o uso ilícito de claves de acceso. Existen tres maneras de obtener una clave de acceso:

- Poseer una clave de acceso: por lo general, la obtienen elementos alejados de la corporación por uno u otro motivo. Dicha clave puede ser usada por el sujeto fuera de la empresa o por otro usuario, lo que generaría una eventual brecha de seguridad para acceder al recurso que se desee.
- Crear una clave de acceso: esto se logra mediante el ingreso ilícito (*hack*) a los servidores y/o las terminales mediante la creación de un nuevo usuario y contraseña.
- *Cracking* de clave de acceso: mediante un programa específico se obtiene la clave de acceso del terminal y/o del servidor (*cracking*). Además, es posible conseguir las listas de claves mediante ingreso ilícito a los servidores/terminales, incluyendo las listas encriptadas, que pueden ser descifradas mediante un programa específico (*crack*).

***E-mail bombing y spamming* (ataque SMTP)**

- *E-mail bombing:* consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el buzón de entrada de correo del destinatario (*inbox*).
- *Spamming:* se refiere a enviar el *e-mail* a centenares o millares de usuarios e, inclusive, a listas de interés. El *spamming* puede resultar aún más perjudicial si los destinatarios contestan el correo, haciendo que todos reciban la respuesta. Esto, combinado con *e-mail poofing* (que altera la identidad de la cuenta que envía el *e-mail* y, por consiguiente, oculta al emisor real) hacen del *spamming* una de las herramientas favoritas para iniciar ataques hacia redes desprotegidas.

En la actualidad, los servicios de mensajería (como Gmail, Yahoo o MSN) poseen filtros de mensajes *spam*, los cuales deben estar bien configurados y actualizados para evitar situaciones que puedan generar un problema mayor a la red. La manera en que afectan este tipo de ataques es en lo que respecta a la conectividad en sí, sobrecargando las conexiones, maximizando la utilización de recursos y saturando la memoria del disco. Es muy importante mantener la bandeja de entrada de los servicios de mensajería limpia, vacía con un respaldo de los mensajes importantes recibidos en otra unidad de la memoria (Terán Pérez, 2010).

En redes privadas que poseen su propio código de mensajería se deben crear o mantener en las terminales filtros *anti-spam* y herramientas de detección de correos iterativos, además de incrementar la capacidad del *log* de las terminales para recibir correo, lo que evitaría al inicio los problemas que generan este tipo de ataques. Otra manera, es por medio de la configuración de las listas de acceso de los encaminadores (puerto 25 para SMTP) para la dirección IP del atacante.

Ataques por FTP. Los ataques por FTP son quizá uno de los favoritos de los *hackers* y de los *crackers* en la actualidad, puesto que el enlace generado ocupa el puerto de preferencia 21 en los servidores y, además, entrega las facilidades obvias de transferencia de archivos, condición muy ventajosa para un ataque. El FTP *Bounce*, por ejemplo, es un recurso usado para ingresar a la terminal de un tercero, utilizando un servidor como escudo y medio de ocultamiento a la vez. Consiste en realizar una conexión FTP regular con un servidor, pero con la diferencia de que la elección del puerto cliente no es arbitraria, esto permite al atacante elegir uno que no sea el de su propio equipo, sino la terminal de la víctima. Esto posibilita, entre otras cosas, realizar una conexión ilícita con el puerto de la víctima, el servidor y el atacante ocultando la identidad de este último con la del servidor.

Para neutralizar estas medidas, es muy importante tener en cuenta que, de acuerdo con su funcionalidad, hay servidores que pueden trabajar sin conexiones arbitrarias, mientras que otros dependen de éstas para llevar a cabo su trabajo. Un caso de los primeros sería el servidor de una empresa y uno de los segundos, un servidor de uso público; para estos últimos existen algunos convenios que entregan mayor seguridad a la hora de iniciar una conexión. Por ejemplo, el comando "PORT" incluye parámetros que indican al servidor cuál dirección IP conectar y qué puerto abrir. Éste es el medio en el cual se manejan los atacantes para organizar toda su estrategia.

Al trabajar en exclusiva conformidad con las funciones del RFC, se puede lograr que la máquina sólo trabaje para una terminal por vez. En líneas generales, esto evita que se realice una conexión con el servidor con la intención de crear otra conexión alterna con diferente dirección. La otra alternativa es realizar un proceso de condicionamiento selectivo de las terminales conectadas al servidor, suprimiendo de manera directa aquellas que no han realizado una conexión inicial. En particular, el servicio FTP es de gran utilidad, puesto que es rápido y confiable a nivel de usuario, pero sus brechas son muchas, por lo que es importante procurar evadir su uso como servicio público (Terán Pérez, 2010).

Ataques por WWW. En líneas generales, los ataques vía *web server* son variados; la mayoría aprovecha los *bugs* de los scripts de las páginas para que el servidor entregue información que no desea. Un ejemplo muy sencillo es ingresar al directorio raíz del *web server* omitiendo la extensión "index.htm".

Otra manera es cambiando los *scripts* de la página; por ejemplo, crear un clon web con el código fuente de la página, luego bajar los scripts y, finalmente, adulterarlos para que entreguen la información solicitada.

1.5.6 Control de acceso, respaldos, autenticación y elementos de protección perimetral

Una vez solucionado el problema interno, es importante abocarse a la seguridad contra elementos externos, estimando las posibles vulnerabilidades que posee la red en cuanto a accesos clandestinos y posibles ataques. Para ello, se deben planificar las acciones a seguir mediante un procedimiento de supervisión con herramientas de control y de seguimiento de accesos que permitan verificar con periódicidad los eventos que ocurren en la corporación (Terán Pérez, 2014). Por ejemplo, verificar a diario el número de correos recibidos y/o enviados, la cantidad de conexiones de red levantadas en las últimas 24 horas, etc. También es posible extraer diaria y semanalmente un estado sobre los ingresos desde el exterior a la Intranet (si es que los hay), de los archivos, del tráfico en la red, etcétera.

Procedimientos de seguridad a nivel de usuario. Todo lo que es recurso humano en una corporación en general debería al menos tener un acceso mínimo, con las limitaciones correspondientes a la red. En caso de que un individuo no posea acceso, éste aún debería ser considerado dentro de un informe de autorización para maximizar las posibilidades de supervisión al interior de la red corporativa. Los datos del usuario deben al menos llenar los siguientes campos:

- Nombre y apellido.
- Puesto que ocupa en la corporación.
- Nombre del superior directo que confirme la posición del individuo.
- Descripción de los recursos a los cuales desea tener acceso y el motivo.
- Consentimiento de que las actividades son susceptibles de ser supervisadas en cualquier momento y de que conoce las normas de uso adecuado de los recursos.
- Explicaciones breves pero claras de cómo elegir su contraseña.
- Tipo de cuenta.
- Fecha de caducidad o expiración.
- Datos referentes a los tipos de acceso; por ejemplo, lectura, lectura y escritura, sin acceso, acceso limitado, etcétera.
- Horario de uso en general.

Con respecto a las contraseñas, es importante verificar si la entregada es segura haciendo correr, por ejemplo, un programa (*crack*) que determine cuánto se demora en descifrarla.

La baja del usuario se realiza cuando un elemento de la organización se aleja o cuando cesa en el cumplimiento de sus actividades por un tiempo determinado (vacaciones, viáticos prolongados, cambio de departamento, etcétera). Ésta debe ser informada por los departamentos correspondientes a la administración de redes, que determinan la inhabilitación o eliminación de una cuenta con las consecuencias que ello implica (respaldo o eliminación de la información, directorios y archivos de la cuenta).

Procedimientos de seguridad a nivel global. Entre los procedimientos a nivel global se encuentran:

- Verificación de accesos: mediante aplicaciones que informen anomalías, incluyendo fecha, hora, recursos y detalles técnicos.
- Verificación del tráfico de la red: también mediante aplicaciones que entreguen informes periódicos de los programas que se ejecutan, quién es el encargado de monitorear los datos generados, los intervalos de monitoreo etcétera.
- Monitoreo de los volúmenes de correo: permite entregar detalles como el ingreso de *spam* a la red, posibles invasiones o mal uso de los recursos de ésta.
- Monitoreo de conexiones activas: este procedimiento se efectúa con el fin de prevenir que algún usuario deje su terminal abierta haciendo posible que alguien distinto a éste use su cuenta. También se utilizan aplicaciones para monitorear la actividad de las conexiones de los usuarios: si la cuenta tiene cierto tiempo inactiva, cierra la sesión y genera un informe (*log*) con el acontecimiento.
- Monitoreo de modificación de archivos: permite determinar la modificación no autorizada de los recursos de *software* y/o de la integridad de ellos. Éste es, quizá, el procedimiento más importante dentro de lo que es seguridad global, pues permite saber si, por ejemplo, un archivo es eliminado o si se tiene la presencia de algún tipo de virus en el sistema.
- Respaldos de seguridad: no sólo es importante respaldar la información que se encuentra en la red, sino además, la configuración de todos los recursos de la red, incluyendo la labor que desempeña cada uno de sus elementos, a fin de crear una respuesta rápida en el momento de que se suscite un problema.
- Verificación de terminales: esto se hace mediante la revisión de los programas instalados en los equipos terminales de la red, lo que permite monitorear qué aplicaciones se encuentran sin licencia, qué archivos bajados desde Internet son potencialmente peligrosos (virus y/o programas satélite), etcétera.
- Monitoreo de puertos: permite saber qué puertos están habilitados en la red, en los enrutadores y en el servidor. Esto se puede hacer incluso con los mismos enrutadores, los cuales poseen aplicaciones integradas que posibilitan administrar los puertos en forma más eficiente.
- Información de los procedimientos: esto es la clave para cualquier sistema que desee evitar el mayor número de problemas en una red. Informando apropiada y cotidianamente mediante seminarios internos de seguridad, vía *e-mail* y por medio de publicaciones periódicas se llega a más gente de forma más efectiva.
- Determinación de los niveles de responsabilidad y acceso: es sumamente importante, además, identificar a cada usuario en un grupo establecido (por ejemplo, del equipo técnico, de la oficina gerencial, de la oficina zonal, de los alumnos, del profesor, etcétera) para determinar el nivel de acceso a los recursos de la red.

- Recuperación del sistema: en caso de un ataque o un colapso eventual del sistema (si se dañó el servidor y se tiene la necesidad de actualizar todos o algunos recursos de la red), es necesario preparar un procedimiento que regule la forma de recuperarlo a través de los respaldos de seguridad realizados. Para ello, se debe estimar la forma y los costos (en materiales y en tiempo), con el objetivo de llevar a cabo la restauración a la brevedad posible.
- Listas de elementos a verificar (*check-list*): es importante enlistar todos los procedimientos con el fin de asegurar la realización de cada uno en su totalidad.

1.5.7 Seguridad en NetBIOS

El sistema operativo más usado actualmente es Windows. La mayoría de las redes corporativas ocupan éste por una razón muy sencilla: es amigable y fácil de usar, pero es un sistema cerrado que no admite modificaciones ni libertad de acción en sus subrutinas. Esto quizá es positivo porque también entrega un sistema muy difícil de romper, desde el punto de vista de un atacante. Como sea, los sistemas operativos de Microsoft usan el protocolo NetBIOS para comunicarse entre sí, lo cual significa una gran desventaja comunicacional, debido a que otros no requieren de éste para comunicarse entre sí, pero sí lo hacen con terminales que usan sistemas operativos de Microsoft. Este protocolo, a su vez, debe ir sobre otro de nivel inferior que puede ser uno de los siguientes: NetBEUI, IPX/SPX o TCP/IP (Terán Pérez, 2010). Desde la implementación de Windows Vista, el protocolo NetBEUI (interfaz de usuario extendida de NetBIOS) ya no se usa.

A la implementación de NetBIOS sobre TCP/IP se le conoce como NBT. La ventaja de las redes Microsoft es que permiten compartir archivos e impresoras. Por lo general, en redes en las que se encuentran presentes equipos Microsoft lo mejor es usar NBT, aunque a veces son mejores otras combinaciones, como es en el caso de una red LAN con conexión a Internet o NetBIOS sobre IPX/SPX, que además tiene la ventaja de compatibilidad con otros sistemas operativos (Comer, 2005).

Dentro del tema, uno de los mayores problemas a enfrentarse cuando se habla de redes bajo aplicaciones de Microsoft son las carpetas compartidas, que son un grave error: la mayoría de las personas considera trivial incluir una contraseña para acceder a una carpeta compartida de sólo lectura; además, ignora absolutamente que ésta puede ser vista por todos los usuarios de Internet. En efecto, si se tiene montado el protocolo NetBIOS sobre TCP/IP, la carpeta será considerada como compartida no sólo por todos los usuarios de la red local, sino por aquellos de Internet. Esto se evita de manera relativamente sencilla a través del siguiente procedimiento: se configura el enrutador filtrando los puertos que usan NBT para uso exclusivo de la red local, lo que también aplica a redes WAN. Otras maneras de incrementar la seguridad de las redes son el uso de *boot disks* en las terminales de la red, trabajar con enrutadores confiables (Cisco Systems para redes WAN y no menos de D-Link para redes LAN) y, por supuesto, informar a los usuarios acerca de las normas y regulaciones de uso de la red.

1.5.8 Herramientas de control y seguimiento de accesos

Como se ha observado, para cualquier administrador de redes es indispensable poseer herramientas que permitan diagnosticar, supervisar, realizar estimaciones, obtener datos y, sobre todo, defenderse de posibles ataques y resolver los problemas que se generan

a nivel interno y externo de una red corporativa. Éstas permitirán mantener un control sobre todos los paquetes que entran por la capa de red y de aplicación de la máquina; sin embargo, su instalación debe ser de manera aislada, preferentemente de uso particular del administrador y en una terminal que no sea de tipo servidor. Naturalmente, ésta debe permanecer también apartada del uso de otros usuarios de la red. Las herramientas más frecuentes son las siguientes:

Tcp-wrappers. *Software* de dominio público cuya función es proteger determinados servicios de red de los sistemas de operaciones no deseadas, permitiendo ejecutar ciertos comandos ante acciones definidas de manera automática. Con este programa, es posible monitorear y filtrar peticiones entrantes de distintos servicios TCP/IP. Se pueden controlar los accesos mediante el uso de reglas y dejar una traza de todos los intentos de conexión tanto admitidos como rechazados.

Netlog. Herramienta que genera trazas referentes a servicios basados en IP (TCP, UDP) e ICMP, así como tráfico en la red que pudiera ser sospechoso y que indique un posible ataque a la máquina. Está constituido por tres subprogramas independientes para cada servicio (TCP, UDP, ICMP): uno que genera estados de todas las conexiones realizadas indicando hora, máquina de origen y puerto de conexión; uno que monitorea la red buscando ciertos protocolos con actividad inusual (como una conexión TFTP) y otro que entrega las estadísticas de uso de varios protocolos, que puede enseñar cambios sospechosos en los patrones de utilización de la red.

Argus. Herramienta que permite realizar supervisiones del tráfico IP de la red, mostrando todas las conexiones que descubre.

SATAN (*Security Administrator Tool for Analyzing Network*). Posibilita, entre otras cosas, verificar máquinas conectadas en red. Genera información sobre la máquina y con qué servicios cuenta; además de avisar acerca de varios tipos de fallas de seguridad de cada una. La gracia de SATAN es que ocupa una interfaz de sitio web similar a las que usan los enrutadores para su configuración y crea una base de datos de todas las terminales y las va relacionando entre ellas. Por ejemplo, si determina una terminal insegura y nota que está relacionada con otra, a las dos las cataloga de la misma forma; sin embargo, así como puede entregar datos valiosos de potenciales ataques y/o problemas de la red, también es posible usarla como herramienta para encontrar todas las características de sus terminales y así preparar un ataque estratégico. El sucesor actual de esta herramienta es Nessus.

ISS (*Internet Security Scanner).* Esta aplicación verifica una serie de servicios para comprobar el nivel de seguridad que tiene esa máquina. Es capaz de comprobar una dirección IP o un rango de éstas con una IP inicial y una final.

Courtney (*o Anti SATAN*). Como se mencionó anteriormente, SATAN puede ser usado de manera maliciosa para recaudar información de las máquinas de una red. Courtney trabaja conjuntamente con tcp-dump para determinar si se está llevando a cabo una verificación de puertos en un determinado intervalo de tiempo, en cuyo caso da aviso entregando un log con la información de la terminal que está realizando la verificación.

1.6 Conclusiones

Debido a la importancia de las redes, uno o más ingenieros dedicados a dicha área tienen la responsabilidad de planificarlas, instalarlas y administrarlas. Obviamente, éstas surgen por el interés de los usuarios o por una política de posicionamiento de la unidad de negocios de la organización.

Las redes son demasiado complejas por el número y la variedad de equipos; por los paquetes, los programas y los sistemas operativos que utilizan; y por los medios físicos y/o inalámbricos usados; por ello, la organización necesita conocer dónde se encuentran los dispositivos, qué dirección tienen, cómo están interconectados, etc., o sea, establecer la configuración o mapa de la red y contar con la posibilidad de modificar remotamente (desde una consola de control, por ejemplo) lo requerido. Además, requiere conocer cómo se comporta la red y el rendimiento y/o desempeño a fin de saber el uso que se le da: si se presenta una congestión, si hay algún problema que deba ser investigado, si el uso de la red está creciendo de modo que pronto colapsará, etcétera. También es necesario estar pendiente de las fallas que ocurran; éstas deben ser detectadas antes de que los usuarios se den cuenta de que existen. Es deseable que muchas puedan ser corregidas sin necesidad de ir hasta donde están los equipos, haciendo uso de la consola, que permite acceder remotamente a ellos.

Por otra parte, la organización tiene gran interés en evitar el acceso malicioso de intrusos (*hackers*, *crackers*, espías, etcétera) a áreas de la red donde se encuentra información privada, que solo puede ser modificada por personal autorizado o donde existe software vital para su funcionamiento; entonces, la red debe ser asegurada.

Como la red es un recurso compartido, debe garantizarse un uso equitativo entre los usuarios; además, los servicios se prestan con un fin comercial, por ello, la organización requiere un sistema de contabilidad con la finalidad de ratificar que cada usuario reciba el servicio de acuerdo con las normas convenidas.

Estas tareas de configuración, rendimiento, fallas, seguridad y contabilidad constituyen las áreas fundamentales de la administración de redes como las enumeran el Modelo OSI y la Organización Internacional de Estándares (ISO). La administración de redes, consiste específicamente en:

- Un conjunto de procesos para controlar una red de datos compleja.
- Querer maximizar la efectividad y la productividad.
- Englobar la administración, la organización y la regulación.
- Ser clave para mejorar el funcionamiento.

Con el crecimiento indetenible de las redes, hay una multiplicación de conexiones y aumento de la demanda en aplicaciones, protocolos y operaciones que las convierten en más complejas cada día. Estas actividades de administración de redes son cada vez más importantes, tanto debido a su complejidad actual, como a su necesidad de crecimiento racional y organización; además, es necesario automatizarlas, pues requieren de inversión de tiempo y respuestas muy rápidas.

En la redes donde no hay administración, las personas responsables de la configuración, funcionamiento y crecimiento no tienen información precisa para su tarea: ignoran si sus instalaciones son efectivas y de costo razonable; no pueden medir la confiabilidad

y disponibilidad de los equipos y de los servicios que se ofrecen, por lo que las fallas son difíciles de identificar y de corregir, especialmente si son intermitentes, pues carecen de bases de datos y de planos sobre el cableado de los equipos; tampoco saben si las redes necesitan ampliación ni en qué medida.

Si una red colapsa por un crecimiento no previsto de su uso, la solución del problema es larga porque hay que estudiar cómo crecerá la red, con qué tecnología, con qué equipos, de dónde saldrán los recursos financieros y qué impacto tendrá en la red actual el proceso de instalación de la nueva tecnología y de los nuevos equipos; de lo contrario, se corre el peligro de pérdidas enormes, ya que los usuarios se quedan sin saber qué hacer para trabajar y mantener la organización funcionando y, generalmente, todo se paraliza, con detrimentos considerables de tiempo, de dinero y hasta de vidas, como en el caso de hospitales, servicios de emergencia, seguridad y otros, donde no se ha previsto redundancia o enrutamientos alternativos rápidos en las redes respectivas.

Cuestionario

1.1 Explique a detalle qué es la administración de una red de computadoras estableciendo cada uno de los puntos que intervienen en ella y por qué es importante llevar a cabo una óptima administración de éstas.

1.2 Establezca al menos cinco casos de estudio exitosos en el uso de una administración estratégica de las redes de computadoras.

1.3 Establezca mediante un mapa conceptual cómo debe desarrollarse la administración de las redes de computadoras.

1.4 Investigue cuáles son las normas nacionales e internacionales que intervienen en la adecuada gestión de las redes de computadoras.

Referencias

3GPP (s. f.). *(IMS); Stage 2*. Disponible en http://www.3gpp.org/ftp/Specs/html-info/23228.htm, consultado en abril de 2017.

_____ (s. f.). 3rd. *Generation Partnership Project* (3GPP). Disponible en www.3gpp.org/about-3gpp, consultado en junio de 2017.

_____ (2006). *The Internet Engineering Task Force. RFC 4 566: SDP: Session Description Protocol.* Disponible en http://www.ietf.org/rfc/rfc4566.txt?number=4566, consultado en abril de 2017.

Abramson, N. (2000). "Internet access using VSAT" en *IEEE Community Magazine*, (38): pp. 60-68.

Academia de Networking de Cisco Systems (2004). *Serie Cisco Systems CCNA*. USA: CISCO Press, 3rd. ed.

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems*. New York: John Wiley & Sons.

Berghel, H. L. (2001). "Cyber privacy in the new millennium" en *IEEE Computer,* (34): pp. 132-134.

Berners-Lee, T. (1990). *Inventing the Web: Christmas Baby. Seeing the Picture*.

_____ (2009). "Pre-W3C Web and Internet Background" en *World Wide Web Consortium*.

Berners-Lee, T.; Cailliau, A.; Loutonen, A.; Nielsen, H. F. and Secret, A. (1994). "The World Wide Web" en *Community of the ACM*, (37): pp. 76-82.

Berners-Lee, T.; Bray, T.; Connolly, D.; Cotton, P.; Fielding, R.; Jeckle, M.; Lilley, C.; Mendelsohn, N.; Orchard, D.; Walsh, N.; Williams, S. (2004).

Berners-Lee, T. *et al*. (2004). *Architecture of the World Wide Web, Volume One*. USA.

Bertsekas, D. and Gallager, R. (1992). *Data networks*. Englewood Cliffs, New Jersey: Prentice-Hall.

Bhatti, S. N. and Crowcroft, J. (2000). "QOS sentitive flows: Issues in IP packet handling" en *IEEE Internet Computing*, (4): pp. 48-57.

Black, U. (1997). *Redes de computadoras. Protocolos, normas e interfaces*. México: Alfaomega Grupo Editor, 2a. edición.

Boggs, D.; Mogul, J. and Kent, C. (1988). "Measured capacity of an Ethernet: Myths and reality" en *Procedures SIGCOMM ´88 Conference*, pp. 222-234.

Bounoure, F. *et al*., (2006). *Laboratorio de redes: Session Initiation Protocol*. Argentina: Universidad de Buenos Aires.

Braden, R. (1989). "Requirements for Internet hosts-communications layers" en *RFC 1 122*. USA.

Bray, T.; Paoli, J.; Sperberg-McQueen, C.; Maler, E.; Yergeau, F. and Cowan, J. (2006). "Extensible Markup Language (XLM) 1.1" en *Recommendation of the W3C*.

Burleigh, S.; Hooke, A.; Torgerson, L.; Fall, K.; Cerf, V.; Durst, B.; Scott, K. and Weiss, H. (2003). "Delay-tolerant networking: An approach to interplanetary Internet" en *IEEE Community Magazine*, (41): pp. 128-136.

Chase, J. S.; Gallatin, A. J. and Yocum, K. G. (2001). "End system optimization for high-speed TCP" en *IEEE Community Magazine*, (39): pp. 68-75.

Chen, S. and Nahrstedt, K. (1998). "An overview of QOS routing for next-generation networks" en *IEEE Network Magazine*, (2): pp. 64-69.

Cisco Sys (2010a). CISCO *visual networking index: Forecast and methodology*. USA: Cisco Systems.

_____ (2010b). *Resource Reservation Protocol*. USA: Cisco Systems. Disponible en https://www.cisco.com/c/en/us/products/ios-nx-os-software/resource-reservation-protocol-rsvp/index.html, consultado en mayo de 2017.

Clark, D. D. (1988). "The design philosophy of the DARPA Internet protocols" en Procedures SIGCOMM ´88 *Conference, ACM*, pp. 106-114.

Clark, D. D.; Jacobson, V.; Romkey, J. and Salwen, H. (1989). "An analysis of TCP processing over-head" en *IEEE Community Magazine*, (27): pp. 23-29.

Clark, D. D.; Shenker, S. and Zhang, L. (1992). "Supporting real-time applications in an integrated services packet network" en *Procedures SIGCOMM ´92 Conference ACM*, pp. 14-26.

Comer. D. E. (2005). I*nternetworking with TCP/IP*. Englewood Cliffs, New Jersey: Prentice-Hall, 5th. ed.

_____ (2007). *The Internet book*. Englewood Cliffs, New Jersey: Prentice-Hall, 4th ed.

Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública en Argentina (s. f.). *Manual de Seguridad en Redes (ArCERT)*. http://www.psicosocial.net/grupo-accion-comunitaria/centro-de-documentacion-gac/areas-y-poblaciones-especificas-de-trabajo/desgaste-y-seguridad-para-activistas/540-manual-de-seguridad-en-redes-informaticas/file, consultado en junio de 2017.

Croft, B. (2005). RFC 951: *Bootstrap Protocol*. USA: FRC.

Crovella, M. and Krishnamurty, B. (2006). *Internet measurement*. New York: John Wiley & Sons.

Davie, B. and Farrel, A. (2008). *MPLS: Next generation*. San Francisco, California: Morgan Kaufmann.

Davie, B. and Rekhter, Y. (2000). *MPLS technology and applications*. San Francisco, California: Morgan Kaufmann.

Davies, J. (2008). *Understanding IPv6*. Redmon, WA: Microsoft Press.

Day, J. D. and Zimmermann, H. (1983). "The OSI Reference Model" *en Procedures of the IEEE*, (71): pp. 1334-1340.

Deering, S. E. (1993). "SIP: Simple Internet Protocol" en *IEEE Network Magazine*, (7): pp. 16-28.

Deering, S. E. and Cheriton, D. (1990). "Multicast routing in datagram networks and extended LAN" en *ACM Transactions on Computer Systems*, (8): pp. 85-110.

Demers, A.; Keshav, S. and Shenker, S. (1990). "Analysis and simulation of a fair queueing algorithm" en *Internetworking: Research and Experience*, (1): pp. 3-26.

Devarapalli, V.; Wakikawa, R.; Petrescu, A. and Thubert, P. (2005). "Network mobility (NEMO) basic support protocol" en *RFC 3 963*.

Donahoo, M. and Calvert, K. (2008). *TCP/IP sockets in Java*. San Francisco, California: Morgan Kaufmann, 2nd ed.

_____ (2009). *TCP/IP sockets in C*. San Francisco, California: Morgan Kaufmann, 2nd. ed.

Donaldson, G. and Jones, D. (2001). "Cable TV broadband network architectures" en *IEEE Community Magazine*, (39): pp.122-126.

Ericsson (2007). *Introduction to IMS, White Paper*. Disponible en: http://cse.iitkgp.ac.in/~pallab/mob_com/Ericsson_Intro_to_IMS.pdf, consultado en junio de 2017.

Fall, K. (2003). "A delay-tolerant network architecture for challenged Internets" en *Procedures SIGCOMM 2003 Conference ACM*, pp. 27-34.

Faloutsos, M.; Faloutsos, P. and Faloutsos, C. (1999). "On power-law relationships of the Internet topology" en *Procedures SIGCOMM ´99 Conference ACM*, pp. 251-262.

Farrell, S. and Cahill, V. (2007). *Delay and disruption tolerant networking*. London: Artech House.

Fenner, B.; Handley, M.; Holbrook, H. and Kouvelas, I. (2006). "Protocol Independent Multicast-Sparse Mode (PIM-SM)" en *RFC 4 601*.

Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Berners-Lee´s, T. (1999). *Hypertext Transfer Protocol-HTTP/1.1. Request for comments 2616*. USA: Information Sciences Institute.

Ford, W. and Baum, M. S. (2000). *Secure electronic commerce*. Upper Saddle River, New Jersey: Prentice-Hall.

Fouli, K. and Maler, M. (2009). "The road to carrier-grade Ethernet" en *IEEE Community Magazine*, S30-S38.

García, T. (2001). *Redes para proceso distribuido*. México: Alfaomega Grupo Editor, 2a. edición.

Gast, M. (2005). 802.11 *Wireless networks: The definitive guide*. Sebastopol, California: O´Reilly.

Gershenfeld, N.; Krikorian, R. and Cohen, D. (2004). "The Internet of things" en *Scientific American*, (291): pp. 76-81.

Goode, B. (2002). "Voice over Internet Protocol" en *Procedures of the IEEE*, (90): pp. 1495-1517.

Grayson, M.; Shatzkamer, K. and Wainner, S. (2009). *IP design for mobile networks*. Indianapolis: Cisco Press.

Ha, S.; Rhee, I. and Lisong, X. (2008). CUBIC: "A new TCP friendly high speed TCP variant" en *SIGOPS Operating Systems Review*, (42): pp. 64-74.

Hallivuori, V. (2000). *Real Time Transport Protocol (RTP) Security*. Helsinki, Finlandia: University of Technology.

Halsall, F. (1988). *Comunicación de datos, redes de computadoras y sistemas abiertos*. México: Pearson Education, 4a. edición.

Harte, L.; Kellogg, S.; Dreher, R. and Schaffnit, T. (2000). *The comprehensive guide to wireless technology*. Fuquay-Varina, NC: APDG Publishing.

Hecht, J. (2005). *Understanding fiber optics*. Upper Saddle River, New Jersey: Prentice-Hall.

Held, G. (2010). *A practical guide to content delivery networks*. Boca Ratón, Florida: CRC Press.

Hiertz, G.; Denteneer, D.; Stibor, L; Zang, Y.; Costa, X. and Walke, B. (2010). "The IEEE 802.11 iniverse" en *IEEE Community Magazine*, (48): pp. 62-70.

Hoe, J. (1996). "Improving the start-up behavior of a congestion control scheme for TCP" en *Procedures SIGCOMM ´96 Conference ACM*, pp. 270-280.

Hu, Y. and Li, V. O. K. (2001). "Satellite-based Internet: A tutorial" en *IEEE Community Magazine*, (30): pp. 154-162.

Huitema, C. (1999). *Routing in the Internet*. Englewood Cliffs, New Jersey: Prentice Hall, 2nd. ed.

International Telecommunications Union (ITU) (2005). *ITU Internet reports 2005: The Internet of things*. Ginebra, Switzerland: ITU.

_____ (2005a). *Measuring the information society: The ICT development index*. Ginebra, Switzerland: ITU.

Jacobson, V. (1990). "Compressing TCP/IP headers for low speed serial links" en *RFC 1 144*. USA.

Jain, R. and Routhier, S. (1986). "Packet trains-measurments and a new model for computer network traffic" en *IEEE Journal on Select Areas in Communications*, (6): pp. 986-995.

Joel, A. (2002). "Telecommunications and the IEEE communications society" en *IEEE Community Magazine, 50th Anniversary Issue*, pp. 6-14, 162-167.

Johnson, D.; Perkins, C. and Arkko, J. (2004). "Mobility support in IPv6" en *RFC 3 775*. USA.

Kaufman, C.; Perlman, R. and Speciner, M. (2002). *Network security*. Englewood Cliffs, New Jersey: Prentice-Hall, 2nd. ed.

Koodli, R. and Perkins, C. E. (2007). *Mobile internetworking with IPv6*. New York: John Wiley & Sons.

Krishnamurti, B. and Rexford, J. (2001). *Web protocols and practice*. Boston, Massachusetts: Addison-Wesley.

Kurose, James. F. and Keith, W. Ross. (2005). *Computer Networking: A top-Down Approach Featuring the Internet*. USA: Addison Wesley, 3th. ed.

Labovitz, C.; Ahuja, A.; Bose, A. and Jahanian, F. (2001). "Delayed Internet routing convergence" en *IEEE/ACM Transactions on Networking*, (9): pp. 293-306.

Le Point (2010). *Le Web a été inventé en France*. Paris, France.

Lewis, M. (2006). *Comparing, designing and deploying VPN*. Indianapolis, IN: Cisco Press.

Lin, S. and Costello, D. (2004). *Error control coding*. Upper Saddle River, New Jersey: Pearson Education.

Long, T. (2012). Aug. 7, 1991: *Ladies and Gentlemen, the World Wide Web*. Disponible en https://www.wired.com/2012/08/aug-7-1991-ladies-and-gentlemen-the-world-wide-web/, consultado en mayo de 2017.

Lubacz, J.; Mazurczyk, W. and Szczypiorski, K. (2010). "Voice over IP" en *IEEE Sprectrum*, pp. 42-47.

Mani, M, and Crespi, N. (2007). *Adopting IMS in Wi-Fi Technology*. Disponible en http://portal.acm.org/citation.cfm?id=1378117, consultado en junio de 2017.

Maufer, T. A. (1999). *IP fundamentals*. Upper Saddle River, New Jersey: Prentice-Hall.

Metz, C. (2001). "Interconnecting ISP networks" en *IEEE Internet Computing*, (5): pp. 74-80.

Munasighe, K. and Jamalipour, A. (2008). *Interworking of WLAN-UMTS Netwoks: An IMS based Plataform for Session Mobility*. USA: IEEE.

Neuman, C. and Ts´O, T. (1994). "Kerberos: An authentications service for computer networks" en *IEEE Community Magazine*, (32): pp. 33-38.

Palais, J. C. (2004). *Fiber optic communications*. Englewoods Cliffs, New Jersey: Prentice-Hall.

Parameswaran, M.; Susarla, A. and Whinston, A. B. (2001). "P2P networking: An information sharing alternative", en *IEEE Computer*, (34): pp. 31-38.

Pechuán, L. M. (2010). *El nuevo sistema multimedia conocido como IMS que adoptarán las redes UMTS. Universidad de Valencia*. Disponible en https://www.researchgate.net/publication/316214714_El_nuevo_sistema_multimedia_conocido_como_IMS_que_adoptaran_las_redes_UMTS?channel=doi&linkId=58f6356da6fdcc738a11df22&showFulltext=true, consultado en junio de 2017.

Perkins, C. E. (1998). *Mobile IP design principles and practices*. Upper Saddle River, New Jersey: Prentice-Hall.

_____ (2001). *Ad hoc networking*. Boston, Massachusetts: Addison-Wesley.

_____ (2002). "IP mobility support for IPv4" en *RFC 3 344*.

_____ (2003). *Audio and video for the Internet.* Boston, Massachusetts: Addison-Wesley.

Perlman, R. (1985). "An algorithm for the distributed computation of a spanning tree in an extended LAN" en *Procedures SIGCOMM ´85 Conference ACM*, pp. 44-53.

_____ (2000). *Interconnections*. Boston, Massachusetts: Addison-Wesley.

Piscitello, D. M. and Chapin, A. L. (1993). *Open systems networking: TCP/IP and OSI*. Boston, Massachusetts: Addison-Wesley.

Poikselka, Miikka *et al*. (2006). *The IMS IP multimedia concepts and services*. USA: John Wiley & Sons Ltd.

Polo, L. (2003). *World Wide Web technology architecture: A conceptual analysis*. USA: New Devices.

Postel, J. (1981). "Internet control message protocols" en *RFC 792*. USA.

Quittner, J. (2010). "Tim Berners-Lee. *Time 100 People of the Century" en Time Magazine*.

Rabin, J. and McCathienevile, C. (2008). "Mobile web best practices 1.0" en *Recommendation of the W3C*.

Ramaswami, R.; Kumar, S. and Sasaki, G. (2009). *Optical networks: A practical perspective*. San Francisco, California: Morgan Kaufmann, 3th. ed.

Real Academia Uruguaya (s. f.). *Introducción al IPv6*. Disponible en http://www.rau.edu.uy/ipv6/queesipv6.htm, consultado en mayo de 2017.

Ronan, J., Balasubramaniam, S., K Kiani, A., Yao, W. (s. f.). *On the use of SHIM6 for mobility support in IMS Networks*.

Salazar, J. E. *et al*. (2002). *Diffserv como solución a la provisión de Q_0S en la Internet.* España: Universidad Carlos III de Madrid.

Simpson, W. (2008). *Video over IP.* Burlington, Massachusetts: Focal Press.

Spurgeon, C. E. (2000). *Ethernet: The definitive guide*. Sebastopol, California: O´Reilly.

Stallings, William. (2010). *Comunicaciones y redes de computadoras*. México: Pearson Educación, 9a. edición.

Stevens, W. R. (1994). *TCP/IP illustrated: The protocols*. Boston, Massachusetts: Addison-Wesley.

Tanenbaum, A. S. (2007). *Modern operating systems*. Upper Saddle River, New Jersey: Prentice-Hall, 3rd. ed.

Tanenbaum, A. S. and Van Steen, M. (2007). *Distributed systems: Principles and paradigms*. Upper Saddle River, New Jersey: Prentice-Hall.

Telefónica (s. f.). *Evolución al dominio IMS*. Disponible en http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/capitulo_12.pdf, consultado en junio de 2017.

The Internet Engineering Task Force (s. f.). "RFC 2 205" en *Resource ReSerVation Protocol (RSVP)*. Disponible en http://www.ietf.org/rfc/rfc2205.txt?number=2205, consultado en junio de 2017.

_____ (s. f.). "RFC 2 748" en *The COPS (Common Open Policy Service) Protocol*. Disponible en http://www.ietf.org/rfc/rfc2748.txt?number=2748, consultado en abril de 2017.

_____ (s. f.). "RFC 3 550" en *RTP: A Transport Protocol for Real-Time Applications*. Disponible en http://www.ietf.org/rfc/rfc3550.txt, consultado en abril de 2017.

Terán Pérez, D. M. (2010). *Redes convergentes. Diseño e implementación*. México: Alfaomega Grupo Editor.

_____ (2012). *Introducción a la computación cuántica para ingenieros*. México: Alfaomega Grupo Editor.

_____ (2014). *Administración estratégica de la función informática*. México: Alfaomega Grupo Editor.

_____ (2016). *Introducción a la ingeniería*. México: Alfaomega Grupo Editor.

Tompros, S. and Denazis, S. (2007). *Interworking of heterogeneous access networks and QoS provisioning via IP multimedia core networks*. Universidad de Patras. Disponible en: http://www.sciencedirect.com/science/article/pii/S1389128607002356, consultado en junio de 2017.

Wittenburg, N. (2009). *Understanding voice over IP technology*. Clifton Park, New York: Delmar Cengage Learning.

World Wide Web (2009). *Proposal for a Hypertexts Project*. USA.

_____ (2010). *Proposal for a Hypertext Project*. USA.

Znaty, S., Dauphin, Jean L. and Geldwerth, R. (s. f.). *IP Multimedia Subsystem: Principios y arquitectura. EFORT*. Disponible en http://www.efort.com/media_pdf/IMS_ESP.pdf, consultado en junio de 2017.

_____ (s. f.). *SIP: Session Initiation Protocol effort*. Disponible en http://www.efort.com/media_pdf/IMS_ESP.pdf, consultado en mayo de 2017.

Administración de una red de computadoras

No es posible obtener resultados distintos haciendo siempre lo mismo.

Albert Einstein

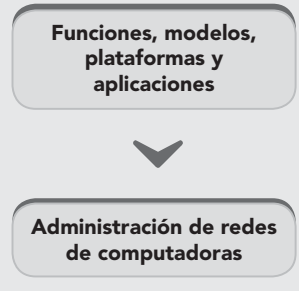
Reflexione y responda las siguientes preguntas:

- ¿Cómo funciona la administración de una red de computadoras?
- ¿Cómo opera el Modelo de Gestión ISO en una red de computadoras?
- ¿Qué son las plataformas de gestión de una red de computadoras?

Después de estudiar este capítulo, el lector será capaz de:

- Entender qué es la administración de una red de computadoras.
- Comprender la importancia de la administración de una red de computadoras.
- Establecer en qué consiste la administración de una red de computadoras.

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:



2.1 Introducción

La gestión de una red de computadoras es el conjunto de tareas de monitorización, información y control necesarias para que ésta opere efectivamente (Kurose y Keith, 2005). Estas actividades pueden estar distribuidas sobre diferentes nodos de la red, lo cual requiere repetidas acciones de recogida de datos y de análisis cada vez que sucede un nuevo evento; aquéllas se llevan a cabo por el personal responsable o por procesos automáticos de gestión, desde los cuales se controla y vigila el correcto funcionamiento de todos los equipos integrados en las distintas redes de la organización en cuestión.

Algunos objetivos específicos de la gestión de una red de computadoras son los siguientes:

- Detección de fallas y corrección con la máxima rapidez posible.
- Monitorización del rendimiento a través de una adecuada detección de "cuellos de botella" con el objetivo de minimizar el efecto.
- Gestión de contabilidad y uso que se hace del sistema.
- Administración de seguridad.
- Instalación y distribución de *software* en el sistema de manera controlada.
- Gestión de los componentes del sistema y configuración del mismo.
- Planificación y crecimiento del sistema.

2.2 Funciones de la administración de redes de computadoras

Un elevado costo en los diseños y desarrollo de las redes de computadoras y el aumento de las capacidades de proceso han conducido a que muchas organizaciones se planteen otras alternativas de migrar sus sistemas de información tradicionales con arquitecturas centralizadas a las distribuidas. Por supuesto, de nada serviría realizar una gestión de aplicaciones y bases de datos, si además no se lleva a cabo en los servidores que los sustentan, dado que el rendimiento del conjunto depende de la disponibilidad de cualquiera de los elementos que lo componen.

Cuando se hace referencia a gestionar servidores, se trata de la supervisión proactiva de su actividad, de los procesos y los usuarios; de la conducción de eventos y de cambios; la planificación de actividades y capacidades; actualización de versiones; la operación de procesos, etc. En otras palabras, consiste en administrar de manera integral, el ciclo de procesos asociados con los servidores distribuidos por medio de tres tipos principales de recursos:

Métodos de gestión. Definen las pautas de comportamiento de los demás componentes del centro de gestión de la red de computadoras ante determinadas circunstancias.

Recursos humanos. Personal encargado del correcto funcionamiento del centro de gestión de la red.

Herramientas de apoyo. Elementos que facilitan las tareas de gestión a los operadores humanos y que posibilitan minimizar el número de estos.

La gran mayoría de los sistemas de gestión que existen actualmente utilizan una estructura básica, conocida por paradigma gestor–agente. Estos se componen, por lo general de:

Una interfaz con el operador o con el responsable de la red. Es una pieza fundamental en la consecución del éxito de un sistema de gestión, pues a través de ella el operador puede invocar la realización de operaciones de control y vigilancia de los recursos que están bajo su responsabilidad. Se puede componer de alarmas y alertas en tiempo real, análisis gráficos y reportes de actividad.

Elementos de *hardware* y *software*. Repartidos entre los diferentes componentes de la red de computadoras y de transmisión de datos.

Por otro lado, los elementos de dicho sistema se clasifican en dos grandes grupos:

Gestores. Recursos que interaccionan con los operadores humanos y desencadenan acciones necesarias para llevar a cabo las tareas por ellos invocadas.

Agentes. Componentes invocados por el gestor o gestores de la red.

Por lo regular, los agentes mantienen en cada nodo gestionado información acerca del estado y las características de funcionamiento de un determinado recurso de la red. El gestor pide al agente, a través de un protocolo de gestión de red, que realice determinadas operaciones con base en los datos proporcionados, gracias a los cuales podrá conocer el estado del recurso e influir en su comportamiento. Cuando se produce alguna

situación anómala en un recurso gestionado, los agentes, sin necesidad de ser invocados, emiten los denominados eventos o notificaciones que son enviados a un gestor para que el sistema pueda actuar en consecuencia (figura 2.1).

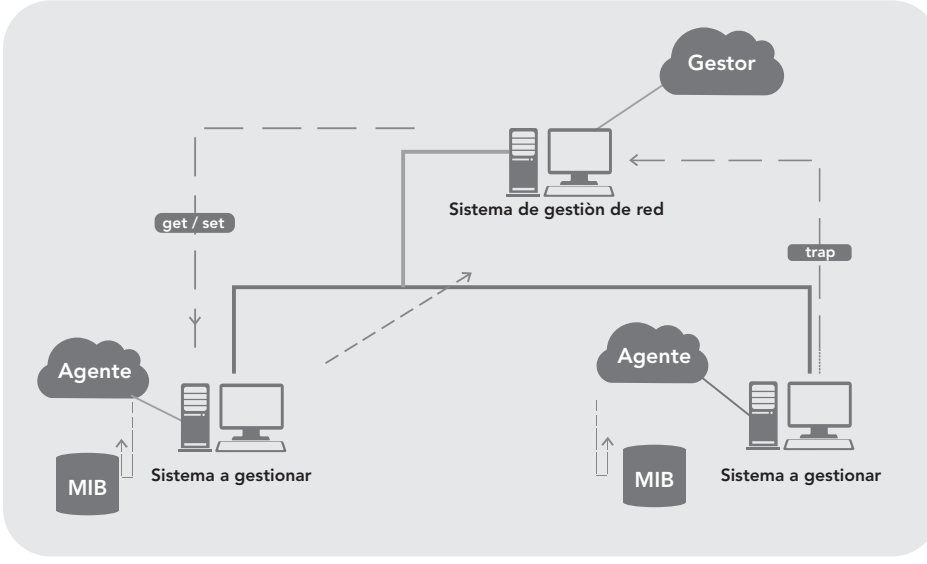


Figura 2.1 El paradigma gestor-agente

Existen distintos protocolos de gestión de red, dentro de los cuales destaca SNMP. Como se describió en el capítulo 1, es el protocolo idóneo para utilizarse en redes empresariales porque todos los equipos lo soportan, de forma que es considerado el estándar de facto. Otro protocolo estándar, es el CMIP (*Common Management Information Protocol*), de la familia de protocolos OSI (*Open Systems Interconnection*) de la ISO (*International Organization for Standarization*), que si bien no está implantado en la organización, sí está presente en la mayoría de los operadores de los servicios de telecomunicación para la gestión de redes.

Existe también la posibilidad de configurar la administración de la red con las herramientas que se tienen a disposición para controlar diversas actividades; por ejemplo, para redes con pocas terminales se quiere controlar cuando los dispositivos de conmutación fallan, están fuera de servicio por mantenimiento y cuando hay errores en las líneas de comunicación u otro *hardware*; en cuanto a esto, es posible configurar SGMP y SNMP para que usen *traps* (mensajes no solicitados) para un *host* en particular o para una lista de estos cuando ocurre un evento crítico (por ejemplo, líneas activas o desactivas); no obstante, no es realista esperar que un dispositivo de conmutación notifique cuando falla incluso cabe la probabilidad de que dichos *traps* se pierdan por un error en la red o por sobrecarga, así que no se puede depender por completo de ellos, aunque es conveniente que los dispositivos de conmutación reúnan regularmente este tipo de información.

Existen varias herramientas que visualizan un mapa de la red donde los objetos cambian de color cuando modifican su estado; y hay cuadros que muestran estadísticas sobre los datagramas y otros objetos. Otro tipo de monitorización deseable es recolectar infor-

mación para hacer reportes periódicos del porcentaje de uso de la red y prestaciones; para ello, se necesita analizar cada dispositivo de conmutación y quedarse con las cifras de interés. Un ejemplo se genera en la Universidad de Rutgers, en la cual cada hora se hace dicho procedimiento para la obtención de datos del número de datagramas reenviados a Internet u otra red, además de errores varios.

Sería posible que cualquier tipo de conmutador pudiese usar la técnica de monitorización deseada; sin embargo, por lo general los repetidores no proporcionan ningún tipo de estadística, debido a que no tienen un procesador para abaratar el precio.

Por otro lado, es posible usar un *software* de administración de redes con repetidores incluyendo *buffer*[1], *bridges* y *gateways*. Para estos últimos, en la mayoría de los casos, se pueden manejar direcciones IP y los protocolos de monitorización mencionados. Por su parte, casi todos los *bridges* tienen medios para recoger algunos datos de prestaciones; además, puesto que no están dirigidos a ningún protocolo en particular, la mayor parte de ellos no tiene el *software* necesario para implementar los protocolos TCP/IP de administración de redes.

En algunas ocasiones, el monitoreo puede hacerse tecleando algunos comandos a una consola directamente conectada; en las restantes, es posible recoger datos a través de la red, pero el protocolo requerido no se basa en algún estándar.

Dejando de lado algunas pequeñas redes, se debe insistir en que cualquier dispositivo conmutador más complejo que un simple repetidor es capaz de recolectar estadísticas de forma remota. Aquellas partes de la red que no soporten dicha operación pueden monitorizarse mediante *pinging* (aunque éste sólo detecta errores graves y no permite examinar el nivel de ruido de una línea en serie y otros datos necesarios para llevar a cabo un mantenimiento de alta calidad). Se espera que la mayoría del *software* disponible cumpla los protocolos SGMP/SNMP y CMIS (Terán Pérez, 2010).

[1] Un *buffer* es un canal de retención temporal de información.

2.3 Modelo de gestión ISO

La tarea del administrador de una red empresarial será evaluar la plataforma de gestión a utilizar con la finalidad de que ésta resuelva las problemáticas en cada una de las cinco áreas funcionales en las que el modelo de gestión ISO clasifica las tareas de los sistemas (Terán Pérez, 2010); las cuales se presentan a continuación:

- **Gestión de configuración.** El objetivo es obtener datos de la red y utilizarlos para incorporar, mantener y retirar los distintos componentes y recursos a integrar. Consiste en la realización de tres tareas fundamentales: recolección automatizada de datos sobre el inventario y estado de la red como versiones de *software* y *hardware* de los distintos componentes; cambio en la configuración de los recursos y almacenamiento de los datos de configuración.
- **Gestión de rendimiento.** Tiene como objetivo principal el mantenimiento del nivel de servicio que la red ofrece a sus usuarios, asegurándose de que está operando de manera eficiente en todo momento. Ésta se basa en cuatro tareas:
  - Recolección de datos o variables indicadoras de rendimiento como el *troughput* de la red, los tiempos de respuesta o latencia, la utilización de la línea, etcétera.
  - Análisis de la información para determinar los estándares normales de productividad.
  - Establecimiento de umbrales como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.
  - Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos para un análisis continuo.

  Gestión de contabilidad. La misión es medir los parámetros de utilización de la red que permitan al prestador de servicios preparar las correspondientes facturas a los clientes. Entre las tareas que se deben realizar en esta área están:
  - Recolección de datos sobre el uso de los recursos.
  - Establecimiento de cuotas.
  - Cobro a los usuarios con las tarifas derivadas del empleo de los recursos.

  Gestión de fallas. Tiene por objetivo la localización y recuperación de los problemas de la red; esto implica las siguientes tareas:
  - Determinación de los síntomas del problema.
  - Aislamiento y resolución de la falla.
  - Comprobación de la validez de la solución en todos los subsistemas importantes de la red.
  - Almacenamiento de la detección y resolución del problema.

  Gestión de seguridad. La tarea es ofrecer mecanismos que faciliten el mantenimiento de políticas de seguridad (orientadas a la protección contra ataques de intrusos). Entre sus funciones están:

- Identificación de recursos sensibles en la red como ficheros o dispositivos de comunicaciones y sus relaciones con los grupos de usuarios.
- Monitorización de los puntos de acceso a los recursos sensibles de la red.
- Almacenamiento de los intentos de acceso no autorizados para su posterior análisis.

Como objetivo final de la gestión de red está garantizar cierto nivel de servicio en los sistemas de una organización el máximo tiempo posible, minimizando la pérdida que ocasionaría una caída o el funcionamiento incorrecto del sistema. Los elementos que son objeto de control en este caso son los equipos conectados: los servidores, las terminales, las computadoras personales, las estaciones de trabajo; así como los elementos y equipos de interconexión tales como cables, concentradores, *bridges*, *gateways*, *routers*, etc.

2.4 Plataformas de gestión de una red de computadoras

La gestión de redes surgió con las redes mismas, puesto que siempre hubo necesidad de controlar, seleccionar y configurar sus recursos de interconexión. Ahora bien, al igual que las redes han ido cambiando, los sistemas de gestión han evolucionado con el paso del tiempo. Se pueden distinguir tres etapas fundamentales en el desarrollo de estos:

Gestión autónoma. Las primeras redes tenían pocos nodos y cada uno de ellos poseía su propio sistema de gestión local. Las decisiones que afectaban a más de un nodo implicaban la comunicación con cada uno de los administradores correspondientes.

Gestión homogénea. Es una etapa posterior, las redes sufrieron un aumento considerable en el tamaño, pero siempre utilizando equipos y protocolos de un mismo fabricante, el cual aportaba su propio sistema de gestión que, en la mayoría de las ocasiones, estaba centralizado en un nodo único.

Gestión heterogénea. Más tarde, las redes han ido creciendo y evolucionando mediante la incorporación de una amplia variedad de tecnológicas. Ya no se puede hablar de entornos homogéneos, sino que en una misma red se encuentran componentes de una gran amalgama de fabricantes que tienen que inter-operar entre sí. De esta forma, se ha conseguido aumentar los servicios ofrecidos por la redes, a la vez de que los usuarios de éstas han podido maximizar el rendimiento de sus inversiones; tras lo que ha surgido la necesidad de que coexistan sistemas de gestión de red de muy diversa naturaleza, sin embargo, esto plantea una serie de problemas desde varios puntos de vista:

- Del usuario: la necesidad de que las personas encargadas de la administración de la red conozcan perfectamente todos y cada uno de los sistemas que se deben utilizar.
- De integración de sistemas: debe garantizarse la incompatibilidad entre los datos de gestión, los procedimientos y los protocolos de comunicación con funcionalidad similar. También es necesario que se conozca la duplicidad y posible inconsistencia de la información almacenada en las bases de datos.

Como respuesta a estas situaciones, se han definido los modelos de gestión integrada, que permiten, teóricamente, la interconexión de una manera abierta de los recursos de telecomunicación y las aplicaciones de gestión de la red. De esta forma, se podrá evolucionar a modelos capaces de administrar redes heterogéneas. Para llegar a esta integración es necesario tener en cuenta lo siguiente:

Normalizar las comunicaciones. Entre los diferentes componentes del sistema de gestión queda claro que si uno de estos quiere controlar un *router* es necesario que sepa entender las preguntas que se le hagan con independencia del tipo de cada uno.

Normalizar la información. Este aspecto es una de las claves de los modelos de gestión de red, que la diferencian de otras aplicaciones de comunicación. El objetivo es conseguir una definición sintácticamente uniforme de todos los elementos de la red con independencia del fabricante.

Lo anterior plantea un gran trabajo, pues es necesario realizar una definición de las propiedades de gestión de todos los recursos de comunicación existentes, lo que será una tarea más en el diseño de nuevos recursos de comunicaciones; sin embargo, el mercado de las herramientas de control y supervisión de las redes se caracteriza por la presencia de tres plataformas que se reparten el mercado: *Open View* de Hewlett Packard, *Sun Net* de Sun Microsystems y *Net View* de IBM; a éstas se aúnan otras como *Spectrum Enterprise* de Cabletron Systems, *Optitivity* de Bay Networks o *Transcend* de 3Com.

Todas estas herramientas se encargan de la recepción de informes y datos mediante el sondeo automático o iniciado por el usuario a diferentes dispositivos de la red como computadoras, concentradores, encaminadores, conmutadores, etc. En el caso de reconocer algún problema en dichos parámetros, las entidades de gestión notificarán al operador, almacenarán los eventos e intentarán reparar el sistema de manera automática. Sobre todas ellas, es posible también montar aplicaciones adaptadas a cada uno de los dispositivos SNMP de la red, solucionando así el problema de gestión de redes heterogéneas.

La tecnología web como forma de acceso fácil, barata, estándar e integrada a la información de gestión de red constituye una de las tendencias de futuro más prometedoras en el mercado de plataformas de este tipo (World Wide Web, 2009). Por medio de un navegador frontal es posible leer informes y reiniciar aspectos importantes del funcionamiento de los equipos de una red empresarial que se pueden convertir en HTML sin demasiada dificultad. Este formato permite a los desarrolladores aprovechar la gran disponibilidad y bajo costo de los navegadores en cualquier tipo de computadora para confiarles las pesadas tareas de desarrollo de *software* de clientes. Por otro lado, el navegador está tan extendido que facilita la integración de paquetes de *software* a la configuración orientada al *hardware* y a programas de supervisión que se adjuntan a muchos equipos.

A pesar de la condición de fragilidad relativa de los tipos de gestiones de redes observadas, es posible identificar en éstas núcleos potenciales para su desarrollo, los cuales se refieren a estructuras al interior de ellas donde se encuentra un subgrupo de actores que cumplen con un grado mínimo de cohesión entre sí; esto consiste en contar con al menos dos vínculos: que partan desde el actor o sean recibidos por él, o uno recibido y el otro dado; sin embargo, cabe resaltar que el tipo de núcleos identificados obedecen a aquellos con el menor grado de cohesión posible, lo cual sigue corroborando la tendencia a un grado de conectividad bajo en estas redes.

Se halló el núcleo en cada una de las redes aplicando el método de suprimir de forma progresiva los actores y los vínculos más periféricos hasta encontrar estructuras que no son susceptibles de ser reducidas. En un sentido metafórico, estos son el corazón de ellas, subgrupos con potencialidad relevante para estructurar al resto del conjunto en tanto que conforman configuraciones irreductibles. En tanto, el núcleo de la red, al igual que ésta en su globalidad, es inconexo.

2.4.1 OpenView

Como se mencionó, la plataforma es una de las principales en el ámbito de la gestión de redes y está disponible para Windows y varios tipos de sistemas Unix (figura 2.2). Se trata de un completo conjunto de productos con tres módulos principales:

> ***Network Node Manager.*** Herramienta que se encarga de descubrir la topología de la red, manejar las alarmas procedentes de los distintos dispositivos y conectar cualquier otra plataforma de gestión al mapa de red.

Operations Center. Constituye la interfaz de usuario gestionando funciones como impresoras, copias de seguridad de servidores, etcétera.

Center Administration. Se encarga de ajustar configuraciones de puestos de trabajo, servidores, etcétera.

El problema de Center Administration es que debido a la presencia de parámetros específicos del fabricante del dispositivo en cuestión no es realmente útil para su configuración, pues se obtienen mejores resultados utilizando las aplicaciones de cada fabricante sobre el *Network Node Manager*; por ello, en la práctica, la gestión de configuración no se realiza con dicho módulo.

Lo mismo ocurre con la administración de prestaciones y contabilidad, donde de nuevo se recurre a aplicaciones específicas del fabricante de los equipos sobre *Network Node Manager*. Otra de las limitaciones de OpenView está en la dirección de fallas por la inexistencia de un paquete estándar de HP que realice la correlación de estos, que procederán de distintos dispositivos de red con diferentes caracterizaciones. Por último, el control de la seguridad, en entornos de una Intranet, se ha de implementar por medio de cortafuegos a nivel de aplicación, que tampoco se inclyen en OpenView.

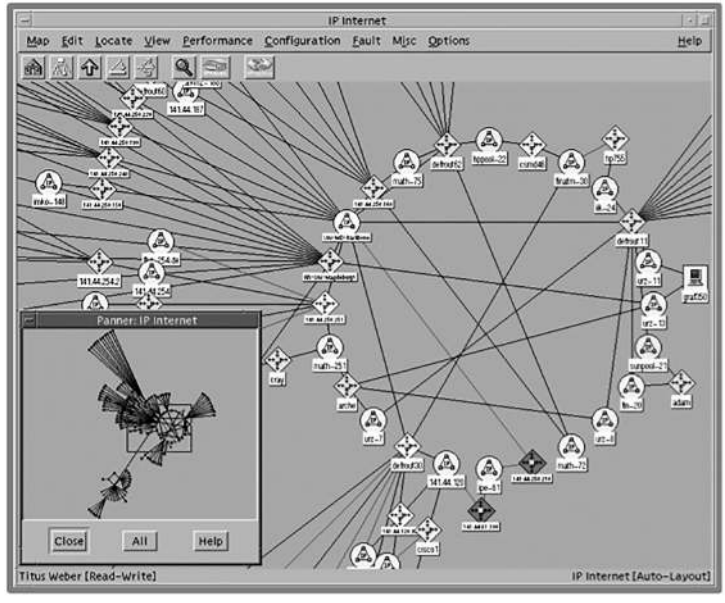


Figura 2.2 Ejemplo de HP OpenView

2.5 Aplicaciones de la gestión de redes convergentes

Las redes convergentes, o redes de multiservicio hacen referencia a la integración de los servicios de voz, datos y video sobre una sola red basada en IP como protocolo de nivel de red (Technical Guides, 2001b). Tradicionalmente, estos servicios se han ofrecido en forma separada sobre redes especializadas. En la gran mayoría de organizaciones; por ejemplo, la red de voz se basa en uno o varios PBX (*Private Branch eXchange*) conectados a la PSTN (*Public Switched Telephone Network*) externa; mientras que la red de datos se basa en conmutadores y enrutadores IP (*Internet Protocol*) interconectando redes LAN (*Local Area Network*) y permitiendo el acceso a Internet.

Sin embargo, cada vez es mayor la necesidad de una red única en la que tanto la voz como los datos y el video converjan de modo natural y permitan además, reducir los costos de administración, de mantenimiento y manejo de la información; así como aumentar la productividad y disminuir los tiempos de atención a los clientes (Cisco Systems, 2001; Alzate, 1995; Technical Guides, 2001b). Aunque en la década de los años 80, se consideró la posibilidad de integrar la red sobre el PBX y acceder a la ISDN, una característica fundamental de las redes de convergencia actuales (y futuras) es que los diferentes tipos de tráfico se soportan mediante protocolos basados en el concepto de conmutación de paquetes.

Por supuesto, ATM y *Frame Relay* son opciones importantes para considerar como fundamento de las redes de convergencia, pero dada la actual y creciente ubicuidad de Internet y las modificaciones que la IETF introduce en las nuevas versiones de IP para atender el tráfico en tiempo real con una adecuada calidad de servicio, y la conmutación de etiquetas en MPLS, el protocolo dominante en el desarrollo actual de las redes de convergencia es IP (Alzate, 1995; Technical Guides, 2001a). En efecto, la aplicación del protocolo IP para la transmisión integrada de voz y de datos, es un concepto que ha revolucionado la industria de las telecomunicaciones, elevando la posición de Internet a un plano de competencia comercial. En la actualidad, sobre Internet, ya se pueden ofrecer servicios de transmisión de voz, a precios muy inferiores a los tradicionales, gracias al desarrollo de aplicaciones de tiempo real sobre IP. De hecho, se registró en 2016 más de 80% de las líneas telefónicas comerciales contratadas en los Estados Unidos de América como líneas IP (Technical Guides, 2001b).

Por supuesto, las redes de convergencia han tenido aún dificultades técnicas que superar ya que los distintos servicios por ofrecer tienen diferentes características y requerimientos de red. Por ejemplo, los datos se presentan en ráfagas que consumen grandes volúmenes de ancho de banda durante cortos intervalos de tiempo; mientras que el tráfico de voz requiere un ancho de banda constante y un bajo retardo de transmisión. Estas demandas del tráfico de voz han sido satisfechas mediante conmutación de circuitos basada en Multiplexaje por División de Tiempo (TDM); mientras que el tráfico de datos ha sido satisfecho por las redes de conmutación de paquetes.

Sin embargo, la existencia de dos redes independientes, implica procesos de mantenimiento y administración también individuales con el correspondiente incremento en costos y la dificultad para dar respuesta oportuna a los requerimientos de servicio de los clientes (Alzate, 1995; Technical Guides, 2001b). Por otra parte, el tráfico de datos no sólo ya es mayor al tráfico de voz, sino que el primero crece de forma exponencial; mientras que el segundo lo hace linealmente. Esta situación contrasta con el hecho de que las

principales ganancias económicas de las empresas de telecomunicaciones provienen en su gran mayoría del tráfico de voz generando un interés especial en la integración de voz sobre la infraestructura ya existente, lo cual permitirá mejores servicios a sus clientes y mayores ingresos para las empresas (Technical Guides, 2001b). Así pues, desde la perspectiva de los proveedores de servicios de comunicación, es de fundamental importancia introducir nuevos servicios en respuesta a las necesidades de sus clientes para adquirir y mantener una porción del mercado. Y desde la perspectiva de los fabricantes de equipos, esta condición les exige la rápida innovación de los equipos y sistemas. Es en estas condiciones donde las redes de convergencia basadas en IP adquieren su importancia.

A diferencia de los modelos de servicios integrados con anterioridad, las redes de convergencia basadas en IP permiten aprovechar las habilidades de los desarrolladores de aplicaciones de Internet en la innovación y desarrollo de nuevos productos, reduciendo de modo significativo el tiempo de introducción al mercado. Más aún, como los fabricantes no pueden construir todas sus soluciones "*desde cero*", deben recurrir a la terciarización (*Outsourcing*), y para que esta sea efectiva, las soluciones deben basarse en estándares abiertos, de manera que los diferentes equipos y redes puedan inter-operar de manera totalmente compatible (Braden, *et al.*, 1997; Iovana, 2003). Dichas condiciones no sólo se presentan en redes alambradas, sino también en las redes móviles inalámbricas, donde el advenimiento de la última generación, implica la transición de la conmutación de circuitos a la conmutación de paquetes para convergencia de servicios. Y en este esfuerzo, también se conduce al uso de voz (y video) "paquetizada", y a la aplicación de IP a través de toda la red (Iovana, 2003).

2.5.1 La gestión y tecnología en redes

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN, *Local Area Network*) como forma de normalizar las relaciones entre las máquinas que se utilizan como sistemas ofimáticos (Terán Pérez, 2010). Esto, como su propio nombre lo indica, constituye una manera de interconectar una serie de equipos informáticos.

Por su parte, una LAN no es más que un medio compartido al que se conectan todas las computadoras con sus equipos periféricos por medio de un cable UTP o una fibra óptica; que cuenta con una serie de reglas que rigen el acceso.

La LAN más difundida es la Ethernet, que utiliza un mecanismo denominado *Call Sense Multiple Access-Collision Detect* (CSMS-CD), lo cual significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro lo use. Si hay algún conflicto, el equipo que está intentando establecer la conexión se anula y efectúa un nuevo intento más adelante.

La Ethernet transfiere datos a 10 Mbits/s, lo suficientemente rápido para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente entre ellos.

En Ethernet y CSMA-CD hay topologías muy diversas (*bus*, estrella, anillo, etc.), y diferentes protocolos de acceso. A pesar de esto, todas las LAN comparten la característica de poseer un alcance limitado (por lo regular, abarcan un edificio) y tener la velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan. Además, las LAN modernas también proporcionan al usuario una gran multitud de funciones avanzadas.

Es importante considerar que existen paquetes de *software* de gestión para controlar la configuración de los equipos en la LAN, los usuarios y los recursos de la red; estos, por lo general, proporcionan servicios como control de impresión, ficheros compartidos y correo a usuarios sobre computadoras personales. En la actualidad, dado que la gestión de red se encuentra en un estado de madurez suficiente y es utilizada en la mayoría de entornos de red, está surgiendo la necesidad de expandir sus tecnologías a otros campos como servicios, aplicaciones y sistemas, existiendo múltiples productos en el mercado que proporcionan soluciones en dichos ámbitos. Sin embargo, hay aspectos los cuales no es posible una usanza directa de la tecnología tradicional de gestión de red. Un ejemplo es la gestión de herramientas basadas en plataformas de procesamiento distribuido como OMG-CORBA, COM/DCOM y Java-RMI, en las que no es aplicable el tradicional paradigma gestor–agente, porque su funcionalidad se encuentra repartida en diversas infraestructuras.

La gestión y operación de red es en la actualidad una actividad fundamental en el negocio de las telecomunicaciones, que permite proporcionar servicios finales con una calidad determinada y optimizar el rendimiento de las infraestructuras. Una posible definición es el conjunto de procesos y acciones que realiza un operador o proveedor de telecomunicaciones para prestar sus servicios, de forma que se cumplan tanto los criterios de calidad y costo establecidos en los objetivos de la empresa como los reflejados en los correspondientes contratos con los clientes.

Además, y fruto de la competencia en las telecomunicaciones desde finales de los años 90, la gestión y la operación de la red ha pasado de ocuparse casi en exclusiva de aspectos ligados al propio funcionamiento para evolucionar a un modelo donde el eje de actividad es la atención al cliente. Para ello, es necesario coordinar e integrar a todos los posibles agentes que intervienen en la prestación de un servicio, lo que implica la condensación de diferentes sistemas de gestión para mejorar la calidad y optimizar costos.

2.6 Modelos de gestión de redes de computadoras y sus servicios

Desde un punto de vista histórico, la situación en las décadas de los años 80 y 90 se caracterizaba por el hecho de que cada suministrador utilizaba una interfaz propietaria entre los elementos de red y los sistemas de gestión; de este modo, la implementación se convertía en una tarea compleja que sólo el suministrador podía desarrollar con garantías. Estas dificultades llevaron a crear diferentes grupos de trabajo en los organismos de estandarización con el objetivo de definir las interfaces de gestión que debían incorporar los elementos de red para así facilitar la conexión de equipos de los distintos fabricantes. El fruto de este proceso, nacieron los dos principales modelos de gestión que en la actualidad se utilizan: *Telecommunication Management Network* (TMN) y *Simple Network Management Protocol* (SNMP), este último descrito forma ampliamente en el capítulo 1.

Modelo TMN. Se creó para garantizar la interoperabilidad y la verdadera comunicación entre redes y sistemas de telecomunicaciones heterogéneos, considera la conexión de sistemas desde tres aspectos:

- Funcional: define las actividades que se deben realizar y la organización de las mismas.
- De información: modela la información de gestión que se intercambia entre los diferentes sistemas interconectados.
- De comunicación: especifica los protocolos de comunicaciones utilizados para el intercambio de información entre sistemas.

El modelo TMN no se utiliza por lo regular en redes de conmutación de paquetes, siendo más apto para los sistemas de conmutación de circuitos como GSM.

Modelo SNMP. El SNMP es el protocolo de comunicaciones más utilizado para la gestión de redes IP; éste forma parte de las especificaciones del protocolo IP diseñado por el *Internet Engineering Task Force* (IETF).

SNMP parte de una estación de gestión que sirve de interfaz para los operadores humanos y que incluye un conjunto de aplicaciones de gestión, y se comunica con uno o varios agentes encargados de responder a las peticiones de información o ejecución de acciones sobre los recursos provenientes de la estación de gestión; en este proceso SNMP se basa en el protocolo mediante el cual los actores implicados (gestores y agentes) intercambian información.

Quedan fuera de los estándares SNMP aspectos como la definición de las propias aplicaciones de gestión, el mecanismo concreto utilizado en el diálogo del agente con los recursos a los que representa, los detalles de implantación, etc.

2.6.1 Modelo funcional OSI-NM

En la arquitectura de administración OSI, para cada una de las SMFA (*System Management Funtional Area*), se han definido cierto número de funciones de administración generales (SMF, *Systems Management Functions*), buscando especificar o detallar mejor cada área de administración FCAPS (*Fault, Configuration, Accounting, Performance, Security*). La definición de un SMF implica la especificación de las MO (*Management Object*) relacionadas.

Cierta SMF puede soportar requerimientos para una o más de las SMFA; un ejemplo es la función de administración de reporte de eventos. Cada una provee un mapeo sobre CMIS (*Content Management Interoperability Services*) y una aplicación de administración puede hacer uso de las SMF como funciones predefinidas genéricas (Day, 1995); las cuales son tan complejas que, para flexibilidad y reúso, se definen de forma general. Los modelos para funciones específicas son utilizados para definir las tareas y la información de administración asociada como clases de objetos de soporte como se muestra en la figura 2.3.

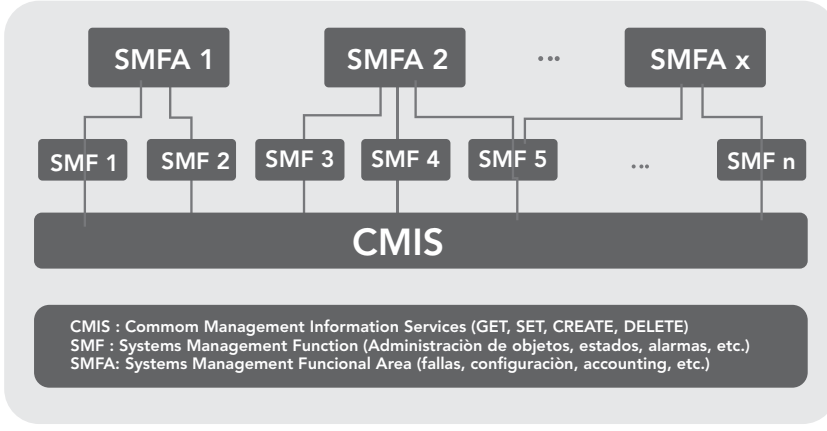


Figura 2.3 Arquitectura OSI-NM

Las funciones especificadas por la administración de sistemas OSI (ISO 10 164-n) incluye la siguiente lista, en la cual "n" corresponde al número en el documento OSI:

Object Management Function. Esta función provee un esquema uniforme que resume un número de notificaciones predefinidas para la creación de reportes y borrado de MO, así como cambios a los atributos.

State Management Function. Provee las operaciones generales para administrar el estado de las MO. Implica establecer un modelo general de estados y definir un conjunto de aquéllas para controlar y monitorear las transiciones de estado.

Attributes for Representing Relationships. Brinda soporte al establecimiento y a la manipulación entre MO utilizando características como "operado por", "reemplazado por", "primario/secundario". Se tiene una plantilla para describir los roles y las propiedades de MO relacionados.

Alarm Reporting Function. Clasificación general de alarmas (es decir, eventos especiales) de acuerdo con el tipo de causa (*Communications Alarm, Quality of Service Alarm*) y del problema específico (*Communicaction Protocol Error, I/O Device Error*).

Event Report Management Function. La función que especifica las condiciones viables a ser satisfechas por reportes de eventos, los cuales serán enviados a destinos específicos.

Log Control Function. Proporciona las operaciones para recopilar y archivar las notificaciones generadas por los MO en bitácoras. Se define un modelo genérico para éstas y su manejo.

Security Alarm Reporting Function. Es una función análoga al reporte de alarmas que relaciona específicamente aquello que tiene que ver con la administración de seguridad.

Security Audit Trail Function. Refinamiento de la función de control de logs en la cual los requerimientos relacionados con el archivado y recopilación de notificaciones y operaciones relevantes a la seguridad son realizadas a través de la generación de reportes especiales.

Objects and Attributes for Surface Control. Una definición de las operaciones para introducir y manipular las reglas de control de acceso asegura que los MO sean protegidos de acciones de administración externa no autorizada. Cuando se realizan solicitudes de información de administración no autorizadas debe existir la manera de reportar dicho evento. Esto también aplica para el intento de establecer conexiones de comunicaciones para administración no autorizadas. La función de decisión de control de acceso (ADF, *Access Decision Facility*) permite la formulación de diferentes políticas de seguridad. Sobre esta base, la función de ejecución del control de acceso (AEF, *Access Enforcement Facility*), que puede configurarse entre el iniciador y el objetivo de una función de administración, asegura que las políticas de seguridad sean ejecutadas.

Usage Metering Function for Accounting Purpose. La definición de un esquema de descripción uniforme para los datos de contabilidad de uso de recursos y la especificación de la funcionalidad requerida para recopilarlos aseguran que un eficiente y efectivo intercambio de información de contabilidad sea soportado.

Metric Objects and Attributes. Un modelo genérico para el monitoreo de umbrales proporciona la funcionalidad para una revisión continua de atributos dinámicos y la activación de alarmas cuando los umbrales seleccionados son excedidos.

Test Management Function. Una taxonomía general para pruebas es utilizada para proveer operaciones de inicio y finalización de pruebas y los formatos de intercambio para transmitir los resultados de éstas. Las clases de objetos administrados como *Test Perfomer, Test Conductor, Test Objects y Uncontrolled Tests* son presentados como parte de este SMF. Las definiciones más utilizadas son aquellas de las pruebas de conformidad.

Summarization Function. Permite que los datos dentro de un agente sean reprocesados y reducidos aun antes de ser enviados al sistema de administración; además, proporciona los algoritmos estadísticos para calcular promedios y desviaciones estándar.

Confidence and Diagnostics Test Categories. La taxonomía presentada para la administración de pruebas, se refina a través de categorías concretas que soportan exámenes sobre la disponibilidad y desempeño funcional de los elementos; por ejemplo: recursos internos, conectividad, integridad de datos, protocolos, etcétera.

Scheduling Function. Soporta el control de tiempo de operaciones de administración sobre la base de periodos seleccionables. En particular, permite que cualquier operación sea iniciada o terminada diaria, semanal o mensual de forma recurrente.

Management Knowledge Management Function. Posibilita a un sistema consultar a otro sobre cuáles son las capacidades que soporta relacionadas con la administración. Incluye MOC soportadas; MIT, relaciones entre MO; así como esquemas de nombres, dominios, políticas y usuarios.

Changeover Function. Comunica relaciones y roles entre MO que permiten redundancia y recuperación de fallas de manera automática.

Software Management Function. Modela la activación y la desactivación de *software* al igual que los aspectos interactivos de la descarga de éste.

Management Domains and Management Policy Management Function. Establece y administra dominios, también asigna políticas que deben implementarse.

Time Management Function. Define un servicio genérico utilizando mecanismos de sincronización de tiempo con propósitos de administración.

Command Sequencer. Utiliza un lenguaje de *scripting* para la ejecución de funciones de gestión. Puede mejorar la forma en que la funcionalidad de la administración es elaborada para un agente, permitiéndole la delegación dinámica a través de *scripts* antes que una implementación estática.

Response Time Monitoring Function. Mide retardos de ida y vuelta (*Round-Trip Delay*) de los PDU para una conexión punto a punto o *multicast* predeterminada sobre la base de diferentes procedimientos de evaluación.

En conexión con la definición de las SMF, un amplio rango de especificaciones genéricas para clases de objetos administrables (MOC para soporte y control) fueron estandarizadas para describir objetos para los *log*, *test*, control, estadísticas, procedimientos de medida de desempeño y contabilidad.

El modelo funcional se expande de manera continua permitiendo que la funcionalidad de la administración sea más formalizada para ser definida genéricamente, posibilitando el reúso como módulos de aplicación dentro de las soluciones de administración.

Otro aspecto importante es que en la actualidad, se desarrollan lenguajes de administración por delegación: dependiendo de la disponibilidad y la necesidad, podrían ser utilizados para asignar dinámicamente cierta funcionalidad a componentes individuales del sistema distribuido (Day y Zimmermann, 1983).

2.7 Los objetivos de las redes en el mercado y su importancia en las empresas

Las redes, en general, consisten en "compartir recursos", como el primero de los principales objetivos que todos los programas, los datos y el equipo se encuentren disponibles para cualquiera que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que un usuario cualquiera se encuentre a 1000 km de distancia de los datos, no debe evitar que éste los pueda utilizar como si fueran originados de manera local.

Un segundo objetivo consiste en proporcionar una alta fiabilidad al contar con fuentes alternativas de suministro (Tanenbaum y Van Steen, 2007). Por ejemplo, todos los archivos podrán duplicarse en dos o tres máquinas, de manera que si una de ellas no se encuentra disponible, pueda utilizarse una de las otras copias. Además, la presencia de múltiples procesadores significa que si una de ellas deja de funcionar, las otras son capaces de encargarse del trabajo, aunque se tenga un rendimiento global menor.

Por último, se busca el ahorro económico: las computadoras pequeñas tienen una mejor relación costo/rendimiento comparada con la ofrecida por las máquinas grandes. Éstas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas los construyan constituidos por poderosas computadoras personales (una por usuario) con los datos guardados en una o más máquinas que funcionan como servidor de archivo compartido.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual, a medida que crece la carga, sea posible añadir más procesadores. Con máquinas grandes, cuando el sistema está lleno deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Existen además otros motivos para instalar redes:

Disponibilidad. Es esencial disponer de un *software* multiusuario de calidad que se ajuste a las necesidades de la empresa; por ejemplo, se puede diseñar un sistema de puntos de venta ligado a una red local concreta. El *software* de redes puede bajar los costos si se necesitan muchas copias de éste.

Trabajo en común. Conectar un conjunto de computadoras personales formando una red que permita que un grupo o equipo involucrados en proyectos similares puedan comunicarse fácilmente y compartir programas o archivos.

Actualización del *software*. Si el *software* se almacena de forma centralizada en un servidor, es más fácil actualizarlo, pues el administrador tendrá que renovar la única copia almacenada en el servidor.

Copia de seguridad. Las copias de seguridad son más simples porque los datos están centralizados.

Control de los datos. Como los datos se hallan concentrados en el servidor, resulta mucho más fácil controlarlos y recuperarlos. Los usuarios pueden transferir sus archivos vía red antes que usar dispositivos de almacenamiento externo.

Uso compartido. Algunos periféricos de calidad de alto costo pueden ser compartidos por los integrantes de la red como impresoras láser de alta calidad.

Correo electrónico. El correo electrónico permite que los usuarios se comuniquen más fácilmente entre sí. A cada usuario se le puede asignar un buzón de correo en el servidor para que se le dejen mensajes que leerá cuando los vea en la red.

Ampliación del uso con terminales "tontas". Una vez montada la red local, pasa a ser más barato el automatizar el trabajo de más trabajadores por medio del uso de terminales "tontas" (máquina sin disco duro) conectadas a la red. En la actualidad, el uso de éstas es limitado por la funcionalidad.

Seguridad. La seguridad de los datos puede conseguirse por medio de los servidores que posean métodos de control, tanto de *software* como de *hardware*. Las terminales "tontas" impiden que los usuarios puedan extraer copias de datos para llevárselos fuera del edificio.

2.7.1 Aplicación de las redes en la actualidad

El reemplazo de una máquina grande por estaciones de trabajo sobre una LAN no ofrece la posibilidad de introducir muchas aplicaciones nuevas, aunque podría mejorarse la confiabilidad y el rendimiento (Stallings, 2010). Sin embargo, la disponibilidad de una WAN, sí genera nuevas aplicaciones viables y algunas de ellas pueden ocasionar importantes efectos en la totalidad de la sociedad. Por ejemplo, una organización que ha producido un modelo que simula la economía mundial, puede permitir que sus clientes se conecten usando la red y corran el programa para ver cómo es posible que las diferentes proyecciones de inflación, tasas de interés y fluctuaciones de los tipos de cambio afecten sus negocios. Con frecuencia, se prefiere este planteamiento que vender los derechos del programa, en especial si el modelo se ajusta de modo constante o necesita una máquina de gran capacidad para correrlo; además, el llamar a una computadora remota mediante una red resulta más económico que hacerlo manera directa (Terán Pérez, 2010). La posibilidad de tener un precio más bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red hace que sólo se ocupen los enlaces de larga distancia cuando se transmiten los datos.

2.7.2 Aplicación de las redes al trabajo

La forma en que las redes son usadas ha cambiado y beneficiado la forma de trabajo, alcanzando a los académicos e investigadores, pues el antiguo modelo de una gran computadora, centralizada, es cosa del pasado. Ahora, la mayoría de las instalaciones tienen diferentes tipos de computadoras: desde personales y estaciones de trabajo, hasta súper computadoras; cualquiera de éstas, por lo general, se encuentran configuradas para realizar tareas particulares llamando a otros sistemas en la red para servicios especializados. Esto ha dado origen al modelo de servicios de red cliente-servidor, los cuales no se ubican necesariamente en distintas computadoras porque podrían usar diferentes programas en la misma computadora.

El trabajo a distancia entre instituciones y personas muy diversas ha recibido un gran impulso gracias a la introducción del ya mencionado correo electrónico. Ello está acelerando el ritmo del intercambio al punto que es posible plantearse acciones concretas e investigaciones de todo tipo coordinadas a distancia. Como lo señaló Toffler (2010):

"Lo que ha cambiado en el equilibrio del poder en el mundo moderno es la combinación de nuevas tecnologías de comunicación cada vez más accesibles (computadoras, teléfonos móviles, módems, satélites) que se traducen en auténticas autopistas electrónicas."

Las nuevas tecnologías permiten trabajar sin salir de las casas, así el teletrabajo ha dejado de ser un mito lejano: ocho millones de tele-trabajadores europeos y veinticinco en Estados Unidos de América son los primeros tecnómadas del ciberespacio, los cuales asumen su condición de pioneros sin importar su lugar de residencia, ya que las telecomunicaciones les permiten adquirir el don de la ubicuidad.

La revolución del teletrabajo no ha hecho más que dar inicio. Como muy bien sugiere Ettinghoffer (2013) en su libro *La empresa virtual:* "El hombre contemporáneo entra en el siglo XXI con la perspectiva de ver cómo se modifica su relación con las cosas, el trabajo, la empresa y otros. Está en curso una formidable mutación en nuestra evolución". De hecho, recientes estudios confirman que la computadora modifica el lenguaje de las personas que lo emplean en su actividad productiva: "Delante del monitor, la gente tiende a ser más desinhibida y espontánea" (Sproul, 2012).

No cabe duda de que la autonomía que ofrece esta nueva forma de trabajo podría servir para mejorar las relaciones familiares, ampliar el tiempo libre, cuidar mejor la imagen individual y, sobre todo, mejorar la productividad al racionalizar las ocupaciones. Además, es una forma mucho más ecológica de dedicarse al trabajo cotidiano.

Por su parte, la telemática (telefonía + computación) está produciendo transformaciones profundas en las formas de realizar investigación, debido al proceso de conversión de datos en bruto en información, que posteriormente se convierte en registros interpretativos y, luego, en resultados. Existe potencial en algunos usos de las telecomunicaciones y la teleinformática que puede cambiar en forma radical el modo de hacer investigación en las ciencias sociales, ya que se plantean a distintos niveles y son una consecuencia directa del teletrabajo mencionado porque permitirán que una cantidad importante de investigadores y académicos (en el ámbito educativo), interactúen de manera frecuente unos con otros. Al mismo tiempo, posibilitan que ellos mismos, dispersos y situados en sitios de difícil acceso en la región y a los cuales les está vedado el consumo de información primaria, puedan mantener el contacto con la palabra impresa a costos accesibles (Terán Pérez, 2010). El aspecto más interesante para un proyecto de estas características consiste en la coordinación en tiempo real de una cantidad significativa de investigaciones simultáneas tanto a nivel regional como intercontinental.

Por otro lado, dada la necesidad de alta tecnología en los países latinoamericanos, se presenta una forma de recuperar parte del camino perdido en la repatriación de científicos latinoamericanos residentes en el exterior, aunque los ejemplos conocidos de programas de este tipo han empero fracasado. Una forma alternativa de esta repatriación física es el contacto electrónico permanente con ellos.

Cada día, miles de personas se anotan en la nueva moda de las autopistas de la comunicación: a medida que avanza el tiempo, el estar conectado será una verdadera necesidad; cualquiera que no lo haga quedará en definitiva aislado del mundo, que cada vez se encuentra más interrelacionado y cambia a gran velocidad, pues el modelo clásico de procesamiento de la información (emisor-mensaje-receptor), que ha guiado durante décadas gran parte de la institucionalización y comunicación de los resultados de la investigación, se reformula aceleradamente (Terán Pérez, 2010). Además, el tratamiento de la información (incluyendo el procesamiento visual tan poco atendido en la literatura académica) se aborda desde nuevas perspectivas, teniendo en cuenta conceptos nuevos como "conversación multidireccional" que hasta hace poco no estaban difundidos ni

eran técnicamente factibles. Las posibilidades de acumular y recuperar cantidades importantes de información y compartirla con usuarios a larga distancia permiten imaginar escenarios de "dialogo de alta precisión" que den lugar a nuevas redes de comunicación más rápidas y eficientes.

Con base en lo anterior, y a fin de comprender la complejidad del campo de las redes en la región, se puede clasificar a los países de América Latina y el Caribe, según su nivel de conectividad a Internet, como se muestra a continuación:

Países sin conectividad. Guyana, Surinam, Haití y otros pocos.

Países donde existe una red pública. (Redes con protocolos X-25 de conmutación de paquetes con un costo caro para uso extensivo de la comunidad académica y de investigación) Guatemala, Honduras, El Salvador y la mayoría de los países del Caribe.

Países en los que existe un nivel básico de conectividad. (Existe una o más estaciones conectadas a Internet usando el protocolo de copia de Unix a Unix sobre líneas telefónicas estándar) Bolivia, Paraguay, Uruguay, Nicaragua, Perú, etcétera.

Países con enlaces satelitales dedicados a Internet. Chile, Argentina, Venezuela, Ecuador, Costa Rica, etcétera.

2.7.3 Ejemplo de una aplicación del sistema operativo Android en redes de telefonía móvil

Como forma de brindar respuestas y soluciones en diferentes campos relacionados con Internet y el mundo de la informática, la compañía Google trabaja en el desarrollo de *software* para varias plataformas. Como es el caso de Android (figura 2.4) creado para ofrecer a los usuarios una herramienta eficaz en la telefonía móvil.

Figura 2.4 Logotipo de Android

Android es un sistema operativo basado en el núcleo Linux diseñado para dispositivos móviles, cuyo desarrollo se expandió para soportar otros dispositivos como reproductores MP3 y MP4, Notebook, computadoras personales, televisores, lectores de e-book e incluso, se aprecia en hornos de microondas y lavadoras.

Para llevar a cabo el desarrollo de Android, se fundó a nivel mundial una alianza en la que podían participar todos aquellos interesados en la creación de un sistema operativo libre para celulares. Así fue que el grupo estuvo conformado por las más destacadas empresas de telefonía móvil y los más importantes líderes tecnológicos actuales.

El anuncio de Android, se realizó el 5 de noviembre del 2007 junto con la creación de la *Open Handset Alliance*, un consorcio de 78 compañías de *hardware*, *software* y telecomunicaciones dedicadas al desarrollo de estándares abiertos para dispositivos móviles. El objetivo principal del consorcio es la creación de novedosas tecnologías *Open Source*, tanto para los teléfonos móviles con los respectivos servicios con el fin de disminuir los elevados costos que afectan a todo lo relacionado en la programación y distribución.

Google liberó la mayoría del código de Android bajo la licencia Apache. En la actualidad, Android posee aproximadamente 32.9% de cuota de mercado a escala mundial de los teléfonos inteligentes, por delante de Symbian OS que posee una cuota aproximada del 30.6%. En tercer lugar se sitúa iOS con un mercado del 16%.

Por todos los beneficios que representa la utilización de Android en los teléfonos celulares es inevitable que la mayoría de los *Smartphones* que se comercializan en el mercado incorporen este novedoso sistema operativo, el cual tiene una gran comunidad de desarrolladores escribiendo aplicaciones para extender la funcionalidad de los dispositivos. A la fecha, se han sobrepasado las 250 000 aplicaciones disponibles para la tienda oficial de Android (Android Market), sin tener en cuenta aplicaciones de otras tiendas no oficiales, como pueden ser la App Store de Amazon o la tienda de aplicaciones de Samsung.

Google pone a disposición de los desarrolladores el SDK (*Software Development Kit*) de Android de cada nueva versión que lanza al mercado; de esta manera, cada empresa de telefonía móvil puede ajustar el sistema operativo a los requerimientos específicos de sus celulares.

Este novedoso sistema operativo para telefonía portátil representa una gran ventaja, no sólo para las compañías de teléfonos celulares y operadoras, que se benefician al reducir los costos y ofrecer productos actualizados; sino que, además, mediante la implementación de Android los consumidores pueden adquirir los equipos a precios inferiores con mejores servicios (tanto de telefonía como de Internet) y una interfaz de usuario más sencilla, práctica y eficaz.

2.8 Conclusiones

El primer paso para administrar una red es documentarla; para ello, se deben realizar las siguientes auditorías:

De inventario e instalaciones. Se pueden utilizar para ayudar a resolver problemas en la red.

Operacional. Permite ver las operaciones diarias de la red mediante el uso de unas herramientas de hardware y *software* especializadas.

De seguridad. Revisa las peticiones de seguridad de la red y el tipo de sistema de seguridad más adecuado.

De efectividad. Permite determinar si la red funciona a todo su potencial.

Las auditorías son necesarias para establecer una base para medir el rendimiento continuo de la red. Además, los procedimientos y preguntas pueden ser útiles para resolver problemas, particularmente los que han sido identificados por los clientes.

Las evaluaciones periódicas de la red son herramientas importantes de mantenimiento y prevención, que pueden ayudar a asegurar el continuo funcionamiento a nivel aceptable.

La información que se obtiene durante dichas evaluaciones se utiliza para preparar un informe que puede transformarse en la base para una petición de cambios.

2.9 ◉ Banco de preguntas para la certificación de CISCO

2.1 ¿Cuál es la importancia de los estándares EIA/TIA?

- **a)** Proporcionan un marco de trabajo para implementación del modelo de referencia OSI.
- **b)** Ofrecen pautas para que los fabricantes de NIC (*Networking Interface Cards*) aseguren la compatibilidad.
- **c)** Suministran los requisitos mínimos de los medios para entornos de múltiples productos y fabricantes.
- **d)** Ninguna de los anteriores.

2.2 El proceso de instalar dispositivos de red complejos que dividan los dominios mediante la utilización de *bridges*, *switches* y *routers*, se llama:

- **a)** Seccionamiento
- **b)** Segmentación
- **c)** Reducción del dominio de colisión
- **d)** Ninguno de los anteriores

2.3 Los seis primeros números hexadecimales en una MAC, representan un:

- **a)** Número de serie de una interfaz
- **b)** Identificador único organizativo
- **c)** Identificador único de una interfaz
- **d)** Ninguno de las anteriore.

2.4 ¿Dónde reside la dirección MAC de una computadora?

- **a)** Transceptor
- **b)** BIOS de la computadora
- **c)** NIC
- **d)** CMOS

2.5 ¿A qué se refiere el control de acceso al medio?

- **a)** Al estado en que una NIC ha capturado el medio de la red y está preparada para transmitir.
- **b)** A las reglas que gobiernan la captura y la liberación del medio.
- **c)** Al protocolo que determina a qué computadora se le permite transmitir los datos en un entorno de medios compartidos.
- **d)** A una secuencia formal de *bytes* que se ha transmitido.

Continuación

2.6 El proceso de transmisión de testigos implica:

- **a)** Escuchar el tránsito de testigos y transmitirlo cuando no se detecte ninguno.
- **b)** Utilizar la posesión del testigo para garantizar la correcta transmisión.
- **c)** Adjuntar tramas testigo a las tramas de datos para acceder a la red.
- **d)** La circulación del testigo a través de un anillo hasta que alcance el destino que se pretende.

2.7 ¿Qué técnica utiliza Ethernet?

- **a)** La transmisión de testigos (*Token Passing*) para asegurar que no se den colisiones en una red.
- **a)** *Beaconing* para ayudar a las redes a recuperarse de las fallas en los enlaces.
- **b)** Acceso múltiple con detección de portadora y de colisiones (CSMA/CD) para localizar los destinos.
- **c)** Difusiones para propagar el tránsito entre las entidades de la red.

2.8 Los puentes dividen el tránsito en segmentos y filtran el tránsito basándose en…

- **a)** las direcciones IP.
- **b)** las direcciones MAC.
- **c)** las normas de prioridad.
- **d)** las direcciones IPX.

2.9 ¿Qué especifica el estándar EIA/TIA-569?

- **a)** Cada piso debe tener un mínimo de un recinto cableado.
- **b)** En una LAN Ethernet el recorrido del cableado horizontal se debe conectar con el punto central de una topología en estrella.
- **c)** El recinto de cableado debe ser lo suficientemente grande para acomodar todo el equipo y el cableado a colocar en el interior.
- **d)** Ninguna de los anteriores.

2.10 En una topología en estrella extendida, ¿qué es una conexión cruzada?

- **a)** El cableado del *backbone*.
- **b)** El MDF
- **c)** El IDF
- **d)** El cableado horizontal.

Continuación

2.11 ¿Cuáles son los cuatro objetivos principales del diseño de redes de computadoras?

a) Funcionalidad, escalabilidad, adaptabilidad y manejabilidad.
b) Comunicaciones, aplicaciones, compatibilidad y operatividad.
c) Control, seguridad, estabilidad y escalamiento.
d) Aplicabilidad, portabilidad, crecimiento y conectividad.

2.12 ¿Qué puede causar congestión en una red de computadoras?

a) El acceso a Internet.
b) El acceso a las bases de datos centralizadas.
c) La transmisión de audio, video y datos.
d) Todas las anteriores.

2.13 ¿Qué tipo de conmutación tiene lugar cuando se conectan dispositivos de ancho de banda desigual?

a) Prométrico
b) Simétrico
c) Asimétrico
d) Dúplex

2.14 ¿Qué efectos similares tienen el *router* y el *switch* en un segmento LAN?

a) Reducción de difusiones
b) Reducción de dominios de colisión
c) Aumento del ancho de banda
d) Todas las anteriores

2.15 ¿Qué puede crear la introducción de un *switch* en una LAN?

a) Un dominio de difusión adicional
b) Un dominio de colisión adicional
c) Un segmento de red adicional
d) Todas las anteriores

Continuación

2.16 ¿En qué se diferencian las direcciones MAC de las direcciones de la capa de red?

a) La capa de red necesita un esquema de direccionamiento jerárquico en oposición al esquema de direccionamiento plano de las direcciones MAC.

b) La capa de red utiliza las direcciones en formato binario; mientras que las direcciones MAC están en formato hexadecimal.

c) La capa de red utiliza una dirección única transferible.

d) Ninguna de las anteriores.

2.17 ¿Cuántos bits hay en una dirección IP?

a) 16

b) 32

c) 64

d) Ninguna de los anteriores

2.18 ¿Cuál es el valor máximo de cada octeto en una dirección IP?

a) 128

b) 255

c) 256

d) Ninguna de los anteriores

2.19 ¿Qué papel desempeña el número de red en una dirección IP?

a) Especifica la red a la que pertenece el *host*.

b) Especifica la identidad de la computadora de la red.

c) Especifica qué nodo de la subred se va a direccionar.

d) Especifica con qué redes se puede comunicar el dispositivo.

2.20 ¿Qué papel desempeña el número de *host* en una dirección IP?

a) Designa la identidad de la computadora de la red.

b) Designa qué nodo de la subred se direcciona.

c) Designa la red a la que pertenece el *host*.

d) Designa los *host* que se pueden comunicar al dispositivo.

Continuación

2.21 ¿Qué parte de la siguiente dirección de clase B es la dirección de red 154.19.2.7?

a) 154
b) 154.19
c) 154.19.2
d) 154.19.2.7

2.22 ¿Qué parte de la dirección IP 129.219.51.18 representa la red?

a) 129.219
b) 129
c) 14.1
d) 1

2.23 ¿Qué dirección es un ejemplo de una dirección de difusión en la red 123.10.0.0 con una máscara de subred de 255.255.0.0?

a) 123.255.255.255
b) 123.10.255.255
c) 123.13.0.0
d) 123.1.1.1

2.24 ¿Cuántas direcciones de *host* se pueden utilizar en una red de clase C?

a) 253
b) 254
c) 255
d) 256

2.25 ¿Cuántas subredes puede tener una red de clase B?

a) 16
b) 256
c) 128
d) Ninguna de las anteriores

2.26 ¿Cuál es el número mínimo de bits que se pueden tomar prestados para formar una subred?

a) 1
b) 2
c) 4
d) Ninguna de los anteriores

Continuación

2.27 ¿Cuál es la razón principal para utilizar subredes?

a) Reducir el tamaño del dominio de colisión.
b) Aumentar el número de direcciones de *host*.
c) Reducir el tamaño del dominio de difusión.
d) Ninguna de las anteriores.

2.28 ¿Cuántos bits hay en una máscara de subred?

a) 16
b) 32
c) 64
d) Ninguna de los anteriores

2.29 ¿Cuántos bits se pueden tomar prestados para crear una subred en una red de clase C?

a) 2
b) 4
c) 6
d) Ninguna de los anteriores

2.30 Con una dirección de clase C de 197.15.22.31 y una máscara de subred de 255.255.255.224, ¿cuántos bits se deben tomar prestados para crear una subred?

a) 1
b) 2
c) 3
d) Ninguna de los anteriores

PRÁCTICAS

Para realizar estas prácticas es requisito indispensable que descargue del sitio web: www.cisco.com el simulador Packet Tracer 7.0.

Después para familiarizarse con el uso de este simulador, busque en Internet, descargue y lea los tutoriales, vea los videos que existen sobre dicha aplicación informática.

PRÁCTICA 2.1 Cableado de una red de computadoras simple utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Desarrollar la comprensión de las funciones básicas del simulador Packet Tracer versión 7.0.
- ☑ Crear una red simple con dos host.
- ☑ Observar la importancia del uso del tipo de cable correcto para conectar de forma adecuada computadoras personales (PC).

Introducción

El cable es el medio en que las computadoras de una red se pueden comunicar una con la otra. Hay distintitos tipos de cables para conectar una red, cada tipo está sujeto a la topología de la red con esto se deberá tener en cuenta varios factores. Estos son los distintos tipos que se pueden encontrar en una LAN (*Local Area Network*, Red de Área Local):

- ☑ Cable de par trenzado sin apantallar/UTP (*Unshielded Twisted Pair*).
- ☑ Cable de par trenzado apantallado/STP (*Shielded Twisted Pair*).
- ☑ Cable coaxial.
- ☑ Cable de fibra óptica.
- ☑ LAN sin cableado.

Procedimiento

Primera Parte. Creación de un diagrama de red con dos PC

La esquina inferior izquierda de la pantalla de Packet Tracer muestra los iconos que representan las categorías o grupos de dispositivos; por ejemplo, *routers*, *switches* y dispositivos finales. Entonces, pase el cursor sobre éstas para mostrar el nombre de cada una en la casilla centrada entre las filas de dispositivos.

Para seleccionar un dispositivo, primero seleccione su categoría; luego, las opciones correspondientes aparecerán en un recuadro, del cual deberá elegir la que necesite:

- ☑ Elija "*End Devices*" de las opciones que aparecen en la esquina inferior izquierda.
- ☑ Arrastre y coloque dos PC genéricas (PC-PT) en el "*Logical Workspace*".
- ☑ Seleccione "*Connections*" en la esquina inferior izquierda y elija un tipo de cable "*Copper Straight-Through*".
- ☑ Haga clic en el primer *host* (PC0) y asigne el cable al conector "*FastEthernet*".
- ☑ Después seleccione el segundo *host* (PC1) y asigne el cable al conector "*FastEthernet*".
- ☑ Los puntos rojos indican que el tipo de cable es incorrecto. Haga clic en la "X" roja que aparece del lado derecho de Packet Tracer para eliminar el cable "*Copper Straight-Through*".

- ☑ Mueva el cursor al cable y haga clic en éste para eliminarlo; después, elija un tipo de cable "*Copper Cross-Over*".
- ☑ Haga clic en el primer *host* (PC0) y asigne el cable al conector "*FastEthernet*".
- ☑ Seleccione el segundo *host* (PC1) y asigne el cable al conector "*FastEthernet*". Los puntos verdes en ambos extremos del cable indican que el tipo de cable es correcto.

Segunda Parte. Configuración de los nombres de *host* y las direcciones IP en las PC

- ☑ Tras hacer clic en PC0 aparecerá una ventana de PC0; en ésta seleccione la ficha "*Config.*", cambie el "*Display Name*" de la PC a PC-A.
- ☑ Seleccione la ficha "*FastEthernet*" que aparece a la izquierda.
- ☑ Escriba la dirección IP 192.168.1.1 y la máscara de subred 255.255.255.0 en la sección "*IP Configuration*".
- ☑ Seleccione la "X" ubicada en la esquina superior derecha para cerrar la ventana de configuración de PC-A.
- ☑ Haga clic en PC1; tras ello aparecerá una ventana de PC1, en ésta seleccione la ficha "*Config.*" y cambie el "*Display Name*" de la PC a PC-B.
- ☑ Seleccione la ficha "*FastEthernet*" que aparece a la izquierda.
- ☑ Escriba la dirección IP 192.168.1.2 y la máscara de subred 255.255.255.0 en la sección "*IP Configuration*".
- ☑ Seleccione la "X" ubicada en la esquina superior derecha para cerrar la ventana de configuración de PC-B.

Tercera Parte. Creación de un diagrama de red con dos PC y un *hub*

En la primera parte de la práctica se conectaron dos computadoras con un cable de cobre de conexión cruzada, que es una forma sencilla de interconectarlas. Ahora, utilice un *hub* para conectar dos o más computadoras:

- ☑ Comience esta nueva configuración con la "X" roja que aparece del lado derecho de Packet Tracer para eliminar el tipo de cable de cobre de conexión cruzada que conecta PC-A a PC-B.
- ☑ Seleccione los *hubs* de las opciones que aparecen en la esquina inferior izquierda.
- ☑ Arrastre y coloque un *hub* genérico (Hub-PT) en el espacio de trabajo lógico.
- ☑ Seleccione "*Connections*" en la esquina inferior izquierda.
- ☑ Elija un tipo de cable de cobre de conexión cruzada.
- ☑ Haga clic en el primer *host* (PC-A) y asigne el cable al conector "*FastEthernet*".
- ☑ Seleccione el Hub0 y el puerto de conexión "Port 0" para conectar a PC-A.
- ☑ Los puntos rojos indican que el tipo de cable es incorrecto. Haga clic en la "X" roja del lado derecho de Packet Tracer y elimine el cable de cobre de conexión cruzada.
- ☑ Elija un tipo de cable "*Copper Straight-Through*".
- ☑ Haga clic en el *host* "PC-A" y asigne el cable al conector "*FastEthernet*".
- ☑ Escoja el "Hub0" y elija el puerto de conexión "Port 0" para conectar a PC-A.

- ☑ Seleccione de nuevo el tipo de cable de cobre de conexión directa.
- ☑ Haga clic en el *host* "PC-B" y asigne el cable al conector "*FastEthernet*".
- ☑ Elija el "Hub0" y "Port 1" para conectar a PC-B.

Cuarta Parte. Reemplazo del *hub* por un *switch*

En la tercera parte, se creó una red con un *hub*; sin embargo, el rendimiento podría mejorarse con un *switch*, lo cual se llevará a cabo a continuación:

- ☑ Seleccione el *hub* y haga clic en la "X" roja ubicada del lado derecho de *Packet Tracer*. Esto eliminará el *hub* y los cables conectados a él.
- ☑ Elija "*switches*" en las opciones que aparecen en la esquina inferior izquierda.
- ☑ Arrastre y coloque el *switch* 2950-24 en el "*Logical Workspace*".
- ☑ Seleccione "*Connections*" en la esquina inferior izquierda y elija un tipo de cable "*Copper Straight-Through*".
- ☑ Haga clic en el *host* "PC-A" y asigne el cable al conector "*FastEthernet*".
- ☑ Escoja el "Switch0" y seleccione el puerto de conexión "*FastEthernet 0/1*" para conectar a PC-A. Después de aproximadamente un minuto aparecerán dos puntos verdes en ambos lados del cable de cobre de conexión directa; esto indica que se utilizó el correcto.
- ☑ Haga clic de nuevo en el tipo de cable de cobre de conexión directa y luego en el *host* "PC-B"; después asigne el cable al conector "*FastEthernet*".
- ☑ Elija el "Switch0" y "*FastEthernet0/2*" para conectar a PC-B.

Cuestionario

2.1.1 ¿Cuántos puntos de falla se pueden detectar?

2.1.2 Explique a detalle por qué es importante elegir el cableado adecuado para interconectar una red de computadoras.

2.1.3 Explique a detalle los diferentes tipos de cables que se utilizan en la conexión de una red de computadoras.

PRÁCTICA 2.2 Topologías simples de redes de computadoras utilizando Packet Tracer 7.0 de Cisco Systems

Objetivo de aprendizaje

Familiarizarse con las topologías físicas de malla.

Introducción

En esta actividad se crearán varias topologías físicas distintas con los dispositivos mostrados; éstas son las siguientes:

- ☑ Estrella
- ☑ Estrella extendida (también conocida como jerárquica)
- ☑ Malla

Una vez que se cablean los dispositivos conforme a la topología física específica se interconectarán dichas topologías.

Procedimiento

Primera Parte. Cableado en una topología física en estrella

- ☑ Para realizar el cableado de la primera estrella inicie con la ubicación de los siguientes dispositivos: PC00, PC01, PC02, PC03 y SW0, que deben estar en la esquina superior izquierda del área de trabajo de simulador Packet Tracer; estos formarán una topología en estrella.
- ☑ En el menú "*Connections*" elija "*Copper Straight-Through*".

Sugerencia: mantenga presionado "*Control*" cuando haga clic en el icono del cable de cobre de conexión directa para agregar varias conexiones.

- ☑ Realice el cableado de las PC mencionadas a SW0. Conecte PC00 a "*FastEthernet0/1*" de SW0; PC01 a "*Fast-Ethernet0/2*" de SW0; PC02 a "*FastEthernet0/3*" de SW0; y PC03 a "*Fast-Ethernet0/4*" de SW0.
- ☑ Los dispositivos mencionados ahora están conectados en una topología en estrella en la que SW0 actúa como centro.

Segunda Parte. Creación de las demás estrellas

Para realizar la conexión del cable de la segunda estrella lleve a cabo el siguiente procedimiento:

- ☑ Ubique SW1, PC10, PC11, PC12 y PC13, que deben estar ubicados en la esquina inferior izquierda del área de trabajo del simulador Packet Tracer 7.0.

- ☑ Al igual que en la Parte 1, realice el cableado de la segunda estrella. En el menú "*Connections*" elija "*Copper Straight-Through*".
- ☑ Conecte PC10 a "Fast-Ethernet0/1" de SW1; PC11 a "*Fast-Ethernet0/2*" de SW1; PC12 a "*Fast-Ethernet0/3*" de SW1 y PC13 a "*Fast-Ethernet0/4*" de SW1.
- ☑ Se debe realizar el cableado del segundo conjunto de dispositivos en forma de estrella.

Después, para llevar a cabo el cableado de la tercera estrella:

- ☑ Ubique SW2, PC20, PC21, PC22 y PC23. Estos dispositivos deben estar ubicados en el área central superior del área de trabajo del simulador Packet Tracer.
- ☑ Realice el cableado de la tercera estrella. En el menú "*Connections*" elija "*Copper Straight-Through*".

Sugerencia: mantenga presionado "Control" cuando haga clic en el icono del cable de cobre de conexión directa para agregar varias conexiones.

- ☑ Conecte PC20 a "*Fast-Ethernet0/1*" de SW2; PC21 a "*Fast-Ethernet0/2*" de SW2; PC22 a "*Fast-Ethernet0/3*" de SW2 y PC23 a "*Fast-Ethernet0/4*" de SW2.
- ☑ La tercera estrella ahora debe estar definida.

Las topologías en estrella presentan con frecuencia fallas. En caso de que "Fast-Ethernet0/1" de SW1 falle, solamente se verá afec tada la PC10. Un diseño muy común se basa en colocar una estrella como orilla (*spoke*) y de este modo, se crea una estrella extendida.

Tercera Parte. Creación de una estrella extendida

- ☑ Ubique SW0, SW1, SW2, SW3 y Dist_SW.
- ☑ En el menú "*Connections*" elija un cable de cobre de conexión cruzada.
- ☑ Conecte SW0, SW1, SW2 y SW3 a Dist_SW según la tabla 2.1.

Tabla 2.1 Matriz de conexiones.

Dispositivos	Puerto del switch	Puerto en Dist_SW:
SW0	*Fast-Ethernet0/24*	*Fast-Ethernet0/10*
SW1	*Fast-Ethernet0/24*	*Fast-Ethernet0/11*
SW2	*Fast-Ethernet0/24*	*Fast-Ethernet0/12*
SW3	*Fast-Ethernet0/24*	*Fast-Ethernet0/13*

- ☑ Ahora debe tener una estrella extendida con cuatro estrellas más pequeñas que actúan como *spoke*.

Cuarta Parte. Creación de una topología de malla completa

El mayor defecto de la topología en estrella es que introduce un punto de equivocación importante. En caso de que falle el dispositivo que actúa como hub de la estrella, ésta también lo hará. En los casos en que no se admite un único punto de falla, los dispositivos se cablean como malla completa, creando una topología redundante.

En esta parte, se conectarán los dispositivos núcleo "MainCluster_SW1", "MainCluster_SW2" y "MainCluster_SW3" como malla completa mediante el cableado de estos a todos los restantes. Si se cuenta con tres dispositivos, cada uno debe tener dos enlaces salientes.

Con el objetivo de llevar a cabo la interconexión de los switches de núcleo, lleve a cabo los pasos planteados a continuación:

- ☑ Ubique "MainCluster_SW1", "MainCluster_SW2" y "MainCluster_SW3"; estos dispositivos deben encontrarse en la parte derecha del área de trabajo del simulador Packet Tracer.
- ☑ En el menú "*Connections*" elija cable de cobre de conexión cruzada.

Sugerencia: mantenga presionado "*Control*" cuando haga clic en el icono del cable de cobre de conexión directa para agregar varias conexiones.

Tabla 2.2 Matriz de conexiones de dispositivos.

Dispositivo de origen	Puerto de origen	Dispositivo de destino	Puerto de destino
MainCluster_SW1	*GigabitEthernet0/1*	*MainCluster_SW2*	*GigabitEthernet0/1*
MainCluster_SW1	*GigabitEthernet0/2*	*MainCluster_SW3*	*GigabitEthernet0/1*
MainCluster_SW2	*GigabitEthernet0/2*	*MainCluster_SW3*	*GigabitEthernet0/2*

- ☑ Una vez que todos los switches de "MainCluster" estén interconectados entre sí, se creará una malla completa entre ellos.

Para crear una topología híbrida, tome en cuenta los siguientes pasos:

- ☑ En el menú "*Connections*" elija cable de cobre de conexión cruzada.
- ☑ Conecte "*Fast-Ethernet0/24*" de "*MainCluster_SW1*" a "*Fast-Ethernet0/24*" de "Dist_SW". Mediante la conexión de la topología de malla completa a la estrella extendida se crea una topología híbrida.
- ☑ Packet Tracer debe informar ahora la finalización del 100%; de no ser así, vuelva a verificar los puertos utilizados. Packet Tracer también califica la elección de puertos durante esta actividad.

Cuestionario

Después de analizar los puntos de falla y el incremento de la redundancia, responda las siguientes preguntas:

2.2.1 ¿Cuántos puntos de falla se pueden detectar?

2.2.2 ¿Cómo se podría reducir la cantidad de puntos de falla?

PRÁCTICA 2.3 Incorporación de computadoras en una red utilizando Packet Tracer 7.0, de Cisco Systems

Objetivos de aprendizaje

- ☑ Configurar computadoras para que utilicen DHCP.
- ☑ Ajustar el direccionamiento estático.
- ☑ Utilizar *ipconfig* para recuperar la información IP del *host*.
- ☑ Emplear el *ping* para verificar la conectividad.

Introducción

Durante esta actividad se agregarán dos computadoras a la red de la empresa Branch Office; la cual utiliza DHCP para el direccionamiento dinámico de todas las PC.

Procedimiento

Al analizar la topología, se observan un *switch*, un servidor, un *router*, una nube y dos PC; con respecto a éstas:

- ☑ Observe que estén conectadas a "BranchSwitch" a través de cables de conexión directa. Packet Tracer utiliza líneas sólidas para representar los enlaces de conexión directa de Ethernet.
- ☑ Estudie los puntos verdes de cada lado de los enlaces de conexión directa (junto a cada PC y a "BranchSwitch"); estos, en ambos lados de un enlace, indican que se utilizó el tipo de cable correcto para interconectar los dispositivos.

Nota: en los dos extremos de cada conexión de cable deben haber puntos verdes; de no ser así vaya a "Options" y luego a "Preferences" en Packet Tracer; después, active la casilla de verificación "Show Link Lights".

Configurar DHCP en las PC implica atender los siguientes pasos:

- ☑ Haga clic en PC0 para que aparezca una ventana de PC0 donde debe seleccionar la ficha "*Desktop*".
- ☑ Elija "*IP Configuration*" y seleccione el botón "DHCP" para permitir que la PC actúe como cliente DHCP con el objetivo de recibir la información de configuración de la dirección IP en forma dinámica.
- ☑ El siguiente mensaje debe aparecer luego de hacer clic en el botón "DHCP": "*DHCP Request Successful*".
- ☑ Seleccione la "X" ubicada en la esquina superior derecha para cerrar la ventana de configuración de PC0.
- ☑ Tras hacer clic en "PC1" aparecerá una ventana de PC1, donde debe seleccionar la ficha "*Desktop*" y luego "*IP Configuration*"; después seleccione el botón DHCP para permitir que la PC actúe como cliente DHCP.
- ☑ Por último, cierre la ventana de configuración de PC1.

Para observar la información de configuración IP asignada a cada PC:

- ☑ Haga clic en PC0, seleccione la ficha "*Desktop*" y luego "*Command Prompt*".
- ☑ En el indicador "PC>" ingrese el comando "*ipconfig /all*".
- ☑ Anote la dirección IP, la máscara de subred, la puerta de enlace predeterminada y la información de dirección del servidor DNS que se asignaron de forma dinámica a través de DHCP a PC0 y a PC1.
- ☑ Con el comando "*ping*" pruebe la conectividad a nivel de capa 3 entre las PC y el *router* predeterminado. Luego, cuando aparezca "PC0>", escriba "*ping* <dirección IP de la PC1>".
- ☑ En el indicador "PC0>" ingrese "*ping* <dirección IP del *router*>"; cuando aparezca "PC1>" escriba "*ping* <dirección IP de PC0>" y al aparecer "PC1>" anote "*ping* <dirección IP del *router*>".

A pesar de todas las ventajas de los esquemas de direccionamiento dinámico como DHCP, a veces es necesario un esquema estático. Cambie PC1 de DHCP a direccionamiento estático por medio de los siguientes pasos:

- ☑ Haga clic en PC1 para que aparezca la ventana de configuración.
- ☑ Seleccione la ficha "*Desktop*", haga clic en "*IP Configuration*" y luego en "*Static*".
- ☑ Ingrese la información IP como se indica a continuación:

Dirección IP: 172.16.1.20
Máscara de subred: 255.255.255.0
Gateway predeterminado: 172.16.1.254
DNS: 200.75.100.10

- ☑ Ahora PC1 está configurada con dirección estática; cierre la ventana "*IP Configuration*".

Para probar la conectividad, envíe los pings a través de la red de la siguiente manera:

- ☑ Haga clic en PC1 para que se abra la ventana de configuración, luego en "*Desktop*" y por último en "*Command Prompt*".
- ☑ Para hacer ping al *gateway* predeterminado escriba "*ping* 172.16.1.254".
- ☑ Para realizar *ping* de Server0 escriba "ping 172.16.1.100".
- ☑ Para hacer *ping* al *router* utilizado como punto de entrada para la nube Corporate escriba "*ping* 172.16.200.1".
- ☑ Para realizar *ping* del servidor ubicado dentro de la nube *Corporate* escriba "*ping* 200.75.100.10".
- ☑ Se obtuvo plena conectividad dentro de la red.

Cuestionario

Como se observa en la topología, los cables de conexión directa se utilizaron para conectar PC0 y PC1 a "*BranchSwitch*". Suponga que se utilizó un cable de conexión cruzada para conectar PC1 a "*BranchSwitch*" con esto en mente, responda las siguientes preguntas:

2.3.1 En dicha situación, ¿PC1 hubiera adquirido una dirección IP a través de DHCP? ¿Por qué?

2.3.2 ¿PC0 hubiera adquirido una dirección IP a través de DHCP, si PC1 estaba conectada a "*BranchSwitch*" a través de un cable de conexión cruzada?

PRÁCTICA 2.4 Configuración de un *router* Cisco

Objetivo de aprendizaje

Configurar un *router* de la marca Cisco en sus diferentes modos de operación a través del simulador Packet Tracer 7.0.

Introducción

Para comenzar con la configuración es importante tomar en cuenta que los *routers* tienen varios modos y submodos de configuración; estos son:

Modo Exec Usuario. Solamente permite ver información limitada de la configuración del *router*; no admite modificación alguna de ésta.

Modo Exec Privilegiado. Posibilita ver en detalle la configuración del *router* para hacer diagnósticos y pruebas. También permite trabajar con los archivos de configuración del *router* (Flash-NVRAM).

Modo de configuración global. Admite la configuración básica del *router* y el acceso a submodos de configuración específicos.

Procedimiento

Para nombrar al *router* tome en cuenta los siguientes pasos donde deberá establecer los parámetros mostrados:

Paso	Instrucción	Descripción adicional
1	router> enable	
2	router# configure terminal	
3	router(config)# hostname RouterA	
4	RouterA(config)#	Nombra al *router* como "RouterA".

Paso	Instrucción	Descripción adicional
1	RouterA> enable	
2	RouterA# configure terminal	
3	RouterA(config)# enable secret contraseña	Configura la contraseña "*Enable Secret*".
4	RouterA(config)# enable password contraseña[2]	Configura la contraseña "*Enable Password*".
5	RouterA(config)#	

[2] Es recomendable configurar "*Enable Secret*" que genera una clave global cifrada en el *router*.

Con el objetivo de configurar una contraseña de consola se requiere de los siguientes parámetros:

Paso	Instrucción	Descripción adicional
1	RouterA> enable	
2	RouterA# config terminal	
3	RouterA(config)# line con 0	Ingresa a la consola.
4	RouterA(config-line)# password contraseña	Configura la contraseña.
5	RouterA(config-line)# login	Habilita la contraseña.
6	RouterA(config-line)# exit	
7	RouterA(config)#	

Para configurar la contraseña VTY (TELNET), se requiere:

Paso	Instrucción	Descripción adicional
1	RouterA> enable	
2	RouterA# config terminal	
3	RouterA(config)# line vty 0 4	Crea las cinco líneas VTY, pero podría ser una sola. Por ejemplo, line vty 0.
4	RouterA(config-line)# password contraseña	Contraseña para las cinco líneas.
5	RouterA(config-line)# login	Habilita la contraseña.
6	RouterA(config-line)# exit	
7	RouterA(config)#	

La configuración de interfaces Ethernet o FastEthernet será:

Paso	Instrucción	Descripción adicional
1	RouterB> enable	
2	RouterA# config terminal	
3	RouterA(config)# interfce FastEthernet 0/0 [3]	Ingresa al submodo de configuración de interfaz.
4	RouterA(config-if)# ip address 192.168.0.1 255.255.255.0	Configura la IP en la interfaz.
5	RouterA(config-if)# no shutdown	Levanta la interfaz.
6	RouterA(config-if)# description lan	Asigna un nombre a la interfaz.
7	RouterA(config-if)# exit	
8	RouterA(config)#	

[3] Tome en cuenta que la interfaz puede ser Ethernet o Fast Ethernet y que el número de interfaz puede ser 0, 1, 0/0, 0/1, etc. Lo anterior varía según el *router*.

Para configurar interfaces serial como DTE, establezca:

Paso	Instrucción	Descripción adicional
1	RouterA> enable	
2	RouterA# config terminal	
3	RouterA(config)# interface serial 0/0 [4]	Ingresa al submodo de configuración de interfaz.
4	RouterA(config-if)# ip address 10.0.0.1 255.0.0.0	Configura la IP en la interfaz.
5	RouterA(config-if)# no shutdown	Levanta la interfaz.
6	RouterA(config-if)# description red	Asigna un nombre a la interfaz.
7	RouterA(config-if)# exit	
8	RouterA(config)#	

Para configurar interfaces serial como DCE, se requieren los siguientes pasos:

Paso	Instrucción	Descripción adicional
1	RouterA> enable	
2	RouterB# config terminal	
3	RouterB(config)# interface serial 0/1 [5]	Ingresa al submodo de configuración de interfaz.
4	RouterB(config-if)# ip address 10.0.0.2 255.0.0.0	Configura la IP en la interfaz.
5	RouterB(config-if)# clock rate 56000	Configura la sincronización entre los enlaces.
6	RouterB(config-if)# no shutdown	Levanta la interfaz.
7	RouterB(config-if)# description red	Asigna un nombre a la interfaz.
8	RouterB(config-if)# exit	
9	RouterB(config)#	

Por último, una vez configurada la interfaz LAN (*FastEthernet*), se conectará un *switch* al *router* y las computadoras al *switch*, tras lo que podrán comunicarse entre sí.

Cuestionario

2.4.1 Explique a detalle, la teoría de operación de un ruteador.

2.4.2 Explique en qué consiste la configuración de un ruteador.

2.4.3 Describa cuántas maneras existen para configurar un ruteador y establezca las condiciones y requerimientos técnicos para cada tipo de configuración.

[4] Se debe tener en cuenta que el número de interfaz puede ser 0, 1, 0/0, 0/1, etcétera. Esto varía según el *router*.

[5] Se debe tener en cuenta que el número de interfaz puede ser 0, 1, 0/0, 0/1, etcétera. Esto varía según el *router*.

PRÁCTICA 2.5 Configuración de un *router* simple para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Ajustar una interfaz para evitar problemas de conectividad.
- ☑ Configurar un *router* en formato estático, en formato dinámico y utilizando el IOS de Cisco Systems.

Introducción

Un *router* posee muchas más características de configuración que el *switch*, dado que se comporta en capas superiores. Es posible tratar el tema de enrutamiento, que puede ser estático o dinámico (RIP), lo que se puede configurar explícitamente a través de la interfaz gráfica.

Procedimiento

Primera Parte. Configuración de interfaces

Como primer paso es de vital importancia encender la interfaz, ya que en el caso de un *router* físico, por lo general se encuentra apagada, produciendo conflictos de conectividad. Además, se procede a la configuración de IP que pasará a ser el *gateway* de la red.

La conexión de un *router* a una LAN o una WAN se llama interfaz, aunque también se denomina puerto. Por ejemplo, una conexión a una LAN *Token-Ring* se hace en una interfaz *Token-Ring*.

Cuando se tratan las conexiones de un *router* a una red, es habitual decir lo siguiente: "Se ha conectado la red *Token-Ring* del Departamento de Finanzas al *Backbone* corporativo mediante la primera interfaz T*oken-Ring* del *Bbone 1*". El Bbone 1, en este caso específico, es el nombre lógico de un *router* en una red corporativa.

Por lo regular, los *routers* tienen asignados nombres que proporcionan información sobre su posición y su función. Cuando un *router* es de enrutamiento IP, cada LAN o WAN a la que está conectado debe tener una dirección única IP de red o de subred. En el caso de algunos tipos de enlaces en serie, un *router* debe "tomar prestada" una dirección desde otra interfaz. El proceso de implementar este tipo de enlaces en serie en un *router* se llama IP no numerado, ya que no se utilizan direcciones IP de red adicionales. La figura 2.5 muestra cómo configurar una interfaz para un *router*.

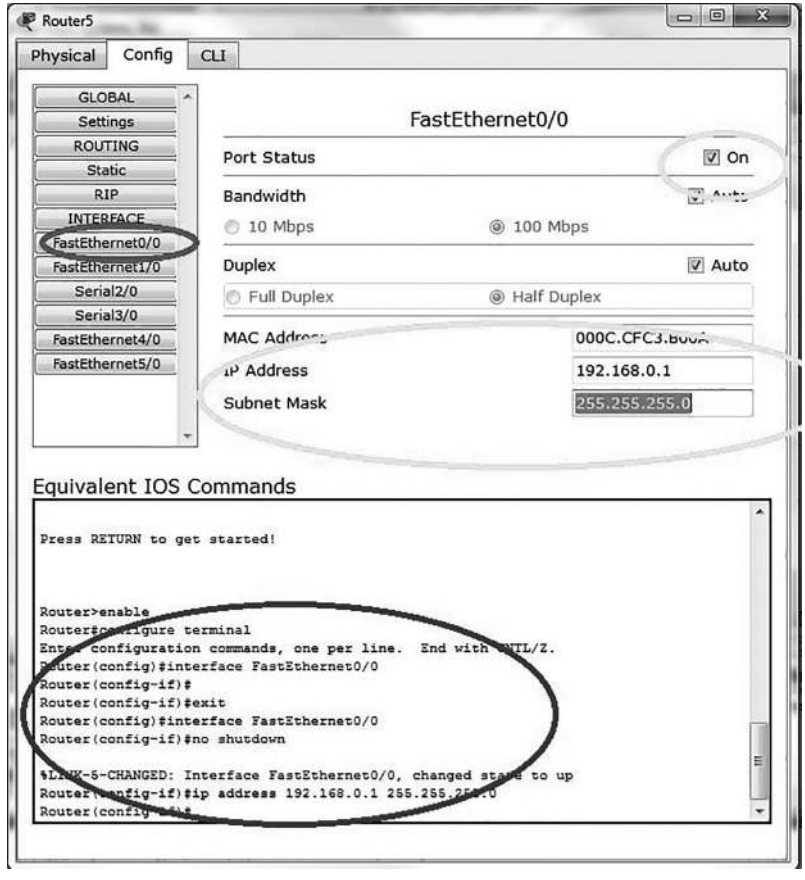


Figura 2.5 Configuración de una interfaz para un *router*

Segunda Parte. Definición de un ruteo estático

Se hace rferencia al tipo de enrutamiento en donde el usuario tiene que definir las redes que no están conectadas al *router*. Asumiendo que una de sus entradas tiene la red 192.168.3.0, el usuario trata de conectarse a la red 192.168.10.0; para lograrlo, realice lo mostrado en la figura 2.6.

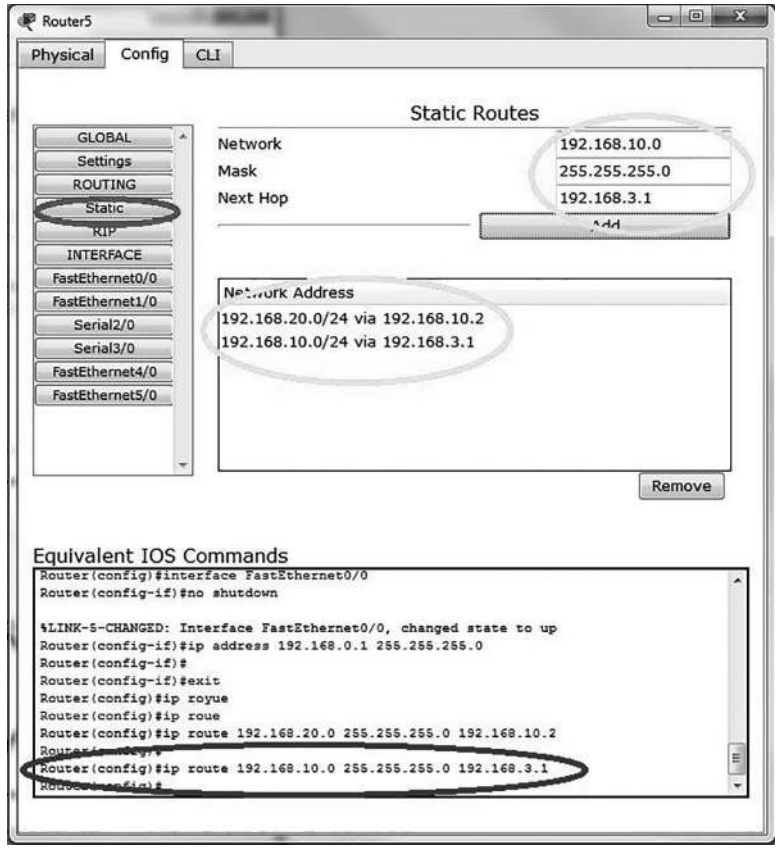


Figura 2.6 Configuración para un ruteo estático

Tercera Parte. Definición de un ruteo dinámico (RIP)

Este apartado es el más simple de los procedimientos de ruteo porque se le indica al *router* cuáles son las demás rutas que comparte con el resto de los dispositivos. La figura 2.7 muestra el procedimiento para realizarlo.

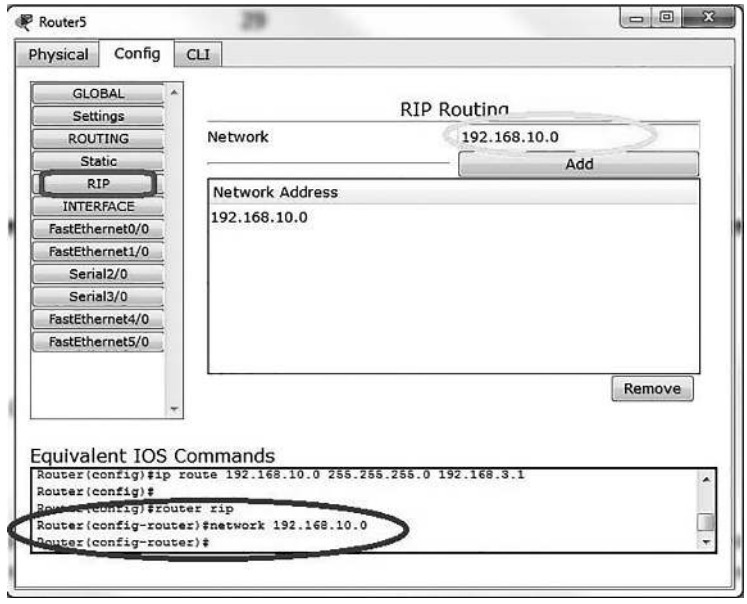


Figura 2.7 Configuración para un ruteo dinámico (RIP)

Cuarta Parte. Manejo de IOS

La interfaz de usuario incluye un modo de edición mejorado que proporciona un conjunto de funciones de teclas que permiten editar una línea de comandos mientras se escribe; la tabla 2.3 muestra los más utilizados para mover el cursor por la línea de comandos y efectuar cambios o correcciones.

Tabla 2.3 Comandos de edición

Comando	Descripción
Ctrl+A	Mueve el cursor hasta el principio de la línea de comandos.
Ctrl+E	Mueve el cursor hasta el final de la línea de comandos.
Esc+B	Retrocede una palabra.
Ctrl+F	Avanza un carácter.
Ctrl+B	Retrocede un carácter.
Esc+F	Avanza una palabra

Aunque el modo de edición mejorado se activa de manera automática con la descarga real del *software*, aquél se puede desactivar si se han escrito *scripts* que no interactúan correctamente mientras está activada la edición mejorada. Para llevar esto a cabo, debe escribirse "*terminal no editing*" en el indicador de modo privilegiado.

El conjunto de comandos de edición proporciona una función de desplazamiento horizontal para los comandos que siguen una línea en pantalla: cuando el cursor alcanza el margen derecho, la línea de comando se desplaza diez espacios a la derecha.

Cada vez que el cursor alcanza el final de la línea, ésta se mueve otra vez diez espacios a la izquierda. [6] No se pueden ver los primeros diez caracteres de una línea, pero puede desplazar el cursor y verificar la sintaxis al principio del comando.

Para moverse hacia atrás, se debe pulsar la secuencia de teclas Ctrl+B o la tecla flecha izquierda, repetidamente hasta encontrarse al principio de la entrada del comando, o se debe pulsar la secuencia de teclas Ctrl+A para volver al comienzo de la línea. Por último, es posible realizar modificaciones a la configuración del *router* de forma directa en el IOS, lo cual permite que el usuario se familiarice con el equipo como lo muestra la figura 2.8.

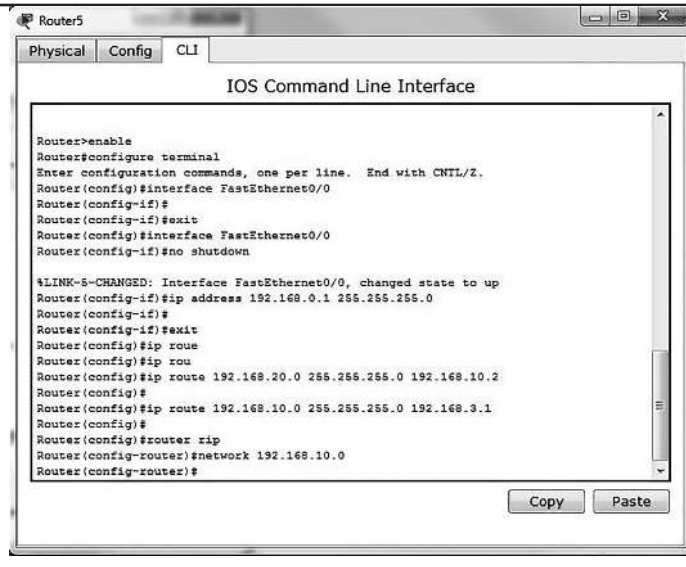


Figura 2.8 Modificaciones a la configuración del *router* de forma directa en el IOS

Cuestionario

2.5.1 ¿Por qué debe configurarse un ruteador dentro de una red de comunicaciones?

2.5.2 Establezca la importancia del uso de un ruteador dentro de una red de comunicaciones en una red de computadoras.

2.5.3 ¿Es posible que otro dispositivo de conectividad, pueda realizar las funciones de un ruteador?

[6] El signo "$" indica que la línea se ha desplazado a la izquierda.

PRÁCTICA 2.6

Establecimiento de la conexión a un *router* inalámbrico configurando sus parámetros básicos para transferir datos por medio de Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Configurar una PC para unirse a una red inalámbrica.
- ☑ Probar la conexión inalámbrica.

Introducción

El método inalámbrico de acceso a Internet de alta velocidad (también denominado inalámbrico fijo) utiliza frecuencias de radio (RF) para transmitir señales de datos. Es un método de banda amplia que funciona bajo el concepto de huella o área geográfica extensa, a la que torres estratégicamente ubicadas, dan servicios que proporcionan señales a toda la zona.

La ventaja de este tipo de acceso es la simplicidad del servicio. Los abonados dentro de un área no necesitan infraestructura para la WAN inalámbrica o para el cableado físico de la casa. El inconveniente es que la mayoría de los proveedores de servicio inalámbrico operan en una frecuencia más baja y necesitan una línea de vista de la torre de telecomunicaciones; además, los grandes objetos físicos como los árboles, las montañas, las construcciones, entre muchos otros, pueden bloquear la señal.

Durante esta actividad, se configurará el *router* inalámbrico Linksys WRT300N para que admita "The Company Laptop" como cliente inalámbrico y enrute los paquetes IP.

Procedimiento

Primera Parte. Cambio del nombre para mostrar de WRT300N

- ☑ Haga clic en WRT300N y vaya a la ficha "Config.", luego reemplace "Display Name" con WRS1; y cierre.
- ☑ Tome en cuenta que la topología ahora muestra WRS1.

Segunda Parte. Preparación de la red

Nota: esta actividad ignorará la existencia de la ficha WRT300N GUI para que se asemeje a una situación real. Una PC de administración (PC0) estará preparada para acceder al *router* inalámbrico Linksys mediante una conexión por cable. Un explorador web que se ejecute en PC0 se utilizará para realizar todas las tareas de configuración.

- ☑ Seleccione "*Connections*" del lado inferior izquierdo de Packet Tracer y luego "*Copper Straight-Through*".
- ☑ Una vez que el cursor cambie al modo de conexión, haga clic en "PC0" y elija "*FastEthernet*"; posteriormente, elija el *router* inalámbrico Linksys y seleccione "Ethernet 1".

Observe que WRT300N tiene dos segmentos de red: Intranet e Internet. Los puertos Ethernet 1 a 4 e inalámbrico se consideran parte del segmento de la primera; mientras que el puerto "Internet" es parte del segundo.

WRS1 actuará como *switch* de capa 2 para los dispositivos conectados a su segmento de red interna y como *router* de capa 3 entre los dos segmentos; por su parte, PC0 ahora está conectada al segmento de red interna (*Ethernet 1*).

Cuando Packet Tracer muestre los puntos verdes de ambos lados de la conexión entre PC0 y WRS1, continúe con la tercera parte.

Nota: si no se muestran los puntos verdes, asegúrese de habilitar la función *"Show Link Lights"* en "*Options*" > "*Preferences*".

Tercera Parte. Preparación PC0

Para alcanzar la página de administración de WRS1 se debe habilitar a PC0 con el objetivo de comunicarse satisfactoriamente en la red.

La configuración de fábrica de los *routers* Linksys incluye un servidor DHCP, que está habilitado en forma predeterminada en la sección LAN interna del *router*. Para asegurarse de que PC0 adquiera una dirección IP de WRS1, configúrelo para que consiga información IP a través de DHCP:

- ☑ Haga clic en PC0 y seleccione la ficha "Desktop".
- ☑ Luego elija "*IP Configuration*" y seleccione DHCP.
- ☑ ¿Cuál es la dirección IP de la computadora?
- ☑ ¿Cuál es la máscara de subred?
- ☑ ¿Cuál es la puerta de enlace predeterminada?

Nota: los valores pueden variar dentro del rango de la red durante el funcionamiento normal de DHCP.

Cuarta Parte. Conexión al *router* inalámbrico

Inicie sesión en el *router* inalámbrico; luego:

- ☑ Cierre la ventana "*IP Configuration*".
- ☑ En la ficha "*Desktop*" en PC0 elija "*Web Browser*" y escriba la dirección IP del *router* inalámbrico: 192.168.0.1.
- ☑ Cuando se le solicite nombre de usuario y contraseña, utilice "admin" para ambos, que son los datos predeterminados para todos los productos Linksys.
- ☑ Cuando se cargue la página de configuración web WRS1 continúe con la quinta parte.

Quinta Parte. Análisis de la página de configuración principal de WRS1

La página principal se ocupa de la configuración de la red del *router*. Observe en ésta el servidor DHCP que ya está habilitado de fábrica y el rango de las direcciones IP proporcionadas actualmente por WRS1 a través de DHCP es 192.168.0.100/24.

Responda:

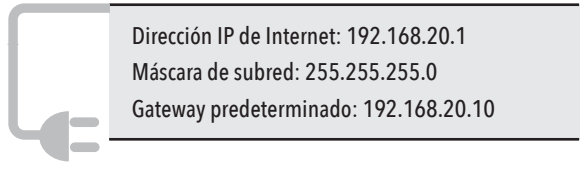
- ☑ ¿La dirección IP de PC0 está dentro de este rango?
- ☑ ¿Es un resultado esperable? ¿Por qué?

Sexta Parte. Configuración del puerto de Internet de WSR1

Debido a que WRS1 ruteará paquetes de clientes inalámbricos a redes remotas, es necesario configurar su puerto de Internet, que es denominado por Linksys "Interfaz de Internet", que se conecta a una red externa.

Durante esta actividad se conectará dicha interfaz al segmento de red que contiene Server0:

- ☑ Cambie el método de direccionamiento IP de Internet de "*Automatic Configuration-DHCP*" a "Static IP".
- ☑ Escriba la dirección IP que se asignará a la interfaz de Internet de la siguiente manera:



- ☑ El resto de la información se mantiene igual.
- ☑ Desplácese hacia abajo de la página, haga clic en "*Save Settings*" y en "*Continue*"; luego siga con la séptima parte.

Séptima Parte. Configuración SSID de WSR1

- ☑ Mediante un explorador web en PC0 vuelva a iniciar sesión en WRS1 (para más información consulte la cuarta parte).
- ☑ Vaya a "*Wireless*" > "*Basic Wireless Settings*" y cambie "*Network Name (SSID)*" de "linksys" a "Company" tomando en cuenta que los SSID distinguen entre mayúsculas y minúsculas. Las demás configuraciones de la página permanecen con sus valores predeterminados.
- ☑ Desplácese hacia abajo de la página y haga clic en "*Save Settings*"; ahora debe asociarse Laptop0 a WRS1.

Octava Parte. Configuración avanzada

- ☑ Mediante un explorador web en PC0 vuelva a iniciar sesión en WRS1 como se ha establecido anteriormente.

- ☑ Luego vaya a "*Administration*" > "*Management*" y cambie la contraseña actual de WRS1 a "cisco".
- ☑ Posteriormente, desplácese hacia abajo de la ventana y haga clic en "*Save Settings*". Tras esto se abrirá una página que mostrará el mensaje "*Settings are successful*"; después haga clic en "*Continue*" para que aparezca la ventana para iniciar sesión, pero esta vez utilice la contraseña "cisco".

Cuestionario

2.6.1 Explique la teoría de operación de un ruteador inalámbrico.

2.6.2 ¿Cuáles son las diferencias operativas entre un ruteador inalámbrico y uno alambrado o cableado?

2.6.3 Establezca cuáles son los protocolos de comunicación que se utilizan para utilizar un ruteador inalámbrico, en una red de comunicaciones, dentro de una red de computadoras.

PRÁCTICA 2.7 Prueba de una conexión inalámbrica utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Configurar una PC para unirse a una red inalámbrica.
- ☑ Probar la conexión inalámbrica.

Introducción

El término red inalámbrica (Wireless Network) se utiliza en informática para designar la conexión de nodos que se da por medio de ondas electromagnéticas sin necesidad de una red cableada o alámbrica donde la transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas son los costos porque se elimina el cableado Ethernet; así como las conexiones físicas entre nodos; empero, también cuenta con una desventaja considerable, puesto que para este tipo de red se debe tener una seguridad mucho más exigente y robusta con el objetivo de evitar a los intrusos.

Durante esta actividad se configurará la PC3 para que se conecte a una red a través de Linksys WRT300N. Utilice el armado de la red de la práctica anterior para integrar ahora la PC3.

Procedimiento

Primera Parte. Configuración de la conexión inalámbrica

Para configurar PC3 con el objetivo de que se conecte a WRS1 tome en cuenta los siguientes pasos:

- ☑ Haga clic en PC3 para abrir la "*Physical Device View*".
- ☑ Seleccione la ficha "*Desktop*" para PC3 y elija el botón "*PC Wireless*", tras lo que se abrirá la ventana de "*Link Information*" con la nota "*No association with access point*".
- ☑ Haga clic en la ficha "*Connect*" en la ventana. Cuando aparezca WRS_LAN como red inalámbrica disponible seleccione nuevamente "*Connect*".
- ☑ Ingrese "ABCDE12345" como la clave WEP y haga clic en "*Connect*".
- ☑ Seleccione la ficha "Link Information", tras lo que se mostrará el mensaje "*You have successfully connected to the access point*"; de no ser así, resuelva los problemas que surgieron en los pasos anteriores de esta actividad.

Segunda Parte. Verificación de la configuración de dirección de PC3

Consulte la configuración de dirección IP de PC3 de la manera presentada a continuación:

- ☑ Cierre la ventana "*PC Wireless*" y haga clic en "*Command Prompt*", donde ingresará "ipconfig /all" y luego presione la tecla "Entrar".
- ☑ Conteste:
  - ➔ ¿Cuál es la dirección física de la computadora?
  - ➔ ¿Qué otro nombre recibe la computadora?

- Cuál es la dirección IP de la computadora?
- Cuál es su máscara de subred?
- ¿Cuál es la puerta de enlace predeterminada?
- ¿Cuál es la dirección del servidor DNS?
- ¿Qué servicio ofrece éste a la red?

Tercera Parte. Verificación de la conexión de la red entre PC3 y el resto de la red

☑ En la ventana "*Command Prompt*" realice *ping* de la puerta de enlace predeterminada hacia la PC3. Un *ping* correcto se asemeja al siguiente resultado:

```
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=203ms TTL=255
Reply from 192.168.2.1: bytes=32 time=164ms TTL=120
Respuesta de 192.168.2.10: bytes=32 time=94ms TTL=255
Reply from 192.168.2.1: bytes=32 time=78ms TTL=255
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 78ms, Maximum = 203ms, Average = 117ms
```

☑ En la ventana "*Command Prompt*" realice ping de PC1 con la dirección IP 192.168.1.11.

Luego verifique la conectividad y la ruta entre PC3 y el resto de la red con el comando *tracert*, que se utiliza para determinar la ruta entre un *host* local (en este caso PC3 y un *host* remoto).

☑ En "*Command Prompt*" verifique la ruta entre PC3 y PC2 con el siguiente comando:

"*tracert* 192.168.1.12"; luego presione la tecla "Entrar".

☑ El resultado del comando debe asemejarse a la siguiente información:

```
PC>tracert 192.168.1.12
Tracing route to 192.168.1.12 over a maximum of 30 hops:
1 187 ms 94 ms 93 ms 192.168.2.1
2 * 125 ms 125 ms 192.168.1.12
Trace complete
```

- ☑ Después del resultado del comando, los paquetes ICMP generados por *tracert* muestran la transmisión de paquetes a través de la interfaz LAN WRS1 al *host* PC2.

Cuarta Parte. Con DNS

Verifique la conectividad al servidor web con el uso de DNS:

- ☑ Cierre la ventana "*Command Prompt*" en PC3.
- ☑ Haga clic en el botón "*Web Browser*".
- ☑ Ingrese "www.example.com" en la ventana URL y haga clic en el botón "Go". Debe aparecer la página web para el servidor.
- ☑ Se utiliza DNS para resolver los nombres de dominio de direcciones IP. Para verificar la resolución, cierre la ventana "*Web Browser*" en PC3 y haga clic en "*Command Prompt*" para abrir el símbolo del sistema en PC3.
- ☑ En "*Command Prompt*" realice ping del servidor web con el nombre de dominio "www.ejemplo.com". Esto debería generar el siguiente resultado:

```
PC>ping www.example.com
Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=138ms TTL=126
Reply from 192.168.3.100: bytes=32 time=156ms TTL=126
Reply from 192.168.3.100: bytes=32 time=172ms TTL=126
Reply from 192.168.3.100: bytes=32 time=140ms TTL=126
Ping statistics for 192.168.3.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 138ms, Maximum = 172ms, Average = 151ms
```

Observe que el servidor DNS tradujo el nombre de dominio "www.ejemplo.com" a la dirección IP para el servidor web 192.168.3.100. Esto verifica que el servidor DNS funciona correctamente.

Hasta este momento, todas las solicitudes DNS fueron llevadas a cabo en automático por otras aplicaciones. En el punto tres de esta parte fue realizada por el explorador web y en el punto cinco por el comando ping. Para generar solicitudes DNS directamente al servidor utilice el comando nslookup:

- ☑ En PC3 "*Command Prompt*" ingrese "*nslookup* www.ejemplo.com". El comando seguido de su resultado debe asemejarse a lo siguiente:

Al ingresarse en el formato anterior, nslookup enviará una solicitud al servidor DNS con la siguiente pregunta: "*What's the IP address associated to the name www.example.com*"? (¿Cuál es la dirección IP asociada al nombre www.ejemplo.com?).

```
PC>nslookup www.ejemplo.com
Servidor: [192.168.3.100]
Dirección: 192.168.3.100
Respuesta no autoritativa:
Nombre: www.ejemplo.com
Dirección: 192.168.3.100
PC>
```

La primera línea del resultado del comando informa el nombre del servidor DNS que recibió la solicitud DNS. PC3 envió la solicitud a 192.168.3.100, dirección que obtuvo de WRS1 a través de DHCP; aquélla debía utilizarse para resolver nombres, sin embargo, como no se definió ninguno, se mostró la dirección IP.

La segunda línea informa la dirección IP del servidor DNS utilizado en la solicitud y la tercera, cuarta y quinta líneas revelan la respuesta real a la solicitud: el nombre www.ejemplo.com está asociado a la dirección IP 192.168.3.100.

Cuestionario

2.7.1 Establezca el procedimiento completo que debe seguirse para interconectar un ruteador inalámbrico, dentro de la red de comunicaciones de una red de computadoras.

2.7.2 ¿Cómo se integró PC3 a la configuración solicitada en la práctica?

2.7.3 ¿Qué protocolo de comunicaciones se utilizó en la configuración de equipos en esta práctica?

PRÁCTICA 2.8 Instalación de una NIC inalámbrica para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Instalar una NIC inalámbrica.
- ☑ Configurar una PC para unirse a una red inalámbrica.

Introducción

Una NIC es una tarjeta inalámbrica (Wireless) que viene en diferentes variedades dependiendo de la norma a la cual se ajuste; por lo regular son 802.11b, 802.11g y 802.11n. Las más populares son la primera, la cual transmite a 11 Mbit/s (1 375 MB/s) con una distancia teórica de 100 m y la segunda, que lo hace a 54 Mbit/s (6.75 MB/s).

La velocidad real de transferencia que alcanza una tarjeta Wi-Fi con protocolo 11.b es de unos 4 Mbit/s (0.5 MB/s), y las de 11.g llegan como máximo a 20 Mbit/s. El protocolo 11.n se utiliza con capacidad de transmitir 600 Mbit/s.

La capa física soporta una velocidad de 300 Mbit/s con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede traducirse en un rendimiento percibido por el usuario de 100 Mbit/s.

En esta práctica, se configurará PC2 como PC inalámbrica para conectarse a la red inalámbrica existente a través de Linksys WRT300N (WRS1). De inicio, se tienen conectadas dos PC al equipo Linksys WRT300N (WRS1) a través de un cable Ethernet (PC1 y PC2).

Primera Parte. Mover las PC conectadas por cable a una red inalámbrica

Reemplazar la NIC conectada por cable a la PC2 con una NIC inalámbrica se lleva a cabo de la siguiente forma:

- ☑ Para quitar el cable Ethernet que conecta PC2 a WRS1 haga clic en el botón "X" (ubicado en la barra del lado derecho) y luego seleccione el cable Ethernet.
- ☑ Elija PC2 para abrir la ventana de configuración ("*Configuration*").
- ☑ Haga clic en la ficha "*Physical*".
- ☑ Para desactivar PC2 seleccione el botón de encendido.
- ☑ Para desinstalar la tarjeta cableada, selecciónela y arrástrela desde el cuerpo de la computadora a la lista de módulos.
- ☑ En la lista "*Modules*" del lado izquierdo haga clic y arrastre el módulo Linksys-WMP300N hacia la ranura vacía de la PC2 para instalarlo.
- ☑ Elija el botón de encendido para activar PC2 de nuevo.
- ☑ Debido a que no se configuró PC2 para que se una a la red existente, no se obtuvo conectividad en este momento. Continúe ahora con la segunda parte.

Segunda Parte. Configuración de PC2 para que se una a la red inalámbrica existente

- ☑ Haga clic en PC2 para abrir la ventana "*Configuration*".
- ☑ Seleccione la ficha "*Desktop*" y elija "*PC Wireless*". Tenga en cuenta que PC2 aún no está asociada a ninguna red inalámbrica; luego haga clic en la ficha "*Connect*".

- ☑ Deje transcurrir unos segundos para que PC2 detecte los *beacons* [7] enviados por WRS1 por el aire. Debe observar que la red inalámbrica existente se identifica como "aCompany" enumerada en la columna "*Wireless Network Name*".
- ☑ Para seleccionar el uso de una red haga clic en la red identificada como "aCompany", y luego en el botón "*Connect*".
- ☑ Tome en cuenta que para que PC2 esté asociada a WRS1 debe hacer clic en la ficha "*Link Information*".
- ☑ Vaya a "*Desktop*" > "*IP Configuration*" y seleccione DHCP.
- ☑ PC2 ahora debe estar lista para comunicarse con otros dispositivos conectados a la red.

Tercera Parte. Verificación de la configuración de la dirección de PC2

Para ver la configuración de la dirección IP de PC2 siga los pasos presentados a continuación:

- ☑ Haga clic en PC2 para abrir la ventana de configuración ("*Configuration*").
- ☑ En la ficha "*Desktop*" haga clic en el botón "*Command Prompt*".
- ☑ Escriba "*ipconfig /all*" y luego presione la tecla "Entrar".
- ☑ ¿Cuál es la dirección IP de la computadora?, ¿cuál es su máscara de subred?, ¿cuál es la puerta de enlace predeterminada?
- ☑ En "*Command Prompt*" de PC2 realice *ping* a PC0 y PC1 de la red.

Nota: debido a que la información IP se adquiere a través de DHCP, las direcciones IP pueden ser diferentes a las enumeradas con anterioridad.

Cuestionario

2.8.1 Establezca con sus propias palabras, cómo se integró la NIC en el desarrollo de esta práctica.

2.8.2 ¿Qué protocolo de comunicaciones se utilizó en esta práctica?

2.8.3 Establezca aplicaciones prácticas reales de lo que configuró en esta práctica.

[7] Un *beacon* es un pequeño dispositivo que emite una señal en la onda corta de la tecnología *Bluetooth*

PRÁCTICA 2.9

Conexión de una PC inalámbrica a un equipo WRT300N para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Establecer la configuración inalámbrica básica en una computadora personal.
- ☑ Configurar la seguridad básica en Linksys-WRT300N.
- ☑ Verificar la conectividad plena del arreglo.

Introducción

La comunicación inalámbrica o sin cables es aquella que no se encuentra unida por un medio de propagación física, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio. En este sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, entre los cuales se encuentran las antenas, las computadoras portátiles, los asistentes personales digitales (PDA, *Personal Digital Assistant*), los teléfonos móviles, etcétera

La comunicación inalámbrica, que se realiza a través de ondas de radiofrecuencia, facilita la operación en lugares donde la computadora no se encuentra en una ubicación fija. En la actualidad, se utiliza de una manera general y accesible para todo el público. Cabe también mencionar que en hoy en día las redes cableadas presentan ventaja en cuanto a transmisión de datos sobre las inalámbricas: mientras que las primeras proporcionan velocidades de hasta 1 Gbit/s (Red Gigabit), las segundas alcanzan sólo hasta 108 Mbit/s; sin embargo, es posible realizar una "mezcla" entre arreglos inalámbricos y alámbricos que puede funcionar de la siguiente manera: el sistema cableado será la parte principal y el inalámbrico proporcionará movilidad al equipo y al operador para desplazarse con facilidad en distintos campos.

Las redes a larga distancia no tienen problemas en pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en vez de comunicaciones por voz. En resumen, las transmisiones inalámbricas constituyen una eficaz herramienta que permite el traslado de voz, datos y video sin la necesidad de cableado en una red convergente.

Durante esta práctica, se configurarán las PC inalámbricas para conectarlas a una red a través de Linksys WRT300N; para ello, cambie el SSID y la contraseña predeterminados y agregue la encriptación WEP, lo cual se llevará a cabo durante la misma.

Primera Parte. Conexión al *router* Linksys WRT300N

- ☑ Para conectarse al *router* inalámbrico acceda al "*Desktop*" de la WirelessPC1 y luego a "*PC Wireless*"; luego seleccione la ficha "*Connect*" y conecte el equipo a la red predeterminada.
- ☑ Luego, verifique las configuraciones de conectividad: en el escritorio de la PC acceda a "*Command Prompt*" e ingrese el comando *ipconfig*.

```
PC>ipconfig
Dirección IP.....: 192.168.1.100
Máscara de subred.....: 255.255.255.0
Gateway predeterminado.....: 192.168.1.1
PC>
```

Nota: la dirección IP puede ser diferente, ya que se adquirió de forma dinámica.

Segunda Parte. Acceso a Linksys WRT300N mediante el explorador web

- ☑ En WirelessPC1 cierre el "Command Prompt" y luego haga clic en "*Web Browser*". Ingrese la URL 192.168.1.1 (puerta de enlace predeterminada de la PC).
- ☑ Ingrese la información de autenticación: se le pide que introduzca un nombre de usuario y una contraseña, que es "admin" en ambos casos. Una vez que escriba los datos para iniciar sesión, debe ver la página por defecto de la herramienta web de WRT300N de Linksys.

Tercera Parte. Configuraciones básicas inalámbricas

- ☑ Para activar la protección de la red inalámbrica, acceda a la página "*Wireless*" y cambie "*Network Name (SSID)*" de "*Default*" a WRS1.
- ☑ Para guardar las configuraciones desplácese hacia abajo de la página y haga clic en "*Save Settings*".
- ☑ Cuando Linksys WRT300N admita las configuraciones establecidas aparecerá un mensaje de "*Request Timeout*" en la ventana del explorador web. Después de que aparezca esto, continúe con la Parte 4.

Lleve a cabo la reconexión a la red inalámbrica: como cambió el SSID, WirelessPC1 en este momento no puede acceder a la red. En "*Desktop*" vuelva a "*PC Wireless*" y seleccione la ficha "*Connect*" para conectarse a la red WRS1.

Cuarta Parte. Habilitación de la seguridad inalámbrica

- ☑ Desde el explorador web de WirelessPC1 vuelva a conectarse a la página de configuración del *router* (http://192.168.1.1).
- ☑ Después, vaya a la página inalámbrica y luego seleccione la pestaña de seguridad inalámbrica.
- ☑ En el modo de seguridad seleccione WEP e ingrese la clave "1234567890" en el campo *Key1*

Una red es tan segura como su punto más débil, y un *router* inalámbrico es un lugar muy conveniente para comenzar en caso de que alguien desee dañar su red; empero, al solicitar una clave WEP para conectar el *router* se agrega un nivel de seguridad. Desafortunadamente, existen herramientas que pueden descifrar esta encriptación.

Una forma más poderosa de seguridad inalámbrica es WPA y WPA-2, que aún no admite Packet Tracer.

Quinta Parte. Guardado de las configuraciones

- ☑ Desplácese hacia abajo de la página y haga clic en "*Save Settings*". Se desconectará de la red nuevamente después de guardar la configuración.
- ☑ Cuando Linksys WRT300N admita las configuraciones establecidas, aparecerá un mensaje de "*Request Timeout*" en la ventana del explorador web; después, continúe con la sexta parte.

Sexta Parte. Configuración de WirelessPC1 para utilizar la autenticación WEP

- ☑ Vuelva a "*Desktop*" y haga clic en "*PC Wireless*".
- ☑ Seleccione la ficha "*Connect*".
- ☑ De la lista de redes inalámbricas disponibles, elija WRS1 y haga clic en "*Connect*".
- ☑ Aparecerá una pantalla en la que se solicita la clave WEP. En "*WEP Key 1*" ingrese la clave "1234567890" y luego haga clic en "*Connect*".
- ☑ Haga clic en "*Link Information*" para verificar la conectividad con el punto de acceso.

Séptima Parte. Administración y aseguramiento de la herramienta web del *router*

Para configurar la contraseña de acceso a la web:

- ☑ Desde "*Web Browser*" en WirelessPC1 vuelva a la página de la herramienta web del *router* (http://192.168.1.1) y vaya a la sección "*Administration*".
- ☑ Para cambiar la contraseña predeterminada cambie la contraseña del *router* a "cisco" con el objetivo de asegurar el acceso a Linksys WRT300N. Observe que "*HTTP Web Utility Access*" ya está seleccionado de forma predeterminada.
- ☑ Haga clic en "*Save settings*".
- ☑ Después de aplicar la nueva contraseña, la página mostrará el siguiente mensaje: "*Settings are successful*".
- ☑ Para continuar, debajo de este mensaje aparece un enlace de inicio de sesión en la herramienta web para Linksys WRT300N. Haga clic en "*Continue*" y se abrirá una ventana emergente de inicio de sesión.
- ☑ Ingrese el nombre de usuario "admin" y utilice "cisco" como contraseña para volver a conectarse a las páginas de configuración web de Linksys WRT300N.

Octava Parte. Cambie el canal inalámbrico en uso

- ☑ Para acceder a Linksys WRT300N WRS1 mediante el explorador web: en WirelessPC1 haga clic en el "*Web Browser*" e ingrese la URL 192.168.1.1.
- ☑ Para autenticarse ingrese "admin" como nombre de usuario y "cisco" como contraseña.

Muchos puntos de acceso pueden seleccionar en forma automática un canal según el uso del adyacente. Algunos productos monitorean de manera continua el espacio de radio para ajustar la configuración de canal de modo dinámico en respuesta a los cambios del ambiente. En esta práctica, se forzará el punto de acceso para trabajar en el canal 6.

Muchos puntos de acceso pueden seleccionar en forma automática un canal según el uso del adyacente. Algunos productos monitorean de manera continua el espacio de radio para ajustar la configuración de canal de modo dinámico en respuesta a los cambios del ambiente. En esta práctica, se forzará el punto de acceso para trabajar en el canal 6.

Como los clientes son únicamente 802.11b/g, la banda de radio permanecerá como "*Standard-20MHz Channel*":

- ☑ En la página que se carga vaya a "Wireless" > "*Basic Wireless Setup*", ubique el área "*Standard Channel*" y cámbiela a 6-2.437GHz.
- ☑ Desplácese hacia abajo de la página y haga clic en "*Save Settings*".
- ☑ Cuando Linksys WRT300N admita las configuraciones establecidas aparecerá el siguiente mensaje en la ventana del explorador web: "*Settings are Successful*".
- ☑ Después, haga clic en "*Continue*" para volver a la página inalámbrica y cerrarla.

WirelessPC1 ahora debe estar asociada a WRS1, que es el dispositivo que controla el canal que se utiliza.

Novena Parte. Conexión WirelessPC2 a la red

- ☑ Desde WirelessPC2 vaya a la ficha "*Desktop*" y luego a "*PC Wireless*".
- ☑ Seleccione la ficha "*Connect*".
- ☑ De la lista de redes inalámbricas disponibles seleccione WRS1 y haga clic en "*Connect*".
- ☑ Aparecerá una pantalla en la que se solicita la clave WEP, donde ingresará "1234567890"; luego, elija "*Connect*".
- ☑ Haga clic en "*Link Information*" para verificar la conectividad con el punto de acceso.

Cuestionario

2.9.1 ¿Qué entiende por seguridad básica en una red inalámbrica?

2.9.2 Explique a detalle, porqué es importante la seguridad en la transmisión de datos en una red inalámbrica?

2.9.3 ¿Cuántos tipos de seguridad conoce?

2.9.4 Explique las características tiene cada tipo de seguridad.

Referencias

3GPP (s.f.). 3rd. *Generation Partnership Project (3GPP)*. Disponible en www.3gpp.org/about-3gpp, consultado en junio de 2017.

_____ (2006a). 3rd. *Generation Partnership Project TS 23.228: IP Multimedia Subsystem*. Disponible en http://www.3gpp.org/ftp/tsg_sa/tsg_sa/TSGS_11/Docs/PDF/SP-010121.pdf, consultado en abril de 2017.

_____ (2006b). *The Internet Engineering Task Force. RFC 4566: SDP: Session Description Protocol*. Disponible en http://www.ietf.org/rfc/rfc4566.txt?number=4566, consultado en mayo de 2017.

Abramson, N. (2000). "Internet access using VSAT" en *IEEE Community Magazine*, (38): pp. 60-68.

Academia de Networking de Cisco Systems (2004). *Serie Cisco Systems CCNA*. USA: Cisco Press, 3rd. ed.

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems*. New York: John Wiley & Sons.

Berghel, H. L. (2001). "Cyber privacy in the new millennium" en *IEEE Computer*, (34): pp. 132-134.

Berners-Lee, T. (1990). *Inventing the Web: Christmas Baby. Seeing the Picture*.

_____ (2009). Pre-W3C Web and Internet Background. *World Wide Web Consortium*.

Berners-Lee, T.; Cailliau, A.; Loutonen, A.; Nielsen, H. F. and Secret, A. (1994). "The World Wide Web" en *Community of the ACM*, (37): pp. 76-82.

Berners-Lee, T. *et. al*. (2004). *Architecture of the World Wide Web, Volume One*. Version 20041215. W3C.

Bertsekas, D. and Gallager, R. (1992). *Data networks*. Englewood Cliffs, New Jersey: Prentice-Hall.

Bhatti, S. N. and Crowcroft, J. (2000). QOS sentitive flows: Issues in IP packet handling. *IEEE Internet Computing*, (4): pp. 48-57.

Black, U. (1997). *Redes de computadoras. Protocolos, normas e interfaces*. México: Alfaomega Grupo Editor, 2a. ed.

Boggs, D.; Mogul, J. and Kent, C. (1988). "Measured capacity of an Ethernet: Myths and reality" en *Procedures SIGCOMM ´88 Conference*, pp. 222-234.

Bounoure, Francois, *et al*., (2006). *Laboratorio de redes: Session Initiation Protocol*. Argentina: Universidad de Buenos.

Braden, R. (1989). "Requirements for Internet hosts-communications layers" en *RFC 1 122*. USA.

Bray, T.; Paoli, J.; Sperberg-McQueen, C.; Maler, E.; Yergeau, F. and Cowan, J. (2006). "Extensible Markup Language (XLM) 1.1" en *Recommendation of the W3C*.

Burleigh, S.; Hooke, A.; Torgerson, L.; Fall, K.; Cerf, V.; Durst, B.; Scott, K. and Weiss, H. (2003). "Delay-tolerant networking: An approach to interplanetary Internet" en *IEEE Community Magazine*, (41): pp. 128-136.

Cisco Sys. (2010a). *Cisco visual networking index: Forecast and methodology*. USA: Cisco Systems.

_____ (2010b). *Resource Reservation Protocol*. Disponible en https://www.cisco.com/c/en/us/products/ios-nx-os-software/resource-reservation-protocol-rsvp/index.html, consultado en mayo de 2017.

Clark, D. D. (1988). "The design philosophy of the DARPA Internet protocols" en *Procedures SIGCOMM ´88 Conference*, *ACM*, pp. 106-114.

Clark, D. D.; Jacobson, V.; Romkey, J. and Salwen, H. (1989). "An analysis of TCP processing over-head" en *IEEE Community Magazine*, (27): pp. 23-29.

Clark, D. D.; Shenker, S. and Zhang, L. (1992). "Supporting real-time applications in an integrated services packet network" en *Procedures SIGCOMM ´92 Conference ACM*, pp. 14-26.

Comer, D. E. (2005). *Internetworking with TCP/IP*. Englewood Cliffs, New Jersey: Prentice-Hall, 5th. ed.

_____ (2007). *The Internet book*. Englewood Cliffs, New Jersey: Prentice-Hall, 4th. ed.

Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública en Argentina (s.f.). *Manual de Seguridad en Redes (ArCERT)*. Disponible en http://www.psicosocial.net/grupo-accion-comunitaria/centro-de-documentacion-gac/areas-y-poblaciones-especificas-de-trabajo/desgaste-y-seguridad-para-activistas/540-manual-de-seguridad-en-redes-informaticas/file, consultado en junio de 2017.

Croft, B. (2005). *RFC 951: Bootstrap Protocol*. USA: FRC.

Crovella, M. and Krishnamurty, B. (2006). *Internet measurement*. New York: John Wiley & Sons.

Chase, J. S.; Gallatin, A. J. and Yocum, K. G. (2001). "End system optimization for high-speed TCP" en *IEEE Community Magazine*, (39): pp. 68-75.

Chen, S. and Nahrstedt, K. (1998). "An overview of QOS routing for next-generation networks" en *IEEE Network Magazine*, (2): pp. 64-69.

Davie, B. and Farrel, A. (2008). *MPLS: Next generation*. San Francisco, California: Morgan Kaufmann.

Davie, B. and Rekhter, Y. (2000). *MPLS technology and applications*. San Francisco, California: Morgan Kaufmann.

Davies, J. (2008). *Understanding IPv6*. Redmon, WA: Microsoft Press.

Day, J. D. and Zimmermann, H. (1983). "The OSI Reference Model" en *Procedures of the IEEE*, (71): pp. 1 334-1 340.

Deering, S. E. (1993). "SIP: Simple Internet Protocol" en *IEEE Network Magazine*, (7): pp. 16-28.

Deering, S. E. and Cheriton, D. (1990). "Multicast routing in datagram networks and extended LAN" en *ACM Transactions on Computer Systems*, (8): pp. 85-110.

Demers, A.; Keshav, S. and Shenker, S. (1990). "Analysis and simulation of a fair queueing algorithm" en *Internetworking: Research and Experience*, (1): pp. 3-26.

Devarapalli, V.; Wakikawa, R.; Petrescu, A. and Thubert, P. (2005). "Network mobility (NEMO) basic support protocol" en *RFC 3 963*.

Donahoo, M. and Calvert, K. (2009). *TCP/IP sockets in C*. San Francisco, California: Morgan Kaufmann, 2nd ed.

_____ (2008). *TCP/IP sockets in Java*. San Francisco, California: Morgan Kaufmann, 2nd. ed.

Donaldson, G. and Jones, D. (2001). "Cable TV broadband network architectures" en *IEEE Community Magazine*, (39): 122-126.

Ericsson (2007). *Introduction to IMS, White Paper*. Disponible en http://cse.iitkgp.ac.in/~pallab/mob_com/Ericsson_Intro_to_IMS.pdf, consultado en junio de 2017.

Fall, K. (2003). "A delay-tolerant network architecture for challenged Internets" en *Procedures SIGCOMM 2003 Conference ACM*, pp. 27-34.

Faloutsos, M.; Faloutsos, P. and Faloutsos, C. (1999). "On power-law relationships of the Internet topology" en *Procedures SIGCOMM ´99 Conference ACM*, pp. 251-262.

Farrell, S. and Cahill, V. (2007). *Delay and disruption tolerant networking*. London: Artech House.

Fenner, B.; Handley, M.; Holbrook, H. and Kouvelas, I. (2006). Protocol Independent Multicast-Sparse Mode (PIM-SM). *RFC 4 601*.

Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Berners-Lee´s, T. (1999). *Hypertext Transfer Protocol-HTTP/1.1. Request for comments 2616*. USA: Information Sciences Institute.

Ford, W. and Baum, M. S. (2000). *Secure electronic commerce*. Upper Saddle River, New Jersey: Prentice-Hall.

Fouli, K. and Maler, M. (2009). "The road to carrier-grade Ethernet" en *IEEE Community Magazine*, S30-S38.

García, T. (2001). *Redes para proceso distribuido*. México: Alfaomega Grupo Editor, 2a. ed.

Gast, M. (2005). 802.11 *Wireless networks: The definitive guide*. Sebastopol, California: O´Reilly.

Gershenfeld, N.; Krikorian, R. and Cohen, D. (2004). "The Internet of things" en *Scientific American*, (291): pp. 76-81.

Goode, B. (2002). "Voice over Internet Protocol" en *Procedures of the IEEE*, (90): 1 495-1 517.

Grayson, M.; Shatzkamer, K, and Wainner, S. (2009). *IP design for mobile networks*. Indianapolis: Cisco Press.

Ha, S.; Rhee, I. and Lisong, X. (2008). CUBIC: A new TCP friendly high speed TCP variant. *SIGOPS Operating Systems Review*, (42): pp. 64-74.

Hallivuori, V. (2000). *Real Time Transport Protocol (RTP) Security*. Helsinki, Finlandia: University of Technology.

Halsall, F. (1988). *Comunicación de datos, redes de computadoras y sistemas abiertos*. México: Pearson Education, 4a. ed.

Harte, L.; Kellogg, S.; Dreher, R. and Schaffnit, T. (2000). *The comprehensive guide to wireless technology*. Fuquay-Varina, NC: APDG Publishing.

Hecht, J. (2005). *Understanding fiber optics*. Upper Saddle River, New Jersey: Prentice-Hall.

Held, G. (2010). *A practical guide to content delivery networks*. Boca Ratón, Florida: CRC Press.

Hiertz, G.; Denteneer, D.; Stibor, L; Zang, Y.; Costa, X. and Walke, B. (2010). "The IEEE 802.11 universe" en *IEEE Community Magazine*, (48): pp. 62-70.

Hoe, J. (1996). "Improving the start-up behavior of a congestion control scheme for TCP" en *Procedures SIGCOMM ´96 Conference ACM*, pp. 270-280.

Hu, Y. and Li, V. O. K. (2001). "Satellite-based Internet: A tutorial" en *IEEE Community Magazine*, (30): pp. 154-162.

Huitema, C. (1999). *Routing in the Internet*. Englewood Cliffs, New Jersey: Prentice Hall, 2nd. ed.

International Telecommunications Union (ITU) (2005a). *ITU Internet reports 2005: The Internet of things*. Ginebra, Switzerland: ITU.

_____ (2005b). *Measuring the information society: The ICT development index*. Ginebra, Switzerland: ITU.

Jacobson, V. (1990). "Compressing TCP/IP headers for low speed serial links" en *RFC 1 144*. USA.

Jain, R. and Routhier, S. (1986). "Packet trains-measurements and a new model for computer network traffic" en *IEEE Journal on Select Areas in Communications*, (6): pp. 986-995.

Joel, A. (2002). "Telecommunications and the IEEE communications society" en *IEEE Community Magazine, 50th Anniversary Issue*, pp. 6-14, 162-167.

Johnson, D.; Perkins, C. and Arkko, J. (2004). "Mobility support in IPv6" en *RFC 3 775*. USA.

Kaufman, C.; Perlman, R. and Speciner, M. (2002). *Network security*. Englewood Cliffs, New Jersey: Prentice-Hall, 2nd. ed.

Koodli, R. and Perkins, C. E. (2007). *Mobile internetworking with IPv6*. New York: John Wiley & Sons.

Krishnamurti, B. and Rexford, J. (2001). *Web protocols and practice*. Boston, Massachusetts: Addison-Wesley.

Kurose, J. F. and Keith, W. R. (2005). *Computer Networking: A top-Down Approach Featuring the Internet*. USA: Addison Wesley, 3th. ed.

Labovitz, C.; Ahuja, A.; Bose, A. and Jahanian, F. (2001). "Delayed Internet routing convergence" en I*EEE/ACM Transactions on Networking*, (9): pp. 293-306.

Le Point (2010). Le Web a até inventé en France. Paris, France.

Lewis, M. (2006). *Comparing, designing and deploying VPN*. Indianapolis, IN: Cisco Press.

Lin, S. and Costello, D. (2004). *Error control coding*. Upper Saddle River, New Jersey: Pearson Education.

Long, T. (2012). Aug. 7, 1991: *Ladies and Gentlemen, the World Wide Web*. Disponible en https://www.wired.com/2012/08/aug-7-1991-ladies-and-gentlemen-the-world-wide-web/, consultado en mayo de 2017.

Lubacz, J.; Mazurczyk, W. and Szczypiorski, K. (2010). "Voice over IP" in *IEEE Spectrum*, pp. 42-47.

Mani, M. and Crespi, N. (2007). *Adopting IMS in Wi-Fi Technology*. Disponible en http://portal.acm.org/citation.cfm?id=1378117, consultado en junio de 2017.

Maufer, T. A. (1999). *IP fundamentals*. Upper Saddle River, New Jersey: Prentice-Hall.

Metz, C. (2001). "Interconnecting ISP networks" en *IEEE Internet Computing*, (5): pp. 74-80.

Munasighe, K. and Jamalipour, A. (2008). *Interworking of WLAN-UMTS Netwoks: An IMS based Pltaform for Session Mobility*. USA: IEEE.

Neuman, C. and Ts´O, T. (1994). "Kerberos: An authentications service for computer networks" en *IEEE Community Magazine*, (32): pp. 33-38.

Palais, J. C. (2004). *Fiber optic communications*. Englewoods Cliffs, New Jersey: Prentice-Hall.

Parameswaran, M.; Susarla, A. and Whinston, A. B. (2001). "P2P networking: An information sharing alternative" en *IEEE Computer*, (34): pp. 31-38.

Pechuán, Luis Miralles (2010). *El nuevo sistema multimedia conocido como IMS que adoptarán las redes UMTS*. Universidad de Valencia. Disponible en https://www.researchgate.net/publication/316214714_El_nuevo_sistema_multimedia_conocido_como_IMS_que_adoptaran_las_redes_UMTS?channel=doi&linkId=58f6356da6fdcc738a11df22&showFulltext=true, consultado en junio de 2017.

Perkins, C. E. (1998). *Mobile IP design principles and practices*. Upper Saddle River, New Jersey: Prentice-Hall.

_____ (2001). *Ad hoc networking*. Boston, Massachusetts: Addison-Wesley.

_____ (2002). IP mobility support for IPv4. *RFC 3 344*.

_____ (2003). *Audio and video for the Internet*. Boston, Massachusetts: Addison-Wesley.

Perlman, R. (1985). "An algorithm for the distributed computation of a spanning tree in an extended LAN" en *Procedures SIGCOMM ´85 Conference ACM*, pp. 44-53.

_____ (2000). InterConnections. Boston, Massachusetts: Addison-Wesley.

Piscitello, D. M. and Chapin, A. L. (1993). *Open systems networking: TCP/IP and OSI*. Boston, Massachusetts: Addison-Wesley.

Poikselka, Miikka, *et al.*, (2006). *The IMS IP multimedia concepts and services*. USA: John Wiley & Sons Ltd, 2nd.

Polo, L. (2003). *World Wide Web technology architecture: A conceptual analysis*. USA: New Devices.

Postel, J. (1981). "Internet control message protocols" en *RFC 792*. USA.

Quittner, J. (2010). Tim Berners-Lee. "Time 100 People of the Century" en *Time Magazine*.

Rabin, J. and McCathienevile, C. (2008). "Mobile web best practices 1.0" en *Recommendation of the W3C*.

Ramaswami, R.; Kumar, S. and Sasaki, G. (2009). *Optical networks: A practical perspective*. San Francisco, California: Morgan Kaufmann, 3th. ed.

Real Academia Uruguaya (s.f.). *Introducción al IPv6*. Disponible en http://www.rau.edu.uy/ipv6/queesipv6.htm, consultado en mayo de 2017.

Ronan, John, Sasitharan Balasubramaniam, Adnan K Kiani, Wenbing Yao. (s/a). "On the use of SHIM6 for mobility support" en *IMS Networks*.

Salazar, J. E., *et al.*, (2002). *Diffserv como solución a la provisión de Q_0S en la Internet*. España: Universidad Carlos III de Madrid.

Simpson, W. (2008). *Video over IP*. Burlington, Massachusetts: Focal Press.

Spurgeon, C. E. (2000). Ethernet: *The definitive guide*. Sebastopol, California: O´Reilly.

Stallings, W. (2010). *Comunicaciones y redes de computadoras*. México: Pearson Educación, 9a. ed.

Stevens, W. R. (1994). *TCP/IP illustrated: The protocols*. Boston, Massachusetts: Addison-Wesley.

Tanenbaum, A. S. (2007). *Modern operating systems*. Upper Saddle River, New Jersey: Prentice-Hall, 3rd. ed.

Tanenbaum, A. S. and Van Steen, M. (2007). *Distributed systems: Principles and paradigms*. Upper Saddle River, New Jersey: Prentice-Hall.

Telefónica (s.f.). *Evolución al dominio IMS*. Disponible en http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/capitulo_12.pdf, consultado en junio de 2017.

The Internet Engineering Task Force (s.f.). "RFC 2 205" en *Resource ReSerVation Protocol (RSVP)*. Disponible en http://www.ietf.org/rfc/rfc2205.txt?number=2205, consultado en junio de 2017.

_____ (s.f.). RFC 2 748. The COPS (*Common Open Policy Service*) Protocol. Disponible en http://www.ietf.org/rfc/rfc2748.txt?number=2748, consultado en abril de 2017.

_____ (s.f.). "RFC 3 550" en *RTP: A Transport Protocol for Real-Time Applications*. Disponible en http://www.ietf.org/rfc/rfc3550.txt, consultado en abril de 2017.

Terán Pérez, D. M. (2010). *Redes convergentes. Diseño e implementación*. México: Alfaomega Grupo Editor.

_____ (2012). *Introducción a la computación cuántica para ingenieros*. México: Alfaomega Grupo Editor.

_____ (2014). *Administración estratégica de la función informática*. México: Alfaomega Grupo Editor.

_____ (2016). *Introducción a la ingeniería*. México: Alfaomega Grupo Editor.

Tompros, S. and Denazis, S. (2007). *Interworking of heterogeneous access networks and QoS provisioning via IP multimedia core networks*. Universidad de Patras. Disponible en: http://www.sciencedirect.com/science/article/pii/S1389128607002356, consultado en junio de 2017.

Wittenburg, N. (2009). *Understanding voice over IP technology*. Clifton Park, New York: Delmar Cengage Learning.

World Wide Web (2009). *Proposal for a hypertexts Project.* USA.

_____ (2010). *Proposal for a Hyper Text Project.* USA.

Znaty, S.; Dauphin, J. L. and Geldwerth, R. (s.f.). *IP Multimedia Subsystem: Principios y arquitectura. EFORT*. Disponible en http://www.efort.com/media_pdf/IMS_ESP.pdf, consultado en junio de 2017.

_____ SIP: *Session Initiation Protocol effort*. Disponible en http://www.efort.com/media_pdf/IMS_ESP.pdf, consultado en mayo de 2017.

Seguridad informática

Escribir saca la parte más "oscura" del ser humano;
la religión saca la parte más "noble" de las personas. Por eso… ¡escribe!
Sí, siempre, siempre, ¡escribe!

Eusebio Ruvalcaba

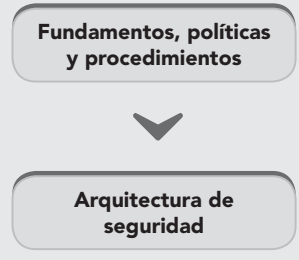
Reflexione y responda las siguientes preguntas:

- ¿Qué se lleva a cabo en la seguridad en una red de computadoras?
- ¿Por qué es importante la seguridad en una red de computadoras?
- ¿En qué consiste la seguridad en una red de computadoras?
- ¿Cómo funciona la arquitectura de gestión de la seguridad en una red de computadoras?

Después de estudiar este capítulo, el lector será capaz de:

- Entender qué es la seguridad en una red de computadoras.
- Comprender la importancia de la administración de la seguridad en una red de computadoras.
- Establecer en qué consiste la administración de la seguridad en una red de computadoras.
- Explicar el funcionamiento de la arquitectura de gestión de la seguridad en una red de computadoras.

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:



3.1 Introducción

En el entorno de las redes de computadoras, un objetivo prioritario es entender la situación de un medio ambiente interconectado en el ámbito de los negocios para fomentar la seguridad informática; es decir, en este punto se debe presentar a los usuarios/clientes del sistema el panorama general, considerando las implicaciones económicas y estratégicas para las empresas actuales.

Igualmente, es primordial identificar los aspectos relevantes sobre la vulnerabilidad de los sistemas informáticos y conocer las funciones, métodos y procedimientos que se emplean para la creación de los esquemas de seguridad para que sea posible actualizar y formar especialistas en seguridad informática que desarrollen habilidades en el planteamiento de soluciones factibles de administración, diseño, gestión y operación de sistemas de seguridad.

Muchos son los peligros a los que está expuesta una organización. En la última década los delitos informáticos han acaparado atención especial ocasionando pérdidas económicas multimillonarias: en 2013, se batió un triste récord de generación de *software* nocivo con cerca de 30 millones de nuevas muestras.

Por otro lado, datos de ese mismo año establecieron que las organizaciones recibieron un ataque de *software* malicioso cada tres segundos; lo cual representa 300 000 ataques diarios de este tipo a nivel mundial; cifras que han aumentado hasta la actualidad (Rico, 2014).

Hoy en día, las personas que participan en estos actos delictivos son cada vez más profesionales; además, cuentan con significativos cursos financieros y una amplia experiencia en Tecnologías de la Información y de las Comunicaciones (TIC), herramientas que los hace capaces de atacar a las organizaciones sin discriminación alguna, sin importar el tamaño o el giro de ésta. Hace años, los ataques eran generalizados y su objetivo radicaba en causar sólo daño al equipo de cómputo o la red de computadoras.

En la actualidad, el interés principal de los delincuentes cibernéticos está enfocado al robo de información secreta o confidencial de una organización específica (lo que se ha llamado *ataque dirigido*, considerado uno de los tipos más peligrosos de amenazas). La filtración de esa información estratégica, confidencial o secreta genera pérdidas importantes.

Según información recopilada por analistas de B2B International y Kaspersky, dichos incidentes pueden llegar a costarle a una organización hasta dos millones de euros (€) en promedio. De esa cantidad, 1.7 millones, se relacionan al incidente en forma de pérdidas derivadas de filtraciones críticas de datos, interrupción de la operación empresarial y gastos por servicios especializados de reparación.

Además, las organizaciones enfrentan un costo aproximado de 200 000 € por las medidas que deben implementar para impedir que esas acciones de intrusión y robo de información se presenten al actualizar *software* y *hardware*, contratar y capacitar al personal. Por su lado, las pérdidas provocadas por ataques dirigidos a las pequeñas y medianas empresas (PyME) son notablemente más bajas, aunque el

monto financiero sigue siendo alto: alrededor de 88 000 €, de los cuales cerca de 68 000 € están destinados a la reparación del ataque, mientras que el resto se dirige a la prevención de posibles daños en el futuro inmediato.

Ahora, la pérdida de información no es el único daño provocado por el *software* malicioso; también se deben sumar la disminución de productividad dado el tiempo que le toma a los colaboradores de la organización esperar que los equipos funcionen mejor cuando son "atacados" y el posible daño a la infraestructura industrial cuando ésta cuenta con sistemas de control y de operación que se conectan a la red de datos pública de Internet (Rico, 2014).

Para los criminales cibernéticos, las empresas que se convierten en el blanco perfecto son aquellas que no protegen sus recursos informáticos, ni colaboradores tanto dentro como fuera de la organización. En especial, las instituciones donde el uso de dispositivos inteligentes ha crecido sin control ni se han implantado estrategias y medidas de seguridad; por ejemplo, la policía cibernética mexicana ha recibido más de 19 mil denuncias relacionadas con algún tipo de amenaza informática, de las cuales 55% corresponde a reportes de *software* malicioso y 40% se relaciona con el reclamo de fraudes derivados al comercio electrónico. La Ciudad de México, así como las regiones de Puebla, Nuevo León, Jalisco y el Estado de México se encuentran entre las entidades mexicanas que han registrado la mayor cantidad de estos actos delictivos (Rico, 2014).

Por otro lado, las tendencias en evolución de la movilidad y la computación en la nube (*Cloud Computing*) están preparando el entorno informático para nuevos tipos y clases de ataques que no se habían concebido hasta hace algunos pocos años, y que, por ende, requieren de nuevas y efectivas técnicas para protegerse. Los teléfonos inteligentes, las tabletas y otros dispositivos móviles se han convertido en herramientas esenciales de la productividad organizacional, pero igual, se han vuelto elementos vulnerables y de alto peligro para perder información valiosa por descuido o por la intrusión de agentes externos.

A medida de que el rendimiento y las funciones en los lugares de trabajo, educación y ocio, se aproximan al uso de las computadoras de escritorio y portátiles, se hace todavía más fácil diseñar y propagar los programas maliciosos para dichos dispositivos móviles, pues, de acuerdo con un estudio realizado por Kaspersky en 2013, se detectaron 145 000 nuevos programas de índole maliciosa tan solo para dispositivos móviles (el doble que se reportaron en 2012) cuyo principal objetivo era robar dinero a los usuarios.

Por eso es muy importante destacar que el crecimiento de la publicidad como amenaza para los usuarios móviles se triplicó en el último año, donde uno de cada cinco avisos web en los *smartphones* redirecciona hacia programas maliciosos, según lo reportó la empresa Blue Coat Systems, la cual indica que los anuncios web han superado incluso a la pornografía como la forma más común en que las personas se encuentran ante una amenaza de *software* malicioso aunque ésta no alcanza ni 1% de todo el contenido solicitado, pero sí representa más del 16% de todos los ataques. En comparación, los anuncios de Internet registran 12% del contenido solicitado con 20% de tasa de infección.

Los datos significan que hoy en día el usuario es el eslabón más débil que existe en la cadena de la seguridad porque los sistemas protegen a los teléfonos, pero no a las personas que inadvertidamente dan acceso a los ataques a través de trucos burdos y bastante trillados como el otorgamiento de "premios" o la descarga de aplicaciones no autorizadas por tiendas oficiales.

Internet denominada también como *la red* o *red de redes*, se ha convertido en un fenómeno que ha revolucionado la sociedad en la última década. Desde la aparición de la televisión, primero en blanco y negro, luego a color, no se había observado ningún otro hecho social que evolucione tan rápido. Hoy en día, la mayoría de la población en el mundo depende de la información que radica y se genera en las computadoras, las cuales ya no se encuentran aisladas como a finales de los años 80 y principios de los 90 del siglo pasado y que, por el contrario, hoy dependen de una conexión para comunicarse. Por otro lado, el avance con las redes ha permitido solucionar problemas y obtener ventaja competitiva de los sistemas que ayudan a manipular, procesar y organizar la información (Rico, 2014).

En la actualidad, tanto las organizaciones como las personas que utilizan una computadora envían y reciben correos electrónicos; comparten información de manera local o a nivel mundial; realizan operaciones y transacciones; ofrecen productos, bienes y servicios y encuentran soluciones a sus requerimientos. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los intrusos; por ello se debe tener una serie de precauciones para evitar que alguien no deseado busque datos relevantes en la información de las organizaciones y las personas como presa fácil de extorsiones, fraudes y pérdidas irreparables (Anderson, 2001).

De los muchos factores que han convergido en este nuevo fenómeno para catapultarlo de forma masiva a la sociedad actual, se pueden destacar tres principales:

- La expansión de los computadoras en todos los ámbitos de la sociedad ha contribuido a informatizar casi cualquier aspecto de la vida.
- La rápida evolución de la tecnología de las comunicaciones ha acelerado aún más el despegue de Internet.
- El carácter universal de Internet, que permite la conectividad global y permanente de todo el planeta de forma económica, práctica e instantánea, la red se ha convertido en una herramienta imprescindible para cualquier tipo de comunicación.

En consecuencia, se calcula que cada día, cientos de millones de personas en todo el mundo utilizan Internet como parte de su trabajo y ocio, de igual forma que en cualquier otro servicio utilizado por gran cantidad de personas (como el sistema de transporte colectivo o las carreteras), la seguridad es un factor básico en cualquier sistema computarizado.

Desde un punto de vista sociológico, en cualquier grupo social un cierto porcentaje de la población posee conductas malévolas. En 2012, Internet alcanzó más de 500 millones de computadoras conectadas, sumando un total estimando de un billón de usuarios en todo el mundo. Si tan sólo 1% de la población pertenece a dicho sector, se tiene casi un millón de posibles atacantes (Anderson, 2001).

3.2 Principios y fundamentos de la teoría de la seguridad informática

La seguridad informática o seguridad de las tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y de los datos contenidos o circulantes en ella; para esto, existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información (Lockhart, 2007). Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de una organización a otra. De manera independiente, cualquiera con una red debe tener una política de seguridad que se dirija a la conveniencia y coordinación (Burnett y Paine, 2001).

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

Infraestructura computacional. Se considera la parte fundamental para el almacenamiento y gestión de la información, así como para el excelente desarrollo de la organización. La función de la seguridad informática en esta área es *velar que los equipos funcionen adecuadamente, así como anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, errores en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.*

Usuarios. Son las personas que gestionan la información por medio de la estructura tecnológica y la zona de comunicaciones. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y que ésta no sea vulnerable.

Información. Se utiliza y reside en la infraestructura computacional.

Por su parte, se concibe como seguro a aquello que resultare infalible, inatacable, libre y exento de todo peligro, daño o riesgo (figura 3.1). La seguridad en los sistemas de cómputo existe, pero no puede ser absoluta; no obstante, es posible que sea elevada a niveles insospechados y para ello, se parte de cinco elementos esenciales a tener en cuenta:

- ¿Cuáles son los puntos débiles del sistema informático a proteger?
- ¿Cuánto tiempo deberá protegerse un dato o la información?
- Las medidas de control se implementan para que tengan un comportamiento efectivo y eficiente para que sean fáciles de usar y apropiadas al medio.
- Ningún sistema de control resulta efectivo hasta que surge la necesidad de aplicarlo.
- Los usuarios deben estar conscientes de las posibles fallas de los sistemas y de la necesidad de asegurarlos.

Como puede verse, los cuatro primeros puntos son meramente técnicos; pero el quinto es el más importante, por considerarse de índole social (Biham y Shamir, 1997). Con base en esto, se toman en cuenta los siguientes principios para el desarrollo de la seguridad informática:

- **Principio del acceso más fácil.** El intruso utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque; para ello existirá una diversidad de

frentes desde los que puede producirse un ataque, lo cual dificulta el análisis de riesgos, ya que el delincuente aplica la filosofía de ataque hacia el punto más débil.

- **Principio de la caducidad del secreto.** Los datos confidenciales deben protegerse sólo hasta que el secreto pierda su valor. Se habla, por lo tanto, de la caducidad del sistema de protección como el tiempo en el que debe mantenerse la confidencialidad. Esto llevará a la fortaleza del sistema de cifrado.
- **Principio de la efectividad de las medidas tomadas.** Las medidas de control se implementan para ser utilizadas de forma efectiva; por lo cual deben ser eficientes, fáciles de usar y apropiadas al medio; es decir, que funcionen en el momento oportuno optimizando los recursos del sistema y que pasen inadvertidas para el usuario.

Lo más importante a recordar es que ningún sistema de control resulta efectivo hasta que surge la necesidad de aplicarlo, lo que es uno de los grandes problemas de la seguridad informática.

Figura 3.1 Arquitectura OSI-NM

Una vez analizados los principios de la seguridad informática, se considera oportuno hacer referencia a los fundamentos sobre los que descansa la misma; así como los diferentes enfoques que hacen posible su fácil estudio; estos son:

Teoría de la información. Conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que se deben proteger ante las amenazas del entorno durante su transmisión o almacenamiento usando, entre otras cosas, las técnicas criptográficas. La teoría de la información mide la cantidad de datos que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.

Teoría de los números. Matemáticas discretas en las que se sustentan las operaciones de cifra.

Teoría de la complejidad algorítmica: Permitirá conocer si un algoritmo cuenta con fortaleza para tener así una idea de su vulnerabilidad computacional.

Para su estudio la seguridad informática se puede dividir en:

- Seguridad física que incluye la protección del sistema ante las amenazas físicas, planes de contingencias, control de acceso físico, políticas de seguridad, normativas, etcétera.
- Seguridad lógica implementa la protección de la información en su propio medio con el apoyo del enmascaramiento usando técnicas de criptografía y protocolos de autenticidad entre el cliente y el servidor.

3.3 Objetivos de la seguridad de la información e informática

La reducción o eliminación de riesgos asociados a cierta información son el objetivo de la seguridad de la información y la seguridad informática (figura 3.2). Los objetivos que persiguen son proteger la confidencialidad, la integridad y la disponibilidad de la información; sin embargo, en la práctica, no son exactamente lo mismo, existiendo algunas diferencias sutiles que radican en el enfoque, las metodologías utilizadas y las zonas de concentración.

Figura 3.2 Objetivos de la seguridad informática

La seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde los datos es el activo primordial; éstas deben tener como punto inicial y primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo; es decir, que ayuden a proteger y salvaguardar tanto la información, así como los sistemas que la almacenan y administran (Fernández, 2008). La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, hospitales y empresas privadas con información confidencial sobre empleados, clientes, productos, investigación y situación financiera.

A continuación, se establecen las características más relevantes de los conceptos involucrados en la seguridad de la información e informática (Terán Pérez, 2013):

> **Confidencialidad.** La propiedad que impide la divulgación de datos a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellos individuos que cuenten con la debida autorización; por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta sea transmitido desde el comprador al comerciante y de éste hacia una red de procesamiento de transacciones; en dicho caso, el sistema intenta hacer valer la confidencialidad mediante el cifrado del número

de la tarjeta y los datos que contiene la banda magnética o del chip durante el uso de los mismos. Si una parte no autorizada obtiene el número de la tarjeta, se ha producido una violación de la confidencialidad.

Integridad. La propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es mantener con exactitud la información como fue generada, sin ser manipulada o alterada por personas o procesos ajenos. La violación de la integridad se presenta cuando un empleado, un programa o un proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad.

Disponibilidad. La característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. En resumen, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad usados y los canales de comunicación protegidos que se emplean para acceder a ella deben estar funcionando de forma correcta. La alta disponibilidad de los sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de la arquitectura de sistemas y de sus actualizaciones. Por otro lado, garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio.

La disponibilidad es también variada en el sentido de que existen diversos mecanismos para cumplir con los niveles de servicio que se requiera; estos se implementan en la infraestructura tecnológica, en los servidores de correo electrónico, en las bases de datos, en los sitios y páginas web, mediante el uso de clusters o arreglos de discos, en los equipos en alta disponibilidad a nivel de red, en los servidores espejo, en la replicación de los datos, en las redes de almacenamiento (SAN), en los enlaces redundantes, etcétera. La gama de posibilidades dependerá de lo que se quiera proteger y del nivel de servicios que se quiera proporcionar.

Autenticación. Propiedad que permite identificar al generador de la información. En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y de contraseñas de acceso.

No repudio. Proporciona protección contra la interrupción por parte de alguna de las entidades implicadas en la comunicación. Este servicio está estandarizado en la norma ISO-7498-2 y se divide en las siguientes categorías:

- No repudio de origen. El emisor no puede negar que envió un mensaje o información porque el receptor recibe una prueba infalsificable del origen del envío. En este caso, la prueba es creada por el propio emisor y la recibe el destinatario.
- No repudio de destino. El receptor no puede negar que recibió el mensaje o la información porque el emisor tiene la prueba de que el destinatario legítimo de un envío realmente lo recibió. En este caso, la prueba irrefutable la crea el receptor y la recibe el emisor.

Lo anterior queda definido según la recomendación X.509 de la UIT-T, es un servicio que suministra la prueba de la integridad y del origen de los datos; ambas acciones (enviar y recibir) consisten en una relación infalsificable que puede ser verificada por un tercero en cualquier momento.

Desde la perspectiva del equipo de seguridad, no importa si ocurre una violación o apertura, pues esas acciones son una parte eventual de cuando se hacen negocios usando un método de poca confianza como es Internet, sino más bien cuando ocurre. El aspecto positivo de entender la inevitabilidad de una violación a los sistemas es que permite al equipo de seguridad desarrollar un curso de acciones para minimizar los daños potenciales. Al combinar un curso de acciones con la experiencia le posibilita al equipo responder a condiciones adversas de una manera formal y oportuna (Stinson, 2002). El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata para detener o minimizar el incidente
- Investigación del suceso
- Restauración de los recursos afectados
- Reporte del hecho a los canales apropiados

La respuesta a los incidentes debe ser decisiva y ejecutarse con rapidez debido a que hay poco espacio para los errores; es crítico que se efectúen prácticas de emergencia y se midan objetivamente los tiempos de respuesta. De esta forma, es posible desarrollar e implantar una metodología que fomente la velocidad y la precisión en la solución de problemas de seguridad de la información, minimizando el impacto de la no disponibilidad de los recursos, bienes y servicios con la reducción del daño potencial a la organización causado por el sistema en riesgo o peligro, ya sea real o latente. Un plan de respuesta a incidentes de este tipo tiene un número de requerimientos, que incluyen:

- Un equipo de expertos locales dedicados a las emergencias de computación que se presentan in situ.
- Una estrategia legal revisada y aprobada.
- Un soporte financiero de la compañía.
- Un soporte ejecutivo de la gerencia superior.
- Un plan de acción factible y aprobado.
- Recursos físicos como el almacenamiento redundante, sistemas en espera y servicios de respaldo.

3.4 Políticas de seguridad

Una política de seguridad es "un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales qué está y qué no se permite en el área de seguridad durante la operación general del sistema" (Huerta Villalón, s.f.).

Por otro lado, la RFC 1 244 establece una política de seguridad como "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán".

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se determinan las medidas a tomar para proteger la seguridad del sistema; pero ante todo, "una política de seguridad es una forma de comunicarse con los usuarios. [Por lo que] Siempre hay que tener en cuenta que la seguridad comienza y termina con las personas" (Spafford, 2000); por lo tanto, ésta debe:

> **Ser holística (cubrir todos los aspectos relacionados con la misma).** No tiene sentido proteger el acceso con una puerta blindada, si a ésta no se ha cerrado con llave.
>
> **Adecuarse a las necesidades y recursos.** No es necesario adquirir una caja fuerte para proteger un lápiz.
>
> **Ser atemporal.** El tiempo en el que se aplica no debe influir en la eficacia y eficiencia.
>
> **Definir estrategias y criterios generales a adoptar en distintas funciones y actividades.** En donde se conocen las alternativas ante circunstancias repetidas.
>
> **Cualquier política de seguridad debe considerar los elementos claves de seguridad .** La integridad, disponibilidad, privacidad, control, autenticidad y utilidad.
>
> **No debe tratarse de una descripción técnica de mecanismos de seguridad ni de una expresión legal que involucre sanciones a las conductas de los empleados.** Es, más bien, una descripción de lo que se desea proteger y el por qué de ello.

Hoy es imposible hablar de un sistema 100 % seguro, porque el costo de esto sería muy alto, debido a que todos los sistemas (físicos y lógicos) son vulnerables.

Algunas organizaciones gubernamentales y no gubernamentales, nacionales y también internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de éstas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo (figura 3.3).

Debe dejarse muy claro que la seguridad informática no tiene una solución definitiva, sino que es y será el resultado de la innovación tecnológica por parte de aquellos que son los responsables de los sistemas. En palabras de Julio C. Ardita (2001):

> Una política de seguridad funcionó muy bien en los Estados Unidos de América, pero cuando esos manuales se llevaron a América Latina, todo fue un fiasco. Armar una política de procedimientos de seguridad en una empresa

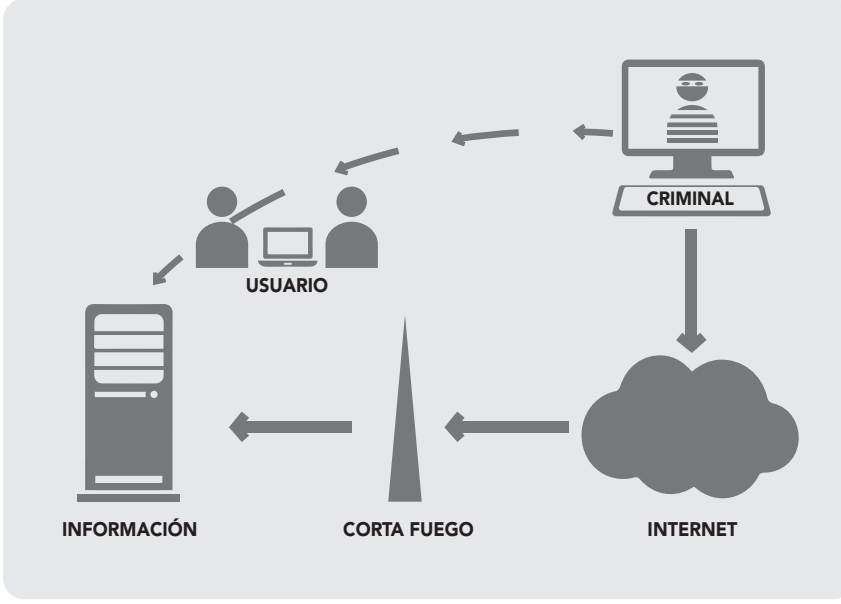


Figura 3.3 Representación de la administración de los usuarios en una red de computadoras

cuesta entre 150 y 350 mil dólares y sin resultado. La razçon es simple porque es un manual que llevado a la implementación nunca se realiza. Es muy difícil armar algo global, por lo que siempre se trabaja en un plan de seguridad real: las políticas y los procedimientos por un lado y la parte física por el otro.

Para continuar hará falta definir algunos conceptos aplicados en la definición de las Políticas de Seguridad Informática (PSI):

Decisión. Elección de un curso de acción determinado entre varios posibles.

Plan. Conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

Estrategia. Conjunto de decisiones que se toman para constituir políticas, metas y programas.

Política. Definiciones establecidas por la dirección que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Meta. El objetivo cuantificado en valores predeterminados.

Procedimiento. Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

Norma. Forma en que se realiza un procedimiento o proceso.

Programa. Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

Proyección. Predicción del comportamiento futuro basándose en el pasado sin el agregado de apreciaciones subjetivas.

Pronóstico. La predicción del comportamiento futuro con el agregado de hechos concretos y conocidos que, se prevé, influirán en los acontecimientos futuros.

Control. Capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho; es una acción tomada para hacer un hecho conforme a un plan.

Riesgo. Proximidad o posibilidad de un daño o peligro; o sea, cada uno de los imprevistos, hechos desafortunados que puede tener un efecto adverso.

Una vez establecidas estas definiciones, es importante establecer que para crear una estrategia adecuada es conveniente pensar en una política de protección en los distintos niveles que ésta debe abarcar y que no son ni más ni menos que los estudiados hasta aquí: física, lógica, factor humano y la interacción que existe entre todos estos factores. En cada caso considerado, el plan de seguridad debe incluir una estrategia proactiva y otra reactiva (Benson, 2011). A continuación, se define en qué consiste cada una de ellas:

Estrategia proactiva (proteger y proceder) o de previsión de ataques. Conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y que ayuda a desarrollar óptimamente planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante éste ayudará a desarrollar esta estrategia.

Estrategia reactiva (perseguir y procesar) o estrategia posterior al ataque. Ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, así como a documentar y aprender de la experiencia y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos tenemos los siguientes puntos a tomar en cuenta:

- *Lo que no se permite expresamente está prohibido:* significa que la organización proporciona una serie de servicios bien determinados y documentados y cualquier otra cosa está prohibida.
- *Lo que no se prohíbe expresamente está permitido:* significa que, a menos de que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no. En la actualidad y "gracias" a las cada día más repetitivas y eficaces acciones que atentan contra los sistemas informáticos, los expertos se inclinan por recomendar la primera política.

Finalmente, las Políticas de Seguridad Informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los integrantes de una entidad sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

3.4.1 Grupo de elaboración de políticas para la seguridad informática

Las políticas de seguridad informática, tienen por objetivo fundamental, establecer las medidas de índole técnica y organización necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes [voz y datos]) y de las personas que interactúan, haciendo uso de los servicios asociados a ellos, y se aplican sin excepción alguna, a todos los usuarios de cómputo de las empresas.

Las políticas de seguridad se elaboran de acuerdo con el análisis de riesgos y de vulnerabilidades en las dependencias de "*Las Empresas*", por consiguiente el alcance de estas políticas se encuentra sujeto a "*Las Empresas*". Las políticas son aplicables sin excepciones a todos los empleados de planta, los contratistas, los consultores, los colaboradores eventuales y otros empleados de "*Las Empresas*" incluyendo a todo el personal externo que cuente con un equipo conectado a la red de la organización. De igual manera, las políticas son aplicables también a todo el equipo y servicios (propietarios o arrendados) que de alguna manera tengan que utilizar local o remotamente la red o los recursos tecnológicos de "*Las Empresas*"; así como de los servicios e intercambio de archivos y de programas. Un ejemplo de la implementación de estrategia de seguridad se aprecia en http://www.gestionintegral.com.co/wp-content/uploads/2013/05/Pol%C3%ADticas-de-Seguridad-Inform%C3%A1tica-2013-GI.pdf.

Así, la elaboración de las Políticas de Seguridad, se fundamentan bajo la Norma ISO/IEC 17799, además han sido planteadas, analizadas y revisadas con el objetivo de no contravenir con las garantías básicas de los usuarios, y no pretende ser una "camisa de fuerza", y más bien muestra una buena forma de operar los sistemas con seguridad, respetando en todo momento, los estatutos y los reglamentos internos de "*Las Empresas*" con dichas políticas de seguridad, se pretende garantizar:

- El control de acceso (aplicaciones, base(s) de datos, área del centro de cómputo o las sedes de "*Las Empresas*" filiales)
- El resguardo de la información
- La clasificación y el control de los activos
- La gestión de las redes (tanto de procesamiento de datos, como de transmisión de los mismos)
- La gestión de la continuidad del negocio
- La seguridad de la información en los puestos de trabajo
- Los controles de cambio(s)
- La protección contra la intrusión en el *software* de los sistemas de información
- El monitoreo de la seguridad
- La identificación y la autenticación de los usuarios de los sistemas de información
- La utilización de los recursos de seguridad
- Las comunicaciones
- La privacidad

3.4.2 Niveles de seguridad

Las Políticas de Seguridad Informática (PSI) constituyen las alarmas y compromisos compartidos en la organización que le permiten a ésta actuar proactivamente ante situaciones que comprometan la integridad. Por lo tanto, deben componer un proceso continuo y realimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y renovación, la aceptación de las directrices y la estrategia de implantación que lleven a una formulación de directivas institucionales que logren aceptación general (Bird; Gopal; Herzberg; Janson; Kutten; Molva y Yung, 1993). Sin embargo, las políticas por sí solas no se tratan de una garantía para la seguridad de la organización; éstas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio que lleven a un esfuerzo conjunto de sus actores por administrar los recursos y reconocer en los mecanismos de seguridad informática los factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización (figura 3.4).

Figura 3.4 Los niveles de seguridad deben ser siempre los máximos para todas las aplicaciones informáticas, tanto a nivel usuario como organizacional

La tabla 3.1 muestra los diferentes niveles de seguridad que las políticas de seguridad consideran en una red de computadoras.

Tabla 3.1 Concentrado de los diferentes niveles de seguridad en una red de computadoras

Nivel de seguridad	Descripción
Nivel D1	El sistema entero no es confiable
Nivel C1	Protección de *hardware*
Nivel C2	Resuelve problemas del nivel C1 y C2
Nivel B1	Protección de seguridad etiquetada
Nivel B2	Protección estructurada
Nivel B3	Dominio de seguridad
Nivel A	Diseño verificado

A continuación, se desarrollan cada una de las diferentes categorías de los niveles de seguridad, de acuerdo con la tabla 3.1.

Nivel D1. Muestra sólo una división que se encuentra reservada para los sistemas que han sido ya evaluados y no cumplen con ninguna especificación de seguridad; con estos no hay protección para el *hardware*, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y a sus derechos en el acceso a la información. MS-DOS y System 7.0 de Macintosh responden a este nivel.

Nivel C1 (protección discrecional). Se requiere la identificación de los usuarios para el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total. Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este súper-usuario, quien tiene la gran responsabilidad en la seguridad. Con la filosofía de la actual descentralización de los sistemas de cómputo, no es raro que en una organización se encuentren dos, tres o más personas cumpliendo este rol; esto, en la práctica, es un problema, pues no hay forma de distinguir entre los cambios que hizo cada uno. A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional (distinción entre usuarios y recursos): se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, discos) sobre los cuales podrán actuar los primeros.
- Identificación y autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización y/o sin identificación.

Nivel C2 (protección de acceso controlado). Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoría de accesos e intentos fallidos de acceso a los objetos. Se tiene la capacidad de restringir aún más la actividad de los usuarios o que ejecuten ciertos comandos o tengan acceso a determinados archivos; además de permitir o denegar datos a usuarios en concreto con base no sólo en los permisos, sino también en los niveles de autorización. Dicha auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad; por ejemplo: las actividades efectuadas por el administrador del sistema y los usuarios.

La mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos. Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de gestión de éste sin necesidad de ser administradores.

Por su parte, permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo.

Nivel B1 (seguridad etiquetada). Dicho subnivel es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel como la secreta y la ultra-secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada

objeto del sistema se le asigna una etiqueta con un nivel de seguridad jerárquico (de alto secreto o de secreto, reservado) y con ciertas categorías (contabilidad, nóminas, ventas, etcétera). Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa; es decir, cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

Nivel B2 (protección estructurada). Requiere que se etiquete cada objeto de nivel superior por ser "padre" de uno inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro a un nivel inferior. Así, por ejemplo, un disco duro será etiquetado por almacenar archivos que son accedidos por distintos usuarios. El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por aquéllos.

Nivel B3 (dominios de seguridad). Refuerza los dominios con la instalación de hardware; por ejemplo, el de administración de memoria se usa para proteger el de seguridad de acceso no autorizado a la modificación. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las admite o las niega según las políticas de acceso que se hayan definido con antelación. Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones.

Este nivel requiere que la terminal del usuario se conecte al sistema de manera segura. Además, cada uno tiene asignados los lugares y objetos a los que puede acceder.

Nivel A (protección verificada). Es el nivel más elevado; incluye un proceso de diseño, control y verificación mediante métodos formales (matemáticos) para asegurar la totalidad de los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. En conjunto, el *software* y el *hardware* son protegidos para evitar infiltraciones ante traslados o ante movimientos del equipamiento.

3.4.3 Esquemas y modelos de seguridad

"Un modelo de seguridad es la presentación formal de una política de seguridad. El modelo debe identificar el conjunto de reglas y prácticas que regulan cómo un sistema maneja, protege y distribuye información delicada" (López Barrientos y Quezada Reyes, 2006). De acuerdo con esto, los modelos se clasifican en:

[1] En seguridad informática, el modelo de seguridad Bell-LaPadula llamado así por sus creadores Billy Elliott Bell y Len LaPadula consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad. Por ejemplo, los sistemas militares estadounidenses categorizan la seguridad en cuatro niveles: no clasificado, confidencial, secreto y ultra-secreto. Este modelo se centra en la confidencialidad y no en la integridad. De modo que se distinguen dos tipos de entidades (sujetos y objetos), se definen estados seguros y se prueba que cualquier transición se hace de uno a otro.

Modelo abstracto. Se ocupa de las entidades como sujetos y objetos. El modelo Bell LaPadula[1] es un ejemplo de este tipo.

Modelo concreto. Traduce las entidades abstractas en otras de un sistema real como procesos y archivos.

Además, dichos modelos sirven para tres propósitos en la seguridad informática:

- Proveer un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas. Un ejemplo es la matriz de acceso.
- Proveer una representación de una política general de seguridad formal y clara.
- Expresar la política exigida por un sistema de cómputo específico.

Para determinar si un modo de acceso específico está permitido, se compara la acreditación de un sujeto con la clasificación del objeto (de manera precisa, la combinación de la clasificación y el conjunto de compartimientos). El esquema de clasificación/acreditación se expresa en términos de un retículo.

El modelo define dos reglas de Control de Acceso Mandatorio (MAC) y una regla de Control de Acceso Discrecional (DAC) con tres propiedades:

Propiedad de seguridad simple. Un sujeto de un determinado nivel de seguridad no puede leer un objeto perteneciente a otro más alto.

Propiedad estrella. (También llamada propiedad de confinamiento). Un sujeto de un determinado nivel de seguridad no puede escribir un objeto perteneciente a otro más bajo.

Propiedad de seguridad discrecional. Se utiliza una matriz de acceso para especificar el control de acceso discrecional.

Por medio del modelo Bell-LaPadula, los usuarios pueden crear contenido sólo en su nivel de seguridad o por encima; es decir, los investigadores en el nivel secreto pueden crear archivos secretos o súper secretos, pero no archivos públicos. De forma inversa, los usuarios pueden ver sólo contenido de su propio nivel o inferior.

El principio de tranquilidad del modelo de Bell-LaPadula establece que la clasificación de un sujeto u objeto no cambia mientras se encuentre referenciada. Hay dos formas para este principio: la fuerte establece que los niveles de seguridad no cambian durante la operación normal del sistema y la débil determina que los niveles de seguridad no cambian de ninguna manera; por lo tanto nunca violarán las reglas de una política de seguridad.

La promoción de una cultura de seguridad requerirá tanto un liderazgo fuerte como una participación amplia para garantizar que se le otorgue un carácter de prioritario a la planificación y administración de la seguridad. Así como la comprensión de la necesidad de que sea plena entre todos los participantes. Los aspectos de seguridad deberían ser objeto de interés y responsabilidad a todos los niveles de la administración de la red de seguridad, la empresa, así como para todos los participantes (figura 3.5).

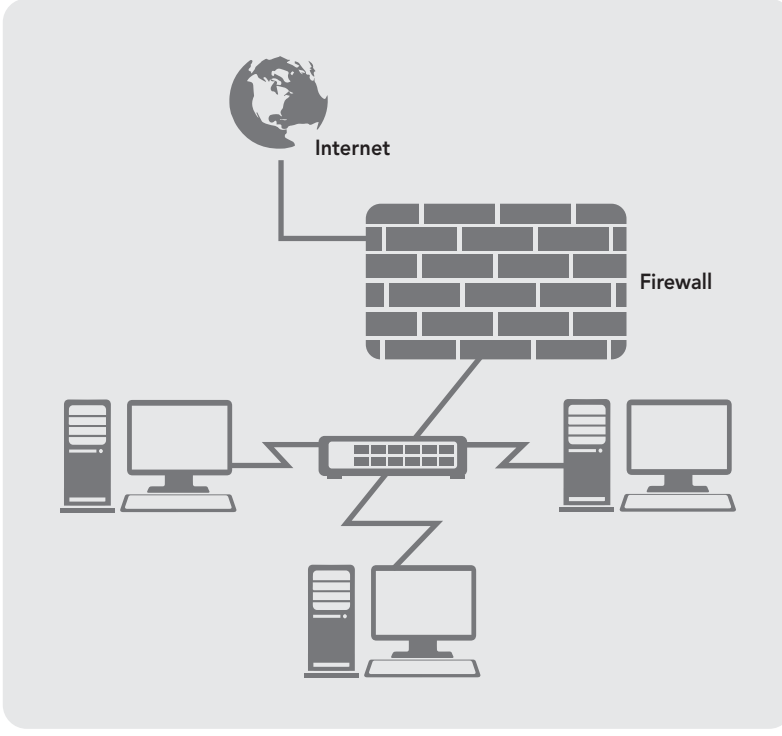


Figura 3.5 Esquema de seguridad para un sistema de información

3.5 Procedimientos de seguridad informática

Una vez que se han determinado las políticas de seguridad que especifican lo que se debe proteger, es necesario realizar los procedimientos que indican cómo llevar a cabo dicha tarea; esto también constituyen los mecanismos para hacer las políticas. Además, resultan útiles, pues precisan lo que se requiere cuando suceden incidentes específicos; entonces, son referencias rápidas en casos de emergencia y ayudan a eliminar los puntos de falla críticos (figura 3.6).

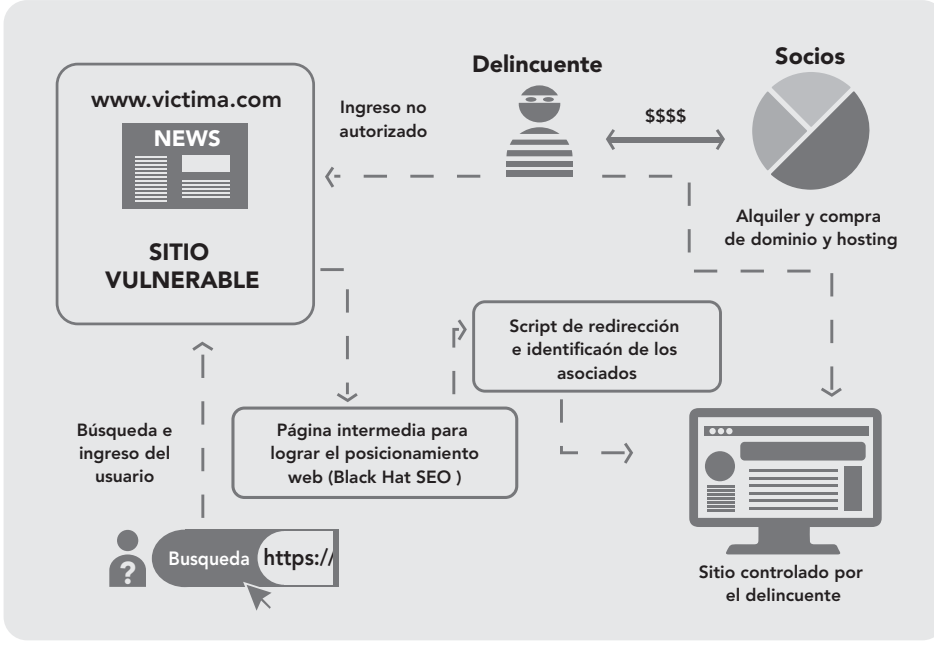


Figura 3.6 Procedimiento para implantar un modelo adecuado de seguridad informática en una organización

Un procedimiento de seguridad "es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las Políticas de Seguridad Informática (PSI) que han sido aprobadas por la organización" (Gómez Vieites, 2008).

En resumen, se describe cómo se implementan en las áreas a proteger las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, atendiendo a las formas de ejecución, periodicidad, personal participante y medios. Un procedimiento de seguridad se sustenta sobre la base de los recursos disponibles y, en dependencia de los niveles de seguridad alcanzados, se elaborará un Programa de Seguridad Informática (PSI) que incluya las acciones a realizar por etapas para lograr niveles superiores. Algunos procedimientos a considerar son los siguientes:

- Otorgar, o en su caso, retirar el acceso de personas a las tecnologías de la información a la vez de que éstas se controlan.
- Asignar o retirar derechos y permisos sobre los ficheros y los datos a los usuarios.
- Autorizar o denegar servicios a los usuarios.
- Definir perfiles de trabajo.
- Dar autorización y control de la entrada/salida de las tecnologías de información.
- Gestionar las claves de acceso considerando objetivamente para cada nivel el tipo de clave atendiendo la longitud, la composición, la frecuencia de actualización, quién debe cambiarla, la custodia, etcétera.
- Realización de respaldos según el régimen de trabajo de las áreas, de forma que estos se mantengan actualizados al igual que las acciones para llevarlos a cabo, garantizando la compartición de la información dependiendo de su nivel de confidencialidad.
- Asegurar que los mantenimientos de los equipos, los soportes y los datos se realicen en presencia y bajo la supervisión del personal responsable y que, en caso del traslado del equipo fuera de la entidad, la información clasificada o limitada sea borrada físicamente o protegida.
- Guardar y analizar los registros o las trazas de auditoría, especificando quién lo realiza y con qué frecuencia.

Se describirán por separado los controles de seguridad implementados en correspondencia con su naturaleza de acuerdo con el empleo que se haga de los medios humanos y técnicos o de las medidas y procedimientos que debe cumplir el personal. A continuación, se establece en qué consisten dichos controles:

Medios humanos. Se hará referencia al papel del personal dentro del sistema de seguridad implementado, definiendo las responsabilidades y funciones respecto al diseño, establecimiento, control, ejecución y actualización de éste.

Medios técnicos de seguridad. Se describirán los medios técnicos utilizados en función de garantizar niveles de seguridad adecuados tanto a nivel de *software* como *hardware*, de la misma forma que en la configuración de ellos. Para lo cual se tendrá en cuenta lo relacionado a la protección física:

- Áreas con tecnologías instaladas: se precisarán, a partir de las definiciones establecidas en el reglamento sobre la seguridad informática, las áreas que se consideran vitales y reservadas en correspondencia con el tipo de información que se procese, intercambie, reproduzca o conserve en éstas; o el impacto que pueda ocasionar la afectación de los activos o recursos que en ellas se encuentren para la organización, relacionando las medidas y procedimientos específicos que se apliquen en cada una. Por ejemplo, las restricciones para limitar el acceso a los locales, los procedimientos para el empleo de cierres de seguridad y los dispositivos técnicos de detección de intrusos.
- Tecnologías de la Información y de las Telecomunicaciones (TIC): se especificarán las medidas y procedimientos de empleo de medios técnicos de protección física directamente aplicados a las tecnologías de la información de acuerdo con la posición de las tecnologías de la información destinadas

al procesamiento de datos con alto grado de confidencialidad o sensibilidad. De forma que se evite la visibilidad de la información a distancia, se minimice la posibilidad de captación de las emisiones electromagnéticas y se garantice un mejor cuidado y conservación de éstas.

- Soportes de información: se describirá el régimen de control establecido sobre los soportes magnéticos de información.

Técnicas o lógicas. Se especificarán las medidas y los procedimientos de seguridad que se establezcan, cuya implementación se realice a través de *software*, *hardware* o ambos:

- Identificación y autenticación de usuarios
- Control de acceso a los activos y recursos
- Integridad de los ficheros y datos
- Auditoría y alarmas

Recuperación ante contingencias. Se describirán las medidas y procedimientos de neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o que degrade su funcionamiento, minimizando el impacto negativo de éstas sobre la organización.

Un procedimiento de seguridad determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de la ejecución. Por lo tanto, es la especificación de una serie de pasos en relación con el desarrollo de un proceso o actividad que trata de cumplir con una norma o garantizar que en la ejecución de actividades se considerarán determinados aspectos de seguridad. Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en la ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a llevar a cabo; además, puede apoyarse en otros documentos, procedimientos o instrucciones del nivel de detalle que se desee.

Cabe tomar en cuenta que las mejores prácticas para la seguridad informática no son otra cosa que una cultura y educación que se deben adquirir para evitar problemas futuros en el uso de equipos y sistemas (Anderson, 2001). Hoy en día, es tan común que se usen computadoras, cajeros automáticos, tecnologías de comunicaciones, redes e Internet, que no se cae en la cuenta de toda la información que se maneja como la propia, los correos electrónicos, los datos bancarios, los archivos de interés y todo el trabajo cotidiano se encuentran manejados por computadoras y equipos que en la práctica son vulnerables y que en cualquier momento pueden sufrir un ataque, alteraciones o descomposturas (figura 3.7) (Berghel, 2001).

Figura 3.7 Uso de las mejores prácticas para la seguridad informática

3.5.1 Estándares de seguridad informática

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO), así como por la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas incluyen (ISO, 2015):

- ISO/IEC 27000: es un vocabulario estándar para los SGSI. Se traduce como la introducción y base para el resto de las normas, la tercera versión se creó en enero de 2014.
- ISO/IEC 27001: es la certificación que deben obtener las organizaciones. La norma que especifica los requisitos para la implantación del SGSI y representa la norma más importante de la familia. Adopta un enfoque de gestión de riesgos, y promueve la mejora continua de los procesos. En octubre de 2005 se publicó como estándar internacional y se revisó en septiembre de 2013.
- ISO/IEC 27002: *Information Technology Security; Techniques Code of Practice for Information Security Management*. Previamente BS 7799 Parte 1 y la Norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de la seguridad de la información. Se publicó en julio de 2005 como ISO 17799:2005 y el 1o. de julio de 2007 recibió su nombre oficial ISO/IEC 27002:2005. La última versión: 27002:2013, se creó en septiembre de 2013.
- ISO/IEC 27003: representa las directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Se publicó el 1o. de febrero de 2010. No es certificable.
- ISO/IEC 27004: son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar las mediciones de la seguridad de la información. Se publicó el 7 de diciembre de 2009, en la actualidad no se encuentra traducida al español.

3.6 Arquitectura de seguridad de la información

Cada día se hace necesario integrar las funcionalidades propias de la seguridad en las arquitecturas de comunicaciones existentes; este proceso compromete la implementación de mecanismos, servicios y funciones de seguridad que se apoyan en otros ya aplicados a la propia arquitectura de comunicaciones. El resultado final será lo que se denomina una "arquitectura de seguridad", la cual permite la trazabilidad desde la estrategia de negocio hasta la tecnología subyacente (figura 3.8).

La arquitectura de seguridad de información se posicionó en primer término por Gartner Inc. en su libro *Incorporating Security into the Enterprise Architecture Process* (2006), gracias al cual ha pasado de ser un silo basado en arquitectura, a una solución enfocada a la empresa que incorpora negocio, información y tecnología.

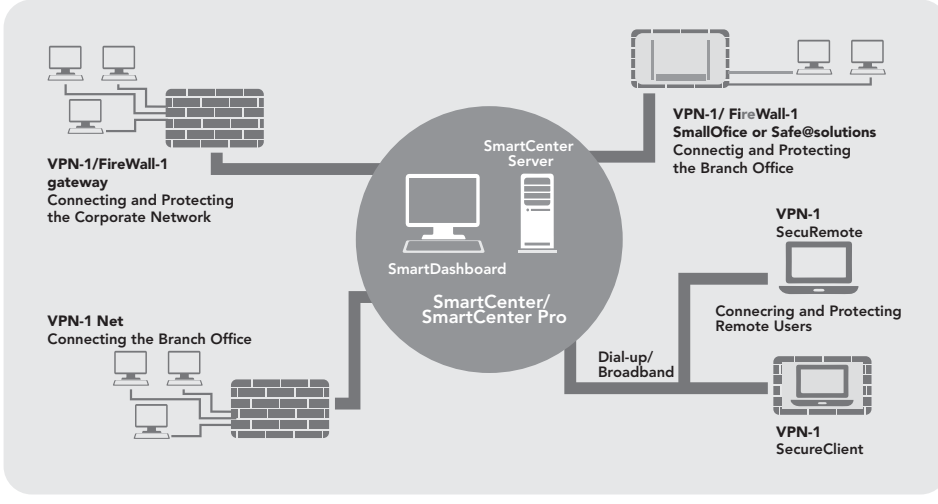


Figura 3.8 Arquitectura de seguridad informática para una organización

Con base en lo anterior, la arquitectura de seguridad de información en la empresa (EISA, *Enterprise Information Security Architecture*) se centra en la seguridad de la información a lo largo de la organización en su conjunto (Benson, 2011). La EISA es la aplicación de un método riguroso y comprensivo para describir una estructura actual y/o futura, así como el comportamiento de los procesos de seguridad, los sistemas de seguridad de información y las subunidades de personal y organizativas para que se alineen con las metas comunes de la empresa y la dirección estratégica. Aunque a menudo se asocie de forma estricta con tecnologías para la seguridad de la información, se relaciona en términos generales con la práctica de seguridad de optimización del negocio, donde se dirigen la arquitectura, la realización de gestiones y también los procesos de seguridad.

La EISA se ha convertido en una práctica habitual dentro de las instituciones financieras alrededor del mundo, donde las metas son las siguientes:

- Proporcionar estructura, coherencia y cohesión.
- Permitir un alineamiento del negocio hacia la seguridad.
- Definir principios *inicio-fin* con estrategias de negocio.
- Asegurar que todos los modelos e implementaciones puedan ser trazados hacia atrás hasta la estrategia de negocio, específicamente en sus requerimientos y principios clave.
- Proveer abstracción para que factores complicados puedan ser eliminados y reinstalados en niveles de detalle diferente sólo cuando sean requeridos.
- Establecer un lenguaje común para la seguridad de la información dentro de la organización.

La práctica de la Arquitectura de Seguridad de Información en la Empresa (EISA) conlleva desarrollar un marco de arquitectura de seguridad para describir una serie de arquitecturas de referencia, corrientes, intermedias y objetivas; y dedicarlas a alinear los programas de cambio. Estos marcos detallan las organizaciones, roles, entidades y relaciones que existen o deberían existir para llevar a cabo un conjunto de procesos de negocio.

El producto final es un conglomerado de artefactos, por lo regular gráficos que se describen en varios grados de detalle, por ejemplo: qué y cómo opera un negocio, qué tipo de controles de seguridad son requeridos. Dadas estas descripciones, quienes toman las decisiones están provistos de medios para establecer dónde invertir recursos, hacia dónde reorientar las metas organizacionales y procesos, así como qué políticas y procedimientos soportarán metas centrales o funciones de negocio.

Un proceso de EISA ayuda a contestar preguntas básicas como:

- ¿La arquitectura actual apoya y añade valor a la seguridad de la organización?
- ¿Cómo podría una arquitectura de seguridad ser modificada para que añada más valor a la organización?
- Basándose en lo que se sabe sobre sobre la organización, se planea mejoras a futuro, entonces ¿la arquitectura actual lo sustentará o lo entorpecerá?
- Al implementar una arquitectura de seguridad de información en la empresa, por lo general empieza documentando la estrategia de la organización y otros detalles necesarios como dónde y cómo opera, ¿el proceso entonces desemboca en documentar competencias esenciales, procesos de negocio y cómo la organización interactúa consigo misma y con partes como clientes, proveedores, y entidades gubernamentales?
- Habiendo documentado la estrategia y la estructura de la organización, ¿el proceso de arquitectura fluye entonces hacia la información diferenciada de los componentes tecnológicos? Como los que se muestran a continuación:
  - Cuadros de organización, actividades y flujo de procesos
  - Ciclos, periodos y distribución en el tiempo de la organización
  - Proveedores de tecnología, *hardware*, *software* y de servicios
  - Inventarios y diagramas de aplicaciones y *software*
  - Interfaces entre aplicaciones como eventos, mensajes y flujo de datos
  - Intranet, Extranet, Internet, comercio electrónico (*e*-Commerce), EDI, links con partes de dentro y fuera de la organización

- Clasificación de datos, bases de datos y modelos de datos soportados.
- *Hardware*, plataformas, *hosting*, servidores, componentes de red, dispositivos de seguridad y dónde se conservan.
- Redes de área local y abiertas, diagramas de conectividad a Internet.

Donde sea posible, todo lo anterior debería estar relacionado explícitamente con la estrategia de la organización, las metas y las operaciones. La Arquitectura de Seguridad de Información en la Empresa (EISA) documenta el estado actual de los componentes técnicos de seguridad listados arriba, así como un estado ideal futuro (Fernández, 2008).

En esencia, el producto es un conjunto de modelos anidados e interrelacionados, dirigidos y mantenidos con *software* especializado y disponible en el mercado. Semejante descripción exhaustiva de las dependencias de la TI se ha solapado notablemente con la llegada de los metadatos y con el concepto de biblioteca de infraestructura de tecnologías de la información (ITIL, *Information Technology Infrastructure Library*) de la configuración de los gestores de bases de datos; por lo que mantener la precisión de esa información puede ser un desafío importante.

Junto con los modelos y diagramas se incluye un conjunto de mejores prácticas dirigidas a la adaptabilidad de la seguridad, la escalabilidad, la manejabilidad, etc. Éstas no son únicas a la EISA, pero sí son esenciales, sin embargo, para su éxito (Anderson, 2001).

Un resultado intermedio de un proceso de arquitectura es un inventario extenso de la estrategia de seguridad del negocio, de los procesos de ésta; de los cuadros organizacionales; de los registros de seguridad técnicos, de los diagramas de sistema e interfaz y de las topologías de la red; así como de las relaciones explícitas entre ellos.

3.7 Vulnerabilidades en la seguridad informática

Las vulnerabilidades son errores que permiten realizar desde fuera actos sin permiso del administrador de sistemas incluso por medio de la suplantación del usuario.

En la actualidad hay muchas amenazas que tratan de acceder de forma remota a las computadoras, ya sea para hacerlas servidores ilegales de spam o para robar información. Entras las más famosas están LSASS (*Local Security Authority Subsystem Service*) y SvcHOST, elemento que aloja varios servicios de Windows y que es esencial en la aplicación de los llamados procesos de servicios compartidos. En estos, algún gusano informático que afecta a los equipos que ejecutan versiones propensas a ataques puede propagarse como Sasser, que se aprovecha de la vulnerabilidad del sistema a través de un puerto de red, por lo que es en particular virulento; como es posible que se extienda sin la intervención del usuario, es posible detenerlo con un cortafuegos configurado de forma correcta o mediante la descarga de las actualizaciones de Windows. Otro ejemplo de gusano es Blaster (también llamado Lovsan o LoveSan 3 a 1), que se aprovecha de una vulnerabilidad en el servicio DCOM para infectar a otros sistemas de forma automática (figura 3.9).

Figura 3.9 Representación de las diversas vulnerabilidades que puede tener el sistema informático de una organización

Aunque no siempre hay una regla general para explotar vulnerabilidades de los sistemas, se puede describir a grandes rasgos una serie de pasos para llegar a tal cometido:

- Conocer la existencia de la vulnerabilidad.
- Documentarse sobre sus propiedades.
- Conocer las características del sistema que se va a explotar.
- Conseguir acceso a éste con los privilegios suficientes.

3.8 Riesgos en la seguridad informática

La incertidumbre existente por el posible desarrollo de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como equipos, instalaciones, programas de cómputo, se encuentra presente en los sistemas de información de una organización (Kaufman, Perlman y Speciner, 2002). Por eso es muy importante contar con un conjunto de herramientas que garantice relativamente la correcta evaluación de los riesgos a los cuales están sometidos los procesos y las actividades que participan en el área informática (figura 3.10).

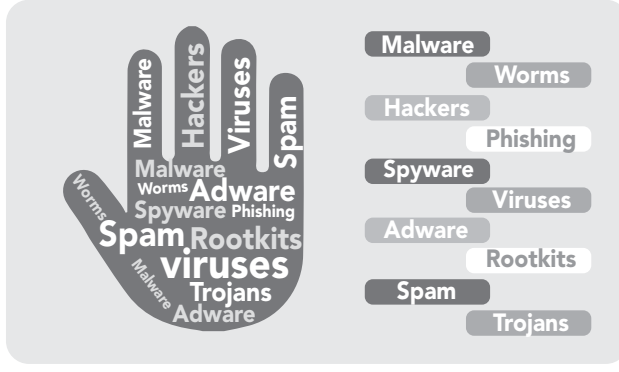


Figura 3.10 Principales riesgos a los que está sujeto el sistema informático de una organización

Los tipos de riesgos informáticos más relevantes son:

Riesgos de integridad. Abarca todos los asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización; los cuales se manifiestan en los siguientes componentes de un sistema:

- Interfaz del usuario: los riesgos en esta área, por lo regular, se relacionan con las restricciones sobre las individualidades de una organización y la autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones. Otros riesgos en esta área se relacionan con controles que aseguren la validez y completitud de la información introducida dentro de un sistema.
- Procesamiento: se enfoca con el adecuado balance de los controles defectivos y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.
- Procesamiento de errores: se relacionan estos riesgos con los métodos que aseguren que cualquier proceso de información de errores sea capturado adecuadamente, corregido y reprocesado con exactitud.

- Administración de cambios: representa los riesgos relacionados con la administración inadecuada de procesos y de cambio de organizaciones que incluyen compromisos y entrenamiento de los usuarios a los cambios de los procesos y la forma de comunicarlos e implementarlos.
- Información: atañe a los riesgos asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y las estructuras.

Riesgos de relación. El uso oportuno de la información creada por una aplicación. Estos se relacionan de manera directa a la información de toma de decisiones.

Riesgos de acceso. Se enfocan al inapropiado acceso a los sistemas, los datos y la información; además, abarcan los riesgos de segregación inadecuada de trabajo, los asociados con la integridad de la información de sistemas de bases de datos y los afiliados a la confidencialidad de ésta. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

- Administración de la información: el mecanismo provee a los usuarios acceso a la información específica del entorno.
- Entorno de procesamiento: los riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.
- Redes: se refiere al acceso impropio al entorno de red y su procesamiento.
- Nivel físico: protección física de dispositivos y un adecuado acceso a ellos.

Riesgos de utilidad. Se enfocan en tres diferentes niveles: direccionamiento de sistemas antes de que los problemas ocurran, técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas y respaldos, así como planes de contingencia que controlan desastres en el procesamiento de la información.

Riesgos de la infraestructura. Se refieren a que en las organizaciones no existe una estructura de información tecnológica efectiva para soportar de modo adecuado las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos se asocian con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente, pago de cuentas, entre muchas otras).

Riesgos de seguridad general. Los estándares IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y disminuyen los siguientes riesgos:

- De choque de eléctrico: niveles altos de voltaje
- De incendio: flamabilidad de materiales
- De niveles inadecuados de energía eléctrica
- De radiaciones: ondas de ruido, de láser y ultrasónicas
- Mecánicos: inestabilidad de las piezas eléctricas

Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de estos, el cual supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas, sino que se ha de poder obtener una evaluación económica del impacto de los sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis frente al costo de volverla a producir.

La evaluación de los riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización (Simmon, 1992), pues así se pueden priorizar los problemas y el costo potencial desarrollando un plan de acción adecuado.

3.8.1 Gestión de riesgos

La función de la gestión de riesgos se relaciona con el análisis; la tarea principal es identificar estudiar y eliminar las fuentes de los eventos perjudiciales antes de que empiecen a amenazar los procesos informáticos. Esto es bastante obvio, ya que la probabilidad de ocurrencia de los riesgos hace vulnerables los sistemas informáticos, lo cual conlleva a que la estrategia de negocio de una organización se vea amenazada (Terán Pérez, 2014). La figura 3.11 muestra la relación existente entre la probabilidad de ocurrencia de dicho riesgo y sus posibles consecuencias.

Figura 3.11 Relación existente entre la probabilidad de ocurrencia de dicho riesgo y sus posibles consecuencias

De acuerdo con Vaughan (1997), la gestión de riesgos se divide en:

Estimación de riesgos. Describe cómo estudiar los riesgos dentro de la planeación general del entorno informático. Ésta cuenta con los siguientes eventos:

- La identificación de riesgos genera una lista de riesgos capaces de afectar el funcionamiento normal del entorno informático.
- El análisis de riesgos mide su probabilidad de ocurrencia y su impacto en la organización.
- La asignación de prioridades a los riesgos.

Identificación de riesgos. En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático. Los principales factores que se ven afectados son:

- La creación de la planificación que incluye proyecciones en exceso optimistas con tareas innecesarias y la organización de un entorno informático sin tener en cuenta áreas desconocidas y la envergadura de éste.
- La organización y gestión, que incluye los presupuestos bajos. El ciclo de revisión/decisión de las directivas es más lento de lo esperado.
- El entorno de trabajo incorpora el mal funcionamiento de las herramientas de desarrollo, espacios de trabajo inadecuados y la curva de aprendizaje de las nuevas tecnologías, que es más larga de lo esperado.
- Las decisiones de los usuarios finales comprenden la falta de participación entre los usuarios y el departamento de informática.
- El personal contratado incluye la falta de motivación, de trabajo en equipo y trabajos de poca calidad.
- Los procesos que hacen referencia a la burocracia y la falta de control de calidad y de entusiasmo.

Análisis de riesgos. Una vez que se hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

Exposición a riesgos. Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.

Estimación de la probabilidad de pérdida. Las principales formas de estimar la probabilidad de pérdida son las siguientes:

- Disponer de la persona que está más familiarizada con el entorno informático para que estime la probabilidad de ocurrencia de eventos perjudiciales.
- Usar técnicas *Delphi*[2] o de consenso en grupo.
- Utilizar la calibración mediante adjetivos, en la cual las personas involucradas eligen un nivel de riesgo entre "probable" y "muy probable", y después se convierten a estimaciones cuantitativas.

[2] El método *Delphi* consiste en reunir a un grupo de expertos para solucionar determinados problemas. Ellos se encargan de la categorización individual de las amenazas y los objetivos del riesgo.

Priorización de riesgos. En este paso se estima que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización, los pequeños riesgos no deben ser de gran preocupación, pues lo crítico se puede dejar en un segundo plano.

Control de riesgos. Una vez que se hayan identificado los riesgos del entorno informático y analizado la probabilidad de ocurrencia, existen bases para controlarlos como:

- Planificación de riesgos: el objetivo es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestas las actividades informáticas.
- Resolución de riesgos: se conformada por los métodos que controlan el problema de un diseño de controles inadecuado; los principales son evitar el riesgo, conseguir información acerca de éste, planificar el entorno informático para que sean cumplidas las actividades informáticas sean cumplidas en caso de riesgo, eliminar el origen de éste si es posible desde su inicio, y asumirlo y comunicarlo.

Monitorización de riesgos. La vida en el mundo informático sería más fácil si los riesgos apareciesen después de que hayamos desarrollado planes para tratarlos. Pero los riesgos aparecen y desaparecen dentro del entorno informático, por lo que se necesita una monitorización para comprobar cómo progresa el control de un riesgo e identificar cómo aparecen nuevos eventos perjudiciales en las actividades informáticas.

La tabla 3.2 muestra la forma en que se pueden controlar algunos de dichos riesgos por medio de los métodos más comunes.

Tabla 3.2 Métodos de control de riesgos

Riesgo	Métodos de control
Cambio de la prestación del servicio	☑ Uso de técnicas orientadas al cliente ☑ Diseño para nuevos cambios
Recorte de la calidad	☑ Dejar tiempo a las actividades de control
Planificación demasiado optimista	☑ Utilización de técnicas y herramientas de estimación
Problemas con el personal contratado	☑ Pedir referencias personales y laborales ☑ Contratar y planificar los miembros clave del equipo mucho antes de que comience el proyecto ☑ Tener buenas relaciones con el personal contratado

El análisis de riesgos utiliza el método matricial llamado "Mapa de Riesgo" para identificar la vulnerabilidad de un servicio o negocio a riesgos típicos (Vaughan, 1997). El método contiene los siguientes pasos:

Localización de los procesos en las dependencias que intervienen en la prestación del servicio. Como se muestra en la tabla 3.3.

Tabla 3.3 Ejemplo de una matriz de dependencias frente a procesos				
Dependencias				
Procesos	**Descripción**			
Gestión de centros transaccionales	✘	✘	✘	
Administración de sistemas		✘		
Atención al cliente		✘	✘	
Conciliación de cuentas	✘			✘

Localización de los riesgos críticos y su efecto en los procesos del negocio. En este paso se determina la vulnerabilidad de una actividad a una amenaza. Para asignar un peso a cada riesgo se consideran tres categorías de vulnerabilidad (1 = baja, 2 = media y 3 = alta). Es decir, si se afirma que el riesgo a una decisión equivocada tiene alto riesgo de vulnerabilidad, entonces tendría alta prioridad dentro de las políticas de seguridad (tabla 3.4).

Tabla 3.4 Ejemplo de una matriz de riesgos frente a vulnerabilidad		
Riesgo	**Porcentaje obtenido**	**Vulnerabilidad**
Decisiones equivocadas	59%	Alta
Fraude	55%	Media
Hurto	54%	Media

Dentro del entorno informático, las amenazas se pueden clasificar de la siguiente forma:

Naturales. Que incluyen principalmente los cambios naturales que pueden afectar, de una manera u otra, el normal desempeño del entorno informático. Por ejemplo, la posibilidad de un incendio en el sitio donde se encuentran los concentradores de cableado, dado que posiblemente están rodeados de paredes de madera.

Accidentales. Son las más comunes que existen e incluyen:

- Errores de los usuarios finales: por ejemplo, el usuario tiene permisos de administrador y, posiblemente sin intención, modifica información relevante.
- Errores de los operadores: si un operador tenía una sesión abierta y olvidó salir del sistema, alguien con acceso físico a la máquina en cuestión de segundos puede causar estragos.
- Error administrativo: instalaciones y configuraciones sin contar con mecanismos de seguridad de protección.
- Errores de salida: impresoras u otros dispositivos mal configurados.
- Errores del sistema: daños en archivos del sistema operativo

- Errores de comunicación: permitir la transmisión de información violando la confidencialidad de los datos.

Deliberadas. Que pueden ser activas (accesos no autorizados, modificaciones no autorizadas, sabotaje) o pasivas (de naturaleza mucho más técnica como emanaciones electromagnéticas y/o microondas de interferencia).

Localización de los riesgos críticos en las dependencias de la empresa y en los procesos que intervienen en el negocio. Dichas amenazas se pueden definir con base en la información de las tablas 3.5 y 3.6.

Tabla 3.5 Ejemplo de una matriz de procesos frente a riesgo

Proceso/Riesgo	Decisiones equivocadas	Fraude	Hurto
Gestión de centros transaccionales		✘	✘
Administración de sistemas		✘	✘
Atención al cliente		✘	✘
Conciliación de cuentas	✘	✘	✘

Tabla 3.6 Ejemplo de una matriz de procesos frente a riesgo

Riesgos frente a dependencias	División financiera	Sistemas	Cartera	Contabilidad
Decisiones equivocadas	✘			✘
Fraudes	✘	✘	✘	✘
Hurtos	✘	✘	✘	✘

Identificar los controles necesarios. En este paso se precisan los controles que son mecanismos que ayudan a disminuir el riesgo a niveles mínimos o, en algunos casos, eliminarlos por completo. Se debe tener en cuenta que dichas medidas tienen tres diferentes capacidades que incluyen mecanismos de prevención, detección y corrección; y que dentro de un proceso o negocio funcionen. En este caso se incluye la funcionalidad y utilidad del control y se identifican las personas responsables de la implantación de los controles.

Diseñar los controles definitivos. Se tienen los productos necesarios para iniciar el proceso de implantación de los controles utilizados, o bien, para empezar la construcción de dichos mecanismos.

3.8.2 Análisis de riesgos

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y las reales amenazas a los que se encuentran expuestos; así como su probabilidad de ocurrencia y el impacto de ésta, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras y/o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles.

Dichos controles, para que sean efectivos, deben ser implementados en conjunto, formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio y las interrelaciones con otras funciones de negocios como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas y los clientes deben ser identificados para lograr una imagen global y completa de estos (Burnett y Paine, 2001).

En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben estar conscientes de que la administración del riesgo informático juega un rol crítico. La meta principal de la administración del riesgo informático debería ser "proteger a la organización y la habilidad de manejar su misión", no solamente la protección de los elementos informáticos. Además, el proceso no sólo debe ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización.

Es importante recordar que el riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia. Por lo que se puede decir, a grandes rasgos, que la administración de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir estos a un nivel aceptable.

El análisis de riesgo informático es un elemento que forma parte del programa de gestión de continuidad de negocio (*Business Continuity Management*) e identifica si existen controles que ayudan a minimizar la probabilidad de ocurrencia de la vulnerabilidad; pues, de no existir, ésta será de riesgo no controlado (Burnett y Paine, 2001).

Dentro de la evaluación del riesgo es necesario realizar las siguientes acciones: calcular el impacto en caso de que la amenaza se presente y evaluarlo de forma que se pueda priorizar, lo cual se realiza de forma cuantitativa o cualitativa. Por lo tanto, el análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede ocurrir?
- ¿Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

A continuación se muestra la manera de cómo se realiza una evaluación de riesgos.

Ejemplo 3.1

El encargado del centro de informática establecerá con los responsables de las diferentes áreas con las siguientes puntualizaciones:

¿A qué riesgos en la seguridad informática se enfrenta la institución?

Fuego. Se pueden destruir los equipos y los archivos.

Robo común. Es posible que haya sustracción de equipos y archivos.

Vandalismo. Se podrían dañar los equipos y los archivos.

Fallas en los equipos. Posiblemente se dañen los archivos.
Equivocaciones. Hay posibilidad de daño en los archivos.
Acción de virus. Podrían dañarse los equipos y los archivos.
Terremotos. Podría haber destrucción del equipo y los archivos.
Accesos no autorizados. Filtración de datos no autorizados.
Robo de datos. Existe la posibilidad de que se difundan los datos sin cobrarlos.
Fraude. Desvío de fondos.

La lista de riesgos que se puede enfrentar en la seguridad es corta. La organización deberá profundizar en el tema para tomar todas las medidas del caso; luego, prepara al personal para responder a los efectos de los riesgos que enfrentarán en la organización. Para cada efecto de riesgo se debe determinar la probabilidad del factor de riesgo. Es decir:

- Factor de riesgo bajo
- Factor de riesgo muy bajo
- Factor de riesgo alto
- Factor de riesgo muy alto
- Factor de riesgo medio

3.8.3 Enfoques cualitativos y cuantitativos

Los términos "administración" y "evaluación" de riesgos, aunque están relacionados, no se pueden usar indistintamente. El primero se define como el esfuerzo global para administrar el riesgo hasta alcanzar un nivel aceptable en la organización. Mientras que el segundo es "el proceso de identificar y asignar prioridades a los riesgos para la organización.

Hay numerosas metodologías distintas para asignar prioridades a los riesgos o evaluarlos, pero la mayoría están basadas en uno de estos dos enfoques o en una combinación de ambos: cuantitativo o cualitativo (UE, 2016).

A continuación se ofrece un resumen y una comparación de ambos seguido de una breve descripción del proceso de administración de riesgos de seguridad y cómo se combinan aspectos de ambos enfoques:

Evaluación de riesgos cuantitativa. El objetivo es calcular valores numéricos para cada uno de los componentes recopilados durante la evaluación de riesgos y el análisis de costo-beneficio. Por ejemplo, se estima el valor verdadero de cada activo de negocios en función del costo de reemplazarlo, la pérdida de productividad, la reputación de marca y otros valores de negocios directos e indirectos; para ello debe intentarse emplear la misma objetividad al calcular la exposición de activos, el costo de controles y el resto de los elementos que identifique durante el proceso de administración de riesgos.

Existen algunos puntos débiles importantes que son inherentes a este enfoque y que no se pueden solventar con facilidad: en primer lugar, no hay un modo formal y riguroso de calcular de forma eficaz los valores de los activos y

de los controles; es decir, aunque pueda parecer que ofrecen más detalle, en realidad los valores financieros oscurecen el hecho de que las cifras se basan en estimaciones.

¿Cómo es posible calcular de un modo preciso y exacto las repercusiones que una incidencia de seguridad de amplia difusión podría tener en la marca? Se pueden examinar los datos históricos si están disponibles. En segundo lugar, las organizaciones que han intentado aplicar en detalle todos los aspectos de la administración de riesgos cuantitativa han comprobado que el proceso es excesivamente costoso. Dichos proyectos tardan mucho tiempo en completar su primer ciclo y por lo regular implican a muchos miembros del personal con discusiones acerca de cómo se han calculado los valores fiscales específicos.

En tercer lugar, en organizaciones con recursos de alto valor, el costo de exposición puede ser tan alto que se gastaría una ingente cantidad de dinero en mitigar los riesgos a los que estuvieran expuestas; pero esto no es realista, una organización no gastaría todo su presupuesto en proteger un solo activo.

Los detalles del enfoque cuantitativo son los siguientes: puede resultar útil disponer de una descripción general de las ventajas y los inconvenientes de esta evaluación. Posteriormente, se examinan algunos de los factores y valores que se evalúan durante un estudio de riesgos cuantitativo, como la valoración de activos, el costo de los controles, la determinación del rendimiento de la inversión en seguridad (ROSI, *Return On Security Investment*), el cálculo de valores para la expectativa de pérdida simple (*SLE, Single Loss Exposure*), la frecuencia anual (ARO, *Annual Rate of Occurrence*) y la expectativa de pérdida anual (ALE, *Annual Loss Exposure*). No se trata en absoluto de un examen exhaustivo de todos los aspectos de la evaluación de riesgos cuantitativa, sino un breve examen de algunos detalles de dicho enfoque para que se compruebe que las cifras que conforman la base de todos los cálculos son subjetivas en sí mismas.

Respecto al análisis de activos, la determinación del valor monetario es una parte importante de la administración de riesgos de seguridad. A menudo, los directores se basan en el valor de un activo como orientación para establecer el dinero y tiempo que deben invertir para protegerlo, y muchas organizaciones conservan una lista de estos como parte de los planes de continuidad de negocios. No obstante, las cifras calculadas en realidad son estimaciones subjetivas: no existe ninguna herramienta o método para definir el valor de un activo.

Evaluación de riesgos cualitativa. La diferencia entre la evaluación de riesgos cualitativa y la cuantitativa estriba en que en la primera no se intentan aplicar valores financieros puros a los activos, pérdidas previstas y costo de controles; pues en su lugar se calculan valores relativos.

El análisis de riesgos cualitativos se lleva a cabo mediante la combinación de cuestionarios y talleres colaborativos que implican a personas de varios grupos de la organización, como expertos en seguridad de información, responsables y usuarios de activos de negocios y directivos.

Si se utilizan los cuestionarios, por lo regular, se distribuyen unos días o unas semanas antes del primer taller, pues están diseñados para descubrir los activos y los controles que ya están implementados; además la información recopilada puede resultar muy útil durante los talleres posteriores. En estos últimos, los participantes identifican los activos y estiman sus valores relativos

para después determinar las amenazas a las que se enfrenta cada activo y los tipos de vulnerabilidades que pueden aprovechar éstas en el futuro.

En la práctica, los expertos en seguridad informática y los administradores del sistema proponen controles con el objetivo de mitigar los riesgos para el grupo en consideración; así como el costo aproximado de cada uno. De modo que los resultados se presentan a los directivos para que los tengan en cuenta durante un análisis de costo-beneficio.

Como se puede comprobar, el proceso básico de las evaluaciones cualitativas es muy similar a la evaluación del enfoque cuantitativo. La diferencia se encuentra en los detalles: las comparaciones entre el valor de un activo y otro son relativas, y los participantes no dedican demasiado tiempo en intentar calcular cifras financieras exactas para la valoración de activos. Lo mismo sucede en el cálculo de las repercusiones posibles si se produce un riesgo, así como en el costo de la implementación de controles.

Las ventajas de un enfoque cualitativo estriban en que se supera la dificultad de calcular cifras exactas para el valor de activos o para el costo de control; y el proceso exige menos personal. Los proyectos de administración de riesgos cualitativa arrojarán resultados importantes al cabo de pocas semanas, mientras que en las organizaciones que optan por un enfoque cuantitativo se apreciarán pocas ventajas durante meses y, en ocasiones, años de esfuerzos.

El inconveniente de un enfoque cualitativo reside en que las cifras resultantes son vagas; algunos de los responsables de la toma de decisiones; es decir, los que disponen de experiencia en cuestiones financieras o contables, pueden no sentirse cómodos con los valores relativos determinados durante un proyecto de evaluación de riesgos cualitativa.

La comparación de los dos enfoques establece que las orientaciones tienen ventajas e inconvenientes, pero determinadas situaciones pueden demandar que las organizaciones adopten el enfoque cuantitativo y, por el contrario, las instituciones de pequeño tamaño o con recursos limitados encontrarán más adecuado el enfoque cualitativo.

En la tabla 3.7, se resumen las ventajas y los inconvenientes de cada uno.

Tabla 3.7 Ventajas e inconvenientes de cada enfoque de administración de riesgos

Riesgo	Porcentaje obtenido	Vulnerabilidad
Ventajas	☑ Se asignan prioridades a los riesgos según las repercusiones financieras y de los activos de acuerdo con los valores financieros. ☑ Los resultados facilitan la administración del riesgo por el rendimiento de la inversión en seguridad. ☑ Los resultados se pueden expresar en terminología específica de administración (por ejemplo, los valores monetarios y la probabilidad expresados como un porcentaje específico).	☑ Permite la visibilidad y la comprensión de la clasificación de riesgos. ☑ Resulta más fácil lograr el consenso. ☑ No es necesario cuantificar la frecuencia de las amenazas. ☑ No se requiere determinar los valores financieros de los activos. ☑ Resulta más fácil involucrar a personas que no sean expertas en seguridad o en informática.

Inconvenientes	☑ Los valores de repercusión asignados a los riesgos se basan en las opiniones subjetivas de los participantes. ☑ El proceso para lograr resultados creíbles y el consenso es muy lento. ☑ Los cálculos pueden ser complejos y lentos. ☑ Los resultados sólo se presentan en términos monetarios y pueden ser difíciles de interpretar por parte de personas sin conocimientos técnicos. ☑ El proceso requiere experiencia, por lo que los participantes no pueden recibir cursos fácilmente durante el mismo.	☑ No hay una distinción suficiente entre los riesgos importantes. ☑ Resulta difícil invertir en la implementación de controles porque no existe una base para un análisis de costo-beneficio. ☑ Los resultados dependen de la calidad del equipo de administración de riesgos que los hayan creado.

En el pasado, los enfoques cuantitativos parecían dominar la administración de riesgos de seguridad informática; sin embargo, esto ha cambiado recientemente a medida de que cada vez más especialistas admiten que el seguimiento estricto de los procesos de administración de riesgos cuantitativa da lugar a proyectos difíciles y de larga duración que muestran pocas ventajas tangibles. En la práctica actual, el proceso de administración de riesgos de seguridad debe combinar los mejores aspectos de ambas metodologías en un único proyecto híbrido.

Método FRAP

En 2001 se desarrolló por Tom Peltier el proceso de evaluación de riesgos facilitado (FRAP, *Facilitated Risk Assessment Process*), además se diseñó como una metodología que podría ser utilizada por los propios directivos con la guía de un profesional capacitado.

El método FRAP consiste de tres pasos, los cuales están diseñados para ser completados en diez días. Éste es un método cualitativo que se auxilia de plantillas y listas de verificación (*checklist*).

Las metodologías de análisis de riesgos existentes describen las etapas en forma teórica: se presentan pocos ejemplos o es necesaria una herramienta para realizarlos cuyo costo es elevado. Por lo anterior, se requiere establecer una metodología cualitativa práctica para realizar un análisis de riesgos a las áreas de TI, estableciendo cómo puede ejecutarse éste. Las etapas y una breve descripción de cada una se muestran a continuación:

Declaración del alcance. En esta primera fase se define el motivo para la realización del análisis; es la delimitación del o los procesos a evaluar.

Establecimiento del equipo de trabajo. Establece el personal necesario que participará en el análisis.

Entrevistas. Fase que permite conocer el proceso desde el punto de vista de los dueños y los usuarios de la información. Las herramientas pueden ser desde una lluvia de ideas hasta cuestionarios.

Identificación de procesos. Como actividades principales se encuentran la elaboración del árbol de procesos a través de un modelo visual para definir todas las variables que se desea estudiar y evaluar.

FRAP analiza un sistema, una aplicación o un segmento del negocio a la vez. Se convoca a un equipo de personas que incluya administradores y soporte para realizar una lluvia de ideas sobre las amenazas potenciales, las vulnerabilidades y los impactos negativos resultantes sobre la integridad, confidencialidad y disponibilidad de los datos/recursos. Además, se analiza el impacto sobre las operaciones de la organización, se priorizan las amenazas y los riesgos y, después de identificarlos y categorizarlos, el grupo dictamina lo que corresponda al respecto.

Por ejemplo, garantizar la seguridad en un software es una tarea muy difícil; por ello, es necesario mitigar los riesgos de que los procesos o la información se vean afectados (figura 3.12).

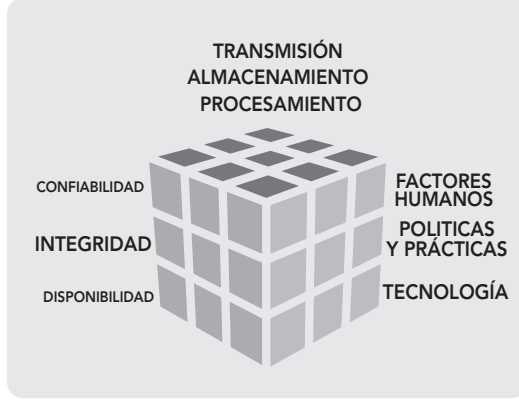


Figura 3.12 Conglomerado de las políticas de seguridad informática en una organización

3.9 Exposición de datos

Al principio, la seguridad de la información de una organización se conseguía por medios físicos y administrativos, ya sea utilizando cajas fuertes donde se guardaban los documentos o procedimientos de investigación de personal durante la fase de contratación. Sin embargo, con la introducción de las computadoras se hizo evidente la necesidad de utilizar herramientas automáticas para proteger los archivos y otras informaciones almacenadas. Este es el caso de los sistemas multiusuarios y los sistemas en los que el acceso se puede hacer desde teléfonos públicos o desde redes de datos.

La utilización de facilidades de comunicación para transportar datos entre computadoras o entre redes de computadoras ha generado un nuevo reto para la seguridad, ya que en dicho proceso hay una exposición de estos; por lo tanto, las medidas de seguridad en la red son necesarias para proteger los datos durante su transmisión y garantizar que estos sean auténticos.

Para ser capaz de entender los tipos de amenaza a la seguridad que existen, se requiere abordar tres exigencias fundamentales de la seguridad a ejecutar en computadoras y en redes (Kaufman, Perlman y Speciner, 2002):

> **Secreto.** Requiere que la información en una computadora sea accesible para lectura de los individuos autorizados. Este tipo de acceso incluye imprimir, mostrar en pantalla y otra forma de revelación que implica cualquier método para dar a conocer la existencia de un objeto.
>
> Integridad. Requiere que los recursos de una computadora sean alterados solamente por personas autorizadas. La modificación incluye escribir, cambiar, suprimir y crear.
>
> **Disponibilidad.** Requiere que los recursos de una computadora estén disponibles a las personas autorizadas.

Los tipos de agresión a la seguridad de un sistema de computadoras o de redes de computadoras se caracterizan mejor viendo la función del sistema como proveedor de información. En general, existe un flujo de información desde un origen, como puede ser un fichero o una región de la memoria principal a un destino (como otro fichero o un usuario).

Como se mencionó en el primer capítulo, la mejor forma de proporcionar la privacidad en los datos es a través del encriptamiento; o sea, ocultando el verdadero contenido del mensaje de forma que si es interceptado no pueda ser descifrado.

3.10 Conclusiones

La seguridad en las redes de computadoras consiste en las políticas adoptadas para prevenir y monitorear el acceso no autorizado, el mal uso, la modificación o la denegación de una red de computadoras; así como de los recursos de acceso a la red; asimismo implica e involucra la autorización del acceso a datos en la red de forma controlada por el administrador: los usuarios escogen o son asignados con un ID y una contraseña u otra información de autenticación que les proporcione acceso a la información y a los programas dentro de su autoridad y jurisdicción.

La seguridad para las redes de computadoras cubre redes públicas o privadas, que se usan en los trabajos de todos los días llevando a cabo transacciones y comunicación entre negocios, organismos gubernamentales e individuos.

La manera más simple y común de proteger un recurso de red es asignando un nombre único y una contraseña. pero un doble factor de autenticación se utiliza con algo que el usuario "tiene"; por ejemplo, un token de seguridad, una tarjeta de crédito o un teléfono celular. También existe un factor de triple de autenticación que usa algo que el usuario "es"; por ejemplo, una huella dactilar o el reconocimiento del iris. Una vez autenticado, un cortafuegos aplica políticas de acceso que determinan los servicios a los cuales pueden acceder los usuarios de la red de computadoras. Aunque esta medida es efectiva para prevenir acceso no autorizado, dicho componente puede fallar al revisar contenido posiblemente dañino; un ejemplo sería un gusano informático o un troyano transmitido en la red.

Un antivirus o un sistema de prevención de intrusos (SPI) ayuda a detectar e inhibir la acción de un *malware*. Éste se encuentra basado en anomalías y también puede monitorear la red; por medio de *wireshark* (analizador de protocolos) es posible revisar el tráfico con propósitos de auditoría o para un análisis de alto nivel. Por otro lado, la comunicación entre dos hosts en una red puede ser encriptada con el propósito de garantizar relativa privacidad.

Finalmente, los *honeypots* (herramienta que atrae a los atacantes) en esencia sirven como distracción para canalizar los recursos de acceso de la red y pueden ser desplegados en una red para vigilar; además, se usan como herramienta de prevención, ya que estos no son normalmente accedidos para propósitos legítimos.

Las técnicas utilizadas por los atacantes que intentan comprometer estos señuelos son estudiados, durante y después del ataque para mantener vigiladas nuevas técnicas de exploit. Dicho análisis puede utilizarse para futuros reforzamientos en la seguridad de la red que está siendo protegida.

Un *honeypot* también puede dirigir la atención del atacante lejos de los servidores legítimos y animar a los atacantes a invertir su tiempo y energía en el servidor de distracción mientras desvía la atención de la información en los servidores reales.

De forma similar, una *honeynet* consiste en una red configurada con vulnerabilidad intencional. Su propósito es, también, el de invitar a los atacantes para que sus técnicas de ataque puedan ser analizadas y ese conocimiento sea utilizado para aumentar la seguridad de la red. Una honeynet normalmente contiene uno o más *honeypots*.

Cuestionario

3.1 Explique a detalle qué es la seguridad en una red de computadoras y establezca estudios de caso exitoso de aplicación.

3.2 Explique a detalle por qué es importante la seguridad en una red de computadoras.

3.3 Explique a detalle en qué consiste la seguridad en una red de computadoras.

3.4 Explique a detalle cómo funciona la arquitectura de gestión de la seguridad en una red de computadoras y establezca estudios de caso exitoso de aplicación.

Referencias

Anderson, R. J. (2001). *Security Engineering*. New York: Addison-Wiley.

Ardita, J. C. (2001). *Entrevista personal*. En instalaciones de Cybsec S. A.

Benson, C. (2011). *Estrategias de Seguridad*. Inobis Consulting Pty Ltd. Microsoft Solutions. USA.

Berghel, H. L. (2001). *Cyberprivacy in the new millennium*. Computer, vol. 34, pp. 132-134.

Biham, E. and Shamir, A. (2007). Differential cryptanalysis of the data encryption standard. Proc. *17th Annual International Cryptology Conference*, Berlin: Springer-Verlag LNCS 1 294, pp. 513-525.

Bird, R.; Gopal, I.; Herzberg, A.; Janson, P. A.; Kutten, S.; Molva, R. and Yung, M. (1993). Systematic design of a family of attack-resistant authentication protocols. *IEEE Jornal on Selected Areas in Communications*, (11): pp. 679-693.

Burnett, S. and Paine, S. (2001). *Security´s official guide to cryptography*. California: Osborne/McGraw-Hill. USA.

Fernández, C. M. (2008). *Seguridad en sistemas informáticos*. España: Ediciones Díaz de Santos S. A.

Huerta Villalón, A. (s.f.). *Seguridad en Unix y redes*. España: Paraninfo.

Kaufman, C.; Perlman, R. and Speciner, M. (2002). *Network security*. New Jersey: Prentice-Hall, 2nd ed.

Lockhart, A. (2007). *Seguridad de redes*. España: Editorial Anaya Multimedia.

Rico, E. (2014). ¡Cuidado con el malware! *Revista Mundo Ejecutivo*, (422), pp. 86-88.

Simmons, G. J. (1992). *A survey of information authentication. Contemporary cryptology: The science of information integrity*. New York: IEEE Press.

Spafford, G. (2000). *Manual de seguridad en redes*. Argentina: ArCERT.

Stinson, D. R. (2002). *Cryptography theory and practice*. Florida: CRC Press, 2nd ed.

Terán Pérez, D. (2013). Introducción a la computación cuántica para ingenieros. México: Alfaomega Grupo Editor.

_____ (2014). *Administración estratégica de la función informática*. México: Alfaomega Grupo Editor.

Union Europea (UE). (2006). *Directiva 2006/43/CE*.

Vaughan, Emmett J. (1997). *Risk Management*. USA: Editorial John Wiley & Sons.

La gestión de la seguridad informática en redes de computadoras

No todo lo que cuenta puede ser cuantificado,
y no todo lo que puede ser cuantificado cuenta.

Albert Einstein

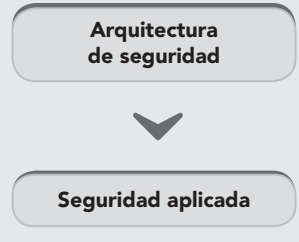
Reflexione y responda las siguientes preguntas:

- ¿Por qué es importante la gestión de la seguridad informática en una red de computadoras?
- ¿Qué es la seguridad por niveles en una red informática?
- ¿Qué son los sistemas unificados de seguridad en una red de computadoras?
- ¿Cómo funciona la arquitectura de gestión de la seguridad en una red informática?

Después de estudiar este capítulo, el lector será capaz de:

- Entender la importancia de la gestión de la seguridad informática en una red de computadoras.
- Comprender la importancia de la seguridad por niveles en una red informática.
- Establecer en qué consisten los sistemas unificados de la seguridad en una red de computadoras.
- Explicar el funcionamiento de la arquitectura de gestión de la seguridad en una red informática.
- Explicar a detalle, cómo se lleva a cabo la seguridad informática aplicada en una red de computadoras.

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:



4.1 Introducción

En la actualidad, cuando se habla de seguridad en las redes de computadoras, se hace referencia a Internet, pues es dentro de esa red de alcance mundial es donde ocurren con mayor frecuencia los ataques a las computadoras. En este contexto, es necesario preguntarse qué alcance tiene el término "seguridad".

En general, se dice que "algo" es seguro, cuando se logra reducir las vulnerabilidades de ese "algo". Pero, ¿qué es la vulnerabilidad en la informática? Según la Organización Internacional de Estándares o Normas, ISO *(International Standarization Organization*), en el contexto de la informática, se considera "vulnerabilidad" a cualquier flaqueza que pueda ser aprovechada para violar un sistema, o la información que éste contiene. De esta manera, se tienen varias posibles violaciones de seguridad a un sistema, o sea, varias amenazas, entre las cuales se destacan las siguientes:

- Destrucción de la información
- Modificación de la información
- Robo, remoción o pérdida de la información, o bien, de los recursos
- Interrupción de los servicios

4.2 Especificación de los principales mecanismos de seguridad

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad o la disponibilidad de un sistema informático. Existen muchos y variados, por lo que su selección depende del tipo de sistema, función y factores de riesgo que lo amenazan. Se clasifican de la siguiente manera según su cometido:

Preventivos. Actúan antes de que un hecho ocurra y su función es detener la intrusión de agentes no deseados.

Detectivos. Actúan antes de que un hecho ocurra, y la tarea es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

Correctivos. Se ejecutan luego de ocurrido el hecho; el principal e importante objetivo es corregir las consecuencias

Según un informe en 2011 del *Congressional Research Service*, las computadoras tienen dos características inherentes que las dejan abiertas a ataques o errores operativos:

- Una computadora realiza exactamente las tareas para las cuales ha sido configurada, eso incluye la revelación de información importante. Sin embargo, un sistema puede ser reprogramado por cualquier persona que tenga los conocimientos adecuados.
- Cualquier computadora hace sólo la tarea para la cual ha sido programada y no le es posible protegerse a sí misma contra un mal funcionamiento o un ataque deliberado, a menos de que este tipo de eventos hayan sido previstos de antemano y se hayan puesto medidas necesarias para evitarlos.

4.2.1 Criptografía: algoritmos simétricos, asimétricos e híbridos

Figura 4.1 Proceso de criptografía informática

El vocablo criptografía proviene de dos palabras griegas: *kryto* y *logos*; lo cual significa estudio de lo oculto. La palabra "criptografía" es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica.

Como se explicó en el capítulo 1, la criptografía se basa en que el emisor produce un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave para crear dicho texto cifrado (Dhiren, 2008). Éste, por medio del canal de comunicación establecido, llega al descifrador que busca obtener el texto en original claro (Burnett y Paine, 2001). Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales, dependiendo del sistema utilizado.

En esencia, la criptografía trata de enmascarar las representaciones caligráficas de una lengua de forma discreta (figura 4.1).

Además, según Marreo Travieso (2010), es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad, pues el problema de la confidencialidad se vincula, por lo regular, con técnicas denominadas de encriptación y la autenticidad por medio de técnicas de firma digital, aunque la solución de ambos, en realidad, se reduce a la aplicación de procedimientos de encriptación y desencriptación.

La necesidad de enviar mensajes de forma que sólo fueran entendidos por los destinatarios hizo que se crearan sistemas de cifrado, de manera que un mensaje después de su transformación únicamente pudiera ser leído siguiendo un proceso de descifrado. Uno de los primeros métodos de encriptado que se documentó es atribuido a Julio César, el cual consistía en tomar el número de orden de una letra, sumarle tres y cambiarla por la letra en ese lugar. Por ejemplo, la palabra "fortaleza", con el algoritmo de César, quedaría como "iruwdohcd".

A partir de la aparición de la criptografía como modelo de seguridad, en algunas civilizaciones ha tenido como propósito prevenir algunas faltas de seguridad desde sus sistemas numéricos hasta su escritura y comunicación. El hecho de que gran parte de las actividades humanas sean cada vez más dependientes de los sistemas de cómputo hace que la seguridad desempeñe una función protagónica, para lo que existen distintos métodos. Por ejemplo, enmascarar las referencias originales de la lengua por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información. El uso de ésta, u otras técnicas, permite un intercambio de mensajes que sólo puedan ser leídos por los destinatarios "coherentes".[1]

Con el tiempo, y por la importancia en el uso militar, los sistemas criptográficos avanzaron en complejidad, hasta llegar al nivel del día de hoy, donde la informática ha entrado en las vidas de casi todas las personas en el mundo, y es indispensable el aumento de la necesidad de seguridad al realizar todas las operaciones.

A pesar de que las personas aún están acostumbradas a enviar o recibir cartas postales que vienen encerradas en un sobre para que su lectura esté reservada solamente al destinatario, en el mundo virtual esto ya no es así, porque en este caso se envía la carta sin un "sobre" que lo contenga. Es decir, sin nada que impida la lectura por parte de cualquiera que pudiera interceptarla. Por ello, fue indispensable el uso de herramientas automatizadas para la protección de archivos y de cualquier otro tipo de información almacenada en las computadoras. Éstas son los cortafuegos, los sistemas detectores de intrusos (SDI) y el uso de sistemas criptográficos, que no sólo permiten proteger la información, sino también a los sistemas informáticos encargados de administrar la información.

Dado que en la actualidad los usuarios de las computadoras no quieren que sus confidencias, datos personales, números de tarjeta de crédito, saldos bancarios, etcétera sean vistos por cualquiera, la criptografía puede garantizar, relativamente, la integridad y la confidencialidad de dicha información. Lo primordial es saber cómo utilizarla, por lo que es importante tener claros los conceptos básicos detrás de los sistemas criptográficos modernos (Ferguson, Schneier y Kohno, 2010), lo cuales implican entender qué es la criptografía, cómo está clasificada, el funcionamiento básico de algunos sistemas de cifrado y cómo se forman los documentos como firmas y sobres digitales.

[1] Un destinatario coherente es la persona a la que el mensaje se le dirige con intención por parte del remitente. Así pues, éste conoce el mecanismo usado para el enmascaramiento del mensaje; por lo que, o bien, posee los medios para someter el mensaje criptográfico al proceso inverso, o puede razonar e inferir el desarrollo que lo convierta en un mensaje de acceso público. En ambos casos, no necesita usar técnicas cripto-analíticas (Ferguson; Schneier y Kohno, 2010).

Por otro lado, es importante responder la siguiente pregunta: ¿cómo funcionan algunos sistemas de cifrado en las redes de computadoras? (figura 4.2).

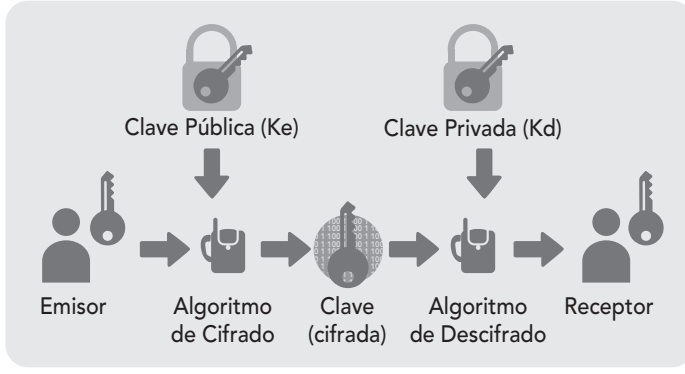


Figura 4.2 Muestra de la operación de la criptografía simétrica y la asimétrica en el envío de información a través de una red de computadoras

Para ello, debe establecerse la existencia de tres tipos de cifrado: el simétrico, el asimétrico y el híbrido.

Sistemas de cifrado simétrico. Son aquellos que utilizan la misma clave para cifrar y descifrar un documento; su principal problema de seguridad reside en el intercambio de datos entre el emisor y el receptor, ya que ambos conocen la contraseña. Por lo tanto, se tiene que buscar también un canal de comunicación que sea seguro para el intercambio.

Es importante que dicha clave sea muy difícil de descubrir, ya que hoy las computadoras pueden adivinar claves de forma rápida y eficiente. Por ejemplo, el Algoritmo de Cifrado DES (*Data Encryption Standard*) [2] usa una clave de 56 bits, lo que significa que hay 72 mil billones de claves posibles (Anderson, 1994), aunque en la actualidad existen computadoras especializadas capaces de probar todas las combinaciones posibles en cuestión de horas.

Hoy por hoy, se utilizan claves de 128 bits que aumentan el "espectro" de claves posibles (2^{128}), de forma que aunque se uniesen todas las computadoras existentes en todo el mundo, no se conseguirían descifrar en miles de millones de años [3] dichas claves (figura 4.3).

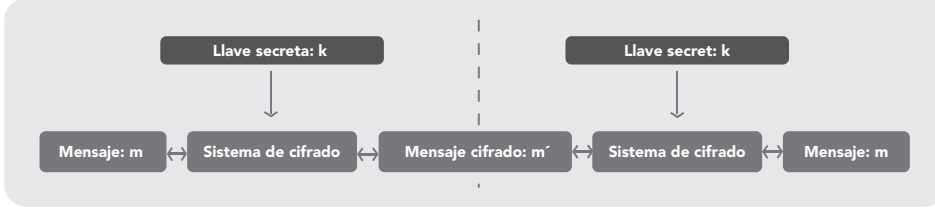


Figura 4.3 Objetivos de la seguridad informática

[2] Estándar de cifrado de datos: algoritmo desarrollado por IBM en requerimiento del NBS (National Bureau of Standards u Oficina Nacional de Estandarización; en la actualidad denominado NIST, National Institute of Standards and Technology o Instituto Nacional de Estandarización y Tecnología de los Estados Unidos de América), y posteriormente modificado, así como adoptado por el gobierno de ese mismo país.

Sistemas de cifrado asimétrico. También son llamados sistemas de *cifrado de clave pública*. Éstos usan dos contraseñas diferentes: una pública, que se puede enviar a cualquier persona; y la otra, privada, que debe guardarse para que nadie tenga acceso a ella.

Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrarse. Una vez hecho esto, solamente con la clave privada del destinatario puede descifrarse; por ello, es posible dar a conocer la clave pública para todo aquel que se quiera comunicar con el destinatario.

Un sistema de cifrado de clave pública, basado en la factorización de números primos, se fundamenta en que la clave contiene un número compuesto de dos números primos muy grandes para cifrar un mensaje. Para descifrarlo, el algoritmo requiere conocer los factores primos, uno de los cuales contiene la clave privada.

En la actualidad, es muy fácil por medio de los complejos sistemas de computadoras, multiplicar dos números relativamente grandes para conseguir un número compuesto; pero es muy difícil la operación inversa. Mientras que 128 bits se consideran suficientes en las claves de cifrado simétrico, y dado que la tecnología de hoy se encuentra muy avanzada, se recomienda en este caso que la clave pública tenga un mínimo de 1 024 bits.

Para un ataque de fuerza bruta, por ejemplo, sobre una clave pública de 512 bits, se debe factorizar un número compuesto de hasta 155 cifras decimales (Brands, 2000).

Tomando en cuenta lo descrito, es necesario considerar que este sistema tiene diversas desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

De modo que los nuevos sistemas de clave asimétrica basados en curvas elípticas tienen características menos costosas (figura 4.4).

Figura 4.4 Sistema de cifrado asimétrico

Sistemas de cifrado híbrido. Es el sistema que usa tanto la clave simétrica como la asimétrica y funciona mediante el cifrado de una clave pública para compartir otra para el cifrado simétrico. Así, en cada mensaje, la clave simétrica utilizada es diferente, por lo que si un atacante pudiera descubrirla, solamente le valdría para ese mensaje y no para los restantes. La clave simétri-

[3] Existe la posibilidad que una computadora cuántica sí pueda resolver este cálculo en algunas horas. Sin embargo, la computación cuántica aún está en fase de investigación e incipiente desarrollo.

ca es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado de manera automática en un solo paquete. El destinatario usa la clave privada para descifrar la clave simétrica y, acto seguido, dicho usuario/destinatario utiliza la clave simétrica con el objetivo de descifrar el mensaje ya mencionado.

Las herramientas como PGP, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan este cifrado híbrido.

Estos tres esquemas se pueden agrupar en dos tipos específicos: centralizados y descentralizados. En los primeros hay varios nodos y cada uno tiene capacidades y derechos. En los segundos hay una arquitectura cliente-servidor donde los servidores juegan un papel central y proveen servicios a los clientes.

Cada esquema tiene sus ventajas e inconvenientes y en cada caso hay que evaluarlos para decidir cuál es el mejor. En general, los sistemas centralizados son más vulnerables a ataques de denegación de servicio debido a que basta con que falle el servidor central para que el sistema de confianza caiga por completo. Éstos se consideran menos seguros contra ataques encaminados a publicar claves públicas falsas, pues al haber varios nodos posibles a atacar, es más difícil garantizar la seguridad.

Los modelos más utilizados son:

Uso de una infraestructura de clave pública (PKI, *Public Key Infrastructure*). En este modelo hay una o varias entidades emisoras de certificados o autoridades de certificación (CA, *Certification Authority*) que aseguran la autenticidad de la clave pública y de ciertos atributos del usuario. Para ello, firman con su clave privada ciertos atributos del usuario incluyendo su clave pública, generando un *certificado del usuario*, figura 4.5.

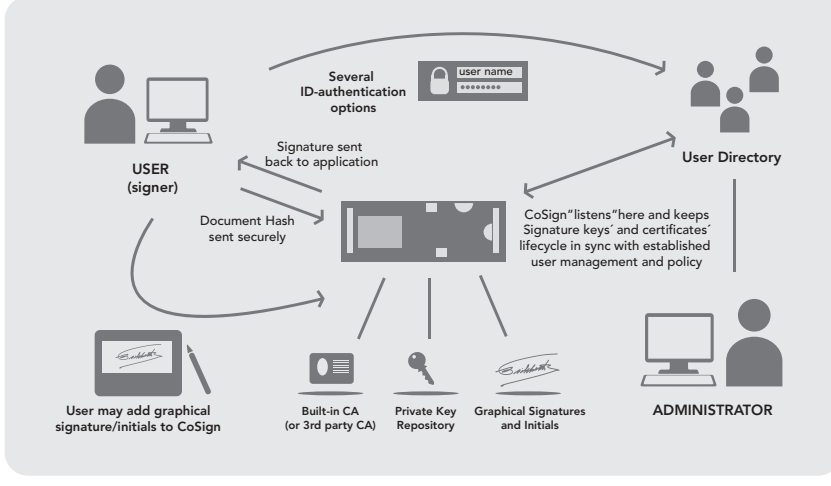


Figura 4.5 Funcionamiento de la arquitectura PKI

Establecimiento de una web de confianza. No hay nodos aparte de los usuarios. Éstos recogen claves públicas de otros usuarios y prometen autenticidad, si están seguros de que la clave privada correspondiente pertenece en exclusiva a dicho usuario. Un individuo, además, puede confiar en el conjunto de cla-

ves públicas en las que otro confía, ya sea de forma directa o a través de otras relaciones de confianza. Dos usuarios que no se conocen pueden fiarse de sus claves públicas, si existe una cadena de confianza que enlace ambas partes. Este tipo de implementación de la confianza es utilizado por PGP (*Pretty Good Privacy*).

Uso de la criptografía basada en la identidad. En este modelo existe un generador de claves privadas o PKG (*Private Key Generator*), que a partir de una cadena de identificación del usuario produce una clave privada y otra pública. La pública la difunde para que el resto de usuarios la sepan y la privada es comunicada en exclusiva al usuario a quien pertenece.

Uso de la criptografía basada en los certificados. El usuario posee una clave privada y otra pública; esta última la envía a una autoridad de certificación que, basada en criptografía fundamentada en identidad, genera un certificado que asegura la validez de los datos.

Uso de la criptografía sin certificados. Es similar al que usa la criptografía basada en identidad, la única diferencia es que lo generado representa una clave parcial. La clave privada completa se produce a partir de la clave privada parcial y un valor originado aleatoriamente por el usuario. La clave pública es creada también por el usuario a partir de parámetros públicos del KGC (*Key Generator Center)* y del valor secreto escogido.

Girault (1991) distingue tres niveles de confianza que dan los distintos modelos a la autoridad que interviene en el proceso (PKG, KGC o CA, según cada caso):

Nivel 1. La autoridad puede calcular claves secretas de usuarios y, por lo tanto, hacerse pasar como cualquier usuario sin ser detectado. Las firmas basadas en identidad pertenecen a este nivel de confianza.

Nivel 2. La autoridad no puede calcular claves secretas de usuarios, pero puede todavía hacerse pasar como cualquier usuario sin ser detectado. Las firmas sin certificados pertenecen a este nivel.

Nivel 3. La autoridad no puede calcular claves secretas de usuarios ni hacerse pasar como un usuario sin ser detectado. Es el nivel más alto de confiabilidad; las firmas tradicionales PKI y las basadas en certificados pertenecen a éste.

Según el segundo principio de Kerckhoffs,[4] toda la seguridad debe descansar en la clave y no en el algoritmo (en contraposición con la seguridad por la oscuridad); por lo tanto, el tamaño de la clave es una medida de la seguridad del sistema, pero no se compara con el tamaño del cifrado de clave pública para medir la seguridad.

Fundamentos de la criptografía

El criptoanálisis es la ciencia que se ocupa del análisis de un texto cifrado para obtener la información original sin conocimiento de la clave secreta. Lo anterior significa que de forma ilícita se rompen los procedimientos de cifrado establecidos por la criptografía; por lo que se dice que criptoanálisis y criptografía son ciencias complementarias, pero contrarias (figura 4.6).

Figura 4.6 Sistemas de criptografía

[4] En 1883 en el campo de la criptografía existen seis principios llamados "de Kerckhoffs" en honor a Auguste Kerckhoffs. Los cuales hacen referencia a las características que son deseables para cualquier sistema criptográfico.

Por otro lado, la esteganografía estudia la forma de ocultar la existencia de un mensaje escondiéndolo en el interior de otro, el cual sólo podrá ser entendido por el emisor y el receptor y pasará inadvertido para todos los demás (Johnson y Jajoda, 1998).

Existen dos tipos de ataques que amenazan las comunicaciones secretas:

Pasivo. Se define cuando el intruso sólo busca obtener información sin hacer algún tipo de modificación, por lo que es difícil percatarse de que se está siendo atacado.

Activo. En este rubro, el intruso además de obtener la información, la modifica; de modo que sirva a sus intereses. Por lo cual, es más fácil percatarse del ataque. Los ataques activos se dividen en dos tipos (ataques a los métodos de cifrado y ataques a los protocolos criptográficos):

Ataques a los métodos de cifrado. Se realizan con la intención de obtener la clave secreta para descifrar libremente cualquier criptograma, para ello se aprovechan una o todas las vulnerabilidades:

- Ataque sólo con texto cifrado: el criptoanalista sólo conoce el criptograma y el algoritmo original. Con esta información pretende obtener el texto en claro.
- Ataque con texto original conocido: el criptoanalista conoce mensajes en claro seleccionados por él mismo y los correspondientes criptogramas, así como el algoritmo que generó cada comunicación. El objetivo primordial de este ataque es conocer la clave secreta y desencriptar con libertad cualquier texto.
- Ataque con texto cifrado escogido: en cual el criptoanalista conoce el algoritmo de cifrado, así como un criptograma seleccionado por él mismo y su correspondiente texto en claro; el objetivo es obtener el mensaje de todo criptograma que intercepte.
- Ataque con texto escogido: el criptoanalista, además de conocer el algoritmo de cifrado y el criptograma que quiere desencriptar, también conoce el criptograma de un texto en claro que él elija y a la inversa.

Ataques a los protocolos criptográficos. Este tipo de ataques no pretenden encontrar la clave secreta para conocer el mensaje en claro, sino que buscan obtener la información vulnerando los protocolos criptográficos; es decir, procuran burlar la serie de pasos establecidos para alcanzar los objetivos de seguridad, los cuales tienen que ser realizados por las entidades involucradas en cierta comunicación (Johnson y Jajoda, 1998). Algunos ejemplos de este tipo de ataques son los siguientes:

- Ataque con clave conocida: el atacante conoce claves utilizadas en cifrados anteriores y con base en ellas intenta determinar nuevas claves.
- Suplantación de personalidad: el atacante asume la identidad de uno de los agentes autorizados en la red y, de esta manera, obtiene libremente y sin tropiezos todos los mensajes en claro.
- Compilación de un diccionario: es un archivo guardado en la memoria de la computadora que contiene contraseñas cifradas de los usuarios autorizados en el sistema. Si el método de cifrado es público, el atacante puede generar claves aleatorias y después cifrarlas con el objetivo de hallar alguna

contenida en éste (previamente obtenido). Cuando una clave generada por el atacante coincide con alguna del diccionario, se ha encontrado una llave de acceso al sistema mediante el usuario correspondiente a ésta.

- Búsqueda exhaustiva: este ataque se lleva a cabo generando de manera aleatoria todos los valores posibles de las claves de acceso y probándolas hasta que una de ellas sea válida en el sistema.
- Ataque de hombre en medio: el intruso se filtra en la línea de comunicación entre dos agentes autorizados en la red; obtiene la información de uno de ellos y se la envía al otro usuario una vez que la ha utilizado.

Herramientas criptográficas

En la actualidad existen multitud de herramientas criptográficas para cifrar datos o comunicaciones en tránsito aplicando criptografía simétrica o asimétrica. Éstas buscan proteger la confidencialidad de la información tanto en el tránsito como al almacenarla. Además, permiten el cifrado y descifrado de la información mediante técnicas criptográficas, lo que impide un uso indebido de ésta por personas no autorizadas; por ejemplo, vía correo electrónico o por medio de la transferencia de ficheros. Así mismo, incorpora mecanismos para detectar las manipulaciones durante su envío o su almacenamiento, por lo tanto, son herramientas que también protegen la integridad de la información. Éstas se subdividen en:

Herramientas de cifrado de las comunicaciones. Se encargan de la protección de la información en tránsito en aplicaciones de mensajería instantánea, correo electrónico, navegación web, etcétera. De igual forma permiten ocultar la información en mensajes y ficheros adjuntos para que se puedan enviar de forma segura a través de una red insegura como es Internet.

Herramientas de cifrado de discos duros y soportes de almacenamiento. Se destinan a la encriptación de todo tipo de soportes de almacenamiento: discos duros internos y externos, memorias USB, etc.

Entre las recomendaciones de uso de estas herramientas criptográficas se destacan las siguientes:

- Es fundamental establecer una adecuada política de gestión de las contraseñas y de las cuentas de acceso utilizadas para cifrar/descifrar la información que se desea proteger.
- Lo ideal es utilizarlas en dispositivos móviles o de almacenamiento que siempre contengan información sensible (figura 4.7).

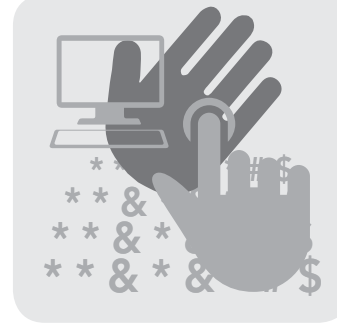


Figura 4.7 Uso de las herramientas criptográficas en el entorno informático actual

Firma digital

Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje determinar la entidad originadora de éste para confirmar que no ha sido alterado desde que fue firmado por el originador.

La firma digital se aplica en aquellas áreas donde es importante verificar la autenticidad y la integridad de ciertos datos, como en documentos electrónicos o *software*, porque proporciona una herramienta para detectar la falsificación y la manipulación del contenido. Para Dhiren (2008), la terminología asociada al concepto de firma electrónica hace referencia a un método para producir firmas digitales que permite verificar la autenticidad y consiste en un algoritmo de generación de firma y verificación, ambos asociados con un método para formatear los datos en mensajes que puedan ser firmados.

La validez se ampara en la imposibilidad de falsificar cualquier tipo de firma, la cual radica en el secreto del firmante (Pastor Franco y Sarasa López, 1998). En el caso de las firmas escritas, el secreto está constituido por características de tipo grafológico inherentes al signatario y, por ello, difíciles de falsificar. Por su parte, en el caso de las firmas digitales, es el conocimiento exclusivo de una clave utilizada para generarla. Para garantizar la seguridad de las firmas digitales es necesario a su vez que éstas sean:

Únicas. Las firmas deben ser producidas sólo por el firmante, porque poseen la característica de ser siempre infalsificables; por lo tanto, la firma debe depender única y exclusivamente del firmante.

Infalsificables. Para falsificar una firma digital el atacante tiene que resolver problemas matemáticos de complejidad muy elevada; es decir, las firmas han de ser computacionalmente seguras.

Verificables. Las firmas deben ser fácilmente verificables por los receptores de las mismas y, de ser necesario, por los jueces o autoridades competentes.

Innegables. El firmante no debe ser capaz de negar su propia firma; es decir, no existe el repudio hacia la firma por parte del firmante en ningún caso.

Viables. Las firmas han de ser invariablemente fáciles de generar por parte del firmante.

Por otro lado, es posible construir esquemas de firma digital basándose en distintos tipos de técnicas, según lo establece Preneel (2010):

En la supuesta seguridad de los dispositivos físicos. Un dispositivo como una tarjeta inteligente, se dice que es resistente a modificaciones (*tamper resistant*), si se cree que es difícil acceder a la clave secreta almacenada en él; por lo tanto, se puede usar una tarjeta inteligente con un algoritmo criptográfico para construir una firma digital de la siguiente forma: el signatario tiene una tarjeta inteligente que puede sólo cifrar con una clave secreta K_1, y cada verificador tiene una tarjeta inteligente que puede únicamente descifrar con una clave secreta K_2, de forma que lo cifrado por K_1 sólo puede ser verificado por K_2. Es importante establecer que K_1 y K_2 pueden ser iguales (*clave simétrica*) o distintas (*claves asimétricas*). En este tipo de mecanismo hay que abordar el problema de instalar y almacenar de forma segura las claves en las tarjetas inteligentes. Falsificar una firma es difícil si el dispositivo es resistente a modificaciones.

La criptografía de clave simétrica. Se han propuesto distintos protocolos de firma basados en la criptografía de clave secreta. Sin embargo, a partir de la aparición de la criptografía asimétrica, estos se encuentran en recesión debido a su superioridad tanto conceptual como operacional en la mayoría de los contextos de uso; dichos esquemas están basados en el uso de una función de un solo sentido (*one-way function*). La gran desventaja de este tipo de protocolos es el tamaño de las claves y las firmas, además del hecho de que

sólo pueden ser usadas un número fijo de veces. Merkle (1990) ha propuesto optimizaciones para este tipo de algoritmos y Bleichenbacher y Maurer (1996) han proporcionado una generalización de ellos. Estos esquemas primitivos han servido en construcciones más complejas. Los esquemas de firma digital de clave simétrica son los siguientes:

- Firma de Desmedt
- Firma de Lamport-Diffie
- Firma de clave simétrica de Rabin
- Firma de Matyas-Meyer

En la criptografía de clave asimétrica. Se han propuesto distintos protocolos de firma basados en la criptografía de clave asimétrica. Los más importantes son los siguientes:

- Firma RSA
- Firma DSA
- Firma ESING
- Firma de clave asimétrica de Rabin
- Firma El Gamal
- Firma con curvas elípticas
- Firma de Guillou-Quisquater
- Firma de Ohta-Okamoto
- Firma de Schnorr
- Firma de Okamoto
- Firma de Feige-Fiat-Shamir

El uso de criptografía asimétrica para firma digital se basa en el concepto de funciones de un solo sentido con trampa (*trapdoor one-way functions*). Éstas son funciones fáciles de programar en una sola dirección y difíciles de hacerlo en otra, excepto para alguien que conozca la información "*trampa*"; por lo que ésta puede, entonces, ser firmada digitalmente si el signatario la modifica con su clave secreta.

El verificador puede comprobar la firma digital aplicando la transformación en el sentido fácil usando la clave pública y observando que aquélla se corresponda con el mensaje que se quería firmar.

Además, hay que evaluar una serie de factores que dan la validez real de la firma:

Es necesario verificar que la clave usada por el signatario sea válida. Por lo regular, las claves para firmar tienen mecanismos que sólo las hacen válidas durante cierto tiempo, el cual se limita mediante uno o varios mecanismos como fechas de caducidad que permiten comprobar que la clave no ha sido revocada por el firmante.

En algunas ocasiones la firma lleva un sello de tiempo (*time-stamping*). Éste registra el momento en que se ha realizado la firma. Dicho sello se puede utilizar por los protocolos para establecer periodos de tiempos después de los cuales la firma no es válida; por ejemplo, podría establecerse un sistema en el que las firmas sólo son válidas durante 30 minutos después de haberse producido.

La figura 4.8 presenta algunos dispositivos que permiten establecer la firma digital.

Figura 4.8 Dispositivos que permiten realizar una firma digital

Las aplicaciones de firma digital son programas informáticos que permiten firmar un documento electrónico. Existen algunos programas de uso cotidiano como Adobe Acrobat o Microsoft Word, que posibilitan firmar el mismo documento que se genera; sin embargo, este tipo de firma tiene dos inconvenientes:

- No todos los programas que producen documentos son capaces también de firmarlos.
- En general, el destinatario del documento firmado deberá tener la misma aplicación para ser capaz de verificar la firma.

Las herramientas o aplicaciones específicas de firma electrónica son capaces de firmar cualquier tipo de documento electrónico y ayudan a superar los inconvenientes anteriores; además, se pueden descargar gratuitamente. La figura 4.9 muestra una pantalla con una firma digital.

Figura 4.9 Pantalla que muestra una firma digital

Gracias a la firma digital, los ciudadanos de todo el mundo pueden realizar transacciones de comercio electrónico seguras y relacionarse con la máxima eficacia jurídica, abriéndose por fin las puertas a la posibilidad de obtener documentos como la Clave Única de Registro Poblacional (CURP) en México, la licencia de conducir, el pasaporte, el acta de nacimiento, etc.

En la vida cotidiana se presentan muchas situaciones en las cuales los ciudadanos deben acreditar fehacientemente su identidad, como al pagar las compras con una tarjeta de crédito o de débito en un establecimiento comercial, al votar en las fechas electorales (locales o federales), al identificarse en el mostrador de una empresa, al firmar documentos notariales, etcétera. En estos casos, la identificación se realiza mediante la presentación de documentos acreditativos como la credencial de elector expedida por el Instituto Nacional Electoral (INE) en México, que contiene una serie de datos significativos vinculados al individuo que los presenta (nombre del titular del documento, número de serie del documento, vigencia, fotografía del titular, etcétera.). En otras situaciones, se requiere una rúbrica para que el documento goce de validez legal, puesto que se vincula al signatario con el documento por él firmado.

Ahora bien, en un contexto electrónico donde no existe contacto directo entre las partes involucradas, ¿resulta posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder la seguridad y confianza de estos últimos? La respuesta, por fortuna, es afirmativa. El uso de la firma digital satisface todos los aspectos de seguridad descritos. A diferencia de la firma manuscrita que es un trazo sobre el papel, la firma digital consiste en el agregado de un apéndice al texto original, que es el resultado de un cálculo realizado sobre la cadena binaria de este último.

La firma digital se puede aplicar en las siguientes situaciones:

- *E-mail*.
- Contratos electrónicos.
- Procesos de aplicaciones electrónicos.
- Formas de procesamiento automatizado.
- Transacciones realizadas desde organizaciones financieras alejadas.
- Transferencias en sistemas electrónicos. En caso de que se busque enviar un mensaje para transferir $100 000 desde una cuenta a otra, éste debe pasar sobre una red protegida, pues, de lo contrario, es muy posible que algún adversario desee alterarlo, tratando de cambiar los $100 000 quizá por $1 000 000. Sin embargo, en caso de no existir información adicional no se podrá verificar la firma, lo cual indicará que ha sido alterada y, por lo tanto, se denegará la transacción.
- En aplicaciones de negocios como el Intercambio Electrónico de Datos (EDI, *Electronic Data Interchange*) de computadora a computadora, intercambiando mensajes que representan documentos de negocios.
- En sistemas legislativos es necesario consignar el grupo fecha/hora a un documento para indicar las condiciones en las cuales el documento fue ejecutado o llegó a ser eficaz (Barriuso Ruíz, 1996).

Certificado digital

Por otro lado, un certificado digital o electrónico es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet (figura 4.10).

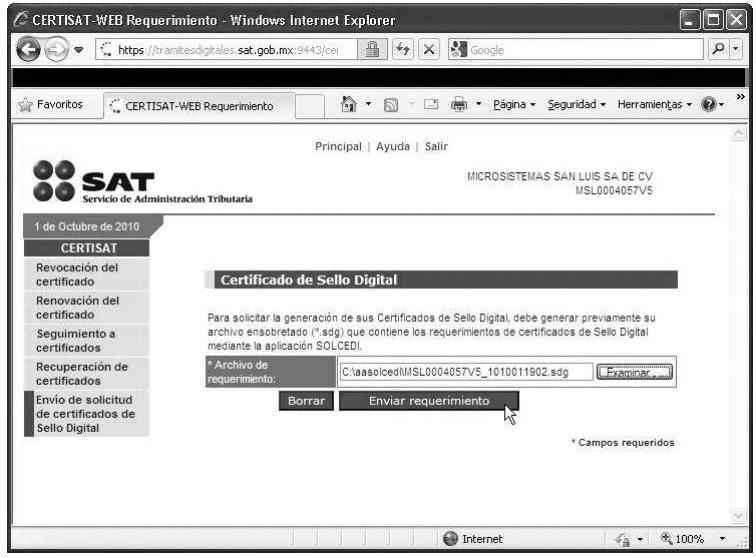


Figura 4.10 Muestra de un certificado digital emitido en la República Mexicana por el Sistema de Administración Tributaria (SAT)

El certificado digital tiene como función principal autenticar al poseedor, pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para realizar ciertos trámites que impliquen intercambio de información sensible entre las partes involucradas.

Un certificado electrónico sirve para:

- Autenticar la identidad del usuario de forma electrónica ante terceros.
- Firmar electrónicamente de manera que se garantice la integridad de los datos trasmitidos y su procedencia. Un documento firmado no puede ser manipulado, ya que la firma está asociada matemáticamente tanto al documento como al firmante.
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

4.2.2 Cortafuegos

Como se mencionó en el capítulo 1, un cortafuegos o *firewall* es la parte de un sistema o red diseñado para bloquear accesos no autorizados, permitiendo, al mismo tiempo, comunicaciones autorizadas. En 1992, Bob Braden y DeSchon Annette de la Universidad

del Sur de California (USC) dieron forma al concepto de cortafuegos. El producto conocido como Visas, se considera el primer sistema con una interfaz gráfica con colores e iconos implementables y compatibles con sistemas operativos como Windows o MacOS (figura 4.11).

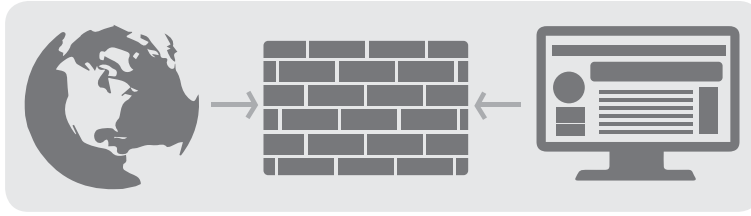


Figura 4.11 Representación del uso de un cortafuegos dentro de una red de computadoras

En 1994, la compañía israelí Check Point Software Technologies patentó como *software* al cortafuegos denominándolo FireWall. De acuerdo con la tecnología y aplicación, los cortafuegos se dividen en los siguientes tipos:

Primera generación. Cortafuegos de red utilizados para el filtrado de paquetes. En 1988, se registró el primer documento para la tecnología de un cortafuegos cuando el equipo de ingenieros de la empresa estadounidense *Digital Equipment Corporation* (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema bastante básico fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad en Internet.

El filtrado de paquetes actúa mediante la inspección de estos: si un paquete coincide con el conjunto de reglas del filtro, se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico; en su lugar, se filtra cada paquete basándose sólo en la información contenida (Rodríguez, 2014).

Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes no puede distinguir entre éstos a menos de que las máquinas a cada uno de sus lados estén a la vez utilizando los mismos puertos no estándar (Rodríguez, 2014).

El filtrado de paquetes llevado a cabo por un cortafuegos actúa en las tres primeras capas del modelo de referencia OSI, lo que significa que todo el trabajo lo realiza entre la red y las capas físicas (Cheswick, Bellovin y Rubin, 2003). Cuando el emisor origina un paquete y es filtrado por el cortafuegos, este último comprueba las reglas de filtrado que lleva configuradas, aceptando o rechazando el paquete.

Segunda generación. El cortafuegos de estado tiene en cuenta la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, si es parte de una existente o es un paquete erróneo.

Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

Tercera generación. Los cortafuegos de aplicación son aquellos que actúan sobre la capa de aplicación del modelo OSI; su clave es que puede entender ciertas aplicaciones y protocolos, además permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de uno de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con uno de filtrado de paquetes porque repercute en las siete capas del modelo de referencia OSI; en esencia es similar a aquél, pero la diferencia radica en que también se puede filtrar el contenido. Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquearla, no obstante, los *cortafuegos de aplicación* resultan más lentos que los *cortafuegos de estado*.

La real funcionalidad existente de inspección profunda de los paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS). Actualmente, el grupo de trabajo de comunicación *Middlebox* de *Internet Engineering Task Force* (IETF) trabaja en la estandarización de protocolos para la gestión de cortafuegos.

Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuegos, por lo que algunos proporcionan características como unir a las identidades de usuario con las direcciones IP o MAC. Otros, como el cortafuegos NuFW, ofrecen propiedades de identificación real, solicitando la firma del usuario para cada conexión (Orera Gracia y Soriano Sarrió, 2012).

Para fines pragmáticos, los cortafuegos se clasifican en los siguientes tipos (Orera Gracia y Soriano Sarrió, 2012):

Cortafuegos de *hardware*. Proporcionan una fuerte protección contra la mayoría de las formas de ataque del mundo exterior; éstos se pueden comprar como producto independiente o en equipos ruteadores de banda ancha. Desafortunadamente, luchando contra virus, gusanos y troyanos un cortafuegos de *hardware* puede ser menos eficaz que uno de *software*, pues podría no detectar gusanos en los correos electrónicos.

Cortafuegos de *software*. Para usuarios particulares, el cortafuegos más utilizado es uno de *software*; éste protegerá una computadora contra intentos de control o acceso, y, por lo regular, proporciona protección adicional contra los troyanos o los gusanos más comunes que se envían a través del correo electrónico. La desventaja de los cortafuegos de *software* es que protegen solamente a la computadora en la que están instalados y no a una red completa de equipos.

Por otro lado, hay varios tipos de técnicas que, en la práctica, muchos cortafuegos utilizan (dos o más a la vez):

Packet filter. Mira cada paquete que entra o sale de la red y lo acepta o rechaza basándose en reglas definidas por el usuario. La filtración del paquete es bastante eficaz y transparente a los usuarios, pero es difícil de configurar. Además, es susceptible al IP *spoofing*.

Application gateway. Aplica mecanismos de seguridad a ciertas aplicaciones como servidores FTP y servidores Telnet. Esto es muy eficaz, pero puede producir una disminución de las prestaciones.

Circuit-level gateway. Aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se haya hecho la conexión, los paquetes pueden fluir entre los anfitriones sin más comprobaciones.

Proxy server. Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta con eficacia las direcciones de red verdaderas.

Políticas de seguridad y su integración en sistemas de cortafuegos

En la batalla para proteger la red de la organización, la política de seguridad continúa creciendo en tamaño y complejidad, pues se intensifica por los cambios en las necesidades de la organización, las repentinas innovaciones en los equipos de Tecnología de la Información (TI) y las aplicaciones empresariales críticas que dependen de muchos componentes interconectados.

La gestión de las políticas de los cortafuegos se ha convertido en una tarea difícil y propensa a errores que consume valiosos recursos, lo que produce impactos negativos en la agilidad de la inteligencia de negocios y da lugar a la formación de brechas en la seguridad y en el cumplimiento.

Un sistema de gestión de la seguridad proporciona una solución automatizada, centrada en las aplicaciones para el manejo de complejas políticas de seguridad mediante cortafuegos y elementos de infraestructura de seguridad relacionados con el objetivo tácito de mejorar tanto la seguridad como la agilidad de los negocios.

Un adecuado sistema de gestión de la seguridad cierra las brechas tradicionales entre los equipos de seguridad, las redes y las aplicaciones para racionalizar y agilizar las operaciones de seguridad y el manejo de cambios, asegurar el real cumplimiento continuo, maximizar la disponibilidad de las aplicaciones y la rapidez de la provisión de servicios, así como proporcionar una política de seguridad más impenetrable que brinde mayor protección contra los ataques cibernéticos.

El fundamento de *Security Management Suite* de un sistema de gestión de la seguridad es la tecnología patentada *Deep Policy Inspection*, denominada en español como una "inspección profunda de políticas", que proporciona un análisis superior de la política de seguridad poniendo al descubierto más resultados procesables con mayor precisión (Microsoft Tech, 2001). Entre los objetivos de las políticas de seguridad y su integración en sistemas de cortafuegos están los siguientes:

Traducir en automático los requisitos de conectividad a reglas de cortafuegos. Permite que los cambios para requerimientos de conectividad de aplicaciones en evolución sean procesados de forma rápida y precisa mediante el cómputo automático de los cambios necesarios en las reglas de cortafuegos subyacentes y la activación de las solicitudes de cambios relevantes.

Evaluar el impacto de los cambios en la red sobre la disponibilidad de las aplicaciones. Esto ayuda a las principales partes interesadas a entender el impacto que los cambios en la red, como migraciones de servidores, pueden tener sobre las aplicaciones de la organización y activar las solicitudes de cambios de cortafuegos necesarios para asegurar la disponibilidad de las aplicaciones.

Garantizar la seguridad en el desmantelamiento de las aplicaciones. Elimina de un modo seguro los accesos a la red de las aplicaciones desmanteladas con el fin de garantizar el fortalecimiento de la política de seguridad sin afectar negativamente la disponibilidad o el funcionamiento de otras aplicaciones del negocio.

Realzar la visibilidad a través de un portal central de conectividad de aplicaciones. Una visión consolidada y actualizada de los requerimientos de conectividad para las aplicaciones permite a los equipos de seguridad y de redes comunicarse eficazmente con los propietarios de las aplicaciones de la empresa para acelerar la provisión de servicios.

Descubrir y mapear las reglas subyacentes y las ACL (listas de control de acceso) a las aplicaciones. Las potentes capacidades de descubrimiento permiten que las reglas de acceso de los cortafuegos y enrutadores se mapeen a aplicaciones existentes, lo que reduce de forma importante el tiempo y el esfuerzo requeridos para poblar el repositorio de aplicaciones.

Entregar un registro de auditoría completo con todos los cambios. Las auditorías y las pruebas de cumplimiento se simplifican mediante la actualización y conservación de una historia completa de todos los cambios realizados a la aplicación que soporta a los mandatos de cumplimiento, tanto internos como externos.

Existen dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

Política restrictiva. Se deniega todo el tráfico excepto el permitido explícitamente, de modo que el cortafuegos debe habilitar sólo el tráfico de los servicios necesarios. Esta aproximación es usada por las empresas y los organismos gubernamentales.

Política permisiva. Se permite todo el tráfico excepto aquel explícitamente denegado. Cada servicio, en potencia peligroso, necesitará ser aislado caso por caso; mientras que el resto del tráfico no será filtrado. Esta aproximación se utiliza en universidades, centros de investigación y servicios públicos de acceso a Internet.

La política restrictiva es la más segura por el alto nivel de autorización que maneja ante un error de tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya considerado algún caso de tráfico peligroso y sea admitido por omisión.

4.2.3 Redes privadas virtuales (VPN)

Una red privada virtual es una tecnología de red que posibilita una extensión segura de la red local (LAN) sobre una pública o no controlada como Internet. Concede que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una privada, con toda la funcionalidad, seguridad y políticas de ésta (Mason, 2002). Ello se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos. Algunos ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando

como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo o que un usuario pueda acceder a su dispositivo doméstico desde un sitio remoto como un hotel; todo ello utilizando la infraestructura de Internet. La conexión VPN a través de Internet es técnicamente una unión *Wide Area Network* (WAN) entre los sitios, pero al usuario le parece como si fuera un enlace privado, de allí la designación *Virtual Private Network (*Microsoft Tech, 2001).

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de SSL y tecnologías de autenticación, las cuales protegen los datos que pasan por la red privada virtual contra accesos no autorizados.

Las organizaciones pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar con rapidez nuevos sitios o usuarios (Microsoft Tech, 2001). También, se les permite aumentar de manera drástica el alcance de la red privada virtual sin expandir significativamente la infraestructura (figura 4.12).

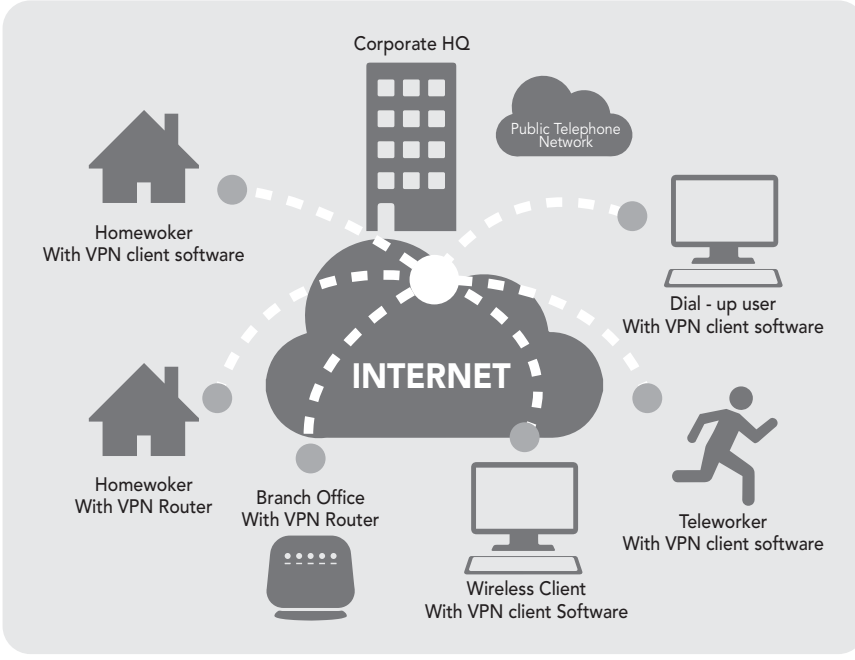


Figura 4.12 Representación de una VPN

Las redes VPN SSL y VPN IPsec se han convertido en las principales soluciones de redes privadas virtuales para conectar de forma segura oficinas y usuarios remotos y socios comerciales (*partners*) (Perlman y Kaufman, 2000) porque:

- Aumentan la productividad al ampliar el alcance de las redes y aplicaciones empresariales.
- Reducen los costos de comunicación y aumentan la flexibilidad.

Los dos tipos de redes virtuales privadas cifradas son las siguientes:

VPN IPsec de sitio a sitio. La alternativa a *Frame Relay* o redes WAN de línea arrendada permite a las empresas extender los recursos de la red a las sucursales, oficinas en el hogar y sitios de los *partners* comerciales.

VPN de acceso remoto. Esto extiende prácticamente todas las aplicaciones de datos, voz o video a los escritorios remotos emulando los de la oficina central. Las redes VPN de acceso remoto pueden desplegarse usando redes VPN SSL, IPsec o ambas; dependiendo de los requisitos de su implementación (Perlman y Kaufman, 2000).

Para emular un vínculo punto a punto, los datos se empaquetan con un encabezado que proporciona la información de enrutamiento que permite recorrer *Internetwork* de transporte público o compartir un canal o túnel para llegar a su punto final. Para emular un vínculo privado, los datos enviados se encriptan para su confidencialidad.

La porción de la conexión en la que se encapsulan los datos privados se conoce como el túnel; en cambio, en la que se cifran los datos privados es la red privada virtual (VPN).

Por lo tanto, la VPN debe proporcionar por lo menos lo siguiente:

Autenticación de usuario. Se debe verificar la identidad del cliente VPN y restringir el acceso solamente a los usuarios autorizados. También debe proporcionar registros de auditoría y contabilidad para mostrar a qué información accedieron y cuándo lo hicieron.

Gestión de direcciones. Es necesario asignar la dirección de un cliente VPN en la Intranet y asegurarse de que las direcciones privadas se mantienen de esa manera.

Cifrado de datos. Los datos transportados en la red pública deben ser ilegibles a clientes no autorizados en la red.

Administración de las claves. Se requiere generar y actualizar las claves de cifrado para el cliente y el servidor.

Soporte multiprotocolo. La solución debe manejar protocolos comunes usados en la red pública. Estos incluyen IP y el *Internetwork Packet Exchange* (IPX).

Una solución VPN de Internet basada en el protocolo de túnel punto a punto (PPTP, *Point to Point Tunneling Protocol*) o protocolo de túnel (L2TP, *Layer 2 Tunneling Protocol*) cumple con todos estos requisitos básicos y se aprovecha de la amplia disponibilidad de Internet. Otras soluciones, incluyendo Internet Protocol Security (IPSec), reúnen sólo algunos de estos requisitos, pero siguen siendo útiles para situaciones específicas (Perlman y Kaufman, 2000).

4.2.4 Creación e infraestructura de redes virtuales

El objetivo de la virtualización de redes consiste en facilitar un uso compartido de sus recursos, eficaz, controlado y seguro para los usuarios y los sistemas, donde el producto final son las redes virtuales clasificadas en dos clases principales:

Externas. Constan de varias redes locales que el *software* administra como una entidad única. Las partes que componen las redes virtuales externas clásicas son el *hardware* de conmutación y la tecnología de *software* de red de área

local virtual (VLAN). Un par de ejemplos son las grandes redes corporativas y los centros de datos.

Interna. Consta de un sistema que usa zonas o máquinas virtuales, cuyas interfaces de red están configuradas mediante, al menos, una NIC física; éstas se denominan tarjetas de interfaz de red virtual o NIC virtual (VNIC).

El aislamiento de esta red interna respecto de otros sistemas externos se consigue configurando las VNIC mediante *Etherstubs*,[5] tras lo que se pueden combinar los recursos para redes virtuales tanto internas como externas. Por ejemplo, es posible ajustar los sistemas individuales con redes virtuales internas en las LAN que formen parte de una gran red virtual externa.

La creación de una red virtual consta de uno o varios pasos para configurar *Etherstubs* o VNIC y de otros tantos para las zonas requeridas. Aunque éstos son conjuntos de procedimientos independientes, ambos deben llevarse a cabo para finalizar la construcción de la red virtual. Los elementos a tomar en cuenta son los siguientes:

- La red virtual de un sistema consta de tres zonas, las cuales están en diferentes etapas de configuración: la primera zona se crea como nueva; la segunda ya existe en el sistema y se debe volver a configurar para utilizar una VNIC, y la tercera está designada como red virtual privada. Por lo tanto, los procedimientos demuestran las diversas maneras para preparar las zonas para la red virtual.
- La interfaz física del sistema está configurada con la dirección IP 192.168.3.70.
- La dirección IP del enrutador es 192.168.3.25.

4.2.5 Ventajas y desventajas de las VPN

Son muchas las ventajas que puede ofrecer una VPN bien planeada, tal vez una de las principales tiene que ver con la utilización de redes públicas como Internet, ya que ésta permite que una organización obtenga ahorros considerables en vez de utilizar una instalación de líneas rentadas; pero también existen otras ventajas relacionadas con la administración, la seguridad, la consolidación y la transparencia. Además, la responsabilidad de su funcionamiento recae sobre el proveedor de servicios, lo cual libera a la organización de los costos y recursos necesarios para operar y mantener una infraestructura de red, algo de especial valor para las organizaciones que cuentan con configuraciones de red de gran complejidad. A continuación, se detallarán algunas de estas ventajas:

- Permiten disfrutar de una conexión a red: que incluye todas las características de la red privada a la que se quiere acceder.
- Son independientes: pueden implementarse en diversas plataformas de sistemas operativos como UNIX, Windows, Linux, etc.
- Cuentan con una diversificación de conexiones: pueden utilizarse en líneas rentadas, enlaces Frame Relay, ATM, RDSI, T1 o Wireless.

[5] Los *Etherstubs* son pseudo-NIC Ethernet. Las VNIC mediante un *Etherstubs* se independizan de las NIC físicas del sistema. Con los *Etherstubs* puede construirse una red virtual privada que esté aislada de las demás redes virtuales del sistema y de la red externa. Por ejemplo, si desea crear un entorno de red cuyo acceso esté limitado únicamente a los desarrolladores de su empresa y no a la red en general, los Etherstubs pueden ser de utilidad.

El cliente VPN adquiere totalmente la condición de miembro de la red: debido a esto se le aplican todas las directivas de seguridad y permisos de una computadora en esa red privada, pudiendo acceder a información tal como bases de datos y documentos internos a través de un acceso público.

Reducción de costos: las VPN, al utilizar Internet como medio de comunicación, reducen los costos drásticamente en comparación con las líneas dedicadas a las infraestructuras de marcación interna.

Ofrecen flexibilidad al poder optar por múltiples tecnologías y proveedores de servicio: esa independencia posibilita que la red se adapte a los requerimientos del negocio.

Aumenta la conectividad geográfica: por medio del uso de Internet cualquier usuario se puede conectar a la LAN de su organización desde cualquier punto del planeta siempre y cuando exista un Proveedor de Servicios de Internet (PSI) en esa área.

Seguridad mejorada: una VPN ofrece múltiples elementos de seguridad, reduce riesgos como el falseamiento de una IP, la pérdida de confidencialidad y la inyección de paquetes.

Facilidad de ampliación: conforme los proveedores de red incrementan el ancho de banda en sus redes, las VPN pueden crecer y aprovecharlo.

Beneficios en el diseño de red: el administrador de red no tiene que lidiar con problemas en el diseño como los de una WAN sobre líneas rentadas, que pueden ser flujo de tráfico entre departamentos ubicados en distintos puntos geográficos y la creación de conductos adecuados para éste, ni con las cuentas de acceso de usuarios remotos por marcación y cargas adicionales al instalar enlaces redundantes en caso de que falle el de comunicación principal.

Asignación de prioridades de tráfico: debido a que una VPN proporciona acceso a una Intranet, Extranet o servidores internos de una organización, varios proveedores ofrecen asignación de tráfico a través de sus productos VPN.

El tipo de tráfico puede pasar libremente: con el fin de conservar el ancho de banda, se determina qué tipo de tráfico puede pasar libremente, mientras que otro queda en cola de espera.

Por último, es importante mencionar las desventajas de instalar una red privada virtual (VPN): inicialmente, implementar tecnología VPN implica ciertos costos adicionales por parte de la organización; éstos se encuentran involucrados con los aspectos de implementación, mantenimiento, precios de las licencias y algunos cargos de telecomunicaciones que no se eliminan por completo.

A continuación, se mencionan los inconvenientes más significativos:

Equipo VPN. La gran variedad de equipos que existen para implementar una VPN puede representar un problema a la hora de la instalación; por lo es necesario saber qué tipo de *hardware* y *software* se añadirá; esto incluye routers, concentradores, servidores, cableado, etcétera. Todo esto se debe multiplicar por el número de sitios que se tienen para obtener un costo aproximado.

Licencias. Éstas tienen un costo para el tipo de producto que se requiera y dependen de los proveedores, quienes cobran por el número de usuarios simultáneos que pasan a través de un dispositivo de red. Mientras que otros

añaden una cuota de licencia simple al *router*, permitiendo conexiones VPN ilimitadas; unos más basan sus cuotas de licencias en el número de túneles que se pueden crear.

Administración y mantenimiento. Si el encargado del mantenimiento y de la administración de la VPN es el propio Proveedor de Servicios de Internet (PSI), se agrega un costo extra por el servicio. Por ejemplo, si surge un problema con el *hardware*, es preciso tomar en cuenta el tiempo que se llevará la reparación, así como su precio. Generalmente, los proveedores ofrecen líneas de mantenimiento con precios variables y pueden abarcar los fines de semana, otro gasto que se incurre con el uso de esta tecnología.

4.2.6 Intranets y extranets en VPN

Las VPN de Intranet suponen reducción en costos frente a la tecnología *Frame Relay* y de líneas dedicadas, por lo general utilizan Internet para reducir distancias entre las sucursales. En la figura 4.13, se muestra un ejemplo de una VPN que se basa en una Intranet.

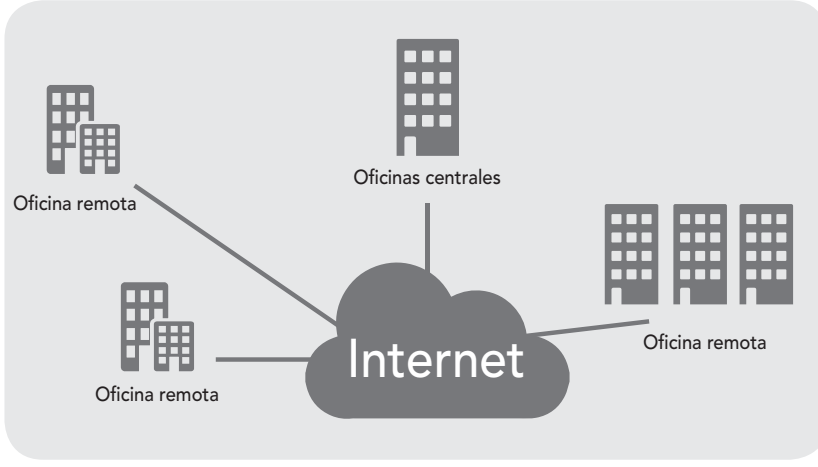


Figura 4.13 VPN que se basa en una Intranet

Las VPN de acceso remoto proporcionan acceso a grandes distancias entre la Intranet o la Extranet de una organización y los usuarios móviles remotos; estos pueden estar ubicados en algún punto geográfico con la posibilidad de acceder completamente a los recursos de su red corporativa, conectándose directamente a través de cualquier Proveedor de Servicios de Internet (PSI) mediante una llamada telefónica, un cable o una línea DSL.

Las VPN de acceso remoto pueden soportar las necesidades de los usuarios móviles, las Extranets cliente a empresa, etcétera; además de terminarse en dispositivos de extremo final como un router, un cortafuegos o un concentrador desplegado en el perímetro de una red. En la figura 4.14 se muestra uno de los tipos de acceso más comunes utilizando un PSI para acceder a la red.

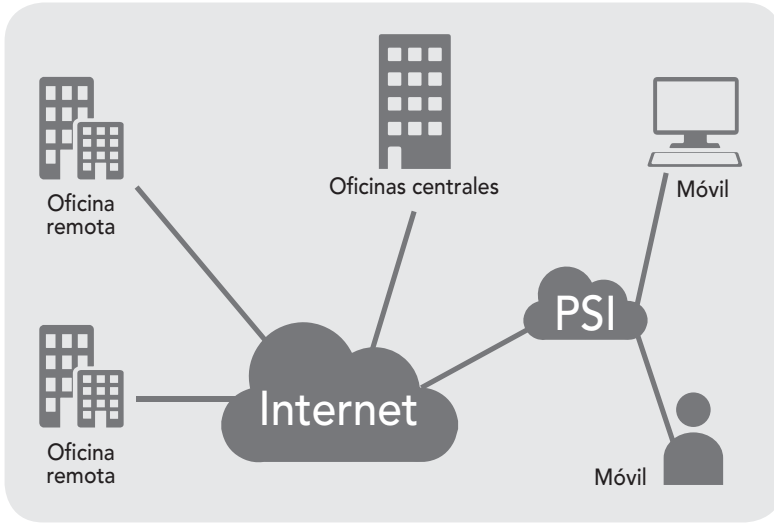


Figura 4.14 Ejemplo de uno de los tipos de acceso más común utilizando un PSI para acceder a la red

Por otro lado, las redes privadas virtuales (VPN) de Extranet son casi idénticas a las de Intranet, aunque cuentan con la diferencia de que éstas se hallan dirigidas a socios externos. Las VPN de Extranet enlazan clientes exteriores, proveedores, socios o comunidades de interés para una empresa con el propósito de intercambiar información y realizar transacciones.

Implementar una VPN de Extranet implica incrementar complejidad en lo referente a la autenticación y el acceso por medio de los túneles VPN y cortafuegos para que las empresas socias accedan de forma segura a ciertos recursos específicos sin tener, por ello, entrada a toda la información corporativa confidencial. En la figura 4.15 se muestra un ejemplo de una VPN basada en Extranet.

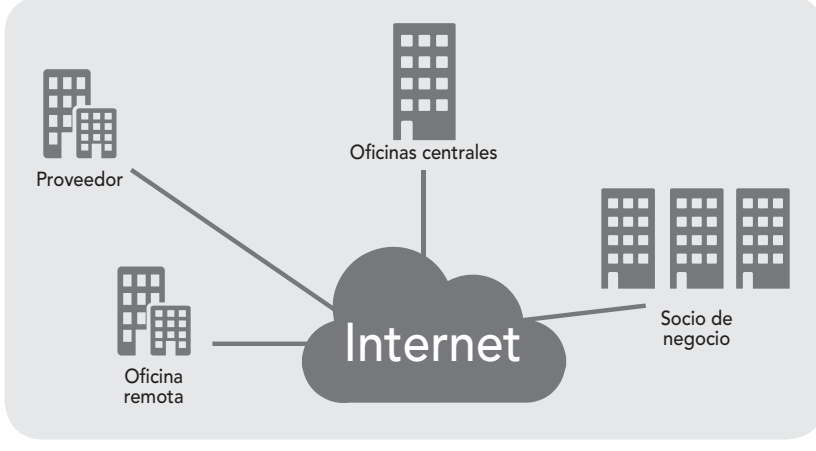


Figura 4.15 Red privada virtual (VPN) basada en una Extranet

4.2.6 Sistema de detección de intrusos (IDS)

Un sistema de detección de intrusos (IDS, *Intrusion Detection System*) es un programa utilizado para localizar accesos no autorizados a una computadora o a una red; éstos pueden ser ataques de habilidosos *crackers*[6] o de *script kiddies*,[7] que usan herramientas automáticas.

El IDS suele tener sensores virtuales con los que el núcleo obtiene datos externos (generalmente sobre el tráfico de red); además, detecta anomalías que pueden ser indicio de la presencia de ataques o de falsas alarmas (Merkle, 2010).

El funcionamiento de estas herramientas se basa en el examen pormenorizado del tráfico de red, el cual, al entrar al analizador, es comparado con firmas de ataques conocidos o comportamientos sospechosos, como puede ser la verificación de puertos o los paquetes malformados. El IDS, normalmente integrado con un cortafuegos para convertirse en una herramienta sumamente poderosa, no sólo analiza qué tipo de tráfico entra, sino que también revisa el contenido y su comportamiento.

Los IDS disponen de una base de datos de "firmas" de ataques conocidos, las cuales permiten distinguir entre el uso normal de la computadora y el fraudulento; y/o entre el tráfico normal de la red y el que puede ser resultado de un ataque o intento de éste.

Existen dos tipos de sistemas de detección de intrusos:

> ***HostIDS* (HIDS).** El principio de funcionamiento depende del éxito de los intrusos, que generalmente dejarán rastros de sus actividades en el equipo atacado cuando pretenden realmente adueñarse de éste con el propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado y hacer un reporte de sus conclusiones.
>
> ***NetworkIDS* (NIDS).** IDS basado en red que localiza ataques a todo su segmento. Su interfaz debe funcionar en modo promiscuo, capturando así todo el tráfico.

Para poner en funcionamiento un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución mediante la utilización de la arquitectura de sistemas, a través del uso de paquetes y de programas o, incluso, una combinación de estos dos. La posibilidad de introducir un elemento de arquitectura de sistemas es debido al alto requerimiento de procesador en redes con mucho tráfico (Merkle, 2010). A su vez, los registros de firmas y de las bases de datos con los posibles ataques necesitan gran cantidad de memoria, aspecto a tener en cuenta.

En redes de computadoras es necesario considerar el lugar de colocación del IDS: si la red está segmentada con un concentrador (capa 1 del modelo OSI) no hay problema en analizar todo el tráfico de la red realizando una conexión a cualquier puerto. En cambio, si se utiliza un conmutador (capa 2 del modelo OSI), se requiere conectar el IDS a un puerto SPAN (*Switch Port Analiser*) para el análisis. La figura 4.16 muestra la operación de un IDS.

[6] Persona malintencionada y experta que rompe algún sistema de seguridad.

[7] Inexperto que interrumpe en los sistemas informáticos mediante el uso de herramientas automatizadas preempaquetadas y escritas por otros, generalmente con poca comprensión del concepto subyacente.

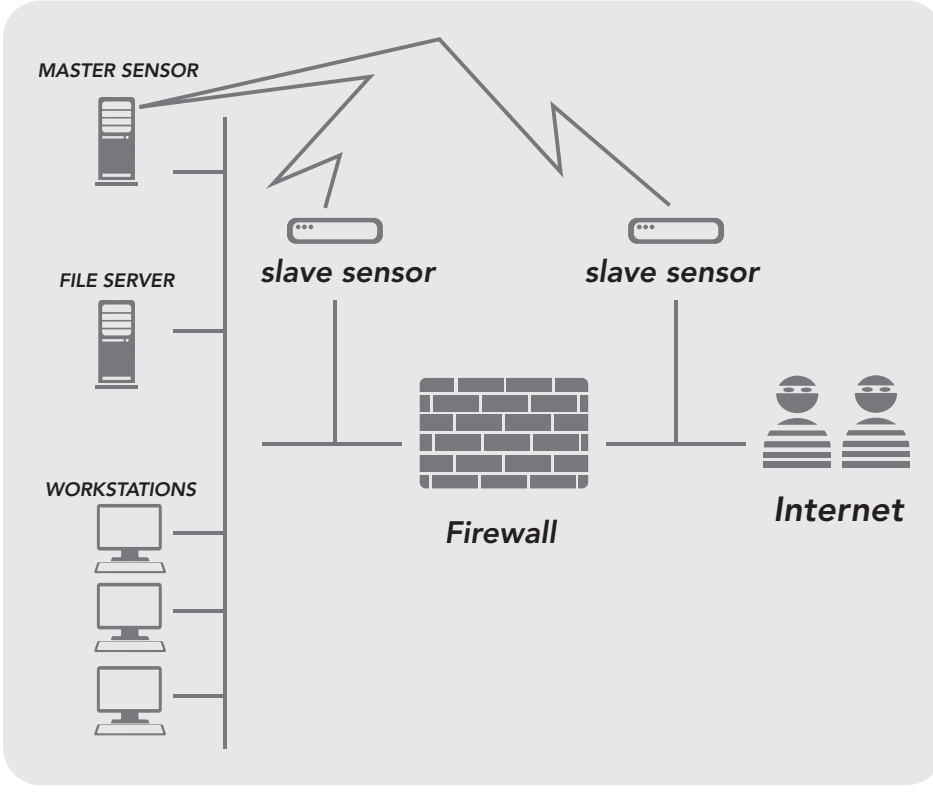


Figura 4.16 Representación del uso de un IDS

4.3 Seguridad por niveles

Las políticas de seguridad informática, que involucran la seguridad por niveles en las organizaciones, constituyen las alarmas y los compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por lo tanto, deben constituir un proceso continuo y realimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y de renovación, la aceptación de las directrices y la estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general. Las políticas por sí solas, no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores, por administrar efectivamente sus recursos, y a reconocer en los mecanismos de seguridad informática, factores que facilitan la formalización y la materialización de los compromisos adquiridos con la organización. Los niveles de seguridad son distribuidos de acuerdo con el sistema operativo que se esté utilizando sobre la red de la empresa o institución, ya sea pública, privada, gubernamental o no gubernamental.

4.3.1 Seguridad a nivel aplicación

Los ataques a nivel de aplicación son una amenaza en constante aumento contra la seguridad web, pues utilizan una gran variedad de medios con el objetivo de paralizar un sitio web e introducirse en él, lo que provoca resultados que varían desde un menor rendimiento de éstos hasta robo de datos y una desprotección de la infraestructura; por esta razón, es sumamente importante desarrollar excelentes esquemas de seguridad (figura 4.17).

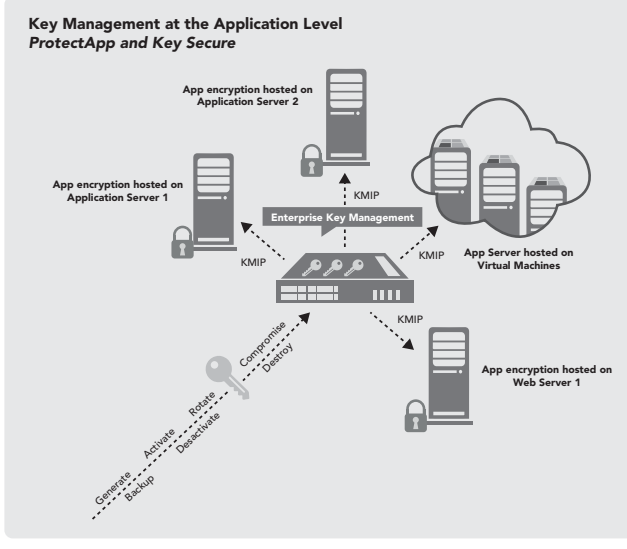


Figura 4.17 Esquema de la seguridad a nivel aplicación

La seguridad en las aplicaciones web involucra principalmente al desarrollador, auncon frecuencia se hallan defectos que pueden ser aprovechados por atacantes en las tecnologías en que se basan los sistemas web; por lo tanto, la atención principal debe dirigirse a los defectos propios en el desarrollo de las aplicaciones (Held, 2010).

Los programadores con frecuencia desconocen que las aplicaciones pueden ser accedidas con herramientas diferentes al navegador web o, incluso, la existencia de aditamentos a los navegadores que potencializan su uso de manera diferente al común. Entendiendo lo anterior, todo programador debe estar consciente de que depende de él rechazar o filtrar las peticiones recibidas que no cumplan con las características esperadas o predefinidas. Ninguna entrada al sistema debe ser digna de una confianza plena, por lo que todas deben pasar por el filtrado de los datos contenidos para confirmar su usabilidad (Crovella y Krishnamurty, 2006). Además, para el programador debe ser claro y fácil de identificar cuando una variable ya ha sido sometida al proceso de limpieza; de esta forma, se evita tener que confiar en la memorización o tener que hacer un mapa de los procesos ejecutados por cada línea de código ejecutada de manera previa.

Otro aspecto a considerar son los procesos de salida de la información del sistema. Es importante siempre tomar en cuenta el significado que pueda tener la información enviada en su nuevo contexto y, en el caso de poder crear problemas de interpretación de las salidas, escalarlas para preservarlas. Al igual que en el proceso de filtrado, es imprescindible mantener un control sobre la codificación que tienen los datos antes de enviarlos. El ejemplo de esto lo tiene la codificación como entidades HTML de las salidas, pero existen otros muchos ambientes o contextos en los cuales la información saliente debe adaptarse para evitar problemas similares, como podría ser el del intérprete de peticiones de la base de datos.

4.3.2 Seguridad a nivel transporte

El uso de un protocolo seguro a nivel de red puede requerir de la adaptación de la infraestructura de comunicaciones; por ejemplo, cambiar los *routers* o encaminadores IP por otros que entiendan IPsec (Day y Zimmermann, 2003).

Un método alternativo que no necesita modificaciones en los equipos de interconexión es introducir la seguridad en los protocolos de transporte. La solución más usada actualmente es el uso del protocolo SSL o de otros basados en éste; por ejemplo:

> ***Secure Sockets Layer* (SSL).** Desarrollado por Netscape Communications a principios de los años 90 del siglo pasado. La primera versión de éste, ampliamente difundida e implementada, fue la 2.0. Poco después, Netscape publicó la versión 3.0 con muchos cambios respecto a la anterior y que hoy ya casi no se utiliza.
>
> ***Transport Layer Security* (TLS).** Elaborado por la IETF *(Internet Engineering Task Force*). La versión 1.0 del protocolo está publicada en el documento RFC 2 246 y es prácticamente equivalente a SSL 3.0 con algunas pequeñas diferencias, por lo que en ciertos contextos se considera el TLS 1.0 como si fuera el protocolo SSL 3.1.
>
> ***Wireless Transport Layer Security* (WTLS).** Pertenece a la familia de protocolos WAP (*Wireless Application Protocol*) para el acceso a la red de dispositivos móviles. La gran mayoría de éstos son adaptaciones de los ya existentes a las características de las comunicaciones inalámbricas y, en particular, el WTLS

está basado en el TLS 1.0. Las diferencias se centran principalmente en aspectos relativos al uso eficiente del ancho de banda y de la capacidad de cálculo de los dispositivos, que puede ser limitada.

En resumen, las medidas de seguridad a nivel de transporte protegen la relación de datos dentro de la red y entre varias redes. Cuando se realizan comunicaciones en una red tan poco fiable como lo es en realidad Internet, no se puede controlar totalmente el flujo del tráfico desde el origen hasta el destino. A menos de que se establezcan medidas de seguridad como la configuración de las aplicaciones para que utilice SSL, los datos direccionados estarán a disposición de cualquiera que desee verlos y utilizarlos.

Las medidas de seguridad a nivel de transporte protegen los datos mientras fluyen entre los otros límites de nivel de seguridad. Cuando se desarrolla una política de seguridad completa en Internet, se debe diseñar individualmente una estrategia para cada capa del Modelo OSI (Day y Zimmermann, 2003). Asimismo, es necesario describir cómo interactuará cada conjunto de estrategias con las otras para ofrecer así una red de seguridad integral en una organización.

4.3.3 Seguridad a nivel de enlace

Existen varios protocolos de comunicaciones que operan a nivel de enlace, sin embargo, los dos más relevantes son 802.3 (CSMA/CD-Ethernet) y 802.11, redes inalámbricas WLAN.

La familia 802.X tiene este nombre justamente porque se crea un comité de IEEE en 1980 durante el mes de febrero, cuando el concepto de las redes LAN comienza a imponerse como algo digno de ser analizado (ITU, 2005). Dentro de este comité se conforman diferentes grupos de trabajo, los cuales en la actualidad son denominados de la siguiente manera:

IEEE 802.1. Normalización de la interfaz
IEEE 802.2. Control de enlace lógico
IEEE 802.3. CSMA/CD (*Ethernet*)
IEEE 802.4. *Token-Bus*
IEEE 802.5. *Token-Ring*
IEEE 802.6. MAN
IEEE 802.7. Grupo asesor en banda ancha
IEEE 802.8. Grupo asesor en fibras ópticas
IEEE 802.9. Voz y datos en LAN
IEEE 802.10. Seguridad
IEEE 802.11. Redes Inalámbricas WLAN
IEEE 802.12. Prioridad por demanda
IEEE 802.13. El uso de éste ha sido usualmente evitado por superstición
IEEE 802.14. Módems de cable
IEEE 802.15. WPAN (*Bluetooth*)
IEEE 802.16. Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX).

IEEE 802.17. Anillo de paquete elástico
IEEE 802.18. Grupo de asesoría técnica sobre normativas de radio
IEEE 802.19. Grupo de asesoría técnica sobre coexistencia
IEEE 802.20. *Mobile Broadband Wireless Access* (MBWA)
IEEE 802.21. *Media Independent Handoff* (MIH)
IEEE 802.22. *Wireless Regional Area Network* (WRAN)

Al igual que en la capa física, las vulnerabilidades de esta capa de enlace están ligadas al medio sobre el que se realiza la conexión y/o transmisión de los datos. La figura 4.18 muestra el uso de un cortafuegos para proteger la red LAN de una conexión WAN; este nivel comprende la conexión con el nodo inmediatamente adyacente, lo cual en una red punto a punto es sumamente claro, pero en una red LAN es difícil de interpretar.

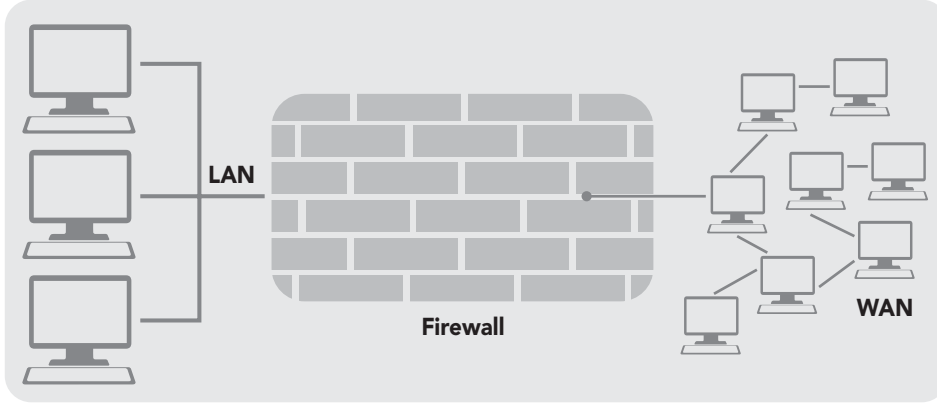


Figura 4.18 Seguridad en la capa de enlace entre una LAN y una WAN.

En esta capa de enlace se debe auditar lo siguiente desde un enfoque de seguridad:

Control de direcciones de *hardware*. El objetivo máximo en este nivel es poseer el control de la totalidad de las direcciones de *hardware* de la red. Esto implica poseer la lista completa del direccionamiento MAC o también llamado NIC (*Network Interface Card*); es decir, de las tarjetas de red.

Auditoría de configuración de un *bridge* o de *switch*. Estos son los dispositivos que operan a nivel 2, es decir, el de un *bridge* multipuerto; su trabajo consta de ir aprendiendo por qué puerto se hace presente cada dirección MAC; y a medida que va aprendiendo, conmuta el tráfico por la puerta adecuada, segmentando la red en distintos "dominios de colisión". La totalidad de estos dispositivos es administrable en forma remota o por medio de una consola; las medidas que se pueden tomar en su configuración son variadas y de suma importancia en el tráfico de una red.

Análisis de tráfico. La transmisión puede ser unicast (de uno a uno), *multicast* (de uno a muchos) o *broadcast* (de uno a todos). El rendimiento de una red se ve seriamente resentido con la presencia de este último arreglo; de hecho, es una de las medidas de mayor interés para optimizar las redes y también es

motivo de un conocido ataque a la disponibilidad llamada "bombardeo de *broadcast*". Otro tipo de medidas es el análisis de los *multicast*, pues éstos son los mensajes que intercambian los *routers* o encaminadores, en los cuales se encontrará servida toda la información de ruteo de la red.

Análisis de colisiones. Una colisión se produce cuando un *host* transmite y otro lo hace simultáneamente en un intervalo de tiempo menor a 512 microsegundos (que es el tamaño mínimo de una trama Ethernet) si se encuentra a una distancia tal que la señal del primero no llegó. Ante este hecho, los dos *host* hacen "silencio" y esperan una cantidad aleatoria de "tiempos de ranura" (512 microsegundos) e intentan transmitir nuevamente. Si se tiene acceso físico a la red, un ataque de negación de servicio es justo generar colisiones, pues obliga a hacer "silencio" a todos los *host* de ese segmento (figura 4.19).

Detección de *sniffers* o analizadores de protocolos. Ésta es una de las tareas más difíciles; pues dichos elementos solamente escuchan y se hacen presentes cuando emplean agentes remotos que recaban información de un determinado segmento o subred y la transmiten al colector de datos en intervalos de sondeo.

Evaluación de puntos de acceso Wi-Fi. Esta tecnología sólo es segura si se configura adecuadamente, por lo tanto en este aspecto es de especial interés verificar en qué tipo de protocolos de autenticación se han configurado los permisos de acceso a estos dispositivos, su potencia de emisión, la emisión de *beacons*, etcétera (Gast, 2005).

Evaluación de dispositivos *Bluetooth*. Aunque no es un tema abordado frecuentemente, no se debe dejar de lado la existencia de este tipo de dispositivos, que en muchas aplicaciones y *hardware* viene activado por defecto, por lo que estando a una distancia adecuada es posible su explotación y uso (Jakobsson y Wetzel, 2001).

Figura 4.19 Es de gran importancia utilizar mecanismos de seguridad en la transmisión de datos y de información en una red de computadoras

4.4 Identificación de ataques y de respuestas con base en las políticas de seguridad

La definición de un ataque es simple: partiendo de que una amenaza se puntualiza como una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad; un ataque no es más que la realización de aquélla.

Por su parte, una técnica de intrusión es un conjunto de actividades que tienen por objetivo violar la seguridad de un sistema informático. Éstas no solamente deben ser conocidas por los atacantes, sino que se hace imprescindible que sean distinguidas por todos aquellos profesionales de las tecnologías de información, a fin de proteger y resguardar los sistemas de manera veraz y oportuna (Anderson, 2008).

A continuación se mencionan algunos de los principales entornos que provocan ataques a las redes de computadoras:

Keyloggers. *Software* encargado de registrar todas las actividades del teclado de un equipo de cómputo sin que el usuario lo note; generalmente son usados para obtener contraseñas de acceso autorizado a sistemas. Los *keyloggers* también pueden ser utilizados en favor de la seguridad informática, pues permiten llevar un registro de lo que hacen los usuarios en los equipos. Por ejemplo, pueden emplearse para determinar qué acciones se llevaron a cabo durante una sesión de trabajo al interpretar las secuencias introducidas por medio del teclado; esto puede delatar si el usuario ingresó a una cuenta que no le corresponde o si modificó información importante del sistema (figura 4.20).

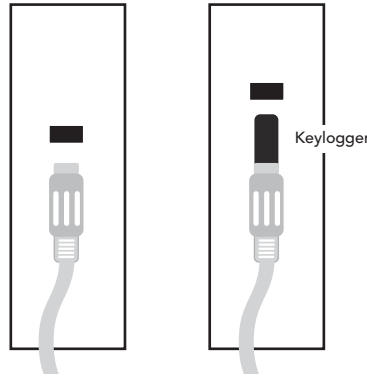


Figura 4.20 Uso de un *keylogger*

Ingeniería social. Es la práctica más frecuente para obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien, a violar las políticas de seguridad típicas. Con este método, se aprovecha la tendencia natural de la gente a confiar en su palabra antes que beneficiarse de agujeros de seguridad en los sistemas informáticos. Generalmente, el principio por el que se rige la ingeniería social es que "los usuarios son el eslabón débil" en seguridad (figura 4.21).

***Jamming* o *flooding*.** Este tipo de agresiones desactivan o saturan los recursos del sistema; por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Figura 4.21 Significado de la ingeniería social

***Packet sniffing*.** Muchas redes son vulnerables al *eaves dropping* (literalmente traducido como "escuchar secretamente"), que consiste en la pasiva intercepción del tráfico de red; o sea, sin modificarlo. En Internet, esto es realizado por paquetes *sniffers* o husmeadores, que pueden ser colocados tanto en una estación de trabajo conectada a la red, a un equipo *router* o a una pasarela de Internet, y esto puede ser realizado por un usuario con legítimo acceso o por un intruso que ha ingresado por otras vías.

***Snooping* y *downloading*.** Los ataques de esta categoría tienen el mismo objetivo que el *sniffing* (obtener la información sin modificarla), sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, *e-mail* y otra información guardada, realizando en la mayoría de los casos una descarga (*downloading*) de la información a su propia computadora.

***Tamppering* o *data diddling*.** Esta categoría se refiere a la modificación desautorizada de los datos o del *software* instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando aquel que los realiza ha obtenido derechos de administrador o de supervisor, por lo que puede, por ende, alterar o borrar cualquier información o llevar el sistema a su baja total en forma deliberada.

Barrido o escaneo de puertos. Consiste en verificar cuáles puertos están disponibles para ser explorados dentro de una o más computadoras en una red. Por sí solo, el barrido de puertos es una actividad normal que frecuentemente es usado para mejorar los servicios de seguridad y rendimiento, pero también es posible que se convierta en una actividad nociva, ya que puede ser usada para buscar puntos de acceso vulnerables para forzar la entrada al sistema: existen casos en que éste tiene varios puertos abiertos y son desconocidos para el encargado de seguridad, por lo que, en consecuencia, no son vigilados y los datos pueden fluir a través de ellos sin ningún tipo de control de seguridad, convirtiéndose en una vulnerabilidad. Esto puede ser consecuencia de una mala configuración de los sistemas de seguridad, los cuales posibilitan dejar de forma predeterminada varios puertos abiertos; además de que los administradores del cortafuegos olvidan revisar minuciosamente la configuración para verificar todos los puertos disponibles.

***OS Fingerpriting*.** Proceso para reconocer el sistema operativo de un usuario remoto de una red; esta identificación se basa en las características que diferencian a cada uno de los sistemas de los demás: distintas implementaciones de la pila TCP/IP, diferentes comportamientos ante el envío de paquetes que presentan una conformación especial, diversas respuestas en función del protocolo utilizado, etcétera. El objetivo no sólo se limita a identificar el sistema operativo remoto, sino que también se puede obtener información de cómo

funciona en caso de ser un sistema personalizado que no es posible encontrar en un listado comercial. El *fingerpriting* tiene aplicaciones benéficas para la seguridad informática, pero, como la mayoría de estos recursos, también puede usarse para un ataque, siendo la identificación de un sistema operativo remoto uno de los primeros pasos a realizar para un ataque.

Redes inalámbricas. Conjunto de dispositivos informáticos comunicados entre sí por medios no tangibles. Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima, en las redes inalámbricas esta tarea es más sencilla. Debido a esto, hay que poner especial cuidado en su protección, pues el primer paso para conectarse a ella es detectar su presencia, así como recabar información sobre su configuración.

Si una red no está cifrada, se dice que está abierta, pero no significa que se encuentre desprotegida, ya que puede estar usando un sistema de resguardo distinto al cifrado WEP/WPA. Estos datos son suficientes para conectarse a una red propia, pero no para entrar a una red a la que no se está autorizado. Los métodos que los intrusos utilizan para recopilar información son las siguientes:

Pasivo. Estos sistemas se limitan a escuchar e interpretar la información que reciben; por ejemplo, las redes suelen emitir su identificación SSID por lo tanto, basta recibir esos paquetes para reconocer este nombre. Los ataques pasivos afectan la confidencialidad pero no influyen necesariamente en la integridad de los datos.

Activo. En este caso, los sistemas no se limitan a escuchar, sino que interactúan de una u otra forma con la red; por ejemplo, si no reciben el nombre SSID buscan el punto de acceso o los equipos de los usuarios para conseguirlo. Los ataques activos pueden llegar a modificar, eliminar o inyectar tráfico a la red. La información que se puede conseguir utilizando estos métodos es del siguiente tipo:

- Nombre SSID, aunque el punto de acceso lo tenga oculto.
- Esquema de direccionamiento IP de la red.
- Marca y modelo del *hardware*.
- Versión del *software*.
- Tipo de cifrado utilizado.
- Clave de cifrado WEP.
- Puertos IP abiertos.
- Información intercambiada.

Todo esto no puede conseguirse en un solo ataque o con una sola herramienta, por lo que el atacante deberá recopilar la información en diversos pasos sin ser descubierto y usar todo tipo de herramientas y de métodos, incluyendo, de ser necesaria, la ingeniería social.

4.5 Sistemas unificados de administración de seguridad

Un sistema unificado de administración de seguridad es un conjunto integrado de productos de primer nivel probados en la industria de cómputo, con base en un análisis de comportamiento y correlación; éste utiliza una arquitectura sistémica que activa la integración del subsistema real y la correlación/información adaptativa compartida de amenazas halladas y alertas que detectan vulnerabilidad entre todos los subsistemas de aplicaciones y dispositivos. Este nivel de integración proporciona un contexto a largo plazo para amenazas y envía alertas anticipadas de éstas, teniendo reconocimiento de ataque que otros productos no pueden ver (Anderson, 2008). Los módulos de aplicación pueden desplegarse como parte de una infraestructura de seguridad o incrementarse poco a poco según los cambios en los requerimientos de la red y del negocio a través del tiempo.

Existen los siguientes servicios:

Gestión de amenazas (GA). Proporciona acceso único e inmediato a la fuente de datos para priorizar la amenaza desde una seguridad múltiple, de fuentes de red y de servidor. El sistema unificado de administración de seguridad monitorea continuamente y actualiza un repositorio de todos los activos, amenazas, vulnerabilidades, registros y comportamientos, así como una firma de las alertas de IDS, que son recopiladas, integradas, correlacionadas y normalizadas para cada organización y comunidad global de fuentes externas. La GA despliega instantáneamente las amenazas a la red más crítica en un formato claro y sencillo, que determina el mejor camino para la solución y recopila datos para un reporte legal. Al utilizar un enfoque innovador de mantenimiento mínimo, el sistema no requiere de agentes, sintonización o de reglas complejas de correlación, así que los recursos críticos de la Tecnología de la Información (TI) se pueden enfocar en tareas más importantes.

Prevención y detección de intrusión (PDI). Reconoce accesos no autorizados y suministra análisis de alerta automáticos, correlación, escalamiento y prioridades; medidas contrarias a ataques de denegación de servicio, finalización de sesiones de ataque, prevención de sondeo y correlación global y de empresa. Los módulos IDS/IPS utilizan un elemento inteligente como sistema de inspección y captura, que selecciona paquetes sospechosos para el análisis de comportamientos futuros. Estos módulos también emplean paquetes de inspecciones profundas de los niveles 1 al 7 y de firmas las 24 horas, los siete días de la semana, los 365 días del año.

Análisis de comportamiento de la red (ACR). Proporciona herramientas de correlación y análisis de comportamiento, que monitorean constantemente las vulnerabilidades y ataques globales y que detecta actividad de amenazas de forma anticipada. El sistema clasifica y prioriza las alertas de las firmas IDS con base en la hostilidad a la red, que se deriva en parte del conocimiento del tráfico normal de ésta, determinado por el análisis de comportamiento, el cual se lleva a cabo por largos periodos de tiempo y que tiene una naturaleza adaptativa.

Gestión de la vulnerabilidad (GV). Ofrece adaptabilidad y escaneos de seguridad en curso, que integran y correlacionan datos y alertas de otros dispositivos, así como una extensa capacidad de investigación para saber desde

dónde se genera el ataque. Este módulo de administración de vulnerabilidad y escaneo por demanda investiga miles de diferentes tipos de vulnerabilidades, además de proporcionar escaneos constantes de seguridad que son integrados y correlacionados con alertas y datos producidos por el motor de análisis de comportamiento, que son priorizados en un escalamiento con base en los ataques contra las vulnerabilidades detectadas.

Consola de gestión unificada (CGU). Consola de monitoreo basada en la navegación, en las firmas en el servidor, en el administrador de cluster y en el servidor de web que utiliza la instalación *plug&play*; ésta guarda todos los reportes y gráficas para el conjunto del dispositivo y los demás módulos del sistema conectados al motor de análisis de comportamiento, que contienen la administración del sistema, las funciones de configuración y sintonización, la consola de monitoreo de la red, programación del escaneo de la vulnerabilidad y reportes, y el tablero de seguridad de la consola. El motor también incluye la opción de proveer los servicios de gestión en solicitud por periodos a la medida, temporales o de tiempo completo.

Manejo de la plataforma de seguridad (MPS). El centro de operaciones de seguridad (SOC, *Security Operation Center*) ofrece una solución única por donde los datos del cliente se agrupan y se procesan en el sitio a través de una infraestructura de seguridad sobre la premisa del cliente. El manejo de la plataforma de seguridad atrae las consolas desde estos discretos sitios del cliente hacia una consola maestra usada por un SOC o cualquier compañía que quiera manejar la seguridad para cada división por separado, pero monitoreado de forma centralizada. Este método no solamente permite más eficiencia, además de seguridad y un servicio de envío costo-efectivo, sino que también reduce la necesidad de una infraestructura central de datos y de recursos. El módulo de manejo de la plataforma de seguridad proporciona una consola de monitoreo unificada.

Monitoreo de acceso al sistema/servidor de seguridad (MASSS). Integra, con la consola de monitoreo, las reglas con base en el análisis de acceso al sistema para programas comerciales de servidores de seguridad disponibles y otros elementos compatibles de acceso al sistema, a los dispositivos y a las aplicaciones. El MASSS también captura y analiza registros desde los dispositivos y servidores de seguridad; combina reglas con base en la lógica booleana en tiempo y en frecuencia; mantiene 14 días de registros por fuente de acceso; provee, además, soporte de respaldo para el sistema externo; admite más de 100 dispositivos de registro de acceso al sistema por MASSS; integra y correlaciona datos con otra empresa y con el subsistema; está respaldado en la consola de monitoreo y el sistema de licencias; y provee reportes especializados para cumplir con los requerimientos de auditoría.

Gestión de acceso a la red (GAR). Define límites para la gestión y el monitoreo de información y acceso a las aplicaciones de información a través de múltiples sistemas y disciplinas; mientras de forma simultánea envía libremente servicios en línea a empleados, clientes y proveedores. El módulo GAR ayuda a definir qué persona puede acceder a la red, a qué hora y desde qué ubicación. Cualquier violación a los límites establecidos generará una alerta de acceso no autorizado.

Módulo de seguridad todo en uno (MSTU). Utiliza una plataforma con base en una arquitectura para unificar las aplicaciones de fortaleza-empresa en un sistema único, que incluye un *firewall*, antivirus y protección *anti-spam*. Hace

una revisión de la reputación IP y del contenido de una red virtual privada y cuenta con un filtro del contenido de la web; un sistema de prevención y detección de intrusos; un análisis y correlación de comportamiento de la red; un escaneo de vulnerabilidad; la gestión de amenazas y el control, monitoreo y acceso a la red.

Manejo de servicios de seguridad (MSS). Los servicios de manejo que lo habilitan para asignar de una manera rentable sus recursos internos y requerimientos de seguridad subcontratados, con base en la demanda, no requieren de firmar un contrato específico y están dentro de la póliza de servicios de seguridad informática generales.

Los servicios profesionales relacionados con los procesos de seguridad garantizan que la información sensible es intocable por personal no autorizado (Anderson, 2008). Esto incluye auditorías periódicas de monitoreo y de pruebas para asegurar que los programas y sistemas de una organización estén actualizados (figura 4.22). Los servicios incluyen:

Evaluación de la seguridad de la empresa (ESE). Incluye análisis de diferencias para evaluar políticas, procesos, productos y personas.

Procedimientos y procesos de seguridad (PPS). Proveen la evaluación y el desarrollo de planes de recuperación de desastres y de continuidad del negocio; así como la gestión de vulnerabilidad y el estudio de riesgos.

Arquitectura de seguridad de la red (ASR). Ayuda a los clientes a crear una defensa profunda usando zonas de redes particionadas y lógicas; el servicio incluye detección de intrusos, registro centralizado, servidores de seguridad y PKI.

Evaluación de aplicaciones de red (EAR). Monitorea y prueba los privilegios de entrada del usuario y asegura que solamente las personas autorizadas puedan tener acceso al sistema e información sensible.

Evaluación de vulnerabilidad (EV). Prueba la efectividad de las medidas de seguridad simulando ataques internos y externos para garantizar que los sistemas de red y de datos de alto riesgo estén seguros.

Figura 4.22 Muestra de un sistema unificado de administración de la seguridad

4.6 Seguridad en las redes inalámbricas

La seguridad es una de las principales preocupaciones de las organizaciones que están interesadas en implementar redes inalámbricas. Afortunadamente, tanto el conocimiento de los usuarios sobre la seguridad como las soluciones ofrecidas por los proveedores de tecnología están mejorando (Bi, Zysman y Menkes, 2001). "Sin embargo, las amenazas aún se consideran importantes, y los proveedores siempre necesitan tener en cuenta la percepción inamovible de que las redes LAN son inseguras", afirma Richard Webb, analista de orientación para redes de área local inalámbricas (LAN) de *Infonetics Research*.

De hecho, la seguridad es el principal obstáculo para la adopción de redes LAN inalámbricas, y esta preocupación no es exclusiva de las compañías grandes. Tener un mayor conocimiento de los elementos de la seguridad de LAN inalámbricas y el empleo de algunas de las mejores prácticas puede ser de gran ayuda para beneficiarse de las ventajas de las redes inalámbricas. Inicialmente, para salvaguardar éstas hay tres acciones que pueden ayudar (Garfinkel y Spafford, 2002):

- Proteger los datos durante su transmisión mediante el cifrado.
- Desalentar a los usuarios no autorizados por medio de autenticación.
- Impedir conexiones no oficiales a través de la eliminación de puntos de acceso dudosos.

Por otro lado, existen tres soluciones disponibles para resguardar el cifrado y la autenticación de LAN inalámbrica: acceso protegido Wi-Fi (WPA), acceso protegido Wi-Fi 2 (WPA2) y conexión de redes privadas virtuales (VPN); esta última descrita anteriormente, pero que en el presente apartado se tocará de forma contextualizada (Nichols y Lekkas, 2002):

WPA y WPA2. Estas certificaciones de seguridad basadas en normas de la Wi-Fi Alliance para LAN de grandes, medianas y pequeñas empresas proporcionan autenticación mutua para verificar a usuarios individuales y cifrado avanzado. WPA ofrece cifrado de clase empresarial y WPA2 (la siguiente generación de seguridad Wi-Fi) admite el cifrado de clase gubernamental.

"Recomendamos WPA o WPA2 para las implementaciones de LAN inalámbrica en grandes empresas y empresas en crecimiento", comenta Jeremy Stieglitz, gerente de productos de la unidad comercial de conexión de redes inalámbricas de Cisco. WPA y WPA2 proporcionan control de acceso seguro, cifrado de datos robusto y protegen la red de los ataques pasivos y activos.

VPN. Como se mencionó anteriormente, VPN brinda seguridad eficaz para los usuarios que acceden a la red por vía inalámbrica mientras están de viaje o alejados de sus oficinas. Con VPN, los usuarios crean un "túnel" seguro entre dos o más puntos de una red mediante el cifrado, incluso si los datos se transmiten a través de redes no seguras como Internet. Los empleados que trabajan desde casa con conexiones de acceso telefónico o de banda ancha también pueden usar VPN.

4.6.1 Política de seguridad inalámbrica

En algunos casos, puede haber parámetros de seguridad diferentes para usuarios o grupos de usuarios de la red; que es posible establecer utilizando una LAN Virtual (VLAN) en el punto de acceso. Por ejemplo, en configurar políticas de seguridad distintas para grupos de usuarios diferenciados dentro de la compañía (como el área de finanzas o de manufactura, o el departamento jurídico o de factor humano); o para clientes, *partners* o visitantes que acceden a la LAN inalámbrica. Esto les permite utilizar un solo punto de acceso de forma económica para ofrecer soporte a varios grupos de usuarios con parámetros y requisitos de seguridad diferentes, mientras la red se mantiene protegida.

La seguridad de LAN inalámbrica, aun cuando está integrada en la administración general de la red, sólo es efectiva cuando se encuentra activada y se utiliza de forma uniforme en toda la LAN inalámbrica. Por este motivo, las políticas del usuario son también una parte importante de las buenas prácticas de seguridad, aunque el objetivo es elaborarlas de manera que sean lo suficientemente sencillas como para que la gente las cumpla y lo bastante segura como para proteger la red. Actualmente, ese equilibrio es más fácil de lograr porque WPA y WPA2 se incorporan a los puntos de acceso Wi-Fi y los dispositivos de clientes certificados (Burnett y Paine, 2001).

La política de seguridad de LAN inalámbrica debería también cubrir cuándo y cómo se pueden utilizar los puntos activos públicos, los dispositivos personales en la red inalámbrica de la compañía, así como la forma en la cual se maneja la prohibición de aquellos de origen desconocido y una política de contraseñas robusta.

4.6.2 Pasos prácticos para una seguridad inalámbrica

Es de gran importancia activar las funciones de seguridad inherentes a los puntos de acceso y las tarjetas de interfaz; esto se realiza normalmente ejecutando un programa de *software* suministrado con el equipo inalámbrico y consultando el sitio web del fabricante del dispositivo para conocer la versión más reciente del *firmware* y actualizar el punto de acceso si no lo está, lo que hará que la red inalámbrica sea más segura y confiable.

Por otro lado, es ideal comprobar qué recursos de seguridad ofrece el proveedor de *hardware*. Cisco, por ejemplo, proporciona un conjunto de productos de *hardware* y *software* diseñados para mejorar la seguridad inalámbrica y simplificar la administración de la red.

Figura 4.23 Objetivos de la seguridad informática

Si no se es capaz de implementar y mantener una red LAN inalámbrica segura, o no se está interesado en ello, debe pensarse en contratar a un revendedor de valor añadido, a un especialista en implementación de redes u otro proveedor de equipos de redes inalámbricas para que ayude a procurar la asistencia de un servicio subcontratado de seguridad administrada, muchos de los cuales cuentan con una oferta de seguridad inalámbrica.

Independientemente de cómo se proceda, debe hacerse de una forma organizada, pues la seguridad es definitivamente un elemento que se debe planificar, igual que la administración de la red, la disponibilidad de acceso y la cobertura, etcétera pero ésta no debe ser un obstáculo real para la implementación de una LAN inalámbrica funcional en una organización (figura 4.23).

4.7 Autentificación y sistemas biométricos

La biometría (del griego *bios* que significa vida y *metron*, medida) es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. En las tecnologías de la información (TI), la "autentificación biométrica" o "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo para su autentificación; es decir, para "verificar" su identidad (Caballero Gil y Hernández Goya, 2000).

Las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o su geometría de la palma representan ejemplos de características físicas (estáticas), mientras que en los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas), tal como se mencionó en el capítulo 1. La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten ambos aspectos (figura 4.24).

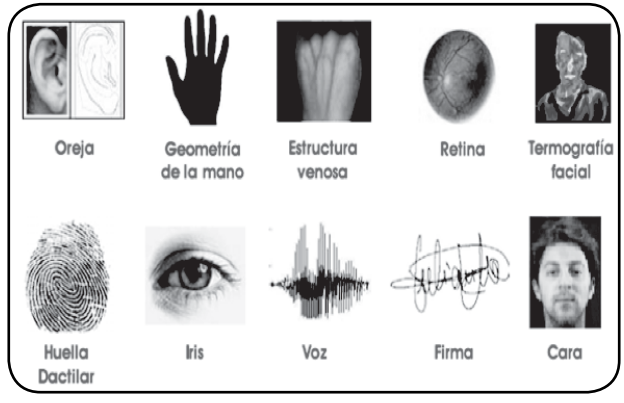


Figura 4.24 Diferentes formas de autentificación biométrica

En un sistema de biometría típico, la persona se registra cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico e introducida en una base de datos. De manera ideal, al entrar, casi todas sus características concuerdan; entonces, cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de acierto que varían mucho (desde valores bajos como 60 %, hasta altos como 99.9 %).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso-positivo (FAR, *False Acceptance Rate)*, falso-negativo (FNMR, *False Nonatch* Rate o FRR, *False Rejection Rate*) y de fallo de alistamiento (FER, *Failure-to-Enroll Rate*). En los sistemas biométricos reales, el FAR y el FRR pueden transformarse en los demás cambiando cierto parámetro.

Una de las medidas más comunes de los sistemas biométricos reales es la tasa llamada de error igual (EER, *Equal Error Rate*), en la cual el ajuste que acepta y rechaza los errores es el mismo; ésta también es conocida como la tasa de error de cruce (CER, *Cross-Over Error Rate*). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exac-

to. Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto para reducir al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si éstos resultaban fallidos. En cuanto a ello, las opiniones pueden variar sobre qué constituye un falso rechazo. Si se entra a un sistema de verificación de firmas usando una inicial y un apellido, ¿puede decirse legítimamente que se trata de un falso rechazo cuando se niegue el nombre y el apellido? A pesar de estas dudas, los sistemas biométricos tienen un potencial para identificar a individuos con un nivel de certeza muy alto. La prueba forense del ADN goza de un grado muy alto de confianza pública actualmente, y la tecnología está orientándose al reconocimiento del iris, que tiene la capacidad de diferenciar entre dos individuos con un ADN idéntico.

Uno de los beneficios que otorga la tecnología biométrica es que no se precisa llevar una tarjeta o llave para acceder a un edificio. Las infraestructuras de grandes redes empresariales, las identificaciones en el gobierno, las transacciones bancarias seguras y los servicios sociales y de salud, entre otros ámbitos, ya se benefician del uso de este tipo de verificaciones (Marino Tapiador, 2005).

Asociada a otras tecnologías de restricción de accesos, la biometría garantiza uno de los niveles de autenticación menos franqueables en la actualidad. Además, los inconvenientes de tener que recordar una contraseña o un número de PIN de acceso serán pronto superados gracias al uso de los métodos biométricos, debido a sus múltiples beneficios: están relacionados de forma directa con el usuario, son exactos y permiten hacer un rastreo de auditorías; su utilización permite que los costos de administración sean más bajos debido a que sólo se debe realizar el mantenimiento del lector, a que únicamente una persona se encarga de mantener la base de datos actualizada y a que las características biométricas de una persona son intransferibles a otra.

Un ejemplo de uso de sistemas biométricos es que actualmente en México se realiza un proceso para la emisión de cédulas que incluyen datos biométricos para menores de edad; esto con la finalidad de que toda aquella persona que no rebase la mayoría de edad tenga un documento fiable que le sirva como identificación en todo el territorio mexicano. Este proceso corre a cargo de la Secretaría de Gobernación.

En la tabla 4.1 se presentan las diferentes características de los sistemas biométricos.

Tabla 4.1 Comparativo de los diversos sistemas biométricos

	Ojo (iris)	Ojo (retina)	Huellas dactilares	Vascular (dedo)	Vascular (mano)	Geometría de la mano	Escritura y firma	Voz	Cara 2D	Cara 3D
Fiabilidad	Muy alta	Muy alta	Muy alta	Muy alta	Muy alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Muy alta	Muy alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Muy alta	Muy alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

En los últimos años, se ha notado una preocupación muy creciente por parte de las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático. Esto es reflejo del creciente interés industrial por dicho ámbito tecnológico y por los múltiples beneficios que su uso aporta. No obstante, aún la estandarización continúa siendo deficiente y, como resultado, los proveedores de soluciones biométricas todavía suministran interfaces de *software* propietarias para sus productos, lo que dificulta a las empresas el cambio de producto o de vendedor.

A nivel mundial, el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del *Joint Technical Committee on Information Technology* (ISO/IEC JTC1), de la *International Organization for Standardization* (ISO) y la *International Electrotechnical Commission* (IEC). En los Estados Unidos de América, desempeñan un papel similar el Comité Técnico M1 del *International Committee for Information Technology Standards* (INCITS), el *National Institute of Standards and Technology* (NIST) y el *American National Standards Institute* (ANSI). Existen, además, otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como *Biometrics Consortium*, *International Biometrics Groups* y BioAPI. Este último se estableció en los Estados Unidos de América en 1998 y está compuesto por las empresas Bioscrypt, Compaq, Iridiam, Infineon, NIST, Saflink y Unisys.

Por su parte, el consorcio BioAPI desarrolló conjuntamente con otros organismos y asociaciones un estándar que promoviera la conexión entre los dispositivos biométricos y los diferentes tipos de programas de aplicación, además de impulsar el crecimiento de los mercados de este tipo.

Algunos de los estándares más importantes son:

ANSI X.9.84. Creado en el 2001 por la ANSI, y actualizado en el 2003; define las condiciones de los sistemas biométricos para la industria de servicios financieros, haciendo referencia a la transmisión y almacenamiento seguro de información biométrica y a la seguridad del *hardware* asociado.

ANSI/INCITS 358. Fue creado en el 2002 por la ANSI y por BioApi Consortium; éste presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.

NISTIR 6529. También conocido como *Common Biometric Exchange File Format* (CBEFF), es un estándar creado en 1999 por NIST y Biometrics Consortium, que propone un formato estandarizado para el intercambio de información biométrica.

ANSI 378. Su creación surgió en el 2004 por la ANSI; éste promueve criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.

ISO 19794-2. Fue creado en el 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud.

PIV-071006. Creado en el 2006 por el NIST y el FBI en el contexto de la norma FIPS 201 del gobierno de los Estados Unidos de América, establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para ser usados en procesos de verificación de identidad en agencias federales.

En el proceso de autentificación, los rasgos biométricos se comparan solamente con los de un patrón ya guardado, lo cual se conoce también como uno-para-uno (1:1). Éste implica conocer presuntamente la identidad del individuo a autentificar por medio de algún tipo de credencial, que después será validada o no.

Por otro lado, existe también el proceso uno-para-muchos (1:N). Éste implica no conocer la identidad presunta del individuo, razón por la cual la nueva muestra de datos biométricos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados. El resultado de esto es la identidad del individuo, mientras que en el proceso de autentificación es un valor verdadero o falso. Este último es más rápido que el de identificación biométrica, sobre todo cuando el número de usuarios (N) es elevado; lo cual sucede debido a que la necesidad de procesamiento y comparaciones es más reducido en el primero; por ello, es habitual usar autentificación cuando se quiere validar la identidad de un individuo desde un sistema con capacidad de procesamiento limitada o en el que se quiere un proceso muy rápido. Un ejemplo de esto es la aplicación móvil *OneID*, diseñada para sistemas *Single Sign-On*, que utiliza la dactiloscopía.

Una coalición de empresas de *hardware* y de *software* denominada Alianza Fido se dedica al estudio de sistemas biométricos para remplazar el uso de contraseñas, ya sea con lectores de huellas dactilares, faciales o identificadores de voz. Un ejemplo de su producción es *YubiKey*, producto de la empresa Yubico.

4.8 Nuevas tecnologías en seguridad

Con las nuevas tecnologías también llegan nuevas amenazas, y los *hackers* parecen estar desarrollando sus armas a una velocidad que está complicando a las empresas de seguridad. En este apartado se muestran tanto las amenazas, como la forma de contrarrestar sus efectos en las organizaciones de la segunda década del siglo XXI.

En los últimos años un "huracán" ha surgido desde diversos frentes de la tecnología, traspasando las fronteras que encierran a los más expertos y llegando con fuerza a usuarios comunes, organizaciones, gobiernos, y a todo aquel que utilice artefactos computacionales, ya sea para trabajar, contactarse o jugar; tras ello, se encuentran los *hackers* y sus distintas formas de vulnerar la seguridad informática.

Los virus y los *hackers* que los programan han sido un concepto conocido desde que se comenzó a masificar el uso de las computadoras en los años 90 del siglo pasado, y si bien el imaginario de aquel tiempo mostraba que los criminales informáticos podían hacer explotar una casa completa desde la seguridad de sus computadoras (es el caso de películas como *The Hackers* o *The Net*), lo cierto es que pocas amenazas cumplieron con causar daños demasiado reales o difundidos a la sociedad (Borisov, Goldberg y Wagner, 2001). Basta echar una mirada a algunos hitos de los últimos dos años para notar que el panorama está cambiando con fuerza: Wikileaks, Anonymous, el robo de información desde Sony Play Station Network, intrusiones a la CIA, a la consultora de seguridad Black & Berg Cybersecurity, etcétera; la lista es larga, y día a día se reportan más ataques a cuanto organismo pueda imaginarse, lo que inevitablemente nos lleva a pensar que nadie está seguro.

"Hoy día estamos frente a un punto de inflexión con respecto a lo que está pasando en seguridad. […] Organismos internacionales indican que algunos de los más grandes problemas que tiene el mundo actualmente son los ataques cibernéticos en infraestructura." (Fuentes, 2014). En la actualidad, se espera que cada vez más países tengan su propia estructura de Internet a fin de protegerse de la gran ola de ataques, por lo cual la intensidad y frecuencia de los distintos tipos de amenazas parece que sólo irá en aumento.

La empresa de seguridad ESET, desarrolladora de la suite de seguridad Nod32, reporta recibir más de 200 000 muestras de *malware* al día, un aumento sustancial con respecto a otras épocas. Esto puede verse claramente al repasar las estadísticas históricas, que indican que más de un tercio de todos los virus producidos en la historia fueron desarrollados durante el 2013; es decir, en los 25 años que han pasado desde la aparición del primer código malicioso nunca ha habido un periodo tan activo como el actual. En concordancia con esto, Marcelo Zanotti, socio de Asesoría en Riesgo y Gestión de Ernst & Young, opina que las empresas de seguridad están en el mejor momento, ya que las compañías, los directorios y los gobiernos van a tener que preocuparse de la seguridad informática necesariamente; para esto es indispensable explorar cuáles son las amenazas más frecuentes y cuáles son los puntos más débiles de las empresas.

Hace diez años estaba instalada en el imaginario común la noción de que bastaba con un antivirus para mantener a salvo la información de las computadoras, lo que en muchas ocasiones era bastante cierto. Las empresas agregaban a esto una solución de cortafuegos para evitar intrusiones indeseadas y todo avanzaba relativamente sin contratiempos (figura 4.25).

Figura 4.25 Nuevas tecnologías de seguridad en las redes de computadoras

El panorama ahora es absolutamente distinto, los virus se dividieron en *worms*, *backdoors*, caballos de Troya y todas sus variaciones, a lo que se le agregaron los *malware*, *rootkits* y *spywares*; Internet se volvió un lugar peligroso, incluso si lo único que se hace es navegar por un sitio común y corriente, pues aumentaron amenazas como el *phishing*, el *pharming* y distintos tipos de fraude; por su lado, la complejidad y habilidad de los *hackers* llegó a niveles en que pueden pasar fácilmente por los actuales sistemas de seguridad. "Hace unos años era fácil conocer cuando te enfrentabas a algún tipo de estafa o código malicioso. […]. Por lo general se encontraban diseñados en otros países y bastaba con prestar más cuidado cuando veías un aviso en inglés o en ruso. Hoy, esas mismas amenazas están diseñadas en español y totalmente localizadas para la zona en la que se despliegan." (Bortnik, 2014).

Aparentemente, ya no son sólo *hackers* probando sus conocimientos computacionales o intentando ganar dinero con publicidad; el negocio es ahora tan rentable que verdaderos criminales se unieron al desarrollo de *software* malicioso. "Ya está pasando que la mafia tradicional y el mundo de la droga están invirtiendo en estas empresas de ciber-crimen. Usar la palabra *hacker* es simplificar el fenómeno, hoy no están ganando la guerra, pero sí están poniendo en jaque a las organizaciones de seguridad. La pelea se hizo mucho más intensa y mucho más peligrosa" (Fuentes, 2014). Lo cierto es que se vuelve necesario tener presentes las amenazas más importantes de la actualidad, sobre todo en el entorno de las empresas.

Los expertos concuerdan en algunas de las menos conocidas y las que mayor peligro pueden presentar son:

Redes sociales. Facebook, Twitter y otras redes sociales han entrado con fuerza en la vida diaria de las personas, y eso incluye su deseo por utilizarlos en el contexto de su trabajo, pero existen varias amenazas que pueden ingresar desde éstas a la computadora del usuario, o bien, controlar directamente una cuenta corporativa dañando su imagen. Si bien la tendencia inicial fue cerrar el acceso a estas herramientas, lo cierto es que en muchos casos presentan una utilidad importante a la hora de establecer contactos o permitir una distención mayor en los trabajadores. Los expertos recomiendan no cerrar el acceso totalmente, a menos de que las redes realmente no representen ningún tipo de beneficio para la empresa.

Dispositivos personales. Actualmente, las personas utilizan cada vez más sus propios *smartphones*, *tablets* y *notebooks* en el trabajo, lo que puede generar diversos riesgos, incluyendo fuga de información y robo de contraseñas. Una de las soluciones es virtualizar los sistemas de trabajo para controlar de forma centralizada los accesos y evitar cualquier tipo de amenaza.

Cloud computing. Hoy, todas las tecnologías están migrando a la nube, por lo que es posible controlar una empresa totalmente desde servidores ubicados en varios países a cientos de kilómetros de la oficina. Esto, por lo general, presenta bastantes beneficios, pero también es necesario reformular las políticas de seguridad a nivel interno, ya que la información es accesible desde cualquier parte, razón por la que es importante tener el control sobre quién, cómo y dónde puede acceder a ella.

Fraudes. Este tipo de amenaza suele afectar a las personas físicas y no a las empresas, pero las primeras son los clientes, quienes podrían estar utilizando a su empresa para engañarlos y que ingresen sus datos personales en sitios que repliquen al de su compañía. Por lo mismo, es necesario prevenir a los clientes sobre cualquier tipo de fraude, así como el monitoreo permanente para frenarlos.

Nuevos *malwares.* Cada día aparecen nuevas y complejas formas de infectar tanto a las computadoras de una organización, como a los servidores de la empresa. Por desgracia, el volumen y la complejidad de estos programas son tales que es muy difícil estar completamente a salvo, por lo que instalar varias herramientas que se encarguen de detectar y eliminar este código malicioso es fundamental, así como contar con copias originales de todo el *software*; esto es un gran paso, dado que las frecuentes actualizaciones tienen relación con la solución a problemas de seguridad.

4.9 Auditoría al sistema de seguridad integral

Una de las características o principales rasgos de las sociedades avanzadas es el caudal de información que se desprende, principalmente, de las organizaciones en la actualidad, la cual no sólo aborda lo vinculado a ellas como capital y trabajo, sino también a otros aspectos relacionados, como son los usuarios, los clientes, las autoridades, etcétera. Para que dicha información suponga una verdadera respuesta adecuada, es necesario que esté acompañada de ciertas garantías que hagan creer en ella (Molina Salgado, 2003), como el trabajo del auditor.

A pesar de que la auditoría ha existido siempre, pues data de la época de la Revolución Industrial, dentro de los elementos de la auditoría moderna se encuentra el nuevo concepto de Auditoría al Sistema de Seguridad Integral; para su estudio, primero hay que tener esclarecido cuál es el concepto de seguridad integral que "Supone una aplicación globalizadora de la seguridad, en la que se tienen en cuenta los aspectos humanos, legales, sociales, económicos y técnicos de todos los riesgos que pueden afectar a todos los sujetos activos participantes en la actividad de una entidad." (Blanco Encinaza, 2010).

Partiendo entonces de esto, es posible conceptuar la Auditoría del Sistema de Seguridad Integral como "Un proceso sistemático de obtención de evidencias para determinar el cumplimiento de los procedimientos de Seguridad Integral implantados en una organización, y su correspondencia con las normas establecidas." (Blanco Encinaza, 2010).

Es necesario conocer que el análisis y la logística de la implantación de un sistema de seguridad lo deba hacer y estructurar la unidad de auditoría interna de una organización o, en su defecto, un grupo de expertos técnicos externos. Además, es importante aclarar que quien audita de forma integral la parte física del riesgo, los accesos y el esquema total de las instalaciones de seguridad es un profesional experto en el tema. Igualmente, apoya con capacitación y procedimientos la localización de las áreas de riesgo y la aplicación de fórmulas de alta eficiencia.

En la aplicación de este concepto, se puede emplear por parte de la organización un Modelo de Auditoría, que permite la utilización de ésta de una manera global, dirigida a la parte de Seguridad Integral y aplicada a las principales áreas de riesgo que se pueden encontrar en la organización, las cuales pueden ser:

- Riesgos laborales
- Riesgos patrimoniales (incendio, explosión e intrusión)
- Riesgos medioambientales

De esta manera, el Modelo de Sistema de Auditoría se adaptará a las necesidades de cada organización en sus respectivos riesgos, y permitirá valorar las acciones y medios desplegados sobre la base del sistema de organización y de gestión dispuesto. Además, éste ofrece a las organizaciones un medio imparcial de comparación, que estimula el desarrollo competitivo en beneficio de un mayor interés por el mejoramiento de la seguridad.

El objetivo fundamental del modelo de auditoría es conocer de una forma imparcial y lo suficientemente amplia la validez de la organización y gestión que la empresa mantiene en materia de seguridad integral, evaluando cada uno de los aspectos fundamentales que la determinan, de acuerdo con los criterios empresariales y sociales que rigen en la actualidad. Ello ha de ofrecer una visión del grado de implantación del sistema y, al mismo

tiempo, una medida del nivel de adecuación de la organización y los medios disponibles. Asimismo, como consecuencia de la evaluación anterior, se derivan la detección de actuaciones y condiciones inadecuadas y la ejecución de acciones correctoras por parte de la organización.

A modo de resumen, se pueden enunciar de la siguiente manera los objetivos del Modelo de Auditoría a aplicar:

- Evolución y seguimiento de resultados con respecto a anteriores auditorías.
- Estudio de los recursos, políticas, estructuras, directivas y resultados para la seguridad de la organización.
- Proporcionar un sistema de medición del nivel de seguridad planificado en la empresa y el grado de cumplimiento del procedimiento de referencia.
- Comprobar la adecuación de la organización de los procedimientos de seguridad y medios de seguridad.
- Identificar/detectar actuaciones y/o condiciones inadecuadas.
- Contribuir en la entidad al desarrollo de actuaciones correctoras a través de procedimientos y aplicación de fórmulas de alta eficiencia a partir de las deficiencias detectadas y sus causas.

Por su parte, el alcance del sistema y de la auditoría se proyecta a:

- La organización y cualificación del personal de seguridad.
- Los planes y procedimientos de seguridad.
- Los sistemas técnicos de seguridad y de protección.
- El análisis de las condiciones de seguridad en los puestos de trabajo por áreas.
- La evaluación del mantenimiento de las medidas establecidas de seguridad.
- La verificación de la adecuación a las normativas sobre seguridad vigentes en el país de origen, las propias del sector y las internas de la entidad.
- La comparación con el nivel de seguridad de otras empresas.

El sistema y la auditoría establecen una estructura de los elementos comunes a todas las áreas de riesgo. Los elementos constitutivos del sistema de seguridad sujetos a auditoría son los siguientes:

- La política de seguridad integral
- Las responsabilidades y las funciones de los colaboradores en la organización
- La definición del programa y de los recursos necesarios para aplicarla
- La estructura organizacional
- La reglamentación y su normativa
- Las actuaciones estructurales comunes

Es importante tener conocimiento de que en diferentes países se elaboran normas que regulan y orientan a las empresas en al proceso de Administración de Riesgos. Éstas deben proporcionar una orientación sobre los principales objetivos de gestión de riesgo que un auditor interno necesita considerar a la hora de formarse una opinión sobre la suficiencia de los procesos de la organización. La norma debe contener la valoración y la posibilidad de generación de informes sobre la efectividad de los procesos de gestión de riesgos de las organizaciones; además, se debe ocupar de éstos y de temas consultivos más exhaustivamente; por último, debe reconocer que un proceso de gestión de riesgos de una organización es un proceso de negocio importante que puede o debe ser analizado de forma similar a otros procesos estratégicos.

4.10 Modelos de seguridad informática: militar y comercial (el caso estadounidense)

Los actuales modelos de seguridad informática deben incluir la certeza de uso de equipos tales como computadoras de escritorio y portátiles, tabletas, servidores de red, equipos de telefonía inteligente, entre muchos otros que son las formas modernas de capturar, procesar, transferir, compartir y utilizar los datos y la información que generan tanto los usuarios independientes como las organizaciones. La figura 4.26 muestra dicho esquema de seguridad informática.

Figura 4.26 Representación de un esquema de seguridad informática para los equipos de una organización

Hace algunos años, más de cien organizaciones extranjeras de inteligencia han estado tratando de lograr el acceso a las redes digitales que aseguran las operaciones militares de los Estados Unidos de América. El Pentágono reconoce la amenaza catastrófica que la ciberguerra representa y se está asociando con gobiernos aliados y empresas privadas para prepararse. Por ejemplo, en el 2008, las redes clasificadas de las computadoras militares del Departamento de Defensa de los Estados Unidos de América se vieron significativamente comprometidas; esto comenzó cuando una unidad de memoria *flash* infectada fue introducida en una computadora portátil en una base en el Medio Oriente (Broad, Markoff, John y Sanger, 2011).

El código de computadora malicioso de la unidad de memoria *flash*, colocada ahí por una agencia de inteligencia extranjera, se autocargó a una red administrada por el Comando Central de los Estados Unidos de América. Éste se esparció sin ser detectado tanto en los sistemas clasificados como en los no clasificados, estableciendo lo que equivale a un puesto de avanzada digital, del cual se podían transferir datos a servidores bajo control extranjero. Fue el peor temor de un administrador de red: un programa infiltrado, funcionando silenciosamente, listo para entregar planes operacionales en las manos de un adversario desconocido.

Este incidente consistió en la infracción más significativa a las computadoras militares de los Estados Unidos de América y sirvió como una alerta importante. La acción del Pentágono para contrarrestar el ataque, conocida como *Operación Buckshot Yankee*,

marcó un momento decisivo para la estrategia de ciberdefensa de los Estados Unidos de América; sin embargo, durante los últimos diez años, la frecuencia y la complejidad de las intrusiones a las redes militares estadounidenses han aumentado exponencialmente, por lo que todos los días son sondeadas y escaneadas millones de veces (Benson, 2011). Ya que dicha intrusión no fue la única penetración exitosa, los adversarios han adquirido miles de archivos de las redes estadounidenses, de sus aliados y de sus principales socios en la industria; inclusive, han obtenido copias de planos de armamento, de planes operacionales y de datos de vigilancia. Por ello, a medida que ha aparecido la escala de la amenaza de la ciberguerra a la seguridad nacional y a la economía de los Estados Unidos de América, el Pentágono ha creado robustas defensas en etapas alrededor de las redes militares e inauguró el nuevo Comando Cibernético de los Estados Unidos de América para integrar operaciones de ciberdefensa en la milicia (Orange Book, 1985).

El Pentágono está colaborando con el Departamento de Seguridad Nacional para proteger las redes del gobierno y la infraestructura crítica, y con los aliados más allegados de este bélico país para extender internacionalmente esas defensas. Aún queda por hacer una enorme cantidad de trabajo básico, pero el gobierno estadounidense ha comenzado a establecer varias iniciativas para defender al país en la era digital, ya que la tecnología de la informática es lo que permite casi todo lo que la milicia estadounidense realiza: el apoyo logístico, el mando y control global de las fuerzas armadas, el suministro de inteligencia en tiempo real y de las operaciones a distancia.

Cada una de esas funciones depende en gran medida del eje de las comunicaciones globales de la milicia, que consta de 15 000 redes y de siete millones de dispositivos de informática a lo largo de cientos de instalaciones en docenas de países (Salido, 2010), donde más de noventa mil personas trabajan tiempo completo para darles mantenimiento.

En menos de una generación, la tecnología de la informática en la milicia ha evolucionado de una herramienta administrativa, para realzar la productividad en la oficina, a un recurso estratégico nacional por derecho propio. La infraestructura digital del gobierno de los Estados Unidos de América ahora le ofrece a la nación supuestas ventajas críticas sobre cualquier adversario, pero su dependencia en las redes de computadoras también potencialmente les permite a éstos obtener información valiosa de inteligencia sobre las capacidades y operaciones de dicho país para obstruir las fuerzas militares convencionales y perturbar el desarrollo de la economía de los Estados Unidos de América.

La ciberguerra es asimétrica; esto significa que el bajo costo de los dispositivos de informática implica que los adversarios de los estadounidenses no tienen que fabricar armamento oneroso, tales como los aviones de combate furtivos o portaaviones, para representar una amenaza significativa a las capacidades de la milicia estadounidense; por ello, una docena de programadores de computadoras determinados pueden, si encuentran una vulnerabilidad de la que aprovecharse, amenazar la red logística global de los Estados Unidos de América, robar sus planes operacionales, cegar sus capacidades de inteligencia o socavar su capacidad de lanzar bombas en los blancos. Conociendo esto, muchos militares están creando capacidades de ofensiva en el ciberespacio y más de cien organizaciones de inteligencia extranjeras están intentando irrumpir las redes estadounidenses. Algunos gobiernos ya cuentan con la capacidad de interrumpir elementos de la infraestructura de informática de este país. En el ciberespacio, la ofensiva lleva la delantera (Salido, 2010).

Internet fue concebido para ser colaborativo, que se extendiera rápidamente y que tuviese barreras bajas a la innovación tecnológica; donde la gestión de la seguridad y la identidad eran prioridades bajas. Por esos motivos estructurales, la capacidad del gobierno

de los Estados Unidos de América para defender sus redes siempre queda rezagada ante la capacidad del adversario de sacarle provecho a los puntos débiles de sus redes (Stuttard y Pinto, 2007). Los programadores expertos encontrarán vulnerabilidades y superarán las medidas de seguridad establecidas para evitar las intrusiones. En un entorno donde domina la ofensiva, una mentalidad de fortaleza no funcionará. Los Estados Unidos de América no pueden retirarse detrás de una *Línea Maginot* (línea de fortificación) de cortafuegos o corren el riesgo de ser invadidos.

La ciberguerra es como la guerra de maniobras en la cual la velocidad y la agilidad son de suma importancia: mientras que un misil viene con un remitente, un virus de computadora por lo general no. La labor forense necesaria para identificar al agresor puede tomar meses si es que ésta fuese del todo posible; e inclusive cuando se identifica al agresor, si es un actor no estatal, como un grupo terrorista, es posible que no cuente con recursos contra los cuales los Estados Unidos de América puedan tomar represalias (Simmons, 1992).

Además, no siempre está claro en qué consiste un ataque. De hecho, muchas de las intrusiones de hoy están más cerca al espionaje que a los actos de guerra. La ecuación de la disuasión se confunde aún más por el hecho de que los ciberataques a menudo se originan desde servidores infiltrados en países neutrales, y que dar respuestas a ellos podría tener consecuencias imprevistas. En vista de las circunstancias, la disuasión necesariamente se basará más en negar cualquier beneficio a los agresores que en imponer costos a través de la represalia.

El reto es lograr que las defensas sean lo suficientemente eficaces para negarle a un adversario el beneficio de un ataque a pesar de la fortaleza de las herramientas de ofensiva en el ciberespacio. Regímenes tradicionales de control de armas probablemente fracasarían en disuadir ciberataques a causa de los retos de atribución, que hacen que la verificación del cumplimiento sea prácticamente imposible, sin embargo, sí debe haber normas internacionales de comportamiento en el ciberespacio que se rijan por un modelo diferente, tales como el de salud pública o cumplimiento de la ley.

Las ciberamenazas a la seguridad nacional de los Estados Unidos de América no se limitan a blancos militares. Los *hackers* y los gobiernos extranjeros pueden lanzar cada vez más intrusiones a las redes que controlan la infraestructura civil crítica: fallas inducidas por computadora a las redes de energía de dicho país, a las redes de transporte o a los sistemas financieros, podrían causar daños físicos masivos y trastornos económicos. Tal infraestructura es también esencial para la milicia, tanto en el extranjero como al interior: coordinar el despliegue y el reabastecimiento de tropas estadounidenses y dotarlas con productos de vendedores privados necesariamente exige que se empleen redes no clasificadas que están unidas al Internet abierto (Salido, 2010). Proteger esas redes y las que apoyan a la infraestructura crítica de los Estados Unidos de América tiene que ser parte de las misiones de seguridad y defensa nacional de Washington.

La tecnología moderna de la informática también aumenta el riesgo del espionaje industrial y el robo de información comercial. A inicios del 2014, Google reveló que había perdido su propiedad intelectual como resultado de una operación compleja perpetrada contra su infraestructura corporativa, la cual también atacó docenas de otras compañías. Aunque la amenaza a la propiedad intelectual es menos dramática que la realizada a la infraestructura nacional crítica, puede que sea la ciberamenaza más significativa que los Estados Unidos de América enfrentarán a largo plazo.

Anualmente, una cantidad de propiedad intelectual mucho más grande que toda la contenida en la Biblioteca del Congreso es robada de redes mantenidas por negocios,

universidades y agencias gubernamentales estadounidenses. En vista de que la fortaleza militar en un final depende de la vitalidad económica, pérdidas constantes de la propiedad intelectual podrían desgastar tanto la eficacia de la milicia estadounidense como su competitividad en la economía global (Salido, 2010).

En cuanto al *hardware*, los "interruptores cortacorriente" (*kills switches*) operados por control remoto y las *backdoors* escondidas se pueden escribir en los circuitos integrados de las computadoras que usan los militares, permitiendo que actores externos manipulen a su antojo los sistemas desde lejos. El riesgo de comprometer el proceso de fabricación es muy real y quizá sea la ciberamenaza menos entendida, pero posiblemente, a futuro, la más extendida.

La interferencia es prácticamente imposible de detectar e inclusive más difícil de erradicar. Ya se ha hallado *hardware* de contrabando en sistemas que el Departamento de Defensa de los Estados Unidos de América ha comprado. El *Trusted Foundries Program* del Pentágono, que certifica las piezas creadas por fabricantes de microelectrónica, es un buen comienzo, pero no es una solución exhaustiva a los riesgos de la base tecnológica.

Microsoft y otras muchas compañías de tecnología de computadoras han diseñado estrategias complejas para la mitigación de riesgos, con el fin de detectar códigos maliciosos y disuadir su inclusión en sus cadenas de abastecimiento global; el gobierno de los Estados Unidos de América necesita emprender una iniciativa similar para las aplicaciones críticas civiles y militares.

Como una cuestión de "doctrina", el Pentágono ha reconocido oficialmente al ciberespacio como el nuevo ámbito de la guerra, pues, aunque está hecho por el hombre, se ha tornado igual de crítico para las operaciones militares, como lo son la tierra, el mar, el aire y el espacio. Como tal, la milicia debe poder defender y operar dentro de él (Salido, 2010).

En vista de la preponderancia de la ofensa en el ciberespacio, las defensas de los Estados Unidos de América deben ser dinámicas. Milisegundos, incluso, nanosegundos pueden hacer una diferencia; por lo tanto, la milicia estadounidense tiene que responder a los ataques a medida que suceden o inclusive antes de que sucedan.

Para lidiar con esto, el Pentágono estadounidense ha desplegado un sistema que incluye tres líneas de defensa que se traslapan: dos se basan en las mejores prácticas comerciales y los sensores que detectan y trazan las intrusiones, y la tercera le saca provecho a las capacidades de inteligencia del gobierno para proveer defensas activas sumamente especializadas (Salido, 2010).

La Agencia de Seguridad Nacional ha sido la primera en aplicar sistemas que, empleando advertencias provistas por las capacidades de inteligencia de los Estados Unidos de América, automáticamente despliega defensas para contrarrestar las intrusiones en tiempo real a través de diversas estrategias; entre ellas las siguientes: una parte son sensores, otra centinelas y una última son francotiradores; esos sistemas de defensa activa representan un cambio fundamental en el método que este bélico país emplea para la defensa de la red. Ellos trabajan colocando tecnología de barrido en la interfaz de las redes militares y de Internet abierta para detectar y detener códigos maliciosos antes de que se infiltren en las redes militares.

En vista de que algunas intrusiones inevitablemente eludirán la detección y no se pueden atrapar en el límite, las ciberdefensas de los Estados Unidos de América tienen que encontrar a los intrusos una vez que están adentro. Esto requiere poder "cazar" dentro de las propias redes de la milicia, una tarea que también es parte de la capacidad de

defensa activa del Pentágono (Salido, 2010), la cual se ha hecho posible consolidando las capacidades colectivas de ciberdefensa del Departamento de Defensa bajo un solo techo y uniéndolas con la inteligencia de señales necesaria para prever intrusiones y ataques.

El gobierno estadounidense también debe fortalecer su capital de recursos humanos; por ello, se ha aumentado la cifra de profesionales capacitados en ciberseguridad y se ha profundizado en su entrenamiento. Siguiendo las prácticas de la industria, los administradores de la red del Pentágono estadounidense ahora están capacitados en el *hacking* ético, que incluye emplear técnicas adversas contra los propios sistemas estadounidenses para identificar los puntos débiles antes de que un enemigo se aproveche de ellos. Inclusive, a medida de que el gobierno estadounidense fortalece su grupo de profesionales en ciberseguridad, debe reconocer que las tendencias a largo plazo en el capital de recursos humanos no son un buen presagio (Salido, 2010). Los Estados Unidos de América cuentan con tan sólo el 4.5 % de la población del mundo, y durante los próximos 20 años muchos países, incluyendo por supuesto China y la India, perfeccionarán a científicos en computadoras de forma más competente que los que el gobierno estadounidense capacitará. Para entonces, los estadounidenses perderán su ventaja competitiva en el ciberespacio si ésta significa sencillamente acumular profesionales de ciberseguridad capacitados; por lo tanto, el gobierno estadounidense debe enfrentar el reto de la ciberdefensa de la misma manera que enfrenta otros retos militares: con un enfoque no en las cifras sino en la tecnología superior y la productividad, donde sensores de gran velocidad, la avanzada analítica y los sistemas automatizados serán necesarios para apoyar a los profesionales de ciberseguridad (Salido, 2010).

Por otro lado, para la seguridad informática, en cuanto a la parte comercial y financiera, se sugiere utilizar el modelo de seguridad informática conocido como La Muralla China, que fue formulado en 1989 por David F. C. Brewer y Michael J. Nash. Éste se diseñó para proporcionar controles que minimizaran los conflictos de intereses en organizaciones comerciales y fue construido sobre un modelo de flujo de información. Dicho plan lleva el mencionado nombre debido a que se basa en crear una pared lógica entre un usuario y la información a la que no debe acceder. Si dos usuarios tienen el mismo nivel de acceso, esto no quiere decir que puedan leer la misma información.

Este modelo no distingue entre sujetos y objetos, por lo que se puede aplicar la misma política de seguridad a ambos elementos. Su principal virtud es la de ofrecer una gran confidencialidad, ya que los datos que se manejan no pueden ser leídos por sujetos distintos a los interesados; en el caso de que esto ocurriera, se garantiza que la información obtenida no pueda ser dada a conocer en otros medios (Salido, 2010).

Ejemplo 4.1

A continuación se presenta un ejemplo de uso del modelo de *La Muralla China*:

> Considérese los conjuntos de datos del banco "A", de la empresa de petróleo "A" y de la empresa de petróleo "B". Un usuario nuevo puede acceder a cualquier conjunto de datos que desee, ya que éste no posee ninguna información y por lo tanto tampoco existe conflicto de intereses. Si el usuario accede primero al conjunto de datos de la empresa de petróleo "A", se dice que éste posee información que le concierne a aquélla.

El usuario podrá siempre acceder a la información del banco "A" porque el conjunto de datos de éste y de la empresa de petróleo "A" pertenecen a diferentes clases de conflicto de intereses.

Si después de esto intenta acceder al conjunto de datos de la empresa de petróleo "B", la petición debe ser negada, debido a que existe un conflicto entre el conjunto de datos que ya posee. De hecho, si el usuario hubiera elegido en primera instancia acceder a la información de la empresa de petróleo "B", las restricciones de este modelo no le permitirían el acceso a la información de la empresa de petróleo "A" porque causaría un conflicto de intereses; sin embargo, todavía podría alcanzar la información del banco "A".

Como se puede observar en este ejemplo, la política de *La Muralla China* es una combinación de elección libre y control obligatorio, ya que el usuario puede elegir libremente cuál será el primer objeto al que accederá, después de esto se creará una muralla china para evitar conflictos de interés (Berghel, 2001).

En el tema de las políticas de seguridad, la industria militar es la que se encarga de realizar los mayores avances; sin embargo, actualmente existe una preocupación por proteger el ámbito comercial, por ello surgió la necesidad de crear políticas específicas para esto. Uno de los escenarios para aplicar la política es el de los consultores comerciales, quienes tienen conocimiento directo de la información confidencial de una compañía con el fin de prevenir el flujo de datos confidenciales, lo cual causa un conflicto de intereses; se recomienda aplicar las reglas de esta política de seguridad, la cual surge como una alternativa para garantizar grados de confidencialidad.

Para todos los modelos formales de seguridad, es importante tener una clasificación de los datos del negocio (Berghel, 2001). Esta información puede ser almacenada en un sistema jerárquico de tres niveles de importancia:

Nivel inferior. Está integrado por partes individuales de información (considerada como objetos), donde cada una forma parte de una sola empresa

Nivel intermedio. Se agrupan todos los objetos pertenecientes a la misma empresa y se denominan como "datos de la empresa".

Nivel superior. Se agrupan todos los conjuntos de datos de las empresas que están en competencia; a dichas agrupaciones se les llama "clases de conflicto de interés".

Para establecer la política de seguridad se asocia cada objeto con el nombre del conjunto de datos de la empresa y el nombre de la clase del conflicto de interés a los que pertenece. La accesibilidad puede ser representada mediante las siguientes reglas:

- Una vez que un sujeto haya accedido a un objeto en particular, solo podrá acceder a otros objetos que se encuentren dentro del mismo conjunto de datos de la organización o que estén en un conflicto de intereses diferente.
- Un sujeto puede acceder, a lo sumo, a un solo conjunto de datos de empresas por cada clase de conflicto de intereses.

4.11 Principios de la seguridad informática en el ámbito legal

Para el estudio de la problemática que se presenta en torno al robo de información, resulta necesario adentrarse en el campo jurídico propiamente dicho. Particularmente interesante resulta el hecho de que como rama científica solamente en los últimos años se haya comenzado a hablar acerca del Derecho y la informática, cuando es evidente que en su papel de regulador de las relaciones sociales el primero juega su parte en el proceso de concientización de los individuos (Davara Rodríguez, 1993).

He aquí cómo el Derecho se entrelaza con esta ciencia de aparición relativamente reciente, dando paso a diversas interrogantes como son las siguientes:

- ¿Existe una clara identificación del bien jurídico a proteger por la norma legal cuando éste se halla relacionado con las TIC?
- ¿Debe optarse por la flexibilidad o por la austeridad de las definiciones legales ante el impetuoso avance de las TIC?
- ¿Qué ámbito de aplicación debe tener la norma que regule las relaciones en la informática: penal, administrativo, civil o mixto?
- ¿Está preparado el personal que imparte justicia para apreciar en su verdadero sentido la responsabilidad del infractor de la seguridad informática?
- ¿En México existe una política gubernamental de carácter normativo uniforme, centralizado y eficaz que prevenga la ocurrencia de hechos que atenten contra la seguridad informática?

Son muchas las interrogantes que en torno al tema se pudieran formular en este apartado, sin embargo, en los cuestionamientos previos se resumen los objetivos de discusión más candentes entre teóricos y especialistas a nivel nacional e internacional. Muy pronto los grandes teóricos enarbolaron clasificaciones en cuanto al *software* de gestión, documental, de control, etcétera; y como era de esperarse, las diferentes ramas del Derecho se apresuraron a tutelar a la recién nacida informática. Específicamente, el ámbito de la propiedad intelectual enseguida vio en el *software* un fruto de la creación humana, susceptible, por lo tanto, de ser regulada.

La creciente importancia del uso de las computadoras personales elevó la significación de éstas; pues dejaron de tratarse de dos o tres juguetes caros en un laboratorio de una institución científica o en manos de un millonario, ya que pasaron a estar accesibles para cualquier persona, que se convirtieron en usuarios potenciales de esos cada vez más potentes adminículos electrónicos. Cuando todo esto sucedió se dio cabida el Derecho Penal: máxima expresión de la tutela del Estado sobre un bien que a partir de ese momento reviste interés social por sobre el particular, o que al menos queda garantizado tutelarmente por sobre los demás; para ello, los penalistas se apresuraron a identificar como una nueva serie de delitos a conductas delictivas tradicionales, que ahora pasaron a llamarse "delitos informáticos".

El punto en común que tienen todas estas conductas antisociales como el fraude, el robo, la estafa o los daños que atacan la información es el bien intangible que asimila esta clase de delitos a los cometidos contra la moral y las buenas costumbres; razón por la que es difícil cuantificarla, evaluarla, tasarla y, en general, apreciar sus distintas facetas.

Resulta innegable que Internet se ha transformado en una inmensa fuente de información de acceso universal que ejerce una importante influencia en la educación y en el ámbito sociocultural; es por ello que el tema de la seguridad informática resulta un tema fundamental en los ámbitos académicos internacionales jurídicos. Como es conocido, la primera respuesta a las necesidades de protección de las redes fueron las técnicas criptográficas, que permiten proteger la información e impiden que los sistemas sean utilizados o accedidos por personas no autorizadas o con fines lícitos; con base en esto, no debe perderse de vista que, en todos los casos, está presente el interés legítimo de los Estados de velar por la seguridad, el orden público y el resguardo de las naciones.

4.11.1 Marco legal en México de servicios electrónicos relacionados con seguridad

Es un hecho innegable que el avance inaudito de la tecnología en materia informática y el desarrollo de las nuevas Tecnologías de Información y de las Comunicaciones (TIC) han excedido con mucho las expectativas más ambiciosas; pero sobre todo y como consecuencia de ello han propiciado una serie de conductas, actos y hechos que inciden de manera trascendente en la vida social, económica, familiar, comercial, laboral, profesional, política y científica en todos los ámbitos de la existencia humana (Berriuso Ruíz, 1996).

Es ahí donde el Derecho, como regulador de las conductas del hombre en sociedad y como creador y organizador de los instrumentos jurídicos idóneos para garantizar la paz social y el bien público temporal, debe intervenir de manera expedita y eficaz para evitar que la estampida de fenómenos informáticos que invade a las sociedades modernas escapen del control legal manteniéndose mientras generan una serie de situaciones que necesariamente afectan de manera importante la vida de las personas y, particularmente, del Estado mexicano. Los siguientes asuntos son los más importantes que en materia informática se regulan:

- Delitos informáticos
- Contratos electrónicos y firma electrónica
- Protección de la privacidad y de la información
- Propiedad intelectual
- Cómputo forense
- Contenidos de Internet

Al estar constituido México como una República representativa, democrática y federal, en la cual los estados que la integran son libres y soberanos en cuanto a su régimen interior (si bien unidos por el pacto federal), se encuentra que en la actualidad los asuntos informáticos que inciden en el ámbito del Derecho Civil o Penal pueden ser regulados por cada una de las entidades federativas a su libre y mejor parecer. De lo anterior, es posible que todo el comercio electrónico, los contratos electrónicos mercantiles, los fenómenos informáticos que afecten vías generales de comunicación, los delitos informáticos regulados por el Código Penal Federal, los contenidos de Internet que impliquen delito federal y el correo electrónico (si legalmente se equiparara al correo convencional) constituyen materia federal; por lo que son o deberán ser regulados por las leyes federales; sin embargo, los estados que conforman la República Mexicana pueden normar, en el ámbito de su competencia, las materias que no están expresamente reservadas a la Federación, donde se incluyen los contratos civiles electrónicos, los delitos informáticos

que incidan en el orden común, la admisión de documentos o medios electrónicos como prueba en los procesos penales o civiles, la protección a bases de datos privadas y todo aquel asunto que no toque la materia en el ámbito federal.

Establecido lo anterior, se procede ahora a esbozar el panorama general que presenta la legislación mexicana en materia de fenómenos informáticos. Como se ha mencionado, el Derecho Penal es materia local, por lo que así como el Código Penal Federal reglamenta ciertas conductas delictivas relacionadas estrechamente con el desarrollo de las nuevas tecnologías de información y de la comunicación; aunque también algunas legislaciones estatales han avanzado en este tema (Cámara de Diputados del H. Congreso de la Unión, 2006). Por lo que se refiere a la regulación federal, se encuentran sancionadas las siguientes conductas:

- Modificar, destruir o provocar la pérdida de información contenida en sistemas o equipos informáticos.
- Conocer o copiar la información contenida en sistemas o equipos.

Es importante señalar que las penas varían si se trata de sistemas o equipos de particulares, del Estado mexicano o de las instituciones que integran el Sistema Financiero, asimismo se agravan si tratándose de sistemas o equipos del Estado, el presunto culpable contaba con autorización para el acceso. Además, las penas se incrementan si son realizadas por empleados del Sistema Financiero o si se obtiene provecho de la información obtenida; sin embargo, inexplicablemente no se sancionan las conductas descritas, tratándose de equipos o sistemas privados cuando el agente tuvo acceso al sistema por medio de una autorización.

Los siguientes casos son algunos de los penados por la ley en cuestión de delitos informáticos:

Uso y/o reproducción no autorizada de programas informáticos con fines de lucro (piratería). Vale la pena resaltar que ésta es una de las conductas anti-jurídicas mejor regulada en virtud de la armonización lograda con la Ley Federal del Derecho de Autor, la cual protege los programas de cómputo. También cabe aclarar que se sanciona al que fabrique, importe, venda o arriende algún sistema o dispositivo destinado a descifrar señales cifradas de satélite para desactivar la protección de un programa de cómputo. Las penas por la reproducción de obras protegidas y que se utilicen después con fines de lucro son relativamente fuertes (dos a diez años de prisión y de 2 000 a 20 000 días de salario mínimo vigente en la Ciudad de México por concepto de multa).

Ataque a las vías de comunicación y obtención de información que pasa por el medio. El Código Penal Federal sanciona con uno a cinco años de prisión y con 100 y hasta 10 000 días de salario mínimo vigente en la Ciudad de México como multa a quien dolosamente y/o con fines de lucro interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica (ya sean telegráficas, telefónicas o satelitales) por medio de las cuales se transmitan señales de audio, video o datos (Cámara de Diputados del H. Congreso de la Unión, 2006).

Aquí encuadran, entre otras, las conductas encaminadas a obtener información financiera o de crédito de las personas (al hacer una compra por Internet, por ejemplo), así como el interceptar correos electrónicos antes de que lleguen a su destinatario; sin embargo, no se tipificaría el hecho de acceder al buzón de correo electrónico de alguien y leer su correspondencia, lo cual crea un vacío legal al resultar controversial.

Pornografía infantil. en este caso, la ley específicamente hace alusión a la exhibición corporal, lasciva o sexual de menores de 18 años mediante anuncios electrónicos; sancionando al que procura, facilita, induce u obliga a los menores, así como a los que elaboran, reproducen, venden, arriendan, exponen, publicitan o transmiten el material referido. Éstas se castigan con prisión que va de los cinco a los 14 años, y una multa que abarca desde 1 000 hasta 3 000 días de salario mínimo vigente en la Ciudad de México, pero a quien dirija asociación delictuosa dedicada a los fines descritos, se le impondrán de ocho a 16 años de prisión y desde 3 000 y hasta 10 000 días de salario mínimo por multa.

Asociación delictuosa y pandilla. El Código Penal sanciona el hecho de formar parte de alguna asociación, banda o pandilla con el propósito de delinquir, entendiendo por éstas la reunión habitual, ocasional o transitoria de tres o más personas que sin estar organizadas formalmente con fines delictivos llegan a cometer alguno. A este respecto, también cabe la consideración de si encuadrarían en la descripción del tipo penal las asociaciones, bandas y pandillas electrónicas; es decir, gente que sin conocerse siquiera se reúne electrónicamente a través de Internet para planear la comisión de ilícitos, o bien, que agrupándose con otros fines llegan a intervenir en la realización de estos; un claro ejemplo es el caso de los integrantes de una sala de chat que al saber que uno de ellos estaba consumiendo estupefacientes, lo alentaron a continuar haciéndolo hasta que falleció de una sobredosis, lo cual pudieron observar a través del uso de *webcam* sin que el hecho tuviera mayor trascendencia. Este caso, al igual que el de violación de correspondencia electrónica, merece especial mención en cuanto a las reuniones electrónicas, sean éstas habituales, ocasionales o de primera vez (Cámara de Diputados del H. Congreso de la Unión, 2006).

Por otro lado, para la protección de la privacidad de la información se tienen las siguientes leyes al respecto:

Ley Federal de Protección al Consumidor. La ley protege como confidencial la información que un cliente proporcione a su proveedor, prohibiendo la difusión de ésta a otros proveedores ajenos, salvo autorización expresa e imponiendo la obligación de utilizar los elementos técnicos disponibles para otorgar confidencialidad y seguridad a los datos proporcionados.

Ley Federal del Derecho de Autor. Protege las bases de datos que por razones de disposición de su contenido constituyan obras intelectuales y establece que la información privada de las personas contenidas no podrá ser divulgada, transmitida ni reproducida bajo ninguna circunstancia; salvo con el consentimiento explícito de la persona del autor (Molina Salgado, 2003).

Ley de Instituciones de Crédito. Sanciona con prisión y multa a quien: "Obtenga o use indebidamente la información sobre los clientes y las operaciones del sistema bancario, sin contar con la autorización expresa correspondiente" (Cámara de Diputados, 2016). Sin embargo, sólo puede imponer pena de prisión un juez penal con base en el Código Penal Federal vigente, que sanciona a quien indebidamente utilice información confidencial reservada a la institución o a persona facultada con el objetivo de producir, alterar o enajenar tarjetas o documentos utilizados para el pago de bienes, productos o servicios o para disposición de efectivo; en resumen, la disposición no va encaminada a proteger la privacidad sino sólo en la medida en que se evita el fraude

> **Ley Federal de Protección de Datos Personales.** Su objetivo es garantizar que el tratamiento de los datos personales se realice con apego a las garantías individuales. La ley establece que toda persona tiene derecho a ser informada sobre la existencia de un archivo de datos sobre ella, su identidad y domicilio, así como su posibilidad de ejercer derechos de acceso, complementación, rectificación, reserva y cancelación. Con base en esto, se determinan los derechos y obligaciones de los responsables de archivos o bases de datos, así como la creación del Instituto Federal de Acceso a la Información (IFAI), quien es el encargado de controlar, organizar, estructurar y vigilar la protección de datos personales. También se crea la acción de protección de datos personales, como procedimiento civil.

Nuevamente, resalta la necesidad de unificar la legislación, elevándola a rango federal para evitar la posible contradicción entre regulaciones estatales o, incluso, la inconstitucionalidad de alguna ley. De la misma manera, se hace necesaria la estricta regulación del manejo de las bases de datos con que cuentan las instituciones crediticias y gubernamentales en virtud de que en la actualidad es evidente en México que muchas empresas de diversa índole tienen acceso a información personal, financiera y de crédito de los particulares, la cual emplean para bombardearlos con propaganda y llamadas telefónicas a su domicilio particular a todas horas, ofreciendo los productos o servicios que comercializan con la consecuente molestia a su derecho a la privacidad y con el peligro del mal uso que pueda darse a sus datos de crédito.

Actualmente, en México no existe ninguna regulación respecto al correo-basura (*spam*), a pesar de que es una de las cuestiones que han sido consideradas internacionalmente como una grave violación a la privacidad de las personas (Cámara de Diputados del H. Congreso de la Unión, 2006).

En el caso de la propiedad intelectual, en México, están protegidos los programas de cómputo, así como las bases de datos que por su composición constituyan obra intelectual, como se apuntó anteriormente (Molina Salgado, 2003). La ley que tutela estos derechos es la Ley Federal del Derecho de Autor (2017), la cual entiende por programa de cómputo: "La expresión original en cualquier forma, lenguaje o código de un conjunto de instrucciones que con una secuencia, estructura y organización determinada tiene como propósito que una computadora o dispositivo realice una tarea o función específica."

La ley protege programas tanto operativos como aplicativos, y deja fuera a los que tienen por objetivo causar efectos nocivos. Además, autoriza al usuario legítimo para hacer las copias que le permita la licencia, o bien, una sola que sea indispensable para la utilización del programa o que sea destinada sólo para resguardo. El autor tiene derecho de prohibir además de la reproducción, la traducción, la adaptación o arreglos al programa, así como su distribución o decompilación. Se prohíbe igualmente la importación, fabricación, distribución y utilización de aparatos o prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo. La violación a lo anterior constituye una infracción en materia de comercio, sancionada con multa por el Instituto Mexicano de la Propiedad Intelectual.

En cuanto al cómputo forense, apenas está legislada esta materia, y diversos ordenamientos legales se limitan a otorgarles valor probatorio a los documentos o instrumentos que se obtengan por medios electrónicos (Código de Comercio, Ley de Instituciones de Crédito, Ley del Mercado de Valores). El Código Federal de Procedimientos Civiles expresamente reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, debiéndose a la fiabilidad

del método con el que haya sido generada, comunicada, recibida o archivada, y si es posible atribuir a las personas obligadas el contenido de la misma siendo accesible para su ulterior consulta (Molina Salgado, 2003).

En este caso, además de la necesidad de unificar las diversas legislaciones del país tanto en materia penal como civil, se requiere ser más específicos ya que no se dice qué determina "La fiabilidad del método con el que haya sido generada", por lo que es necesario remitirse a estándares internacionales como el ISO y el IEEE para legislar al respecto; pero, asimismo, será conveniente establecer ciertas obligaciones para los Proveedores del Servicio de Internet (PSI) y para los titulares de nombres de dominio; tales como el establecer cuentas abuse (para recibir quejas de los usuarios), llevar de manera organizada *logs* o bitácoras, y tener identificables los números de teléfono, la dirección IP asignada y el tiempo de conexión de los usuarios para que sea más fácil para un perito en cómputo reunir los documentos que deban aceptarse como prueba en un juicio.

Finalmente, en cuanto a los contenidos de Internet: es éste un asunto de los más difíciles en cuanto a regulación en virtud del carácter absolutamente internacional de Internet y de la enorme cantidad de sitios que existen, aunque se han hecho algunos esfuerzos aislados por regular un adecuado uso de Internet (por ejemplo en Europa y en los Estados Unidos de América). Se debe considerar que el único contenido en Internet que está prohibido y sancionado en el país es el de la pornografía infantil, ya mencionado en este apartado. En este aspecto vuelve a resaltar la necesidad de establecer obligaciones para los titulares de nombres de dominio, así como para los proveedores de servicio.

A grandes rasgos, se ha descrito el panorama general del marco jurídico en materia informática en México, y se puede concluir que hasta el día de hoy se ha avanzado en ciertas materias, así como hay otras en las que falta aún mucho por hacer. Desde luego que se hace necesario un análisis minucioso, así como iniciativas específicas que sean presentadas al Congreso de la Unión una vez que su diseño idóneo esté terminado, empero, siempre se ha de enfrentar el reto del veloz avance de las tecnologías de información y cada vez se hace más evidente la necesidad de que los estudiosos del Derecho y de la Ingeniería en Sistemas Computacionales trabajen juntos para que la ley no sea rebasada por la compleja realidad (Batiz Álvarez, *et al.*, 2014).

4.12 Conclusiones

Sin importar que estén conectadas por cable o de manera inalámbrica, las redes de computadoras cada vez se tornan más esenciales para las actividades diarias, tanto en el hogasr como en las organizaciones. Tanto las personas como las organizaciones dependen de sus computadoras y de las redes, para funciones como el correo electrónico, la contabilidad, la organización y la administración de archivos, entre muchas otras actividades. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red, y pérdidas de trabajo, los ataques a una red pueden ser devastadores y causar pérdida de tiempo y de dinero, debido a los daños o robos de información o de archivos importantes. A los intrusos que obtienen acceso mediante la modificación del *software*, o la explotación de las vulnerabilidades de éste *software* se les denominan "Piratas Informáticos". Una vez que un pirata tiene el acceso a una red pueden surgir cuatro tipos de amenazas:

- Robo de información
- Robo de identidad
- Pérdida y manipulación de datos
- Interrupción del servicio

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa:

- **Amenazas externas.** Provienen de personas que no tienen autorización para acceder al sistema o a la red de computadoras. Logran introducirse principalmente desde Internet, enlaces inalámbricos o servidores de acceso por marcación o dial.
- **Amenazas internas.** Por lo general, conocen información valiosa y vulnerable, o saben cómo acceder a ésta. Sin embargo, no todos los ataques internos son intencionados.

Cuestionario

4.1 Explique a detalle qué es la seguridad en una red de computadoras y establezca estudios de casos exitosos de aplicación.

4.2 ¿Por qué es importante la gestión de la seguridad informática en una red de computadoras? Establezca estudios de caso exitosos de uso.

4.3 ¿Por qué es importante la seguridad por niveles en una red de computadoras? Establezca estudios de caso exitosos de uso.

4.4 ¿En qué consiste la seguridad en los sistemas unificados en una red de computadoras? Establezca estudios de caso exitosos de uso.

4.5 ¿Cómo funciona la arquitectura de gestión de la seguridad en una red de computadoras? Establezca estudios de caso exitosos de uso.

Referencias

Anderson, R. J. (1994). Why cryptosystems fail. *Community of the ACM*, (37): pp. 32-40.

_____ (2001). *Security Engineering*. New York: Addison-Wiley.

Barriuso Ruiz, C. (1996). *Interacción del Derecho y la Informática*. Madrid, España: Dykinson editores.

Bi, Q.; Zysman, G. I. and Menkes, H. (2001). Wireless mobile communications at the start of the 21st century. *IEEE Communications Magazine*, vol. 39, pp. 110-116.

Blanco Encinaza, L. J. (2010). La auditoría informática al comienzo del tercer milenio. *Revista Cubana de computación*, (6).

Bleichenbacher, D. (1996). Generating El Gamal signatures without knowing the secret key. *Advances in Cryptology, Proceedings Eurocrypt '96*, LNCS 1070, U. Marer, Berlin: Springer Verlag, pp. 10-18.

Borisov, N.; Goldberg, I. and Wagner, D. (2001). Intercepting mobile communications: The insecurity of 802.11. *Seventh International Conference on Mobile Computing and Networking*, ACM, pp. 180-188.

Bornik, S. (2011). Malware y cibercrimen. *CXO Community*. Disponible en http://youtu.be/nL3jIUhX6wk

Brands, S. (2000). *Rethinking public key infrastructures and digital certificates*. Massachusetts: M.I.T. Press.

Broad W. J.; Markoff, J. and Sanger, D. E. (2011). Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*, January, 15th. www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Burnett, S. and Paine, S. (2001). *Security´s official guide to cryptography*. California: Osborne/McGraw-Hill.

Caballero, G., Pino y Hernández Goya, C. (2000). *Criptología y seguridad de la información*. México: McGraw-Hill.

Cámara de Diputados del H. Congreso de la Unión (2006). *Código Penal Federal*. México: H. Congreso de la Unión.

Cámara de Diputados del H. Congreso de la Unión. (2016). *Ley de Instituciones de Crédito*. México: Congreso de la Unión/Banco de México.

Cámara de Diputados del H. Congreso de la Unión. (2017). *Ley Federal del Derecho de Autor*. México: Cámara de Diputados

Cheswick, W. R.; Bellovin, S. M. and Rubin, A. D. (2003). *Firewalls and Internet security: Repelling the wily hacker*. Disponible en: https://books.google.com.mx/books?id=_ZqIh0IbcrgC&lpg=PA142&dq=Firewalls+and+Internet+Security,+by+Cheswick+et+al.&pg=PA176&redir_esc=y&hl=es#v=onepage&q&f=false

Crovella, M. and Krishnamurty, B. (2006). *Internet measurements*. New York: John Wiley & Sons.

Davara Rodríguez, M. A. (1993). *Derecho informático*. Pamplona, España: Aranzadi Editores.

Day, J. D. and Zimmermann, H. (2003). The OSI Reference Model. *Procedures of the IEEE*, vol. 71, pp. 1 334-1 340.

Dhiren R. P. (2008). *Information security*. Theory and practice. New York: PHI Learning Private.

Ferguson, N.; Schneier, B. and Kohno, T. (2010). *Cryptography engineering: Design principles and practical applications*. New York: John Wiley & Sons.

Garfinkel, S. and Spafford, G. (2002). *Web security, privacy and commerce*. Sebastopol, California: O´Reilly.

Girault, M. (1991). Self-Certified public keys. *EUROCRYPT*, vol. 547 of LNCS pp. 490-497. Germany: Springer.

Held, G. (2010). *A practical guide to content delivery networks*. Boca Raton, Florida: CRC Press.

Jakobsson, M. and Wetzel, S. (2001). Security weaknesses in Bluetooth. *Topics in Cryptology: CT-RSA*, Berlin: Springer-Verlag LNCS 2020.

Johnson, N. F. and Jajoda, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, 31, pp. 26-34.

Mason, A. G. (2002). *Cisco secure Virtual Private Network* (VPN. USA: Cisco Press.

Merkle, R. (1990). A certified digital signature. *Advances in Cryptology, Proceedings Crypto, LNCS 435*. G. Brassard. Berlin: Springer Verlag, pp. 228-238.

Microsoft Tech (2001). *Red privada virtual: Una visión general*. EUA: Microsoft Technologies Press.

Molina Salgado, J. A. (2003). *Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial*. México: Editorial Porrúa.

Nichols, R. K. and Lekkas, P. C. (2002). *Wireless security*. New York: McGraw-Hill.

Orange Book (1985). Department Of Defense. Library N° S225, 711. USA. Disponible en http://www.doe.gov

Orera Gracia, A. y Soriano Sarrió, V. (2012). *Firewalls*. España: Universidad Complutense de Madrid. Disponible en http://www.e-sort.net/blog/wp-content/uploads/2012/06/FireWalls_Armando_Orera_Gracia_Infor_-Pro_2012_COLGAR.pdf

Pastor F. J. y Sarasa López, M. A. (1998). *Criptografía digital. Fundamentos y aplicaciones*. España: Prensas Universitarias de Zaragoza.

Perlman, R. and Kaufman, C. (2000). Key exchange in IPsec. *IEEE Internet Computing*, 4, pp. 50-56.

Preneel, B. (2010). *Cryptographic primitive for information authentication*. State of the Art. Germany: Katholieke Universiteit in Leuven.

Rodríguez, E. (2014). *TCP versus UDP*. Disponible en http://www.skullbox.net/tcpudp.php

Referencias de figuras

Figura 4.5

http://www.thebookmyproject.com/wp-content/uploads/Integration-of-Sound-Signature-in-Graphical-Password-Authentication-System.gif

Figura 4.8

http://pcworld.pe/noticias/soluciones-para-captura-digital-de-firmas/

Figura 4.9

https://www.viavansi.com/blog-xnoccio/es/xades-dnie-csharp-aspnet-firma-digital-y-autenticacion-con-viafirma-ii/

Figura 4.10, paso 21

http://saitenlinea.com/wiki/Contabilidad/sat/obtener-certificado-de-sello-digital

Figura 4.11

http://exp-firewall.blogspot.mx/2011/04/cortafuegos.html

Administración de la seguridad informática

El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de hormigón y sellado en una habitación recubierta de plomo con guardias armados… y aun así, tengo mis dudas.

Eugene Spafford

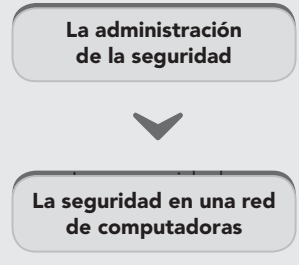
Reflexione y responda las siguientes preguntas:

- ¿Cómo opera el Modelo de Gestión de Seguridad en una red de computadoras?
- ¿Qué son las plataformas de gestión de seguridad en una red de computadoras?

Después de estudiar este capítulo, el lector será capaz de:

- Explicar el funcionamiento de la arquitectura de gestión de la seguridad en una red de computadoras.
- Esclarecer la operación del Modelo de Gestión Seguridad para una red de computadoras.
- Comprender qué son las plataformas de gestión de la seguridad en una red de computadoras.
- Establecer un modelo de administración de la seguridad para una red de computadoras.

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:



5.1 Introducción

El objetivo de la administración de seguridad es lograr la exactitud, la integridad y la completa protección de todos los procesos y recursos de los sistemas de información. De este modo, se minimizan errores, se limitan los fraudes y se busca eliminar las pérdidas en los sistemas de información que interconectan a las empresas actuales, así como a sus clientes, proveedores y todas las otras partes interesadas e involucradas (OCDE, 2004).

La Biblioteca de Infraestructura de Tecnología de Información (ITIL, *Information Technology Infrastructure Library*), desarrollada a finales de 1980, a la fecha es considerada como una de las mejores prácticas en la administración y explotación de la infraestructura de tecnologías de la información (TI). La ITIL implica diferentes procesos para llevar a cabo dicho trabajo, entre los cuales se encuentra la seguridad de la información, aspecto por demás relevante en el ámbito de la interacción a través de redes.

Las actividades de la administración de la seguridad están inmersas en casi todos los procesos de ITIL debido a que es de vital importancia dentro de una adecuada administración identificar los riesgos asociados al proceso para definir líneas de acción con la finalidad de mitigarlos; por lo anterior, cobra especial relevancia el tópico *Security Management* que forma parte de dicha biblioteca.

Los conceptos tratados en la administración de la seguridad son de gran utilidad para todos los responsables de los procesos críticos de TI, y resultan relevantes para los de la organización, ya que les ayudan a determinar el nivel de seguridad necesario en cada uno de sus procesos de negocio y que debe incluirse en el Acuerdo de Nivel de Servicio.[1]

La administración gerencial debe garantizar la seguridad de la información, ya que, desde la perspectiva del negocio, establecer una protección de los activos que soportan las funciones críticas es muy importante, debido a que éstos impactan en el aspecto financiero, en la imagen corporativa y en la calidez percibida por los clientes. El proceso de administración de la seguridad expone, en primer término, los conceptos básicos de una adecuada administración de la seguridad de la información; posteriormente, los relaciona con los demás tópicos, proveyendo, de manera general, las medidas de seguridad adecuadas que deben ser implantadas en cada uno de los procesos que lleve a cabo la administración, y culmina con una guía para administrar la seguridad, con referencia al Código de Prácticas de Administración de la Seguridad de la Información (BS 7799), versión 1999, desarrollado por el Instituto de Estándares Británico (*British Standards Institute*), el cual comprende los siguientes elementos:

Políticas de seguridad. Proporciona a la alta dirección apoyo para la seguridad de la información.

Organización de la seguridad. Ayuda a administrar la seguridad de la información dentro de la organización.

[1] Este acuerdo es un conjunto de factores constantemente medidos para determinar el alcance de los objetivos de la organización; proporciona una metodología para implementar expectativas razonables tanto para el usuario como para el área de TI y sirve como guía para el establecimiento de buenas y sanas relaciones dentro del servicio.

Clasificación y control de activos. Provee las medidas de seguridad necesarias para proporcionar una protección adecuada a los activos de la organización.

Seguridad del personal. Necesaria para reducir los riesgos de errores humanos, robo, fraude o mal uso tanto de las instalaciones como del equipo.

Seguridad física y ambiental. Previene el acceso físico no autorizado a los sistemas de información, así como posibles daños a las instalaciones y a la información del negocio.

Administración de comunicaciones y operaciones. Permite garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.

Control de acceso. Previene el acceso lógico y cambio no autorizado a la información y a sus sistemas, otorgando confidencialidad para evitar interrupciones en los procesos normales de producción.

Desarrollo y mantenimiento de los sistemas. Permite incorporar la seguridad a los sistemas de información.

Administración de la continuidad del negocio. Contrarresta las interrupciones a las actividades del negocio y protege los procesos críticos del negocio contra los efectos causados por fallas mayores o desastres.

Conformidad. Contribuye a evitar infracciones a las leyes civiles, jurídicas, obligaciones reguladoras o contractuales y cualquier otro requerimiento de seguridad.

Todos estos elementos logran combinarse a través de un enfoque de calidad PDCA (*Plan*, *Do*, *Check*, *Act*), aplicado a los procesos del Sistema de Gestión de Seguridad de la Información, otorgando controles claves y las medidas de seguridad más importantes que deben considerarse para su implantación. Lo que hace diferente a esta mejor práctica es el hecho de que no pretende ser una guía de implantación, lo cual la enriquece y le otorga mayor valor porque permite adecuarse a las necesidades del negocio en cuanto a la protección de la información estratégica que soportan sus procesos, como el impacto económico que pudiera ocasionar una inadecuada administración de la seguridad (OGC ITIL, 2002). La figura 5.1 muestra algunos de los aspectos más importantes de la administración de la seguridad informática.

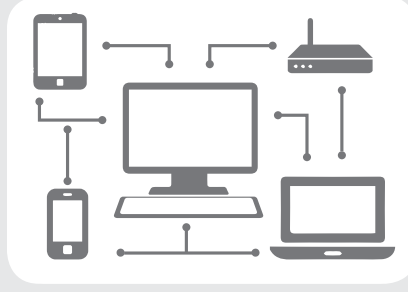


Figura 5.1 Aspectos de la administración de la seguridad informática en las organizaciones

5.2 Auditorías y evaluación de la seguridad informática

La auditoría de la seguridad informática abarca los conceptos de seguridad física y lógica. La primera se refiere a la protección de la arquitectura de sistemas (*hardware*) y los soportes de datos, así como a la seguridad de los edificios e instalaciones que los albergan; el auditor informático debe considerar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etcétera. Por su parte, la segunda se refiere a la seguridad en el uso de paquetes y de programas (*software*) y a la protección de los datos, procesos y programas, así como al del acceso ordenado y autorizado de los usuarios a la información.

El auditar la seguridad de los sistemas también implica que se debe tener cuidado de que no existan copias piratas, o bien, que al conectarse en red con otras computadoras no exista la posibilidad de transmisión de virus (Menezes, Van Orschot y Vanstone, 2010).

La seguridad informática ha tomado gran auge en los actuales sistemas de información debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes a las organizaciones para mejorar su productividad y explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo la aparición de nuevas amenazas. Esto ha llevado a que muchas organizaciones desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de las ventajas y evitar su uso indebido, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y de los servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovarla y actualizarla en función del dinámico ambiente que rodea las organizaciones modernas (Pérez Luño, 1996).

5.3 Evaluación de la seguridad informática implantada

Para empezar, en la evaluación de la seguridad en un sistema informático resulta beneficioso aplicar listas de verificación o de cotejo, las cuales no son un sustituto del análisis formal de los riesgos, sino que constituyen un punto de partida hacia éste en aquellos puntos que quedan sujetos a revisión. Además, se pueden tomar medidas correctivas en forma rápida que no implican mayor costo ni esfuerzo.

El proceso de auditoría es planeado para realizarse periódicamente, lo que indica que se llevará a cabo tiempo después de que se ha realizado un análisis de riesgos con el objetivo de verificar si se están cumpliendo los controles y las políticas de seguridad previstos. Independientemente de si existe en la organización o no información estadística de los elementos que determinan los riesgos, es recomendable que el grupo evaluador realice el proceso de análisis de riesgos, así sea en forma cualitativa y/o cuantitativa, con el objetivo de crear esta cultura de la seguridad informática en la organización (Reynolds y Holbrook, 1991).

La protección no ha de basarse solamente en dispositivos y medios físicos, sino también en aspectos lógicos. Por otro lado, el factor humano es el principal a considerar, ya que si las personas no quieren colaborar, de poco sirven los medios y dispositivos de protección, aunque sean caros y complejos; por lo tanto, es necesaria una separación de funciones: es muy peligroso que una misma persona realice una transacción, la autorice y revise después los resultados, pues ésta podría planificar un fraude o autocubrir cualquier anomalía.

Si la entidad auditada está en medio de un proceso de implementación de la seguridad, la evaluación se centrará principalmente en los objetivos, los planes y los proyectos que hay en curso; así como en los medios usados o previstos para llevarlos a cabo.

La evaluación de riesgos puede y debe ser global con base en todos los sistemas de información con que cuenta la organización, y que debe hacerse tan frecuentemente como sea posible. En la auditoría interna y externa a los sistemas de información de una organización se trata de saber si ésta, a través de funciones tales como la administración de la seguridad o de una auditoría interna o externa, cumple con los criterios normativos de seguridad informática y en qué medida. Al hablar de seguridad siempre se toman en cuenta sus tres dimensiones:

Confidencialidad. Se cumple cuando sólo las personas autorizadas pueden conocer los datos o la información correspondientes a la empresa.

Integridad. Consiste en que solamente el usuario autorizado puede variar los datos. Deben quedar pistas para un control posterior y para cualquier auditoría.

Disponibilidad. Se alcanza si las personas autorizadas pueden acceder a tiempo a la información.

5.4 Problemas en los programas de control de la seguridad informática

Es importante establecer cuáles son los principales problemas que deben resolverse como parte de los programas de control de la seguridad informática; los más significativos se plantean a continuación:

Se debe reducir el número de vulnerabilidades útiles. Los cibercriminales han hecho durante años un festín con el sistema operativo Windows. Afortunadamente, Microsoft™ ha invertido en explotar formas para mitigar dichas vulnerabilidades, lo que hace que escribir un código de ataque sea cada vez más difícil. A medida de que la dificultad para atentar contra los sistemas operativos y las aplicaciones de Microsoft™ se ha incrementado, algunos atacantes están regresando a la ingeniería social para tratar de acceder a dichas aplicaciones, aunque en la actualidad también se ven atacantes que ahora se centran en plataformas operativas que no son de Microsoft™.

Los ataques del Internet de las cosas (IoT) se mueven a partir de que no existe un concepto de prueba para riesgos generales. En 2014 se vio más evidencia de que los fabricantes del Internet de las cosas (IoT) no han aplicado las normas básicas de seguridad en los dispositivos que utilizan, por lo que es probable que tengan impacto en el mundo real de una forma muy desagradable. La industria de la seguridad tiene que evolucionar para hacer frente a las vulnerabilidades de dichos dispositivos.

El cifrado de los datos se convierte en estándar, pero esto no siempre es bueno. Debido a la creciente conciencia de las preocupaciones de seguridad y privacidad, resultado de las revelaciones de la agencia de inteligencia de espionaje y violaciones de datos de interés periodístico, la encriptación se está convirtiendo finalmente en un defecto.

Defectos importantes en el *software* que se utilizan ampliamente en la actualidad, y que habían escapado a la industria de la seguridad durante los últimos 15 años se han retomado. Se ha hecho evidente que hay piezas significativas en el *software* actual que tienen código inseguro, el cual es utilizado en un gran número de sistemas informáticos de hoy. Los acontecimientos de los últimos años han aumentado el interés de los cibercriminales para atacar mediante *malware* los sistemas informáticos, tanto de las organizaciones como de los particulares, con el objetivo de obtener beneficios económicos en la mayoría de los casos; y en los menos, para demostrar supremacía, por lo que en los años venideros habrá que protegerse asiduamente.

Un nuevo panorama normativo obliga a una mayor divulgación de las leyes y a asumir la responsabilidad en el uso de las aplicaciones informáticas, sobre todo en Europa. La ley se mueve lentamente en comparación con el movimiento en los campos de la tecnología y de la seguridad; sin embargo, los cambios regulatorios masivos se han presentado primero en Europa y luego en otras regiones. Es probable que éstos provoquen una regulación masiva en la protección de los datos en otras jurisdicciones.

Los atacantes incrementan su presencia en los sistemas de pagos móviles, aunque también lo siguen haciendo en los espacios tradicionales. Los sistemas de pagos móviles eran la comidilla hasta 2014, cuando Apple irrumpió con su

aplicación *Apple Pay*, con la cual pudo mejorarse la seguridad en los pagos y en las transacciones. Es un hecho que los cibercriminales estarán buscando fallas en esos sistemas, pero los diseños actuales tienen varias características positivas de seguridad. Debe esperarse que los cibercriminales continúen abusando del uso de las tarjetas de crédito y de débito tradicionales por un periodo significativo de tiempo, porque son el blanco más fácil por ahora.

Supervisión, control y adquisición de datos (SCADA, *Supervisory Control y Data Adquisition*). Es el *software* para computadoras que permite controlar y supervisar procesos a distancia. Facilita la retroalimentación en tiempo real con los dispositivos de campo y controla el proceso automáticamente. Provee el control de toda la información que se genera en el proceso productivo y permite su gestión e intervención.

Un sistema SCADA incluye un *hardware* de señal de entrada y salida, controladores, una interfaz hombre-máquina (HMI), redes, comunicaciones, bases de datos y *software*. El término SCADA se refiere a un sistema central que monitoriza y controla un sitio completo o una parte de un sitio o, finalmente, un sistema que se extiende sobre una gran distancia (kilómetros/millas). La mayor parte del control del sitio es en realidad realizada de forma automática por una Unidad Terminal Remota (RTU, *Remote Transmission Unit*), por un Controlador Lógico Programable (PLC, *Programmable Logic Controller*) y, más actualmente, por un Controlador de Automatización Programable (PAC, *Programmable Automation Controller*). Las funciones de control del servidor están casi siempre restringidas a reajustes básicos del sitio o a capacidades de nivel de supervisión. Por ejemplo, un PLC puede controlar el flujo de agua fría a través de un proceso, pero un sistema SCADA puede permitirle a un operador cambiar el punto de consigna (*set point*) de control para el flujo, y permitirá grabar y mostrar cualquier condición de alarma como la pérdida de éste o una alta temperatura. La retroalimentación del lazo de control es cerrada a través del RTU o el PLC; el sistema SCADA monitoriza el desempeño general de dicho lazo. Este sistema también puede mostrar gráficas con históricos, tablas con alarmas y eventos, permisos y accesos de los usuarios. La figura 5.2 muestra una aplicación típica de SCADA.

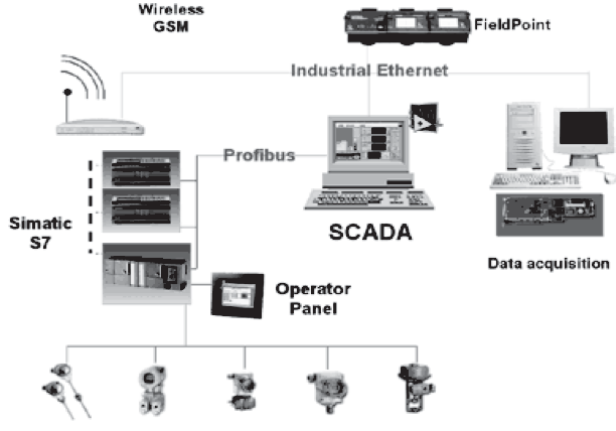


Figura 5.2 Uso de la arquitectura de un sistema SCADA

Necesidades de la supervisión de los procesos. Existen limitaciones en la visualización de los sistemas de adquisición y de control de los datos que se introducen en los procesos.

Control del *software* para recoger, almacenar y visualizar la información. Para este caso existen capacidades de *rootkit* [2] y de *bot* [3] muy interesantes, ya que a través de ellos pueden aparecer nuevos vectores de ataque; entonces, en este momento nos encontramos en el proceso de cambio de las principales plataformas operativas; así como de los protocolos en los que tradicionalmente se ha confiado durante algún tiempo, ya que no sirven para las condiciones informáticas de hoy.

[2] Un *rootkit* es un programa que oculta la presencia de un *software* malicioso (*malware*) en el sistema.

[3] Aféresis de robot.

5.5 Mejores prácticas de integridad de los sistemas de información

La seguridad de la información (Pinilla, 1997) ha cobrado visibilidad en distintos ámbitos: en el trabajo, en el hogar y durante el traslado de un lugar a otro. Se trata, principalmente, de prevenir los ataques destinados a restringir la disponibilidad (por ejemplo, la denegación del servicio) y a introducir *software* malintencionado (*malware*) que permita a un tercero manipular datos e información sin autorización (por ejemplo, para robar, divulgar, modificar o destruir datos).

Por ejemplo, el gusano informático *Stuxnet* descubierto en 2010 alteró el funcionamiento de un proceso industrial, porque fue diseñado con la finalidad de dañar equipos físicos y modificar las indicaciones de los operadores a cargo de la supervisión, para impedir, de este modo, que se identificara cualquier anomalía en los equipos (Farwell y Rohozinski, 2011). Si esta modalidad de ataque a la integridad de los datos (denominado también "ataque semántico") se hubiera replicado en otros sistemas, podría haber causado problemas graves en infraestructuras informáticas de importancia crítica, como las de los servicios públicos, los servicios de urgencia, el control de tráfico aéreo, y cualquier otro sistema que dependa en gran medida de la Tecnología de la Información (TI) y resulte indispensable para la sociedad.

Por otra parte, el Gobierno de la Información es un factor esencial para la consolidación de la integridad de los datos. Por ejemplo, un artículo publicado recientemente en *ISACA Journal* presenta una infraestructura de gobierno de datos desarrollada por Microsoft™, para garantizar la privacidad, la confidencialidad y el cumplimiento normativo. El artículo analiza las funciones que desempeñan las personas, los procesos y la tecnología; el ciclo de vida de los datos, y los principios de privacidad y confidencialidad de la información. También incluye enlaces a trabajos más pormenorizados sobre la Informática de Confianza (*Trustworthy Computing*).

En el presente subtema se ampliará el análisis de estos puntos, enfocándose en la integridad de los datos, las normas y los procedimientos recomendados a los que ésta debe ajustarse, y la función del Gobierno de los Datos. Este apartado también presenta un marco para el gobierno de datos sin control exclusivo. De los tres principales dominios de la seguridad de la información, el de la disponibilidad es el que se encuentra más estrechamente ligado a la tecnología, y es posible su medición. El Tiempo Improductivo (*Downtime*) es visible, y puede expresarse como valor absoluto (por ejemplo, en minutos por incidente), o como porcentaje, y no se requiere demasiado esfuerzo para entender que una disponibilidad de "cinco nueves" (99 999 %) representa en total unos cinco minutos de tiempo improductivo acumulado en un año. Los operadores de los centros de datos saben lo que se necesita para alcanzar este valor (Salido, 2010).

La confidencialidad es un concepto que se puede explicar de manera fácil, pero solamente tiene alguna utilidad cuando los datos y los documentos han sido clasificados en categorías (como "público", "restringido a", "embargado hasta" y "reservado"), que reflejan la necesidad que tiene una empresa de protegerlos. No es conveniente que los técnicos que se encargan de la infraestructura y servicios de TI se ocupen de realizar esta clasificación, ya que probablemente no tengan un conocimiento cabal del negocio, y en caso de emplearse la modalidad de externalización o terciarización (*Outsourcing*) o un sistema de computación en la nube (*Cloud Computing*), es posible que además no pertenezcan a la empresa (Terán Pérez, 2014).

Por lo tanto, el control y el proceso de clasificación de datos debe quedar en manos del personal del negocio; mientras que los proveedores de servicios y soluciones de TI deben ocuparse de proporcionar las herramientas y los procesos necesarios, como son los controles para la gestión de accesos e identidades (IAM, *Identity Access Management*) y la encriptación. El método más sencillo para medir la confidencialidad tiene una lógica binaria: el carácter confidencial de la información puede haberse preservado (si la información no se ha divulgado) o no (si se ha divulgado).

Lamentablemente, este método no resulta demasiado útil, ya que no refleja los efectos de la divulgación de los datos, que abarcan desde situaciones bochornosas hasta atentados contra la seguridad nacional. Si se analiza la noción de integridad, la situación se torna más compleja, porque se trata de un concepto que puede tener distintas interpretaciones. Éste es un terreno fértil para los problemas de comunicación y los malentendidos, con el consiguiente riesgo de que una actividad no se lleve a cabo de forma cabal y satisfactoriamente, por las confusiones en torno a las responsabilidades pertinentes.

La importancia de la integridad de los datos se puede ilustrar con un sencillo ejemplo: una persona necesita un tratamiento hospitalario que incluye la administración diaria de un medicamento en dosis de 10 mg. Accidental o intencionalmente, se produce una modificación en el registro electrónico del tratamiento y las dosis quedan establecidas en 100 mg, con consecuencias mortales. Para tomar otro ejemplo, se podría imaginar una situación propia de una obra de ficción que antecediera al ataque del virus *Stuxnet* en 2010 y preguntarse qué ocurriría si alguien interfiriera los sistemas de control de una central nuclear para que simularan condiciones de funcionamiento normal cuando, en realidad, se ha provocado una reacción en cadena (Dobbs, 2008). ¿Puede afirmarse que los profesionales reconocen las múltiples definiciones de la "integridad de los datos"? Véanse los siguientes puntos:

- Para un encargado de seguridad, la "integridad de los datos" puede definirse como: "La imposibilidad de que alguien modifique datos sin ser descubierto. Desde la perspectiva de la seguridad de los datos y de las redes, la integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria. Si se examina el concepto de 'integridad', podría concluirse que no solamente alude a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del desarrollo de sistemas estructurados [SDLC], revisión de códigos fuente por expertos, pruebas exhaustivas, etcétera), sino también a la integridad personal (responsabilidad, confianza, fiabilidad, etcétera)".
- Para un administrador de bases de datos, la "integridad de los datos" puede depender de que los datos introducidos en una base de datos sean precisos, válidos y coherentes. Es muy probable que los administradores de bases de datos también analicen la integridad de las entidades, la integridad de los dominios y la integridad referencial (conceptos que podría desconocer un experto en infraestructuras instruido en normas ISO 27000 o en la serie 800 de publicaciones especiales (SP 800) del Instituto Nacional de Normas y Tecnología [NIST, *National Institute of Standards and Technology*]) de los Estados Unidos de América.
- Para un arquitecto o modelador de datos, la "integridad de los datos" puede estar relacionada con el mantenimiento de entidades primarias únicas y no nulas. La unicidad de las entidades que integran un conjunto de datos se define por la ausencia de duplicados en el conjunto de datos y por la presencia de

una clave que permite acceder de forma exclusiva a cada una de las entidades del conjunto.

- Para el propietario de los datos (es decir, para el experto en la materia), la "integridad de los datos" puede ser un parámetro de la calidad, ya que demuestra que las relaciones entre las entidades están regidas por reglas de negocio adecuadas, que incluyen mecanismos de validación, como la realización de pruebas para identificar registros huérfanos.
- Para un proveedor, la "integridad de los datos" es: "La exactitud y coherencia de los datos almacenados, evidenciada por la ausencia de datos alterados entre dos actualizaciones de un mismo registro de datos. La integridad de los datos se establece en la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores." (IBM, s/a).
- En un diccionario disponible en línea, se define la "integridad de los datos" de este modo: "Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos. La integridad de los datos es uno de los seis componentes fundamentales de la seguridad de la información." (YourDictionary.com). Sin duda, es posible encontrar muchas otras definiciones. Pero todas contienen superposiciones, aluden a temas de distinta índole y producen cierta confusión semántica, uno de los principales motivos por los que las bases de datos son los objetos menos protegidos de la infraestructura de TI. El planteamiento del problema no termina aquí. La descentralización de los sistemas de información y la disponibilidad de entornos de programación eficaces para los usuarios finales, como las hojas de cálculo, han creado vulnerabilidades potencialmente descontroladas en la integridad de los datos, ya que esas hojas de cálculo se utilizan como fundamento de decisiones ejecutivas, sin evaluar, muchas veces, la calidad e integridad de los datos. ¿Cómo se debería abordar este problema?

En primer lugar, podría considerarse que se trata de un problema que atañe:

- **A la seguridad de la información.** Dado que no se puede garantizar la integridad de los datos.
- **A la calidad del *software*.** Dado que la mayoría de las hojas de cálculo no está sujeta a un proceso de gestión del ciclo de vida.
- **A la inteligencia de negocios.** Dado que la introducción de datos erróneos produce resultados erróneos, algo que en inglés se conoce como "GIGO" ("*Garbage In*, *Garbage Out*", lo que significa que si "entra basura, sale basura").

Quizá podría concluirse que abarca los tres aspectos; en tal caso, el siguiente paso consistirá en determinar quién(es) deberá(n) abordar el problema (el propietario de los datos, el usuario final que diseñó la hoja de cálculo, el departamento o proveedor de servicios de TI, o todos juntos).

Los ataques a la integridad de los datos consisten en la modificación intencional de los datos, sin autorización alguna, en algún momento de su ciclo de vida. En el contexto del presente capítulo, el ciclo de vida de los datos comprende las siguientes etapas:

- Introducción, creación y/o adquisición de datos
- Procesamiento y/o derivación de datos
- Almacenamiento, replicación y distribución de datos
- Archivado y recuperación de datos
- Realización de copias de respaldo y restablecimiento de datos
- Borrado, eliminación y destrucción de datos

El fraude (el más antiguo de los métodos destinados a atacar la integridad de los datos) tiene múltiples variantes, las cuales no analizaremos en el presente capítulo, excepto para mencionar un caso que, en el 2008, apareció en la primera plana de los periódicos de todo el mundo: un empleado de *La Societé Genérale de la France*, incurrió en delitos de "abuso de confianza, falsificación y uso no autorizado de los sistemas informáticos del banco", que produjeron pérdidas estimadas en €4 900 millones de euros (Kerviel, 2010).

A juzgar por la cantidad de publicaciones y conferencias internacionales que abordan el tema del fraude, es probable que este caso siga estando vigente durante algún tiempo. Hace años que las organizaciones que operan tanto en el sector público como en el privado, sufren alteraciones en sus sitios web, pero más allá del eventual perjuicio a la reputación de una empresa, ninguno de los daños ocasionados puede considerarse "catastrófico".

Las bombas lógicas, el *software* no autorizado que se introduce en un sistema por acción de las personas encargadas de programarlo/mantenerlo, los troyanos y demás virus similares, también pueden afectar la integridad de los datos a través de la introducción de modificaciones (por ejemplo, al definir una fórmula incorrecta en una hoja de cálculo), o la encriptación de datos y posterior exigencia de un "rescate" para revelar la clave de desencriptación. En los últimos años se han producido numerosos ataques de características similares a las mencionadas, que afectan principalmente los discos duros de las computadoras personales. Debería esperarse que tarde o temprano se produzcan ataques de este tipo destinados a los servidores.

La modificación no autorizada de sistemas operativos (servidores y redes) y/o de *software* de aplicaciones (como los "*backdoors*" o códigos no documentados), tablas de bases de datos, datos de producción y configuración de infraestructura, también se consideran ataques a la integridad de los datos. Es lógico suponer que los hallazgos de las auditorías de TI incluyen con regularidad las fallas producidas en procesos clave, particularmente en la gestión del acceso privilegiado, la gestión de cambios, la segregación de funciones y la supervisión de registros. Estas fallas posibilitan la introducción de modificaciones no autorizadas y dificultan su detección (hasta que se produce algún incidente).

Otro método de ataque a la integridad de los datos es la interferencia en los sistemas de control de supervisión y adquisición de datos (SCADA, *Supervisory Control and Data Acquisition*), como los que se utilizan en infraestructuras críticas (suministro de agua, electricidad, gas, etcétera) y en los procesos industriales. A menudo, la función de TI no interviene en la instalación, el funcionamiento ni la gestión de estos sistemas.

El ataque dirigido a plantas de enriquecimiento de uranio en Irán durante el 2010 había sido planeado con la finalidad de alterar el comportamiento de los sistemas de centrifugación, sin que los tableros de control indicaran ninguna anomalía (Farwell, 2011). Cabe destacar que muchos de estos sistemas de control no están conectados a la Internet, y que en el caso de la inyección del *software* Stuxnet, debió realizarse una intervención manual (Broad; Markoff; y Sanger, 2011), hecho que confirma la teoría de que el "hombre" sigue siendo el eslabón más débil de la cadena de aseguramiento/seguridad de la información.

Para las empresas que aún no han comenzado a preparar estrategias de defensa, un buen punto de partida es la adopción de los procedimientos recomendados, como es el de *Security Requirements for Data Management* (Requerimientos de Seguridad para la Gestión de los Datos), descrito en la sección de "Entrega y Soporte" (DS, *Deliver and Support*) 11.6 de COBIT (objetivos de control para la TI y tecnologías afines), junto con los procedimientos indicados en la correspondiente sección de la guía de aseguramiento *IT Assurance Guide: Using COBIT®* (IT, 2007).

Estas publicaciones resumen el objetivo de control y los factores determinantes de valor y de riesgo, e incluyen una lista de pruebas recomendadas para el diseño del control. ISACA también publicó una serie de documentos que establecen correspondencias entre las normas sobre seguridad de la información y COBIT 4.1, y que resultan muy valiosos para profesionales y auditores. Además, se ha publicado recientemente en COBIT Focus un excelente artículo que establece una correspondencia entre la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS, *Payment Card Industry Data Security Standard*) versión 2.0 y COBIT versión 4.1.10.

La Asociación Internacional de Gestión de Datos (DAMA, *Data Management Association International*) ofrece un recurso adicional: *The DAMA Guide to the Data Management Body of Knowledge* (DMBOK); se recomiendan especialmente los capítulos 3 ("*Data Governance*"), 7 ("*Data Security Management*") y 12 ("*Data Quality Management*") [DAMA, 2009].

Desde la perspectiva del cumplimiento normativo, existe un marco legislativo cada vez más amplio que asigna a las organizaciones la responsabilidad de garantizar la integridad de los datos; así como del aseguramiento de la información (*Information Assurance*, IA). En los Estados Unidos de América se han aprobado las siguientes leyes, que imponen severas sanciones en caso de incumplimiento: *Data Quality Act* (Ley de Calidad de los Datos), *Sarbanes-Oxley Act* (Ley Sarbanes-Oxley), *Gramm-Leach-Bliley Act* (Ley Gramm-Leach-Bliley), *Health Insurance Portability and Accountability Act* (Ley de Transferibilidad y Responsabilidad de los Seguros de Salud) y *Fair Credit Reporting Act* (Ley de Garantía de Equidad Crediticia). También existe la F*ederal Information Security Management Act* (Ley Federal de Gestión de Seguridad de la Información), que establece sanciones económicas en caso de incumplimiento de las disposiciones vigentes. (El análisis de las leyes vigentes fuera de los Estados Unidos de América excede el alcance del presente apartado; sin embargo, cabe destacar dos excelentes ejemplos de legislación comparada, como la directiva de la Unión Europea [UE] para la protección de los datos ["*Directive on Data Protection*"], y la 8a. Directiva de la UE sobre Derechos de Sociedades ["*8th Company Law Directive*"] con relación en las auditorías legales) [UE 1995 y 2006].

Ahora, la pregunta importante es la siguiente: ¿cómo se puede garantizar una mayor integridad de los datos? La respuesta es la siguiente: la adopción de mejores prácticas debe complementarse con la formalización de las responsabilidades correspondientes a los procesos de negocio y de TI que soportan y mejoran la seguridad de los datos. En todo programa de aseguramiento de la integridad de los datos, deben estar definidas

las responsabilidades de "Detección y Detención" (2D, "*Detect, Deter*"); de "Prevención y Preparación" (2P, "*Prevent, Prepare*"); y de "Respuesta y Recuperación" (2R, "*Respond, Recover*") [*US Chiefs of Staff Joint Publication*, 2007]. Como propietarias de los datos, las áreas de negocio deben tomar la iniciativa, mientras que el proveedor de servicios de TI (se trate de personal interno o contratado mediante la modalidad de terciarización de servicios) debe ocuparse de la implementación.

La adopción de mejores prácticas para los sistemas de seguridad debe complementarse con la formalización de las responsabilidades correspondientes a los procesos de negocio y de TI que soportan y mejoran la seguridad de los datos. En éstas deben estar definidas las responsabilidades de "detección y detención" ("*Detect*, *Deter*" o 2D); de "prevención y preparación" ("*Prevent*, *Prepare*" o 2P), y de "respuesta y recuperación" ("*Respond*, *Recover*" o 2R) [*US Chiefs of Staff Joint Publication*, 2007]. Como propietarias de los datos, las áreas de negocio deben tomar la iniciativa, mientras que el proveedor de servicios de TI (se trate de personal interno o contratado mediante la modalidad de externalización de servicios) debe ocuparse de la implementación.

La figura 5.3 es la representación de cómo lograr la integridad de los datos en un sistema de información.

Figura 5.3 Representación de la manera de lograr la integridad de los datos en un sistema de información

Las buenas prácticas a adoptar son:

Tomar posesión de los datos y asumir la responsabilidad de garantizar su integridad. Solamente el personal de la unidad de negocio correspondiente puede ocuparse de esta tarea. Cuando se aplica la modalidad de externalización de servicios y de operaciones de TI este requisito resulta obvio, pero cuando esos servicios y operaciones se suministran a nivel interno, se suele caer en el error de considerar que los datos pertenecen al área de TI, y que ésta es la responsable de preservar la confidencialidad e integridad de la información. Para tomar el control de esta última, se debe realizar una evaluación de valores que permita calcular el costo potencial de la pérdida de la integridad de los datos y considere las pérdidas económicas directas (por ejemplo, en caso de fraude o de problemas operativos graves), los gastos judiciales y el perjuicio causado a la reputación de la empresa.

Controlar los derechos y privilegios de acceso. Los principios de necesidad de conocer (NTK, *Need to Know*) y de mínimos privilegios (LP, *Least Privilege*) constituyen prácticas eficaces y no son, en teoría, difíciles de aplicar. El

crecimiento de las redes sociales y la noción de que todas las personas son productores de información exigen mayor amplitud y voluntad de intercambio. Las redes sociales se están transformando en una fuerza que resiste y desafía la aplicación de los principios de NTK y LP; por ello, es necesario formalizar, documentar, revisar y auditar regularmente los procesos de solicitud, de modificación y de eliminación de derechos de acceso.

La acumulación de privilegios supone un grave riesgo para la empresa y podría afectar la segregación correcta de funciones. Es común en las organizaciones no llevar un inventario completo y actualizado sobre quién accede a qué, ni se posee una lista completa de los privilegios de usuario, debido a ello, varios proveedores ofrecen productos capaces de obtener automáticamente toda la información relacionada con esos privilegios. Una vez que se han aplicado los principios de NTK y LP a partir de un proceso exhaustivo de gestión de accesos e identidades, el acceso privilegiado sigue siendo un tema delicado que es indispensable analizar y controlar, ya que permite acceder libremente a los datos de producción y a los códigos fuente.

Cuando un usuario está en condiciones de omitir los procedimientos de control de cambios, existe el riesgo de que se produzcan daños serios. Las unidades de negocio que cuenten con administradores y/o programadores de bases de datos a cargo de la gestión de las aplicaciones deberían, al menos, mantener un registro que consigne quiénes tienen acceso a qué datos, además de asegurarse de que se mantengan y se revisen los registros de cambios. Cuando el tipo de tecnología empleada admita el uso compartido de contraseñas privilegiadas, se debería evaluar la posibilidad de utilizar herramientas que identifiquen claramente a toda persona que acceda a las instalaciones, registren la fecha y hora de acceso, y señalen los cambios realizados.

Segregación de Funciones (SoD). Éste es un concepto de probada eficacia práctica en el que seguramente harán hincapié las auditorías internas cuando se revisen sistemas y transacciones de carácter confidencial. Esto se enfrenta con la presión permanente para reducir costos y personal en las organizaciones, que puede suponer un riesgo para el negocio.

Quien se ocupe de suministrar sistemas informáticos y servicios tecnológicos deberá demostrar que se están tomando las medidas adecuadas para alcanzar un grado de desarrollo apropiado y que se está llevando a cabo una correcta medición y supervisión de rendimiento y riesgos con la consiguiente elaboración de los informes pertinentes. Los equipos de apoyo de usuarios finales (tanto los que integran el área de TI como los que operan de forma independiente) suelen ser los responsables de la creación de cuentas y de credenciales de acceso a los sistemas y los datos, las cuales deben estar plenamente documentadas y sólo podrán ser utilizadas cuando se hayan concedido formalmente las autorizaciones pertinentes. Los auditores se ocupan de efectuar evaluaciones independientes y objetivas para determinar en qué medida se han definido y respetado las responsabilidades de las unidades de negocio y del equipo de TI, respecto de la preservación de la integridad de los datos.

Los proveedores de servicios (como las organizaciones de TI y las empresas dedicadas a la externalización de servicios) tienen una clara responsabilidad en cuanto al control de las tecnologías y su funcionamiento, y deben aplicar las medidas necesarias para preservar la confidencialidad, la integridad y la disponibilidad (CIA, *Confidentiality*, *Integrity*, *Availability*) de la información en un entorno operativo.

Por otro lado, los proveedores de servicios no son responsables del gobierno de datos ni de las diversas actividades relacionadas con este proceso. Los SLA (*Service Level Agreement*) definen claramente las responsabilidades de los proveedores de servicios de TI, pero no se ocupan de las que deben asumir los propietarios de los sistemas. Esto produce cierta confusión respecto de las distintas responsabilidades e impide verificar si los datos están clasificados correctamente, y si las funciones y responsabilidades de los usuarios de datos y, en particular, de los usuarios con acceso privilegiado se adecuan a la función crítica que cada uno desempeña.

Por consiguiente, la integridad de los datos sigue siendo el aspecto más relegado de la seguridad y el aseguramiento de la información. Existen muy pocas publicaciones sobre mediciones clave, rendimiento e indicadores clave de riesgo aplicados a la integridad de los datos en un contexto relacionado con la seguridad de la información.

A continuación, se mencionan algunos puntos que pueden resultar útiles para comenzar:

- Un inventario de los derechos de acceso privilegiado, que indique ¿quién tiene acceso a qué información?, ¿quién tiene autorización para hacer qué? y ¿en qué fecha se revisó y actualizó por última vez un documento?
- Un inventario de los datos que es posible extraer, transformar y cargar en otro sistema.
- El número de usuarios que han mantenido derechos y privilegios de acceso históricos.
- El número de cuentas huérfanas o inactivas.
- El número de sistemas de aplicación que contienen derechos de acceso mediante codificación rígida o códigos ocultos ("*backdoors*").
- El número de veces que fue necesario acceder a los datos de producción, para realizar modificaciones o correcciones.
- El número o porcentaje de accesos y/o cambios no autorizados a los datos de producción, que se hubieren identificado.
- El número de problemas de seguridad relacionados con los datos (en un año/en un mes/en un día).
- El número de sistemas que la solución IAM corporativa principal no cubre.
- Un índice de datos incorrectos o incoherentes.
- El porcentaje del modelo de datos de la empresa (o aplicación crítica), que se ha cubierto con medidas destinadas a preservar la integridad.
- El número de medidas incluidas en bases de datos y aplicaciones para detectar discrepancias en los datos.
- El número de medidas aplicadas para detectar el acceso no autorizado a los datos de producción.
- El número de medidas aplicadas para detectar el acceso no autorizado a los sistemas de información.
- El número de medidas aplicadas para detectar las modificaciones que no han estado sujetas a ningún procedimiento de control de cambios.
- El valor anual de las pérdidas económicas ocasionadas por operaciones de fraude a través de sistemas informáticos.

- La cantidad de ataques destinados a destruir la integridad de los datos en los sistemas de SCADA.
- La cantidad de comunicados de prensa generados a partir de los problemas que afectaron la integridad de los datos.

Finalmente, el gobierno de datos se centra específicamente en los recursos de información que se procesan y difunden. Los elementos clave del gobierno de datos pueden clasificarse en seis categorías básicas: accesibilidad, disponibilidad, calidad, coherencia, seguridad y verificabilidad (mediante auditorías) de los datos.

La DAMA ha publicado la guía DMBOK (DAMA, 2005), que presenta un marco integral para la gestión y el gobierno de datos, incluidas las tareas que deben realizarse, y las entradas, las salidas, los procesos y los controles.

La regla GIGO (que afirma que la introducción de datos erróneos genera resultados erróneos) tiene la misma vigencia hoy que cuando fue formulada, hace 60 años. La diferencia entre aquella época y la actual radica en el crecimiento exponencial del volumen de los datos digitales, pero este crecimiento no ha ido acompañado del desarrollo y la consolidación de las disciplinas vinculadas al gobierno de datos. Las características básicas de la CIA (los tres pilares de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad) no han variado, y la disponibilidad sigue siendo el único componente que se puede medir mediante parámetros bien definidos y ampliamente aceptados. La no aplicación de métricas sobre la integridad de los datos debería considerarse un obstáculo, porque sin ella, una empresa no está en condiciones de reconocer cuánto han "mejorado" o "empeorado" la confidencialidad o la integridad desde la introducción de los procedimientos o procesos para administrarlas. En la medida en que el gobierno de datos no reciba el mismo grado de atención que el gobierno de TI (y éste siga siendo el eslabón más débil de la cadena del gobierno corporativo), las organizaciones estarán expuestas a graves riesgos que podrían afectar sus operaciones, su economía, su capacidad de cumplimiento y su reputación.

5.6 Conclusiones

En un entorno de red debe asegurarse la privacidad de los datos sensibles. No sólo es importante proteger de daños no intencionados o deliberados la información más preciada, sino también las operaciones de la red. El mantenimiento de la seguridad de ésta requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear y garantizar este equilibrio, pues incluso en redes que controlan datos sensibles y financieros la seguridad a veces se considera medida tardía (Lokhart, 2007).

Las cuatro amenazas principales que afectan a la seguridad de los datos en una red son accesos no autorizados, sobornos electrónicos, robos y daños intencionados o no intencionados; sin embargo, hay que ser sinceros: la seguridad de los datos no siempre se implementa de forma apropiada, precisamente por la seriedad de estas amenazas. La tarea del administrador es asegurar que la red se mantenga confiable, segura y, en definitiva, libre de aquéllas.

La magnitud y nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red; por ejemplo, una que almacena datos para un banco importante requiere una mayor seguridad que una LAN que enlaza equipos en una pequeña organización de voluntarios.

Generar la seguridad en una red de computadoras del siglo XXI precisa establecer un conjunto de reglas, regulaciones y políticas que no dejan nada al azar: el primer paso para garantizar la seguridad de los datos es implementar las políticas que establecen los matices de la seguridad y que ayudan al administrador y a los usuarios a actuar cuando se producen modificaciones esperadas como las no planificadas tanto en el desarrollo como en el uso real de la red (Stallings, 2004).

5.7 Banco de preguntas para la certificación de CISCO

5.1 ¿Cuáles son las dos partes de una IP?

b) Dirección de red y dirección de *host*
c) Dirección de red y dirección MAC
d) Dirección de *host* y dirección MAC
e) Dirección MAC y máscara de subred

5.2 ¿Qué protocolo de Internet se utiliza para asignar una dirección IP a una dirección MAC?

a) UDP
b) ICMP
c) ARP
d) RARP

5.2 ¿De qué protocolo TCP/IP es una función para hacer *ping*?

a) UDP
b) ICMP
c) ARP
d) RARP

5.4 ¿Dónde reside la dirección MAC de una computadora?

a) Un dispositivo que no puede localizar la dirección IP de destino en su tabla ARP.
b) El servidor RARP en respuesta a un dispositivo que funciona mal.
c) Una estación de trabajo sin disco con una caché vacía.
d) Un dispositivo que no puede localizar la dirección MAC de destino en su tabla ARP.

5.5 ¿Qué es una tabla ARP?

a) Un método para reducir el tráfico de red proporcionando listas de atajos y de rutas a destinos comunes.
b) Una forma de enrutar datos dentro de las redes que están divididas en subredes.
c) Un protocolo que realiza una conversión de la información de la capa de aplicación de una pila a otra pila.
d) Una sección de la RAM en cada dispositivo que asigna direcciones IP a direcciones MAC.

Continuación

5.6 ¿Qué es una ARP?

a) El proceso de un dispositivo que envía su dirección MAC a un origen en respuesta a una petición ARP.
b) La ruta del trayecto más corto entre el origen y el destino.
c) La actualización de las tablas ARP a través de la interceptación y la lectura de los mensajes que viajan por la red.
d) El método de encontrar direcciones IP basándose en la dirección MAC utilizado principalmente por servidores RARP.

5.7 ¿Cómo se llaman las dos partes de la cabecera de una trama?

a) La cabecera MAC y la cabecera IP
b) La dirección de origen y el mensaje ARP
c) La dirección de destino y el mensaje RARP
d) La petición y el paquete de datos

5.8 ¿Por qué son importantes las tablas ARP actualizadas?

a) Porque prueban los enlaces de la red.
b) Porque limitan la cantidad de difusión.
c) Porque reducen el tiempo de mantenimiento del administrador de red.
d) Porque solucionan conflictos de direccionamiento.

5.9 ¿Por qué se hace una petición RARP?

a) Un origen conoce su dirección MAC, pero no su dirección IP.
b) El paquete de datos necesita encontrar la ruta más corta entre el origen y el destino.
c) El administrador necesita configurar el sistema manualmente.
d) Un enlace de la red falla y se debe activar un sistema redundante.

5.10 ¿Qué es una petición RARP?

a) Una cabecera MAC y el mensaje de petición RARP.
b) Una cabecera MAC, una cabecera RARP y un paquete de datos.
c) Una cabecera RARP y las direcciones MAC e IP.
d) Una cabecera RARP y una información final ARP.

Continuación

5.11 ¿Cuáles son las dos partes de una IP?

- **a)** Contienen las direcciones MAC e IP.
- **b)** Reciben mensajes de difusión y proporcionan la información solicitada.
- **c)** Construyen tablas ARP que describen todas las redes a las que están conectados.
- **d)** Responden a las peticiones ARP.

5.12 Si un dispositivo no conoce la dirección MAC de un dispositivo de una red adyacente, envía una petición ARP a:

- **a)** Una pasarela predeterminada
- **b)** El *router* más cercano
- **c)** La interfaz del *router*
- **d)** Todas las anteriores

5.13 Un ejemplo de un IGP es:

- **a)** OSPF
- **b)** IGRP
- **c)** RIP
- **d)** Todas las anteriores

5.14 ¿Dónde reside la dirección MAC de una computadora?

- **a)** OSPF
- **b)** EIGRP
- **c)** RIPv2
- **d)** BGP

5.15 ¿Cuándo es conveniente el enrutamiento estático?

- **a)** Para probar un enlace en particular.
- **b)** Para mantener el ancho de banda de área amplia.
- **c)** Siempre que haya una sola ruta a un destino.
- **d)** Todas las anteriores.

Continuación

5.16 ¿Qué tipo de amenaza principal a la seguridad de una red de computadoras consiste en intrusos motivados y técnicamente muy competentes?

a) Amenazas internas
b) Amenazas externas
c) Amenazas estructuradas
d) Amenazas no estructuradas

5.17 Si un dispositivo no conoce la dirección MAC de un dispositivo de una red adyacente, envía una petición ARP a:

a) Ataque de acceso
b) Ataque de intrusión
c) Ataque de denegación de servicios
d) Ataque de reconocimiento

5.18 ¿Cuál es el segundo paso en la rueda de seguridad?

a) La prueba de la seguridad
b) La supervisión de la seguridad
c) La mejora de la seguridad
d) Asegurar la red de computadoras

5.19 ¿Qué describe de la mejor manera un ataque de acceso?

a) El descubrimiento y la asignación no autorizados de los servicios y de los sistemas de la red de computadoras.
b) La intrusión en una red de computadoras para obtener datos o para aumentar los privilegios de un usuario.
c) Desactivar o atacar los servicios inutilizándolos para los auténticos usuarios.
d) Corromper o destruir la información que se emplea para operar en los negocios.

5.20 ¿Qué solución de seguridad se utiliza para aplicar remedios o medidas para determinar la explotación de los puntos vulnerables conocidos?

a) Los *firewalls*
b) La encriptación
c) La autenticación
d) Parches de vulnerabilidad

Continuación

5.21 ¿Qué producto de Cisco Systems se ha diseñado especialmente para validar la seguridad en una red de computadoras?

a) Un escáner de seguridad
b) Un cliente VPN de seguridad
c) Un administrador de política de QOS
d) La detección de intrusos de seguridad

5.22 ¿Qué se debe hacer para mantener y garantizar en lo posible una red de computadoras tan segura como se requiere?

a) Definir una nueva rueda de seguridad cada semana
b) Mantener repetidamente el ciclo de la rueda de seguridad
c) Adquirir un cortafuegos para cada puesto de trabajo
d) Desactivar la NAT de todos los dispositivos de *intranetworking*

5.23 ¿Qué paso de la rueda de seguridad lleva a cabo el cortafuegos PIX más efectivo?

a) Asegurar el sistema
b) Mejorar la seguridad corporativa
c) Probar en su ubicación la efectividad de los dispositivos de seguridad
d) Supervisar la red de computadoras para comprobar las violaciones y los ataques contra la política de seguridad

5.24 ¿Qué categoría se da a la mayoría de las personas en una amenaza de seguridad sin estructura?

a) Contratistas
b) *Script kiddies*
c) Empleados convencionales
d) Exempleados

5.25 ¿Cuándo es conveniente el enrutamiento estático?

a) La prueba de seguridad
b) La supervisión de la seguridad
c) La mejora de la seguridad
d) Asegurar la red

Referencias

Ahmadi, S. (2009). "An overview of the next generation mobile Wi MAX technology" en *IEEE Community Magazine*, (47): pp. 84-88.

Alkhatib, H. S.; Bailey, C.; Gerla, M. and McRae, J. (s.f.). "Wireless data networks: Reaching the extra mile" en *Computer*, (30): pp. 59-62.

Anderson, R. J. (1994). "Why cryptosystems fail" en Community of the ACM, (37): pp. 32-40.

_____ (2001). *Security Engineering*. New York: Addison-Wiley.

Andrews, J.; Ghosh, A. and Muhamed, R. (2007). *Fundamentals of Wi MAX: Understanding broadband wireless networking*. Upper Saddle River: Pearson Education.

Astely, D.; Dahlman, E.; Furuskar, A.; Jading, Y.; Lindstrom, M. and Parkvall, S. (2009). "LTE: The evolution of mobile broadband" en *IEEE Community Magazine*, (47): pp. 44-51.

Balacheff, B. et al., (2003). *Trusted computing platforms. TCP: A technology in context*. New Jersey: Prentice Hall.

Bankar, P. and Sharad, V. (2011). "Mapping PCI DSS v2.0 with COBIT 4.1" en *COBIT Focus*, (2). Disponible en www.isaca.org/cobitnewsletter, consultado en septiembre de 2017.

Barrios Garrido, G. (1988). *Internet y Derecho en México*. México: McGraw-Hill.

Barriuso Ruiz, C. (1996). *Interacción del Derecho y la Informática*. Madrid, España: Dykinson Editores.

Batis Álvarez, V. et al., (2004). *Panorama general del marco jurídico en materia informática en México.* Disponible en www.alfa-redi.org/rdi-articulo.shtml?x=1246, www.isaca.org/cobitnewsletter, consultado en septiembre de 2017.

Bellovin, S. (2003). "The security flag in the IPv4 hearder" en *RFC* 3 514.

Bennet, C. H. and Brassard, G. (1984). "Quantum cryptography: Public key distribution and coin tossing" en *International Conference on Computer Systems and Signal Processing*, pp. 175-179.

Benson, C. (2011). *Estrategias de Seguridad*. Inobis Consulting Pty Ltd. Microsoft Solutions.

Beresford, A. and Stajano, F. (2003). "Locations privacy in pervasive computing" en *IEEE Pervasive Computing*, (2): pp. 46-55.

Berghel, H. L. (2001). "Cyberprivacy in the new millennium" en *Computer*, (34): pp. 132-134.

Bi, Q.; Zysman, G. I. and Menkes, H. (2001). "Wireless mobile communications at the start of the 21st century" en *IEEE Communications Magazine*, (39): pp. 110-116.

Biham, E. and Shamir, A. (2007). "Differential cryptanalysis of the data encryption standard" en Proc. *17th Annual International Cryptology Conference*, Berlin: Springer-Verlag LNCS 1 294, pp. 513-525.

Bird, R.; Gopal, I.; Herzberg, A.; Janson, P. A.; Kutten, S.; Molva, R. and Yung, M. (1993). "Systematic design of a family of attack-resistant authentication protocols" en *IEEE Journal on Selected Areas in Communications*, (11): pp. 679-693.

Biryukov, A.; Shamir, A. and Wagner, D. (2000). Real time cryptanalysis of A5/1 on a PC. *Procedures in the Seventh International Workshop on Fast Software Encryption*, Berlin: Springer-Verlag LNCS, pp. 1-8.

Blanco Encinaza, L. J. (2010). "La auditoría informática al comienzo del tercer milenio" en *Revista cubana de computación. Columbus Conectividad*, (6).

Blaze, M. (1994). Protocol failure in the escrowed encryption standard. *Processing in the Second ACM Conference on Computer and Community Security*, ACM, pp. 59-67.

Bleichenbacher, D. (1996). Generating El Gamal signatures without knowing the secret key. *Advances in Cryptology, Proceedings Eurocrypt '96, LNCS 1070*, U. Marer, Berlin: Springer Verlag, pp. 10-18.

Boot, D. and Haas, H. (2004). *Web services architecture. W3C working group note*. Disponible en www.w3.org/TR/2004/NOTE-ws-arch-20040211/, consultado en septiembre de 2017.

Borisov, N.; Goldberg, I. and Wagner, D. (2001). Intercepting mobile communications: The insecurity of 802.11. *Seventh International Conference on Mobile Computing and Networking*, ACM, pp. 180-188.

Bornik, S. (2011). *Malware y cibercrimen*. CXO Community. Disponible en http://youtu.be/nL3jIUhX6wk, consultado en septiembre de 2017.

Brands, S. (2000). *Rethinking public key infrastructures and digital certificates*. Massachusetts: M.I.T. Press.

Broad, W. J.; Markoff, J. and Sanger, D. E. (2011). "Israeli test on worm called crucial in Iran nuclear delay" en *The New York Times*, January, 15th. Disponible en http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html, consultado en septiembre de 2017.

BS ISO/IEC 17799: Information Technology. (2000). *Code of practice for information security management*. UK: British Standard Institute.

BS ISO/IEC 27001: Information Technology. (2005). *Security techniques. Information security management*. UK: British Standard Institute.

BS ISO/IEC 27002: Information Technology. (2007). *Security techniques. Code of practice for information security management*. UK: British Standard Institute.

Burnett, S. and Paine, S. (2001). *Security´s official guide to cryptography*: California: Osborne/McGraw-Hill.

Caballero Gil, P. y Hernández Goya, C. (2000). *Criptología y seguridad de la información.* México: McGraw-Hill.

Cámara de Diputados del H. Congreso de la Unión (2006). *Código Penal Federal*. México: H. Congreso de la Unión.

Cámpoli, G. A. (2004). *Principios de Derecho penal informático*. México: Ángel Editor.

Cisco Sys. (2010). Cisco virtual networking index: Forecast and methodology, 2009-2014. *Cisco Systems Inc*.

Clark, D. D. (1988). The design philosophy of the DARPA Internet protocols. *Procedures SIGCOMM ´88 Conference ACM*, pp. 106-114.

Cheswick, W., R.; Bellovin, S. M. and Rubin, A. D. (2003). *Firewalls and Internet security: Repelling the wily hacker*. Disponible en http://books.google.com.mx/books?id=_ZqIh0IbcrgC&lpg=PA142&dq=Firewalls+and+Internet+Security,+by+Cheswick+et+al.&pg=PA176&redir_esc=y#v=onepage&q=Firewalls%20and%20Internet%20Security%2C%20by%20Cheswick%20et%20al.&f=false, consultado en septiembre de 2017.

Comer, D. E. (2005). *Internetworking with TCP/IP*. Englewood Cliffs, New Jersey: Prentice-Hall, 5th ed.

Corey, M. y Abbey, M. (1997). *ORACLE DataWarehousing: La seguridad de los datos*. España: McGraw Hill.

Correa, C. M. et al. (1987). *Derecho informático*. Buenos Aires, Argentina: De Palma Editores.

Crovella, M. and Krishnamurty, B. (2006). *Internet measurements*. New York: John Wiley & Sons.

Daemen, J. and Rijmen, V. (2002). *The design of Rijndael*. Berlin: Springer-Verlag.

Data Management Association International (DAMA) (2009). *The DAMA guide to the data management body of knowledge*. USA: Technics Publications, LLC. Disponible en www.dama.org/i4a/pages/index.cfm?pageid=3345, consultado en septiembre de 2017.

Davara Rodríguez, M. Á. (1993). *Derecho informático*. Pamplona, España: Aranzadi Editores.

Day, J. D. and Zimmermann, H. (2003). "The OSI Reference Model" en *Procedures of the IEEE*, (71): pp. 1334-1340.

Derrien, Y. (1995). *Técnicas de la Auditoría Informática: La dirección de la misión de la auditoría*. México: Alfaomega Grupo Editor.

Dhiren R. P. (2008). *Information security. Theory and practice*. New York: PHI Learning Private.

_____ (2010). *Information security and practice*. New Jersey: Prentice Hall.

Diffie, W. and Hellman, M. E. (1977). "Exhaustive cryptanalysis of the NBS data encryption standard" en *IEEE Computer*, (10): pp. 74-84.

Dobbs, M. (2008). *The edge of madness*. U. K: Simon & Shuster, Ltd.

Donahoo, M. and Calvert, K. (2009). *TCP/IP sockets in C*. San Francisco, California: Morgan Kaufmann, 2nd ed.

El Gamal, T. (1985). "A public-key cryptosystem and a signature scheme base on discrete logarithms" en IEEE Transaction on Information Theory, (IT-1): pp. 406-472.

Equipo de Economistas DVE (1991). *Curso completo de auditoría: Introducción*. Barcelona: Editorial De Vecchi.

Farley, M. (1996). *Guía de LAN TIMES de seguridad e integridad de datos: Seguridad informática*. España: McGraw-Hill.

Farwell, J. P. and Rohozinski, R. (2011). "Stuxnet and the future of cyber war" en *Survival*, 53(1).

Ferguson, N.; Schneier, B. and Kohno, T. (2010). *Cryptography engineering: Design principles and practical applications*. New York: John Wiley & Sons.

Fernández, C. M. (2008). *Seguridad en sistemas informáticos*. España: Ediciones Díaz de Santos.

Ford, W. and Baum, M. S. (2000). *Secure electronic commerce*. New Jersey: Prentice-Hall.

Fridrich, J. (2009). *Steganography in digital media: Principles, algorithms and applications*. Cambridge: Cambridge University Press.

Fuller, V. and Li, T. 2006). Classless Inter-Domain Routing (CIDR): The Internet address assignment and aggregation plan. *RFC 4 632*.

Galindo, F. (1998). *Derecho e informática*. Madrid, España: Editorial La Ley-Actualidad.

Garfinkel, S. and Spafford, G. (2002). *Web security, privacy and commerce*. Sebastopol, California: O´Reilly.(

Girault, M. (1991). "Self-Certified public keys" en *EUROCRYPT*, (547), pp. 490-497.

Goode, B. (2002). "Voice over Internet Protocol" en *Procedures of the IEEE*, (90): 1495-1517.

Goralski, W. J. (2002). *SONET*. New York: McGraw-Hill, 2nd ed.

Hance, O. (1996). *Leyes y negocios en la Internet*. México: McGraw-Hill.

Harrington, J. L. (2006). *Manual práctico de seguridad de redes*. España: Editorial Anaya Multimedia. Disponible en www.idg.es/comunicaciones.f.rticulo.asp?id=134356, consultado en septiembre de 2017.

Held, G. (2010). *A practical guide to content delivery networks*. Boca Raton, Florida: CRC Press.

Hiertz, G.; Denteneer, D.; Stibor, L.; Zang, Y.; Costa, X. and Walke, B. (2010). "The IEEE 802.11 universe" en *IEEE Community Magazine*, (48): pp. 62-70.

Huerta Villalón, A. (s.f.). *Seguridad en Unix y redes*. España: Paraninfo.

IBM Corporation (1998). *S.O.S. en su sistema de computación*. México: Prentice-Hall Hispanoamericana.

IBM Education and Training. (1995). *Internet Security and firewalls concepts. Student notebook*. Course Code IN30. USA: IBM.

Ingham, K. and Forrest, S. (2002). *A history and survey of network firewalls*. USA: University of New Mexico. Disponible en www.cs.unm.edu/~treport/tr/02-12/firewall.pdf, consultado en septeibmre de 2017.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) (1994). *Sistemas de calidad*. Santa Fe de Bogotá, D. C.

IT Governance Institute, IT Assurance Guide (2007). *Using COBIT®*. USA: IT Governance Institute.

Jakobsson, M. and Wetzel, S. (2001). Security weaknesses in Bluetooth. *Topics in Cryptology: CT-RSA*, Berlin: Springer-Verlag.

Johnson, N. F. and Jajoda, S. (1998). "Exploring steganography: Seeing the unseen" en *Computer*, (31): pp. 26-34.

Johnson, D.; Perkins, C. and Arkko, J. (2004). Mobility support in IPv6. *RFC 3 775*.

Kahn, D. (1995). *The code-breakers*. New York: Macmillan, 2nd ed.

Kaufman, C.; Perlman, R. and Speciner, M. (2002). *Network security*. New Jersey: Prentice-Hall, 2nd ed.

Kerviel, J. (210). L'engranage. Memoires d'un trader. Flammarion, France. Et la Societé Genérale. Disponible en www.societegenerale.com/en/search/node/kerviel, consultado en septiembre de 2017.

Koblitz, N. (2008). *A course in number theory and cryptography*. USA: John Wiley & Sons.

Koodli, R. and Perkins, C. E. (2007). *Mobile internetworking with IPv6*. New York: John Wiley & Sons.

Lockhart, A. (2007). *Seguridad de redes*. España: Editorial Anaya Multimedia.

Lubacz, J.; Mazurczyk, W. and Szczypiorski, K. (2010). "Voice over IP" en *IEEE Spectrum*, pp. 42-47.

Mason, A. G. (2002). *Cisco secure Virtual Private Network (VPN)*. USA: Cisco Press.

Mc Connell, S. (1996). *Desarrollo y gestión de proyectos informáticos: Gestión de riesgos*. Madrid: McGraw Hill.

Méndez, C. E. (1993). *Metodología. Guía para elaborar diseños de investigación en ciencias económicas, contables y administrativas*. Santa Fe de Bogotá: McGraw Hill.

Menezes, A. J.; Van Oorschot, P. C. and Vanstone, S. A. (2010). *Handbook of applied cryptography*. USA: ITU.

Merkle, R. (1990). A certified digital signature. *Advances in Cryptology, Proceedings Crypto, LNCS* 435. G. Brassard. Berlin: Springer Verlag, pp. 228-238.

Mir Puig, S. (comp.) (1992). *Delincuencia informática*. Barcelona, España: Promociones y Publicaciones Universitarias, IURA-7.

Microsoft Tech (2001). *Red privada virtual: Una visión general*. EUA: Microsoft Technologies Press.

Molina Salgado, J. A. (2003). *Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial*. México: Porrúa.

Morón Lerma, E. (1999). *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*. Pamplona, España: Aranzadi Editores.

Nichols, R. K. and Lekkas, P. C. (2002). *Wireless security*. New York: McGraw-Hill.

Orange Book (1985). Department Of Defense. Library N° S225, 711. USA. Disponible en http://www.doe.gov, consultado en septiembre de 2017.

Orera Gracia, A. y Soriano Sarrió, V. (2012). *Firewalls*. España: Universidad Complutense de Madrid. Disponible en www.e-sort.net/blog/wp-content/uploads/2012/06/FireWalls_Armando_Orera_Gracia_Infor_-Pro_2012_COLGAR.pdf, consultado en septiembre de 2017.

Organization for Economic Cooperation and Development (1984). *Computer related criminality: Analysis of legal policy in the OECD Area*. Paris: OCDE/ICCP.

_____ (2004). *Directrices de la OCDE para la seguridad de sistemas y de redes de información: Hacia una cultura de seguridad*. París: Ministerio de Administraciones Públicas, Secretaría General Técnica, España.

Palazzi, P. A. (2000). *Delitos informáticos*. Buenos Aires, Argentina: Ad-Hoc Editores.

Pastor Franco, J. y Sarasa López, M. A. (1998). *Criptografía digital. Fundamentos y aplicaciones*. España: Prensas Universitarias de Zaragoza.

Pepelnjak, I. and Guichard, J. (2001). *MPLS and VPN architectures*. Indiana: Cisco Press.

Pérez Luño, A. E. (1996a). *Manual de informática y derecho*. Barcelona: Ariel.

_____ (1996b). *Ensayos de Informática Jurídica*. México: Fontamara.

Perlman, R. and Kaufman, C. (2000). "Key exchange in IPsec" en IEEE Internet Computing, (4): pp. 50-56.

Pieprzyk, J.; Hardjono, T. and Seberry, J. (2004). *Fundamentals of computer security*. USA: Prentice-Hall.

Pinilla, J. D. (1997). *Auditoría informática. Aplicaciones en Producción: Análisis de riesgos*. Santa Fe de Bogotá: ECOE Ediciones.

Pohlmann, N. (2001). *Firewalls systems*. Germany: MITP-Verlag.

Preneel, B. (2010). *Cryptographic primitive for information authentication*. State of the Art. Germany: Katholieke Universiteit in Leuven.

Ramanujachary, K. and Romero, C. (2009). *Number theory with computer applications*. USA: Prentice Hall.

Reynolds, J. and Holbrook, P. (1991). *RFC 1244: Site Security Handbook*.

Rico, E. (2014). "¡Cuidado con el malware!" en *Revista Mundo Ejecutivo*, (422): pp. 86-88.

Ríos, J. J. (1997). *Derecho e Informática en México: Informática Jurídica y Derecho de la Informática*. México: UNAM.

Rivest, R. L.; Shamir, A. and Adleman, L. (1978). "On a method for obtaining digital signatures and public key cryptosystems" en *Community of the ACM*, (21): pp. 120-126.

Rodríguez, E. (2014). *TCP versus UDP.* Disponible en www.skullbox.net/tcpudp.php, consultado en septiembre de 2017.

Salido, J. (2010). "Data governance for privacy, confidentiality and compliance: A holistic approach" en *ISACA Journal*, (6).

Sallevane, J. P. (1996). *Gerencia y planeación estratégica: El método Delfi*. Colombia: Editorial Norma, 2ª ed.

Scarola, R. (1992). *Novell Netware*. Madrid: McGraw Hill.

Schneier, B. (1995). *E-mail security*. New York: Addison-Wiley.

_____ (2000). *Applied Cryptography*. New York: Prentice Hall.

Senn, J. A. (2000). *The emergence of M-Commerce*. IEEE Computer, (33): pp. 148-150.

_____ (2004). *Análisis y diseño de sistemas de información*. México: McGraw Hill, 2ª ed.

Simmons, G. J. (1992). A *survey of information authentication*. Contemporary cryptology: The science of information integrity. New York: IEEE Press.

Simpson, W. (2008). *Video over IP*. Burlington, Massachusetts: Focal Press.

Skoudis, E. and Liston, T. (2006). *Counter hack reloaded*. Upper Saddle River, New Jersey: Prentice-Hall, 2nd ed.

Spafford, G. (2000). *Manual de seguridad en redes*. Argentina: ArCERT. Disponible en www.arcert.gov.ar, consultado en septiembre de 2017.

Stallings, W. (2004). *Fundamentos de seguridad en redes*. México: Pearson Education.

_____ (2006). *Cryptography and network security: Principles and practice*. USA: Prentice-Hall.

_____ (2010). *Data computer communications*. Upper Saddle River, New Jersey: Pearson Education, 9th ed.

Stinson, D. R. (2002). *Cryptography theory and practice*. Florida: CRC Press, 2nd ed.

Stuttard, D. and Pinto, M. (2007). *The web application hacker´s handbook*. New York: John Wiley & Sons.

Téllez, J. (1995). *Derecho informático*. México: McGraw-Hill, Serie Jurídica, 2ª ed.

Terán Pérez, D. M. (2010). *Redes convergentes. Diseño e implementación*. México: Alfaomega Grupo Editor.

_____ (2012). *Introducción a la computación cuántica para ingenieros*. México: Alfaomega Grupo Editor.

_____ (2014). *Administración estratégica de la función informática*. México: Alfaomega Grupo Editor.

_____ (2016). *Introducción a la ingeniería*. México: Alfaomega Grupo Editor.

Van Der Lubbe, J. (2006). *Basic methods of cryptography*. USA: McGraw-Hill.

Vaughan, E. J. (1997). *Risk Management*. USA: John Wiley & Sons.

Wayner, P. (2002). *Disappearing cryptography: Information hiding, steganography and watermarking*. San Francisco: Morgan Kaufmann.

Xenitellis, S. (1999). *The open–source PKI Book*. Disponible en http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI-html/ospki-book.htm, consultado en septiembre de 2017.

YourDictionary.com (s.f.). Data Integrity. *YourDictorionary.com*. Disponible en http://computer.yourdictionary.com/dataintegrity, consultado en septiembre de 2017.

Yu, T.; Hartman, S. and Raeburn, K. (2004). The perils of unauthentication encryption: Kerveros version 4. *Procedures NDSS Symposium*, Internet Society.

Zacks, M. (2001). "Antiterrorist legislation expands electronic snooping" en *IEEE Internet Computing*, (5): pp. 8-9.

Zhao, B.; Ling, H.; Stribling, J.; Rhea, S.; Joseph, A. and Kubiatowicz, J. (2004). "Tapestry: A resilient global-scale overlay for service deployment" en *IEEE Journal on Selected Areas in Communications*, (22): pp. 41-53.

La administración estratégica de la seguridad informática

En realidad, no me preocupa que quieran robar mis ideas; me preocupa que ellos, no las tengan.

Nikola Tesla

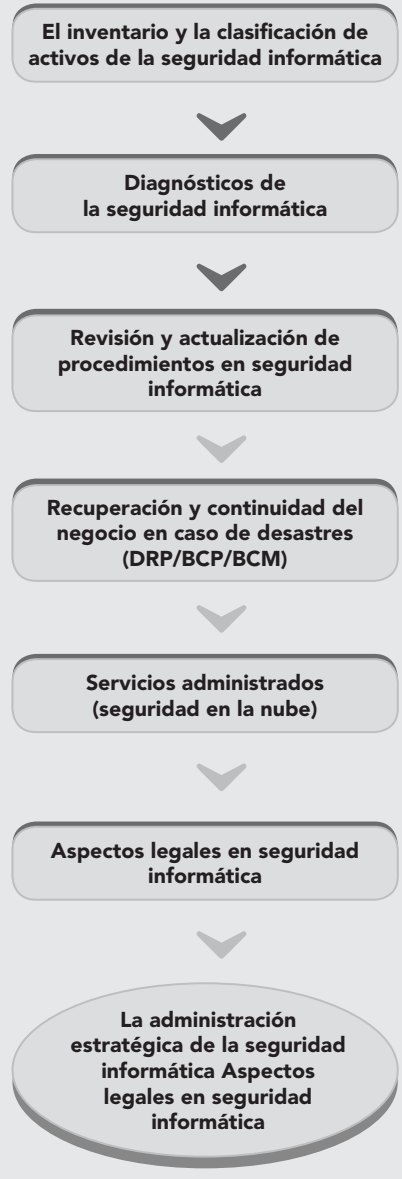
Reflexione y responda las siguientes preguntas:

- ¿Qué es un inventario en seguridad informática, y cómo se clasifican los activos de una organización, desde el enfoque de la seguridad informática?
- ¿Cómo se diagnostica la seguridad informática en una red de computadoras en una organización?
- ¿Cuál es el protocolo para la revisión y la actualización de los procedimientos en seguridad informática en una organización?, ¿existe una normatividad específica para llevar a cabo dichos procedimientos? Si es así, explique dicha normativa.
- ¿Cómo se desarrolla el protocolo de recuperación y de continuidad de la(s) unidad(es) de negocio(s) en las organizaciones, en caso de presentarse un desastre?
- ¿Cuáles son los aspectos legales dentro de la seguridad informática en una red de computadoras en una organización?

Después de estudiar este capítulo, el lector será capaz de:

- Explicar qué es un inventario en seguridad informática, y cómo se clasifican los activos de una organización, desde el enfoque de la seguridad informática.
- Explicar cómo se diagnostica la seguridad informática en una red de computadoras, en una organización.
- Comprender cuál es el protocolo para la revisión y la actualización de los procedimientos en seguridad informática en una organización, y explicará si existe una normatividad específica, para llevar a cabo dichos procedimientos.
- Establecer cómo se desarrolla el protocolo de recuperación y de continuidad de la(s) unidad(es) de negocio(s) en las organizaciones, en caso de presentarse un desastre.
- Explicar cuáles son los aspectos legales dentro de la seguridad informática en una red de computadoras en una organización

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:



6.1 Introducción

La información que se maneja en las organizaciones el día de hoy es considerada un activo cada vez más valioso, la cual puede hacer que una organización triunfe o quiebre; es por eso que debe mantenerse siempre segura. La mayoría de las organizaciones desconocen la magnitud del problema con el que se enfrentan, considerando la seguridad informática como algo secundario y prestando poca atención a los riesgos que en la actualidad existen, como son las amenazas internas, una de ellas los errores humanos y otra la ingeniería social; así como las amenazas externas dentro de las cuales se pueden nombrar los virus informáticos. Esta falta de inversión, tanto en capital humano como en la compra de dispositivos físicos y aplicaciones lógicas (muy necesarios para prevenir principalmente el daño o la pérdida de la información), produce que la información no sea confiable ni íntegra, y mucho menos disponible para la empresa, originando así, en muchos de los casos, la paralización parcial o total de sus actividades, dejando como resultado una pérdida cuantiosa de tiempo, de producción y de dinero; factores importantes para el desarrollo de una organización.

La información es "la sangre" de todas las organizaciones y sin ella la empresa dejaría de funcionar, sobre todo si se trata de empresas altamente automatizadas, por lo que su seguridad sigue siendo un punto pendiente; y por lo tanto, el factor más determinante por el cual fracasan. Es muy importante ser y estar conscientes de que por más que una empresa sea la más segura (relativamente hablando), con el incremento del uso de nueva tecnología para manejar la información, dicha organización está abierta a un mayor número y tipos de amenazas. Es por eso que en el ambiente competitivo de hoy es necesario que las entidades aseguren realmente la confidencialidad, la integridad y la disponibilidad de la información vital corporativa.

Por lo anterior, la seguridad informática debe ser dada por una colaboración entre los encargados de la seguridad de la información, que deben disponer de las medidas a su alcance, y los usuarios, que deben ser conscientes de los riesgos que implican determinados usos de los sistemas y de los recursos que consumen cada vez que les pasa algún problema, ya que esto les hace que pierdan tiempo de producción, y el consumo de recursos en horas de la recuperación de la actividad normal es en muchos casos irrecuperable. Sin embargo, gran parte de esa concientización está en manos de los responsables de seguridad de la información, apoyados en todo momento por la Gerencia y la Dirección de forma explícita y activa. Por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas; impartiendo así procedimientos y protocolos de actuación, que permitan que las medidas técnicas que se disponen desde la informática sean efectivas. Por consiguiente, en este nuevo entorno es imprescindible que las empresas se preparen no sólo para prevenir el peligro de comprometer sus operaciones de negocio por una falla de/en la seguridad, sino también que se preparen en establecer medidas que permitan reducir los problemas de seguridad que pueden surgir.

6.2 El inventario y la clasificación de activos de la seguridad informática

La realización de un inventario y clasificación de activos de información hace parte de la debida diligencia que a nivel estratégico debe considerar cualquier organización dentro de sus elementos a tratar. De esta forma, y con base en las normas técnicas NTC ISO/IEC 17799:2005 y NTC ISO/IEC 27001 en el punto denominado "Gestión de Activos", se persigue dar cumplimiento a tres elementos principales:

Inventario de los activos. Todos los activos deben estar claramente identificados e inventariados dentro de la entidad.

Propiedad de los activos. Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad" de una parte designada de la entidad.[1]

Directrices de clasificación. La información debe clasificarse en términos de su valor, de los requisitos legales, de la sensibilidad y de la importancia para la entidad.

A continuación, se presentan las definiciones más importantes sobre el significado de un inventario en seguridad informática:

Proceso. Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor, y las cuales transforman elementos de entrada y de salida.

Activo de información. Cualquier cosa que tiene información y valor para el ICBF. Puede encontrarse almacenado en diferentes medios como discos duros, USB, CD, impresiones, etc.

Información. Datos relacionados que tienen significado para la organización.[2] La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.[3]

Seguridad de la información. La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de negocio. Adicionalmente, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

Clasificación de la información. Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados a un nivel corporativo. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. La información debe clasificarse en términos de la sensibilidad y la importancia para la entidad.

[1] El término "propietario" identifica a un individuo o a una entidad que tiene responsabilidad aprobada de la Dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. Éste no implica que la persona tenga realmente los derechos de propiedad de los activos.

[2] Adaptado y traducido de *Principles of information warfare*. Hutchinson, W. y Warren, M. (2005). *Journal of information warfare*.

[3] Tomado de NTC ISO/IEC 17799:2005.

Propietario de la información. Es una parte designada de la entidad o proceso que gestiona y tiene la responsabilidad de definir quiénes tienen acceso y qué pueden hacer con la información, así como de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y, a la vez, de definir qué se hace con la información una vez que ya no sea requerida.

Custodio. Es una parte designada de la entidad, un cargo, proceso o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación, borrado.

Responsable de la información. Es el cargo o persona designada que toma decisiones sobre el activo de *información*.

Usuario. Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la entidad en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía. Son las personas que utilizan la información para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. [4]

Mediante la definición de un inventario, una organización específica y reconoce cuáles son los activos de información más importantes del negocio, por lo que se deben determinar aquellos que ayudan al cumplimiento del objetivo de la organización y las salidas de los procesos o macroprocesos según corresponda, tales como controles de seguridad física y estudios financieros o de cálculo de primas de seguros, entre otros.

Las actividades realizadas para obtener un inventario de activos son un prerrequisito de la gestión de riesgos de seguridad de la información. Los activos de información tienen dos tipos de atributos: los "CDI" y los "generales". Los primeros corresponden a la confidencialidad, integridad y disponibilidad de la información y se representan con calificadores que varían en el rango desde muy bajo (MB) hasta muy alto (MA), como se muestra la tabla 6.1.

Tabla 6.1 Criterios de confidencialidad, disponibilidad e integridad (CDI)

Clasificación	Confidencialidad	Integridad	Disponibilidad
Muy alto (MA)	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente a toda la empresa.	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente a toda la empresa.	La falta del activo de información impacta negativamente a la empresa.
Alto (A)	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente algunos negocios.	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente algunos negocios.	La falta del activo de información impacta negativamente algunos negocios.

continúa

[4] "Las personas que se relacionan con el ICBF, están obligadas a utilizar la información a la cual tengan acceso en virtud de sus funciones o relación contractual, exclusivamente para el ejercicio de las mismas".

Medio (M)	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera importante al proceso.	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente algunos negocios.	La falta del activo de información impacta negativamente algunos negocios.
Bajo (B)	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera leve al proceso.	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente de manera leve al proceso.	La falta del activo de información impacta negativamente de manera leve al proceso.
Muy bajo (MB)	El conocimiento o divulgación no autorizada de este activo de información no tiene ningún impacto negativo en el proceso.	La pérdida de exactitud y estado completo de la información y métodos de procesamientos no tiene ningún impacto negativo en el proceso.	La falta del activo de información no tiene ningún impacto en el proceso.

Fuente: NTC ISO/IEC 17799:2005.

Los atributos generales son nueve, y describen con mayor detalle las características del activo (tabla 6.2).

Tabla 6.2 Atributos generales de los activos

Atributo	Descripción
A1	Activo de información de clientes o terceros que debe protegerse.
A2	Activo de información que debe ser restringido a un número limitado de empleados.
A3	Activo de información que debe ser restringido a personas externas.
A4	Activo de información que puede ser alterado o comprometido para fraudes o corrupción.
A5	Activo de información que es muy crítico para las operaciones internas.
A6	Activo de información que es muy crítico para el servicio hacia terceros.
A7	Activo de información que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica.
A8	Activo de información con implicaciones legales.
A9	Activo de información que debe cumplir con las tablas de retención documental.

Fuente: NTC ISO/IEC 17799:2005.

Para la elección del nombre de los diferentes niveles de clasificación, se tuvo en cuenta lo siguiente:

- La etiqueta de confidencialidad es crítica para todos los usuarios de la información. Ésta es descriptiva, de manera que cualquier persona que la lea puede hacerse una idea general de lo que implica a nivel de cuidados y de accesos.

- Las etiquetas de integridad y de disponibilidad son críticas para los propietarios y los custodios de la información, pero de menos importancia para los usuarios generales. En consecuencia, se seleccionaron nombres cortos que simplifican la etiqueta completa del archivo.

A continuación, en la tabla 6.3, se muestra la clasificación de activos de información:

Tabla 6.3 Criterios de confidencialidad, disponibilidad e integridad (CDI)

Clasificación	Descripción	Ejemplos
Pública	Información que puede ser distribuida abiertamente al público, pues no causará ningún daño a las organizaciones, a sus funcionarios o a otras entidades. Para que la información sea pública debe ser clasificada de esta manera por el área que la elaboró; por ejemplo, la Dirección General, el Área de Comunicaciones, el Área Jurídica, el Departamento de Sistemas, etcétera. Los documentos públicos pueden ser distribuidos libremente a entidades o ciudadanos.	Material publicitario, información del sitio web, carteleras en áreas abiertas al público.
Uso interno	Información que no se debe distribuir al público en general, ya que tiene un destinatario específico y es propia de la organización. Se requiere autorización para distribuirla a una persona o entidad diferente a su destinatario definido.	Cartas, memorandos, boletines internos, manuales, guías de entrenamiento, bases de datos, nóminas, documentos de trabajo de las áreas, archivos de configuración de equipos, información personal de los funcionarios, llamadas telefónicas, correos electrónicos, acuerdos de nivel de servicio, etc.
Confidencial	Documentos clasificados como altamente sensitivos y reservados por la ley. La divulgación solamente se autoriza a terceros bajo la responsabilidad del nivel directivo o una orden proporcionada por una autoridad judicial competente.	Contraseñas de usuarios, números de cuenta corrientes o de ahorros de los empleados o de la propia organización, evaluaciones de propuestas antes de su publicación, información personal de funcionarios, etc.
Reservada	Información que está catalogada como reservada por la ley.	Toda aquella estrictamente confidencial.

Fuente: NTC ISO/IEC 17799:2005.

Para asignar el nivel de clasificación de un activo de información, de acuerdo con su integridad, se deben tener en cuenta los atributos de la manera que se explica en la tabla 6.4.

Tabla 6.4 Nivel de clasificación de un activo de información

Nivel	Atributo
1	Disponibilidad muy alta (MA)
2	Cualesquiera de los atributos A5 o A6 o disponibilidad alta (A) o media (M)
3	Disponibilidad baja (B) o muy baja (MB)

Fuente: NTC ISO/IEC 17799:2005.

Finalmente, los activos de información deben manejarse de acuerdo con las recomendaciones establecidas a continuación. Se aplican según su nivel en confidencialidad, integridad y disponibilidad, como lo muestran las tablas 6.5, 6.6 y 6.7. La confidencialidad es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Tabla 6.5 Clasificación de la información según su nivel de confidencialidad

Clasificación	Controles físicos y administrativos	Reproducción	Distribución	Destrucción y disposición
Pública	Distribución autorizada por el creador de la información.	Ilimitada	Sin restricción	Lo que indique y exprese la tabla de retención documental.
Uso interno	Autor: es el responsable de colocar el pie de página del documento. Custodio: se encarga de almacenar la información apropiadamente y de controlar su circulación sólo para uso interno. Debe solicitar autorización al autor o a una autoridad superior para su distribución; inclusive, dentro de la organización. Ejemplos: los reportes de control interno, la información financiera de la organización, la información de la nómina, entre muchas otras.	Limitar el número de copias. La distribución a contratistas solamente se realiza bajo la autorización de un superior jerárquico y con previa firma de acuerdos de confidencialidad.	Interna: usar el correo electrónico con nota de información de uso interno. Externa: utilizar sobres externos. Electrónica: uso del correo institucional. Si es viable, usar cifrado de datos cuando se intercambia con personas de control o terceros autorizados que han formado acuerdo de confidencialidad.	Documentos en papel: usualmente se convierten en tiras que se mezclan antes de enviarlas a la basura; posteriormente, se debe verificar que el papel se destine a reciclaje interno. Datos electrónicos: se debe aplicar el borrado o destrucción para CD, DVD y discos duros.
Confidencial	Autor: responsable de asegurar la confidencialidad de la información, así como de garantizar su distribución únicamente bajo autorización. Custodio: responsable de asegurarse de que la información confidencial sea almacenada bajo llave cuando no esté en uso; cifrada si es electrónica y bajo aplicación de los controles definidos por el comité de seguridad de la información.	Uso limitado de copias solamente bajo autorización del generador o sus designados. Para tramitar la copia se requiere de una autorización firmada.	Interna: sobre manila sellado y entregado personalmente. Externo: sobre sellado sin marcas. Se entrega de manera personal o por correo certificado. Electrónico: uso del correo electrónico institucional, deseablemente con cifrado.	Documentos en papel: utilizar una destructora de papel. Datos electrónicos: borrado seguro o destrucción física del medio

Fuente: NTC ISO/IEC 17799:2005.

Por otro lado, la integridad se define como la propiedad de salvaguardar la exactitud y estado completo de los activos. Los niveles de clasificación de los activos de información definidos para una organización, de acuerdo con la Norma NTC ISO/IEC 17799 en su versión de 2005, son A, B y C, como se muestra a continuación:

A. La información que de ser alterada podría conllevar a fraudes o corrupción. La modificación no autorizada del activo tendría un impacto grave para la entidad, para terceros o para una nación.

B. La información que de ser alterada podría conllevar a fraudes o corrupción. La modificación no autorizada del activo tendría un impacto importante para la entidad o para terceros.

C. La modificación no autorizada del activo tendría un impacto leve para la entidad o para terceros.

Para asignar el nivel de clasificación de un activo de información de acuerdo con su integridad se deben tener en cuenta los atributos de la manera en que indica la tabla 6.6:

Tabla 6.6 Nivel de clasificación de un activo de información de acuerdo con su integridad

Nivel	Atributo
A	A4 y A8, integridad alta (IA) o muy alta (MA)
B	A4, integridad media (IM)
C	Integridad baja (B) o muy baja (MB)

Fuente: NTC ISO/IEC 17799:2005.

Tabla 6.7 Clasificación de la información según su nivel de integridad

	Nivel de clasificación		
	C	B	C
	Etiquetado		
Documentos en papel	No es requerido.	No es requerido; queda a discreción del propietario de la información. En caso de etiquetarse, si un documento que se haya impreso no posee el campo "Nivel de integridad" previamente diligenciado por medio de un formato electrónico, se deberá etiquetar en su primera página, como mínimo, con un sello de tinta correspondiente a su clasificación.	Sí es obligatorio por parte del propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de integridad" previamente diligenciado por medio de un formato electrónico, se deberá etiquetar en su primera página, como mínimo, con un sello de tinta correspondiente a su clasificación.

continúa

Archivos electrónicos (por ejemplo, Word, Excel, PowerPoint, Access)	No es requerido.	No es requerido, por lo que queda a discreción del propietario de la información. En caso de etiquetarse, si un documento que se haya impreso no posee el campo "Nivel de integridad" previamente diligenciado por medio de formato electrónico, se deberá etiquetar en su primera página, como mínimo, con un sello de tinta correspondiente a su clasificación.	Sí es obligatorio por parte del propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de integridad" previamente diligenciado por medio de formato electrónico, entonces se deberá etiquetar en su primera página, como mínimo, con un sello de tinta correspondiente a su clasificación.
Aplicaciones	No es requerido.	No es requerido, pero queda a discreción del propietario de la información. En caso de etiquetarse, las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.	Sí es obligatorio por parte del propietario de la información. A las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.
Carpetas en sistemas	No es requerido.	No es requerido y queda a discreción del propietario de la información. En caso de etiquetarse, a las carpetas en servidores de archivos o en computadoras personales (de escritorio o portátiles), se les debe colocar un nombre o identificador distintivo (como en algunos sistemas), con el nivel de clasificación	Sí es obligatorio por parte del propietario de la información. A las carpetas en servidores de archivos o en computadoras personales (de escritorio o portátiles), se les debe colocar un nombre o identificador distintivo con el nivel de clasificación.
Distribución			
Información electrónica	No hay restricciones para la distribución de este tipo de información.	Mediante el sistema de correo electrónico de la organización y a través de las redes de datos y sistemas internos. De ser posible, deben utilizarse controles de integridad y de no repudio del mensaje, como las firmas digitales. Adicionalmente, los controles de acceso a la red y a las aplicaciones correspondientes al envío del mensaje deben discriminar por niveles de privilegio para usuarios, de manera que solamente las personas autorizadas para modificar la información puedan hacerlo.	Puede transmitirse a través del sistema de correo electrónico de la organización y mediante las redes de datos y de sistemas internos. Siempre deben utilizarse controles de integridad y de no repudio del mensaje, como por ejemplo las firmas y los certificados digitales, totales de verificación de archivos (*hash*) y de encriptación. Adicionalmente, los controles de acceso a la red y a las aplicaciones correspondientes al envío del mensaje deben discriminar por niveles de privilegios para usuarios, garantizando que solamente las personas autorizadas para modificar la información puedan hacerlo; además, se debe monitorear la red y registrar los eventos relacionados con la modificación del mensaje durante el tránsito.

Información impresa	No hay restricciones para la distribución de este tipo de información.	Proceso de manejo de correspondencia interno, utilizando controles de integridad, como la entrega de copia al remitente y sobres cerrados con sello de seguridad. Adicionalmente, todos los documentos deben estar firmados por la persona autorizada.	El original no debe distribuirse, únicamente habrá copias autenticadas de éste. Se deben utilizar otros controles de integridad como sobres cerrados con sello de seguridad. Además, todos los documentos deben estar firmados por la persona autorizada y seguir un procedimiento similar a una cadena de custodia.
Almacenamiento y archivado			
Información impresa	No requiere precauciones especiales	Se deben implementar controles básicos de integridad del documento como no admisibilidad de correcciones o tachones sobre éste; o evitar dejar espacios en blanco que podrían prestarse para adiciones no autorizadas.	Se debe archivar en áreas seguras bajo llave e implementar un procedimiento para el registro de cambios en el que se incluyan la descripción del cambio con fecha y hora, la firma de la persona que lo autoriza y la firma de quien lo ejecutó. Se deben implementar controles de integridad del documento, tales como no admisibilidad de correcciones o tachones sobre éste, uso de tintas indelebles o evitar dejar espacios en blanco que podrían prestarse para adiciones no autorizadas.
Información electrónica	No requiere precauciones especiales.	Se debe almacenar en repositorios que permitan la autenticación de los usuarios; así como la discriminación de privilegios de acceso y modificación, de manera que sólo los usuarios autorizados puedan cambiar la información; por ello, los eventos de modificación se deben registrar y monitorear. Los equipos en que se encuentre almacenada la información deben estar protegidos con un software antivirus y de detección de intrusos para evitar la instalación de aplicaciones maliciosas. Por otro lado, los repositorios deben estar ubicados en áreas seguras y protegidas contra amenazas que puedan afectar la integridad de la información.	Se debe almacenar en repositorios que permitan la autenticación de los usuarios; así como la discriminación de privilegios de acceso y la modificación y verificación de la integridad, tales como totales de suma (*hash*). Los sistemas de procesamiento de información deben cumplir cualquier norma o código de práctica publicado para la producción de evidencia admisible. La autenticación de los usuarios autorizados para cambiar la información debe ser fuerte y todos los eventos de modificación se deben registrar y monitorear; por ello, es necesario implementar controles para garantizar que la modificación de la información esté autorizada por alguien con potestad para hacerlo, diferente a quien realiza la modificación, tales como el uso de una contraseña compartida o conocida de manera parcial por ambos usuarios. Además, se requiere un procedimiento de control de cambios que incluya como mínimo la descripción del cambio con fecha y hora, la firma de la persona que lo autorizó y la firma de quien lo ejecutó.

continúa

			También se deben implementar controles que garanticen el no repudio de la modificación. Por otro lado, los equipos en que ésta se encuentre almacenada deben estar protegidos con un software antivirus y de detección de intrusos para evitar la instalación de aplicaciones maliciosas. Los repositorios deben estar ubicados en áreas seguras y protegidas contra amenazas que puedan afectar la integridad de la información. Es imprescindible investigar formalmente la presencia de modificaciones no autorizadas.
Procesamiento			
Información electrónica	No requiere precauciones especiales.	Se deben establecer controles en los sistemas de procesamiento para proteger la información contra software malicioso mediante el uso de sistemas antivirus. Los cambios significativos se deben identificar, registrar, planear y probar rigurosamente. Asimismo, se requiere que las funciones y las áreas de responsabilidad se distribuyan para reducir las oportunidades de modificación. La información será procesada en sistemas que permitan la autenticación de los usuarios y la discriminación de los privilegios de acceso y de modificación. Se debe garantizar que los datos de entrada estén completos, que el procesamiento se dé por terminado adecuadamente y que se aplique la validación de la salida.	Se deben establecer controles en los sistemas de procesamiento para proteger la información contra *software* malicioso mediante el uso de sistemas antivirus y de detección de intrusos; además, deben cumplir cualquier norma o código de práctica publicado para la producción de evidencia admisible. Los cambios significativos se deben identificar, registrar, planear y probar rigurosamente. Asimismo, las funciones y las áreas de responsabilidad serán distribuidas para reducir las oportunidades de modificación. La información será procesada en sistemas que permitan la autenticación de los usuarios, la discriminación de los privilegios de acceso y la modificación, y las verificaciones de integridad. La autenticación de los usuarios autorizados para modificar la información debe ser fuerte, y todos los eventos de modificación se tienen que registrar y monitorear. Se debe garantizar que los datos de entrada estén completos, que el procesamiento se lleva a cabo adecuadamente y que se aplica la validación de la salida. Las etapas de diseño e implementación de las aplicaciones deberían garantizar que se minimicen los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad. Las áreas específicas que se han de considerar incluyen:

			☑ Utilización de las funciones "agregar, modificar y borrar" para implementar los cambios en los datos. ☑ Procedimientos para evitar que los programas se ejecuten en orden erróneo, o su ejecución después de falla previa del procesamiento. ☑ Utilización de programas adecuados para la recuperación después de fallas con el objetivo de garantizar el procesamiento correcto de los datos. ☑ Verificaciones para garantizar que los programas de aplicación se ejecutan en el momento y orden correctos; además de que el procesamiento posterior se detiene hasta resolver el problema. ☑ Verificaciones de la verosimilitud para probar si los datos de salida son razonables. ☑ Cuentas de control de conciliación para asegurar el procesamiento de todos los datos. ☑ Suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, la totalidad, la precisión y la clasificación de la información.
Información impresa	No requiere precauciones especiales.	El acceso de los usuarios autorizados para modificar la información debe ser controlado.	Todos los cambios se deben identificar, registrar, planear y probar rigurosamente. Las funciones y las áreas de responsabilidad se distribuyen para reducir las oportunidades de modificación. El acceso de los usuarios autorizados para modificar la información debe ser controlado, registrado y monitoreado. Es necesario investigar formalmente la presencia de cambios no autorizados. Se precisa garantizar que los datos de entrada están completos, que el procesamiento se lleva a cabo adecuadamente y que se aplica la validación de la salida.

Fuente: NTC ISO/IEC 17799:2005.

Finalmente, la disponibilidad es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada cuando ésta así lo requiera. Los niveles de clasificación de los activos de información definidos por la Norma NTC ISO/IEC 17799, publicada en el 2005, de acuerdo con su disponibilidad son:

1. El activo de información es muy crítico para las operaciones internas de una entidad, una nación o para el servicio a terceros. La privación del uso del activo de información impacta negativamente y de manera grave a la entidad o a terceras partes.
2. El activo de información es importante para las operaciones internas de una entidad, una nación o para el servicio a terceros. La privación del uso del activo de información impacta negativamente y de manera importante a la entidad o a terceras partes.
3. El activo de información no es crítico para las operaciones internas de la entidad o para el servicio a terceros. La privación del uso del activo de información impacta negativamente y de manera leve a la entidad o a terceras partes.

Para asignar el nivel de clasificación de un activo de información de acuerdo con su disponibilidad, se deben tener en cuenta los atributos de la manera en que se indica en la tabla 6.8.

Tabla 6.8 Nivel de clasificación de un activo de información de acuerdo con su disponibilidad

Nivel	Atributo
1	Disponibilidad muy alta (MA)
2	Cualesquiera de los atributos A5 o A6 o disponibilidad alta (A) o media (M)
3	Disponibilidad baja (B) o muy baja (MB)

Fuente: NTC ISO/IEC 17799:2005.

La tabla 6.9 muestra la clasificación de los criterios de la información de acuerdo con la disponibilidad.

Tabla 6.9 Clasificación de la información según su nivel de disponibilidad

	Nivel de clasificación		
	3	2	1
	Etiquetado		
	No es requerido.	No es requerido, pues queda a discreción del propietario de la información. En caso de etiquetarse, si un documento que se haya impreso no posee el campo "Nivel de integridad" previamente diligenciado por medio de un formato electrónico, se deberá etiquetar en su primera página, como mínimo, con un sello de tinta correspondiente a su clasificación.	Sí es obligatorio por parte del propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de integridad" previamente diligenciado por medio de un formato electrónico, se deberá etiquetar en su primera página, como mínimo, con un sello de tinta correspondiente a su clasificación.

Seguimiento			
Sistemas de información electrónica	No es requerido.	El estado de los sistemas se debe monitorear y guardar en un registro de manera permanente para detectar posibles fallas que podrían suspender el servicio	El estado de los sistemas se debe monitorear y guardar en un registro de manera permanente para detectar posibles fallas que podrían suspender el servicio. Adicionalmente, se deben configurar alarmas que puedan indicar a los administradores del sistema cuando éste deja de hallarse disponible.
Sistemas de información impresa	No es requerido.	Deben establecerse procedimientos que permitan determinar y tener registro en todo momento de la ubicación y el usuario de la información.	Deben centralizarse los documentos por áreas, secciones o divisiones y establecerse procedimientos que permitan determinar y tener registro en todo momento de la ubicación y el usuario de la información.
Protección			
Sistemas de información electrónica	No es requerido.	Los servicios de procesamiento de información clasificada como de disponibilidad 2 deben estar ubicados en áreas seguras y protegidas por perímetros definidos y controles de entrada adecuados. Esto incluye controles lógicos y físicos. Se debe considerar redundancia en el suministro de energía y realizarse periódicamente copias de respaldo y pruebas de verificación de éstas. El mantenimiento que se ejecuta en los sistemas de procesamiento de información clasificada como de disponibilidad 2 debe ser acorde con las especificaciones e intervalos de tiempo recomendados por el proveedor, y realizado únicamente por personal autorizado.	Los servicios de procesamiento de información clasificada como de disponibilidad 1 deben estar ubicados en áreas seguras y protegidas por perímetros definidos, con barreras de seguridad y controles de entrada adecuados. Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial, que podrían conllevar a la suspensión del servicio. Es conveniente monitorear las condiciones ambientales como la temperatura y la humedad para determinar si podrían afectar adversamente el funcionamiento de los servicios. Los sistemas de procesamiento de información de disponibilidad 1 deben incluirse en el plan de continuidad de la entidad, el cual debe considerar, como mínimo, redundancia en el suministro de energía, en los equipos y las aplicaciones; la realización frecuente de copias de respaldo y de pruebas de verificación de éstas; y adquirir las pólizas de seguro para los riesgos transferidos. En caso de ser definido en el plan de continuidad, debe implementarse un sitio alterno ubicado físicamente distante de la sede principal.

continúa

			El mantenimiento de los sistemas de procesamiento de información de disponibilidad 1 debe estar acorde con las especificaciones e intervalos de servicio recomendados por el proveedor, y realizado sólo por personal autorizado. Además, debe ser rigurosamente planeado, considerando todos los riesgos de suspensión del servicio que se puedan presentar y tomando las medidas pertinentes para manejarlos. Para los sistemas de procesamiento de información de disponibilidad 1, que son contratados con terceras partes, deben establecerse acuerdos de nivel de servicio, consistentes con los requerimientos de disponibilidad, y sus cláusulas de incumplimiento deben ser también adecuadas.
Sistemas de información impresa	No es requerido.	Los documentos clasificados como de disponibilidad 2 deben estar ubicados en áreas seguras, protegidas por perímetros definidos y controles de entrada adecuados. Es conveniente monitorear las condiciones ambientales como la temperatura y la humedad, para determinar si podrían afectar adversamente la disponibilidad del documento.	Los documentos clasificados como de disponibilidad 1 deben estar ubicados en áreas seguras, protegidas por perímetros definidos, con barreras de seguridad y controles de entrada adecuados. Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial que podrían conllevar a la suspensión del acceso al documento. Es conveniente monitorear las condiciones ambientales como la temperatura y la humedad para determinar si podrían afectar adversamente la disponibilidad del documento. Los archivos clasificados como de disponibilidad 1 deben incluirse en el plan de continuidad de la entidad.

Fuente: NTC ISO/IEC 17799:2005.

6.3 Diagnósticos de la seguridad informática

La expansión de las redes, la convergencia de servicios, la velocidad con la que se integran nuevas tecnologías, hace que cada día las empresas estén más expuestas a potenciales amenazas que comprometen uno de los activos más importantes: la información. Ejemplo de esto son las bases de datos de las organizaciones, su información contable, los registros de facturación y demás activos; por lo general, esta información se encuentra sustentada sobre la infraestructura informática de la empresa, y que en algún momento puede ser vulnerada por distintos tipos de amenazas, que van desde virus y ataques de terceros hasta usuarios mal intencionados (Pieprzyk; Hardjono y Seberry, 2004).

Adoptar una postura responsable, entender que es posible tomar acciones que pueden prevenir y proteger los sistemas informáticos de esas amenazas, representa en la actualidad una tarea que no es factible, ni recomendable eludir. Si se considera que en una organización se está trabajando en forma adecuada en cuanto a la seguridad de la información, habrá que contestar las siguientes preguntas:

- ¿Cuántos incidentes de seguridad se han tenido en los últimos seis meses?
- ¿Cuántos virus han entrado en la red durante la última semana?
- ¿Qué tan efectiva es la inversión que ha hecho la empresa en materia de seguridad?

Comenzar a trabajar en la gestión de la seguridad de la información definiendo un plan con una visión práctica y estratégica, que considere los marcos normativos y las buenas prácticas, que alcance los objetivos sin degradar la eficiencia de los procesos del negocio, representa un verdadero desafío. Contar con un concienzudo diagnóstico de seguridad permite determinar los principales riesgos a los que se encuentra expuesta la información de una organización, detectando vulnerabilidades a nivel de la infraestructura de los sistemas informáticos.

Además, facilita dirigir las inversiones de modo de proteger los activos más críticos, maximizando así la posibilidad de éxito de los proyectos de seguridad con una mínima inversión. Como resultado de esta práctica, la organización tendrá un informe conteniendo un estado de situación, recomendaciones y un plan de acción para comenzar a mitigar los principales riesgos detectados. También recibirá un conjunto de guías que ayudarán a desarrollar un marco de seguridad desde un punto de vista práctico y de fácil implementación.

Por su naturaleza, todas las organizaciones son un sector que maneja una gran cantidad de información, lo que convierte a este nicho en un blanco ideal para los ladrones de identidad e información. A nivel país, México registra huecos de seguridad en la información bastante profundos.

De los ataques y violaciones a la seguridad, el 80 % se origina por el personal interno, como resultado de la falta de controles administrativos confiables (Barrios Garrido, 1988). La seguridad varía según los requisitos de cada organización; sin embargo, existen tres principios que subyacen a todos los programas e infraestructura:

- Disponibilidad de los recursos (equipo, comunicaciones, personal, datos, cifras, etcétera).

- Integridad de la información (la veracidad y la certeza de los datos capturados por el personal interno).
- Confidencialidad de la misma (el acceso y la consulta por las personas autorizadas para ello).

El objetivo es gestionar la seguridad de la información para preservar su confidencialidad y hacerla accesible sólo a aquellas personas autorizadas para verla, cuidando la integridad y garantizando la disponibilidad de la misma; es decir, el acceso a los datos y a los recursos relacionados a ella cada vez que se requieran.

Los recursos de la Tecnología de la Información (TI), tales como datos, servidores, equipos y personal técnico, deben estar disponibles para su uso cuando sea necesario. Para asegurar dicha disponibilidad, deben prevenirse las razones que causan el riesgo y la amenaza no controlada. La infraestructura informática necesita de una correcta administración y supervisión. La situación actual en las empresas en materia de seguridad informática es la siguiente:

- La problemática principal se asocia a la falta de cultura en la protección y uso de la información, y los riesgos que esto conlleva.
- La información no está clasificada de acuerdo a su valor, temporalidad o vida útil. Por lo tanto, no hay responsabilidad de las personas que la generan, ya que interviene más de una persona en el proceso.
- No existe un inventario de la información por área que describa de manera precisa el tipo de datos y el uso que se le da a dicha información, así como la ubicación, el procesamiento y la transmisión electrónica.
- El acceso y uso de la información no está alineado a los roles y jerarquías del personal.
- Marcada ausencia de monitoreo de acceso a los equipos e información. Se requiere implementar auditorías informáticas a través de programas de supervisión bien definidos.
- No existen planes ni procedimientos para prevenir y reaccionar ante cualquier contingencia, incidencia o vulnerabilidad.
- No existen programas serios de respaldos y aseguramiento de la información.

6.4 Revisión y actualización de procedimientos en seguridad informática

En toda organización que haga uso de las tecnologías de la información, se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones el no seguir un proceso de implementación adecuado como el que establece la Norma ISO 17799, puede generar huecos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información.

Este estándar internacional de alto nivel para la administración de la seguridad de la información fue publicado por la ISO (I*nternational Organization for Standardization*) en diciembre del 2000 con el objetivo de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones. La Norma ISO 17799, al definirse como una "*Guía en la implementación del sistema de administración de la seguridad de la información*", se orienta a preservar los siguientes principios de la seguridad informática (mismos que ya se definieron en los dos apartados anteriores):

Confidencialidad. Asegurar que únicamente personal autorizado tenga acceso a la información.

Integridad. Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Disponibilidad. Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean estas organizaciones de cualquier índole; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad. Como todo buen estándar, la ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la seguridad de la información; se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo.

La aplicación de un marco de referencia de seguridad basado en la ISO 17799 proporciona beneficios a toda organización que la implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información. Las políticas, estándares locales y los procedimientos se encuentran adaptados a las necesidades de la organización debido a que el proceso mismo de su elaboración integra mecanismos de control, y por último, la certificación permite a las organizaciones demostrar el estado de la seguridad de la información, situación que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito contractual la certificación BS 7799.

Es importante entender los principios y objetivos que dan vida a la ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos, puede adquirir al implementarla en sus prácticas de seguridad de la información. El estándar de seguridad de la información ISO 17799,

descendiente del BS 7799 (*Information Security Management Standard*) de la BSI (*British Standard Institute*), que publicó su primera versión en Gran Bretaña en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

Parte 1. Código de prácticas.

Parte 2. Especificaciones del sistema de administración de seguridad de la información.

Por la necesidad generalizada de contar con un estándar de carácter internacional, que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO 17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS 7799 *Part 1: Code of Practice*).

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta. El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce en la jerga del estándar como *Statement of Applicability*, que es la definición de los controles que aplican a la organización con el objetivo de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos. A continuación, se describirán cada una de las diez áreas de seguridad, con el objetivo de esclarecer los objetivos de estos controles:

Políticas de seguridad. El estándar define como obligatorias las políticas de seguridad documentadas; así como los procedimientos internos de la organización, que permitan su actualización y revisión por parte de un Comité de Seguridad.

Seguridad organizacional. Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (ISSO, *Information System Security Officer*), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

Clasificación y control de activos. El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información; es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

Seguridad del personal. Contrario a lo que se pudiera imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información. El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana; es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

Seguridad física y del entorno. Identifica los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

Comunicaciones y administración de operaciones. Integra los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de

los equipos, el manejo de incidentes y la administración de aceptación de sistemas, hasta el control de código malicioso.

Control de acceso. Habilita los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

Desarrollo de sistemas y mantenimiento. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

Continuidad de las operaciones de la organización. El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

Requerimientos legales. La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos; además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle. Actualmente se desarrollan e implementan los sistemas de administración de seguridad de la información descritos en los estándares de seguridad actuales; de igual forma, a través de metodologías como OCTAVE (*Operationally Critical Threat Asset and Vulnerability Evaluation*) se enriquece la implementación de la ISO 17799.

Finalmente, y a manera de conclusión, la correcta selección de los controles es una tarea que requiere del apoyo de especialistas en Seguridad Informática, con experiencia en la implementación de la ISO 17799, ya que cuando éstos se establecen de forma inadecuada, pueden generar un marco de trabajo demasiado estricto y poco adecuado para las operaciones de la organización. Como todo estándar, la ISO 17799 proporciona un marco ordenado de trabajo, al cual deben sujetarse todos los integrantes de la organización, y aunque no elimina el 100 % de los problemas de seguridad, sí establece una valoración de los riesgos a los que se enfrenta una organización en materia de seguridad de la información.

Dicha valoración permite administrar los riesgos en función de los recursos tecnológicos y humanos con los que cuenta la organización; adicionalmente, establece un entorno que identifica los problemas de seguridad en tiempos razonables, situación que no es posible, la mayoría de las veces, si no se cuenta con controles de seguridad como los establecidos en la ISO 17799; es decir, la aplicación del estándar garantiza que se podrán detectar las violaciones a la seguridad de la información, circunstancia que no necesariamente ocurre en caso de no aplicarse el estándar.

6.5 Recuperación y continuidad del negocio en caso de desastres (DRP/BCP/BCM)

Un plan de continuidad del negocio (BCP, *Business Continuity Plan*) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas, parcial o totalmente interrumpidas, dentro de un tiempo predeterminado después de una interrupción no deseada o de un desastre. En los Estados Unidos de América, las entidades gubernamentales se refieren al proceso como Planificación de Continuación de Operaciones (COOP, *Continuity of Operations Planning*).

En lenguaje sencillo, un plan de continuidad del negocio (BCP) es el cómo una organización se prepara para futuros incidentes que puedan poner en peligro a ésta, y a su misión básica a largo plazo. Las situaciones posibles incluyen desde incidentes locales (como incendios, terremotos, inundaciones, tsunamis, etcétera), de carácter regional, nacional o internacional, hasta incidentes como las pandemias. La continuidad del negocio es un concepto que abarca tanto el plan de recuperación de desastres (DRP), como el Plan para el Restablecimiento del Negocio. La recuperación de desastres es la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización.

Ambos se diferencian de la planeación de prevención de pérdidas, la cual implica la calendarización de actividades como el respaldo de sistemas, la autenticación y la autorización (seguridad), la revisión contra virus y el monitoreo de la utilización de sistemas (principalmente para verificaciones de capacidad). En este caso, se trata sobre la importancia de contar con la capacidad para restablecer la infraestructura tecnológica de la organización en caso de una disrupción severa. Este plan es la respuesta prevista por la organización ante aquellas situaciones de riesgo que le pueden afectar de forma crítica.

No importa el tamaño de la organización, o el costo de las medidas de seguridad implantadas, toda organización necesita un plan de continuidad del negocio, ya que tarde o temprano se encontrará con una incidencia de seguridad; ésa es una realidad indiscutible. Lo primero que se debe realizar es un análisis del impacto al negocio (BIA). Éste es básicamente un informe que muestra el costo ocasionado por la interrupción de los procesos de negocio. Una vez obtenido este informe, la organización tiene la capacidad de clasificar los procesos de negocio en función de su criticidad; y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial). En el BIA, se identifican los componentes clave requeridos para continuar con las operaciones de negocio luego de un incidente, dentro de estos componentes se encuentran los siguientes:

- El personal requerido
- Las áreas de trabajo
- Los registros vitales (respaldos de la información)
- Los aplicativos críticos
- Las dependencias de/con otras áreas
- Las dependencias de/con terceras partes
- La criticidad de los recursos de información
- La participación del personal de seguridad informática y los usuarios finales
- Los análisis de todos los tipos de recursos de información

Tres aspectos claves para el análisis son los siguientes:

- La criticidad de los recursos de información relacionados con los procesos críticos del negocio.
- El periodo de recuperación crítico antes de incurrir en pérdidas significativas.
- El sistema de clasificación de riesgos.

Una estrategia de recuperación es una combinación de medidas preventivas para detectar los problemas, y luego las medidas correctivas para:

- Eliminar la amenaza completamente.
- Minimizar la probabilidad de que ocurra o vuela a ocurrir.
- Minimizar el efecto nocivo.

El plan de continuidad del negocio abarca todos los sectores de negocio, dado con más énfasis en aquellos donde la disponibilidad de la información es su mayor activo. Por ejemplo, en los Estados Unidos de América, a partir del 11 de septiembre de 2001, los planes de continuidad de negocio cobraron importancia al dar mayor cobertura a compañías del sector financiero y sus asociados, donde hoy tienen su mayor aplicación.

No hay importancia en el tamaño de la organización, un plan de continuidad puede ser aplicado tanto a organizaciones grandes, medianas, pequeñas e incluso en las microempresas. Como todo proceso, la aplicación de un plan de continuidad involucra determinados pasos obligatorios para garantizar la funcionalidad del mismo, éstos son:

- Una fase de análisis y de evaluación de los riesgos
- La selección de estrategias
- El desarrollo del plan
- Las pruebas y mantenimiento del plan

Las normas de la Organización Internacional de Estándares (ISO) que se utilizan en este rubro son las siguientes:

ISO/IEC 27001:2005 (antes BS 77992:2002). Sistema de Gestión de la Seguridad de la Información

ISO/IEC 27002:2005 (re-numerado ISO17999:2005). Código de Práctica. Gestión de Seguridad de la Información

ISO/IEC 27031:2011. Tecnología de la Información-Técnicas de seguridad-Guías para la Preparación de las Tecnologías de la Información y de las Comunicaciones para la Continuidad de los Negocios

ISO/PAS 22399:2007. Guía para la Preparación frente a Incidentes y la Gestión de Continuidad Operacional

ISO/IEC 24762:2008. Directrices para los Servicios de Recuperación de Desastres de las Tecnologías de la Información y de las Comunicaciones

IWA 5:2006. Preparación para Emergencias

6.5.1 Conceptos y terminología usados en la continuidad del negocio

Figura 6.1 Principales problemáticas en una organización

Hay muchos conceptos relacionados con la continuidad del negocio, pero cada organización adopta diferente terminología, aunque cabe mencionar que hay asociaciones internacionales que están homologando los conceptos.

En la mayoría de las organizaciones hay adhesión a las mejores prácticas internacionales basadas en institutos como el DRII (*Disaster Recovery Institute International*) y en la Norma BS25999 del *British Standard*. Algunos de los términos más utilizados para clasificar las fallas e identificar en qué situación se encuentran tanto la organización como las personas son las que se muestran en la figura 6.1 y que se desarrollan a continuación de ésta:

Respuesta y manejo. Reacción planificada y manejo de un evento adverso.

Recuperación/restauración. Recuperación planificada de los sistemas y la reanudación de las operaciones después de una interrupción.

Retorno a la operación normal. Restitución de la operación normal.

Prevención. Pasos tomados para identificar y mitigar el riesgo, así como el diseño de estrategias de recuperación.

Falla. Situación no generalizada de bajo impacto que afecta a uno o varios equipos o usuarios. No detiene la operación de la organización y generalmente se reporta como una solicitud de auxilio "SOS". Ejemplos:

- Fallas de equipo y de comunicaciones
- Problemas con nombres de usuarios y con las contraseñas
- Errores de impresión
- Problemas de configuración
- Problemas con el *software* de las computadoras personales
- Mal funcionamiento de los nodos de voz y de datos

Incidencia. Situación generalizada que interrumpe parcialmente la entrega de algunos de los servicios de tecnología afectando la operatividad del grupo. Puede estar relacionada con un problema aplicativo, de infraestructura o de comunicaciones. Hay afectación directa sobre la operación y es necesario ejecutar las acciones adecuadas para solucionar la incidencia. La operativa continúa parcialmente en todo aquello que no está afectado, por lo cual la interrupción es aceptable y no es necesario detonar el plan de contingencia. Ejemplos:

- Lentitud en la respuesta de una aplicación requerida.
- Falla parcial en un sistema que impida liquidar o ejecutar operaciones.
- Base de datos de una aplicación y que presenta información errónea.

Contingencia. Se deriva de una incidencia o de un evento no programado que inhabilita a la organización para proporcionar algunas de las funciones críticas del negocio por un periodo inaceptable y que tiene como consecuencia un impacto alto. Ejemplos:

- Corrupción total de una base de datos crítica
- Falta de acceso a una aplicación crítica

Desastre. Es un evento no planeado que inhabilita a la organización para proporcionar las funciones críticas del negocio por un periodo inaceptable, el cual tiene como consecuencia un gran daño o pérdida. La diferencia entre una contingencia y un desastre radica en la duración de la interrupción y la gravedad del impacto. En un desastre, generalmente todas las áreas se ven afectadas y el impacto es daño o pérdida, que puede ser total, por lo que la necesidad de aplicar el plan de recuperación de desastres (DRP) es inminente.

6.5.2 Metodología para el desarrollo de continuidad del negocio

Hoy existen diversos factores que pueden interrumpir la operación de cualquier organización; por ello, es necesario considerar la importancia de la "continuidad del negocio" dentro de la organización y al interior de cada una de las áreas de trabajo. Todas las personas involucradas en éstas pueden hallarse expuestas a una contingencia; por lo tanto, se deben establecer medidas que permitan lo siguiente:

- Mitigar los riesgos.
- Minimizar los impactos.
- Actuar adecuadamente en caso de que se presente una contingencia o desastre.
- Contar con procedimientos alternos para los procesos críticos.
- Tener estrategias de restauración de operaciones y recuperación de información.
- Regresar a la normalidad de forma correcta y ágil.

La continuidad del negocio considera el diseño de estrategias y procedimientos que se determinan de acuerdo con cinco fases, teniendo cuatro principales, las cuales muestra la figura 6.2 (Alexander, 2007).

Figura 6.2 Fases de continuidad del negocio

A continuación, se describe la estructura utilizada en los procesos de recuperación tecnológica para la documentación de todas las actividades del plan de recuperación de desastres (DRP), donde se agrega una fase más a las presentadas en la figura 6.2:

Operación normal para contingencia. En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar para mantener preparada la solución de recuperación compuesta por la infraestructura contratada y el plan de recuperación de desastres (DRP).

Manejo de incidentes. En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar para evaluar un problema que potencialmente lleve a la declaración de contingencia, a la toma de la decisión de ésta y a su notificación, tanto a las áreas internas como a los entes externos (clientes, proveedores, entidades reguladoras y otros). Cubre el periodo desde el momento cero de la contingencia; es decir, aquel en el cual se presenta el evento, hasta que se activen los equipos de trabajo y sus respectivos planes. También se identifican en esta fase las actividades de recuperación del centro de cómputo principal (CCP), así como las de planeación del retorno de la operación de las aplicaciones críticas desde el centro de cómputo de contingencia (CCC) al centro de cómputo principal (CCP), hasta el momento en que se inicia dicho retorno.

Movilización. En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar para trasladar la operación afectada al centro de cómputo de contingencia (CCC) y, en caso de ser requerido, al centro de operaciones de contingencia (COC), desde el momento en que se declara, notifica y activan los planes hasta la puesta en operación de dichos servicios al segundo centro de datos (*datacenter*).

Operación durante la contingencia. En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar durante la operación en el CCC después de concluida la movilización, con el fin de mantener activas las aplicaciones movilizadas hasta el momento en que se inicia el retorno a la normalidad, prestando el servicio con las restricciones propias de la contingencia.

Retorno a la normalidad. En esta fase se agrupan las actividades que cada equipo de recuperación debe desarrollar desde el momento en que se inicia la movilización del CCC hacia el CCP, hasta que el servicio sea recuperado totalmente en éste.

6.5.3 Herramientas de *software* para el desarrollo y mantenimiento del DRP/BCP/BCM

Los sistemas de información de las organizaciones y de las empresas globales poseen clientes que requieren acceso a los datos las 24 horas del día, los 7 días de la semana; lo que quiere decir que no debería haber ninguna interrupción en los sistemas, eso significa alta disponibilidad; sin embargo, las tecnologías no aseguran el estar libres de errores al 100 %, ya sea por agentes internos o externos, se pueden presentar fallas como el que se pierda el acceso a la base de datos, lo que se traduce en pérdida de operaciones de negocio para las organizaciones. Es por eso que las aplicaciones web o los sistemas en línea que generan gran procesamiento de transacciones necesitan altos niveles de disponibilidad para cualquier manejador de bases de datos, los cuales no pueden bajar de 99 % del tiempo en servicio (Alexander, 2007).

Experimentar un porcentaje de tiempo fuera de servicio del 1% al año significa que tendrá un tiempo de 3.65 días para reparar el componente fallido o darle mantenimiento. Claro está que si se quiere aumentar ese porcentaje a casi el 100 %, equivale a encontrar una solución de alta disponibilidad de base de datos, ya sea por medio de *hardware* o de *software*, o una combinación de los dos, que aunque signifique grandes sumas de dinero, si el negocio es de operaciones críticas, claro que no se puede llamar gasto, sino una inversión a largo plazo. En el mercado actual, se encuentran varios manejadores de bases de datos, en el presente apartado se encontrarán los más comunes como Oracle™ y SQL Server™; los cuales tienen soluciones de alta disponibilidad de base de datos de *hardware* así como de *software*, que hacen posible disminuir ese tiempo fuera de servicio (Adding Instances and Nodes, 2002).

Se puede hablar de mecanismos que establecen las pautas de disponibilidad, de acuerdo (sobre todo) a la tecnología que se esté empleando en cada momento. De una forma genérica, se podría hablar del término "alta disponibilidad" aplicado a un sistema computacional del que se requiere un funcionamiento continuo. La alta disponibilidad se aplica a toda la gama de soluciones que sostienen los sistemas de información de las organizaciones: bases de datos, cortafuegos, servidores web, etcétera. Si bien, los mecanismos que se emplean pueden ser distintos en función del entorno (High Availability, 2002). Entonces, habrá distintas configuraciones, entre ellas se ubican las siguientes:

Activo-Pasivo. Se trata de disponer de un nodo funcionando, el cual cuenta con todos los servicios que componen el sistema de información al que se denominará activo, y el otro nodo que se denominará pasivo en el que se encuentran duplicados todos estos servicios, pero detenidos a espera de que se produzca un fallo.

Activo-Activo. La configuración de "alta disponibilidad" en activo-activo es muy similar a la de activo-pasivo, aunque en este caso los dos nodos comparten los servicios de una manera activa, normalmente balanceados, consiguiendo una disponibilidad mayor, ya que los servicios se entregan antes.

Granja de servidores. Normalmente orientado a servicios web, servicios computacionales que se entregan de forma masiva, como puedan ser servicios terminales. En estas configuraciones, no sólo es importante la (con)fiabilidad, también lo es contar con un sistema muy disponible, por lo que se suelen colocar un gran número de máquinas haciendo una tarea común. Esta configuración siempre nos va a permitir que en caso de que un nodo deje de hacer su función, otro asuma su rol. Los principios básicos de la "alta disponibilidad" (también lo encontramos representado frecuentemente con las siglas HD, *High Disponibility*) se asocian con los siguientes conceptos básicos:

Fiabilidad. Marca la medida en la que un dispositivo computacional se mantiene activo.

Disponibilidad. La medida en la que un sistema de información está preparado para su uso.

Confiabilidad. Grado de eficacia del sistema de información.

Failover. Configuración de mínimo dos nodos en el que, en un momento dado y debido a cierta casuística, un nodo continua activo en vez del otro.

TakeOver. Es un *Failover* automático, cuando un fallo es detectado a partir de una monitorización.

Si todos estos mecanismos fallaran debido a una magnitud grande del desastre, se debería tener establecido un plan que marque la *continuidad del negocio*. Los *clúster* son grupos de sistemas independientes que funcionan como un único sistema, éstos proporcionan un mejor rendimiento al distribuir la carga entre los nodos que lo conforman. Combinados con un almacenamiento compartido que proporcione redundancia de los datos y utilizando un arreglo redundante de discos independientes más comúnmente conocido como RAID, se solucionaría el problema del tiempo fuera de servicio (Alexander, 2007).

La replicación es una solución de alta disponibilidad de base de datos por *software* que implica tener una o más copias de la base de datos en producción en más de un lugar, y que la misma se pueda utilizar en caso de una destrucción total del sitio de producción sin que los usuarios noten qué es lo que ha sucedido. Por lo tanto, es necesario comparar las características más relevantes resumidas en un cuadro que contengan las soluciones de alta disponibilidad de base de datos por *hardware* o por *software* como si las mismas proporcionarán recuperación a desastres, disponibilidad, confiabilidad, escalabilidad, costo, etcétera; para tomar una decisión que ayudara a tener un considerable tiempo en servicio de sus sistemas de información. Los planes de contingencia que definen la continuidad del negocio no deben centrarse en procesos específicos, sino en procesos completos del plan de negocio.

Si solamente se centran en procesos específicos, como pueden ser los sistemas de Tecnologías de la Información (TI), claramente asociados a las soluciones de alta disponibilidad, no se cubrirán los mecanismos que marcan la continuidad del negocio. La gestión de continuidad de negocio (BCM) es un método mediante el cual se trata de conseguir este objetivo, y asegurar que la organización seguirá operando con sus actividades de negocio críticas, conforme a un nivel predeterminado, y después de un incidente o de una interrupción no prevista, tal como puede ser un desastre natural (sismo, inundación, o ambos).

Estándares y mejores prácticas

Las Tecnologías de la Información y de las Comunicaciones (TIC) son un medio transformador para las personas, las organizaciones y la sociedad, dichas TIC vienen en un constante crecimiento en el mundo; por lo que hay que realizar actualizaciones constantes y veloces sobre los marcos de referencia existentes para gestionarlas de la mejor manera. Actualmente, existe una brecha importante relacionada con la puesta en marcha de los diferentes marcos de referencia relacionados con las TIC en las industrias, las empresas, las dependencias y los corporativos, por lo que es muy importante potenciar su divulgación, conocimiento, uso y aplicación (Alexander, 2007).

A continuación, se indican algunas de las barreras identificadas en la apropiación, el uso y la divulgación de las normas, las buenas prácticas y los estándares en las organizaciones:

- Las personas en las organizaciones no utilizan un lenguaje común, lo que no permite que a lo largo y ancho de la organización se permeen y usen de forma natural los marcos de referencia para la gestión de las TIC.
- Las personas que vienen del mundo técnico (ingenieros de sistemas, electrónicos, industriales, telecomunicaciones, técnicos entre otros), que es el tipo de personas que normalmente se encuentran en las áreas de las TIC, en general, sólo piensan desde la perspectiva de lo técnico, no piensan en el negocio al que se dedican las organizaciones (que finalmente es el fin de todas las acciones que se realicen en la organización: lograr que las empresas sean competitivas, innovadoras y sostenibles).

En términos generales, las personas que laboran en las áreas de las TIC:

- Desconocen los marcos de referencia para la gestión de las TIC, conociendo en algunos casos sólo los marcos de referencia que están de moda.
- No tienen desarrolladas las habilidades y las competencias relacionadas con la búsqueda de información y la gestión del conocimiento sobre los marcos de referencia para la gestión de las TIC.
- No tienen definido el mapa de ruta (*roadmap*) para la adquisición de conocimientos, habilidades y competencias con respecto a los diferentes marcos de referencia para la gestión de las TIC.

- En las organizaciones no se tiene definido el mapa de ruta (*roadmap*) para la implementación de marcos de referencia que permitan a gestión de las TIC.
- A pesar de que estamos en la era del conocimiento, éste no se gestiona y permanece en las personas y no en las organizaciones, por lo que se cometen los mismos errores en múltiples ocasiones.
- Se usa excesivamente la terciarización (*outsourcing*) para los servicios y componentes de las TIC, lo que está generando poca pertenencia de las personas con las organizaciones, así como una alta rotación de personal en las organizaciones, que conlleva a que el conocimiento que se genera, se fugue y no se mantenga en la organización. Adicionalmente, con el uso excesivo de la terciarización (*outsourcing*), las organizaciones están perdiendo de forma significativa el conocimiento y control de las TIC.
- Se está realizando la incorporación obligada de los marcos de referencia en las organizaciones: se imponen los marcos de referencia, sin tener en cuenta a las personas. Muchas veces se imponen por moda y no como mecanismo para solucionar problemas. Esto hace que sólo se tenga un marco de referencia por cumplir, lo que conlleva a una aplicación solamente en el papel, pero no en la práctica. La gestión para la apropiación de cambios es pobre o no se realiza. No se le da tiempo a las personas para que apropien las nuevas formas de hacer las cosas.
- A veces se es demasiado purista con la implementación de los marcos de referencia. Se implementan sin tener en cuenta la simplificación, optimización y definición de las actividades que no generan valor y se implementan procesos ineficientes e ineficaces.
- Al incluir varios marcos de referencia, entre ellos se pueden contradecir, lo que no permite ser eficiente y eficaz (efectivo), realizando reprocesos; lo que conlleva a malgastar esfuerzos y recursos.
- El cambio constante de los marcos de referencia a utilizar no permite apropiarlos de la mejor manera, y finalmente, no se termina por apropiar ninguno.
- Las organizaciones creen que por contratar personas certificadas en los diferentes marcos de referencia, las dificultades se solucionan por "arte de magia", sin tener en cuenta que los marcos de referencia en términos generales siempre incluyen procesos, los cuales son las formas de hacer las cosas, que requieren de tiempo para ser apropiados en las organizaciones y necesitan de otros recursos (por ejemplo, capacitaciones, implementación, auditorías, entre muchos otros).

Entre las normas, buenas prácticas y estándares para el sector de las TIC que se sugieren evaluar y apropiar en las organizaciones son las siguientes:

- Gestión de servicios de TIC: ITIL, ISO 20000
- Gestión del gobierno de TI: COBIT, ISO 38500
- Gestión de riesgos: ISO 31000, estándar gestión riesgos PMI, NTC 5452
- Gestión de la continuidad: ISO 22301
- Gestión de la seguridad de la información: ISO 27000
- Gestión ambiental: ISO 14000
- Gestión de calidad: ISO 9000, NTC 1000
- Gestión de proyectos, programas y portafolios: PMBOK, ISO 21500, ISO 10006, OPM3
- Gestión de *software*: ISO 25000, IEEE 12207, IEEE 829, IEEE 830, SWEBOK, CMMI
- Auditoría de sistemas de gestión: ISO 19011
- Gestión de requerimientos: BABOK, IEEE 830, PMBOK

Es de máxima importancia evaluar el sector y cada área de las TIC, para definir las normas, buenas y mejores prácticas, y estándares que se requieren cumplir de forma obligatoria, voluntaria, y como factor diferenciador; en el nivel local, regional, nacional e internacional. Siempre se debe encontrar la justificación del porqué seguirlas e implementarlas, definiendo cualitativa y cuantitativamente los beneficios que se espera lograr al aplicarlas. Finalmente, se requieren que las organizaciones hagan caso de las siguientes recomendaciones (Terán Pérez, 2014):

- Las organizaciones deben contar con el respectivo personal que conozca sobre los diferentes marcos de referencia para la gestión de las TIC existentes, y que esté tenga la capacidad de definir los criterios para la definición y adopción de los marcos de referencia más acordes y pertinentes para la organización.
- Se deben definir proyectos para la adopción de los diferentes marcos de referencia de las TIC.
- La gestión del conocimiento es un proceso continuo e iterativo, por lo que los esfuerzos se deben encaminar para que así sea, y la empresa crezca en el tiempo. El cambio en los paradigmas de cómo se hacen las cosas en las empresas, debe generarse desde el interior de la empresa; es decir, desde las personas. Si las personas no ven los beneficios de los cambios van a ser un obstáculo, y no un apoyo.
- Se requiere el apoyo de la alta dirección en las organizaciones para lograr la apropiación de los marcos de referencia de las TIC, esto quiere decir que se requiere que se piense que la implementación es una inversión, que en el corto, mediano y largo plazo va a traer beneficios para la organización.

6.5.4 Factores críticos de éxito de la continuidad del negocio

Las condiciones sociales, políticas, de mercado y tecnológicas actuales hacen más vulnerables a las organizaciones de todos los sectores ante las situaciones de eventos disruptivos, y se requiere, por lo tanto, que ellas cuenten con una estructura institucional que

les permita anticipar, evaluar y responder oportuna y adecuadamente a estos eventos con el fin de preservar sus recursos, mitigar sus consecuencias e impactos y garantizar su supervivencia. Hoy en día no se concibe una organización sin el apoyo de la tecnología informática para soportar sus procesos y responder a su estrategia, sus tácticas y sus técnicas (Terán Pérez, 2014). Por esta razón, no se puede dejar de lado la planeación de los sistemas en correspondencia con las estrategias del negocio.

El fortalecimiento en tecnología informática se inicia justamente con la construcción del plan estratégico de tecnología informática (PETI), cuyo objetivo es modelar el ambiente de tecnología informática de las organizaciones en términos de las estrategias de aplicaciones, tecnología base, comunicaciones y organización, con el fin de soportar sus procesos y responder oportunamente con información consistente a sus requerimientos; fortaleciendo así sus factores críticos de éxito.

El PETI se inicia con el diagnóstico del ambiente tecnológico actual, continúa con la definición de una nueva visión tecnológica, sigue con la determinación de las estrategias y culmina con la documentación de los proyectos y las inversiones que se deben realizar para lograr las estrategias establecidas.

La construcción del PETI implica el desarrollo de las siguientes actividades:

- Diagnóstico del ambiente tecnológico actual
- Establecimiento de la nueva visión tecnológica
- Definición de las aplicaciones-objetivo
- Precisión de la estrategia de las aplicaciones
- Delimitación de la estrategia de la tecnología base
- Puntualización de la estrategia de las comunicaciones
- Especificación de la estrategia de organización
- Identificación de todos los proyectos
- Construcción del presupuesto
- Formulación del plan

El PETI es una herramienta fundamental para el cumplimiento de las estrategias de la organización, y es responsabilidad de la Dirección General velar por su construcción y ejecución.

6.6 Servicios administrados (seguridad en la nube)

El objetivo de los sistemas tecnológicos es hacer efectivos los procesos y cubrir las necesidades de las Tecnologías de la Información (TI) de forma efectiva. Teniendo esto en mente, vale la pena tomar en cuenta que la economía y la dinámica de negocios actuales orillan a las empresas a hacer cada día más con menos, pero sin perder su competitividad. Para ello, hoy existen opciones para tercerizar (*outsourcing*) procesos y servicios, que además de minimizar costos operativos permiten crear estrategias de penetración en mercados locales, regionales y globales; estar actualizados; incrementar su saber hacer (*knowhow*) y tener la capacidad de responder ágilmente a los constantes y rápidos cambios del mundo de los negocios; sin embargo, la oferta dentro del concepto "una talla para todos" (*one size fit sall*) no es la mejor opción. Las organizaciones tienen necesidades propias que requieren de servicios personalizados y adaptados a temas específicos (Terán Pérez, 2014).

En la actualidad, una alternativa son los servicios administrados (*Managed Services*), pues más allá del outsourcing, este concepto le permite a las organizaciones tener mayor flexibilidad en sus actividades y su tiempo; por esto, además del costo que este formato de entrega de servicios tiene, permite a las organizaciones cubrir las diversas necesidades de Tecnologías de la Información (TI) de forma efectiva. Para la cadena de suministro, los *managed* services son una opción no sólo para disminuir costos, sino para hacerla más eficiente, madura y consolidada.

Con los avances tecnológicos, el trabajo en las organizaciones se optimiza constantemente; lo que exige que los periodos de entrega sean cada vez más cortos para impulsar las economías a ser globales.

Dentro de los servicios administrados tradicionales que se pueden manejar están los siguientes: la distribución de contenido, el almacenamiento de datos, la recuperación en caso de desastre, el monitoreo de la red y la seguridad en la red de la cadena de suministro.

Por otro lado, dentro de las tendencias en las Tecnologías de la Información (TI), se tienen las siguientes: la virtualización, la computación en la nube (*cloud computing*) y la movilidad. Estos servicios permiten crear o tener una cadena de suministros más eficiente y ágil administrando altos números de pedidos, inventarios, proveedores, clientes, etcétera, en un menor tiempo. Por eso, al requerir de servicios administrados se considera crítico que las empresas que los brindan cuenten con la infraestructura, la cobertura, el *software* y el soporte técnico necesario y suficiente para proporcionar un servicio de la más alta calidad a los clientes. Con esto, la estrategia empresarial será un éxito, ya que al contar con las herramientas necesarias, la tecnología de punta y una metodología adecuada habrá muy pocos puntos de distracción para los directores en la planeación de la empresa.

Las organizaciones que prestan estos servicios utilizan la inteligencia de las redes y la gestión de problemas predecibles para monitorear y correlacionar eventos; en pocas palabras, emplean soluciones de misión crítica a través de todos los segmentos de una infraestructura administrada, que orquesta tanto acciones correctivas como preventivas contra incidentes potenciales de las TI. Si se implementa la tecnología sin una planificación adecuada, las organizaciones se ponen en riesgo.

Si estos procesos no se concluyen o se quedan a la mitad, la seguridad de la organización estaría en riesgo de sufrir intrusiones (*hackeos*) o robos (*phishing*), entre muchas otras consecuencias. Éstos son algunos de los aspectos a considerar, ya que el tomar decisiones equivocadas, y muchas veces costosas, daría como resultado un proceso de negocio ineficiente.

En la actualidad, a todas las organizaciones se les exige maximizar recursos y, considerando que 91 % de los presupuestos de las Tecnologías de la Información (TI) son requeridos tan sólo para mantener el *statu quo*, las empresas tienen que encontrar formas de reorientar ese gasto en innovación, con proyectos y opciones de servicios administrados para reducir costos, uso de energía y riesgos; así como lograr una calidad óptima. Los servicios *managed services* ayudan a las organizaciones a integrar tendencias tecnológicas en diferentes procesos de negocio. Algunos otros beneficios son los siguientes:

- Crear sistemas de uso de las Tecnologías de la Información (TI) ágiles, flexibles y modernos para cumplir con nuevas políticas y regulaciones tanto de índole local como global.
- Construir medidas de seguridad avanzadas para detectar, prevenir o simplemente sanar amenazas a la seguridad. También ayudan a mantener la confianza de los clientes, los socios y los aliados de negocio.
- Aprovechar las nuevas tecnologías para seguir siendo competitivos e incrementar las demandas de satisfacción de los clientes.
- Crear servicios y productos amigables con los clientes y los proveedores.

Este tipo de servicios algunas veces pueden venir con cuestiones que precisan de una rápida solución de problemas. Por lo anterior, se requiere que la organización que proporcione servicios administrados cuente satisfactoria y sobradamente con soluciones de misión crítica para resolver a la brevedad posible los retos de negocios más exigentes, especialmente para sectores específicos de la industria, como en la cadena de suministro.

Contar con el conocimiento profundo de sistemas de seguridad, integración, *outsourcing*, infraestructura y tecnología de centros de datos, y emplear la tecnología de última generación garantiza la seguridad tanto física como informática.

6.6.1 Seguridad en la nube

La computación en la nube ofrece una manera de utilizar el *software* de almacenamiento y los recursos de datos en demanda a través de una red *online*, conocido como servicios en la nube. Los proveedores de servicios gestionan la infraestructura y las plataformas que operan estos recursos, los cuales se almacenan de forma remota pero accesible a varios usuarios desde su escritorio; esto puede ayudar a lograr economías de escala y reducir el costo de invertir en una compañía de infraestructura de TI específica.

La computación en la nube también permite acceder a los programas, datos y aplicaciones que una organización necesita y son demandados desde cualquier lugar, consiguiendo tener una mayor flexibilidad en la forma en la que se trabaja. A continuación, otros de los beneficios de la seguridad en la nube:

- Visibilidad completa de la alta dirección de la organización para evaluar la efectividad de su sistema de gestión en relación con las expectativas de la norma internacional y la industria de seguridad en la nube.

- Una auditoría adaptada, que reflejará cómo los objetivos de la organización están orientados a la optimización de los servicios en la nube.
- Una organización para demostrar los niveles de progreso y el desempeño a través de un reconocimiento validado independientemente por un organismo de certificación externo.
- Las organizaciones pueden comparar sus resultados con su competencia.

6.7 Servicios administrados (seguridad en la nube)

La seguridad informática, no sólo en México sino a nivel mundial, es uno de los temas que mayor auge comienza a tener en la actualidad, visto ya sea desde las necesidades de promoverla, así como de implementarla (Correa, 1987). Lo anterior atiende a centrar este apartado en una premisa importante: la seguridad informática no implica en forma única y específica a Internet; la seguridad informática se refiere a todo lo que hace referencia a la preservación, respeto y buen manejo de toda la información. Para ello, es de vital importancia aclarar que el valor protegido, tanto tangible como intangible, será siempre la información (Davara Rodríguez, 1993). Sin embargo, el tema de preservar, respetar y manipular en forma correcta la información, al día de hoy no es un tema fácil de entender, dado que se tiene pensado en el mayor de los casos, que la seguridad informática es un tema que sólo debe aplicarse a casos específicos y no a un "todo" empresarial, por ejemplo:

- La importancia de proteger los archivos electrónicos de un alto ejecutivo en una empresa *versus* la falta de importancia de proteger los archivos electrónicos de la persona encargada de llevar el registro de entrada y de salida del personal.
- La constante actualización de programas antivirus en las computadoras personales de los altos ejecutivos en una empresa versus la ausencia de un programa antivirus en las computadoras personales de las secretarias de dichos ejecutivos.

Los ejemplos anteriores permiten entender la forma en que es visto, en muchos de los casos, el cómo deben ser implementados algunos de los controles en materia de seguridad de la información. Ahora véanse las consecuencias de pensar en esta forma:

- El viernes 20 de febrero del 2015, una descarga de alto voltaje recae en la organización, como consecuencia, el procesador y disco duro de la computadora personal del Director de Recursos Humanos sufren daños, y por ende, pierde su información; sin embargo, la consecuencia no es grave dado que su información sí tenía implementado un sistema de respaldo, permitiéndole así no comprometer la integridad y disponibilidad de la misma. Por otra parte, como consecuencia de la descarga, la computadora del encargado de mantener un registro electrónico del control de entradas y de salidas del personal, así como de personas externas a la organización, también sufre daños y la información se pierde definitivamente. ¿Qué sucederá con el control de asistencias del personal?, ¿cómo determinar quién asistió que días, y en qué horario? En el caso de una investigación por robo, ¿con base en qué registro se podrá saber quién accedió a las instalaciones de la empresa?, ¿quién será el responsable ante la ausencia de esta información: el encargado del control o el encargado de sistemas? Más importante aún: ¿a quién despedir y/o fincarle responsabilidad penal por esta negligencia?
- El lunes 5 de enero del 2015 a las 9 horas en punto, un nuevo virus atacó las computadoras de la misma organización vista en el caso anterior, en esa hora es cuando las secretarias de los altos ejecutivos de una empresa están revisando agendas y ajustando las actividades de la semana laboral. Una de las computadoras de las secretarias es infectada por el nuevo virus, obviamente sin

tener conocimiento de que dicho hecho sucede, dado que no tiene instalado un antivirus. Al momento de intercambiar información con las demás secretarias y con su propio jefe, ella infecta las computadoras de las otras secretarias; afortunadamente la computadora de su jefe no es afectada. Las consecuencias de ejecutar el virus son fatales dado que empieza a borrar la información, así como el acceso a ciertos programas en las demás computadoras, situación que sucede en todas las computadoras de las secretarias de los altos ejecutivos de la organización. Consecuencia fatal: al inicio de una semana laboral, el área operativa más importante de una empresa es detenida en sus actividades aun cuando la toma de decisiones permanece intacta; sin embargo, ¿cómo pueden ejecutarse las decisiones si el área operativa es inoperable?

De los dos ejemplos anteriores, mismos que reflejan consecuencias mínimas, (existen más graves, como el robo de información, los fraudes, la revelación de secretos, la difamación, etcétera), surge la pregunta más utilizada en el tema: ¿quién es el responsable de que sucedan estos hechos? Para abrir las opciones en esta respuesta, se abordará el tema a discutir desde dos puntos de vista: uno será el de los aspectos éticos, y el otro, el de los aspectos legales, no sin antes mencionar que aun cuando se separen los puntos de vista, se debe dejar claro que la ética y el derecho, son dos temas que siempre van unidos. *Los medios y el fin*, la premisa principal cuando de ética se habla. El fin justifica los medios o los medios justifican el fin, ambas frases son las que salen a relucir cuando se está frente a un conflicto ético. Con la intención de no entrar en teorías filosóficas, se parte de una definición objetiva de lo que la palabra ética significa de acuerdo a lo que la Real Academia Española (RAE), indica:

- Parte de la Filosofía que trata de la moral, y de las obligaciones del hombre.
- Conjunto de normas morales que rigen la conducta humana (Real Academia Española, 2016).

De ahí que cuando se enfrenta un conflicto ético, no es más que cuando una persona está en una situación que compromete, por una parte, a la moral, y por la otra, a sus obligaciones; es decir, el ser y el deber ser (la Ontología y la Deontología). Lo que siempre se menciona con respecto a este tema, es que indudablemente los valores éticos no son universales, sería imposible asegurar que existe un *Manual único*, que enliste cómo debe ser la ética de todos los seres humanos, es por ello que ante las preguntas: ¿quién me dice sí soy ético o no?,y ¿quién me enseña cómo ser ético?, existe para la primera pregunta sólo una respuesta: uno mismo; mientras que para la segunda pregunta, la respuesta es que los valores éticos se van aprendiendo del entorno (la familia, el trabajo y el núcleo social), aun así, retornando al "yo", es uno mismo quien construye su propia ética y por ende, la aplica en forma distinta ante casos específicos.

Para lo que respecta al tema de seguridad informática, el cómo ser ético es definido desde varios aspectos, principalmente por los Códigos de Ética estipulados por instituciones dedicadas al tema de la Seguridad Informática (https://www.isc2.org/) e incluso por autoridades [Request for Comments Editor, 2012] (no gubernamentales, precisamente) dedicadas al tema de las Tecnologías de la Información y de las Comunicaciones (TIC). En el tema de la Seguridad Informática, el Consorcio para la Certificación Internacional de Seguridad en Sistemas de Información (ISC, *International Information Systems Security Certification Consortium*) emite una de las más importantes certificaciones en el tema de Seguridad Informática, el cual conlleva como requisito indispensable el compromiso y conocimiento del Código de Ética establecido por el Consorcio (Código de Ética de ISC).

Dentro de los cánones a seguir, se indica lo siguiente:

- Proteger a la sociedad, a la comunidad, y a la infraestructura
- Actuar en forma honorable, honesta, justa, responsable y legal
- Proveer servicios diligentes y competitivos a sus superiores
- Actuar siempre, protegiendo y promoviendo el crecimiento de la profesión

Con respecto a las autoridades no gubernamentales que establecen políticas y costumbres en materia de Tecnologías de Información (TI), *Request for Comments* 1087: Ética e Internet, generado desde enero de 1989 por DARPANET: *Defense Advanced Research Projects Agency, Internet Activities Board* define, a contrario, lo que se entiende como un comportamiento no ético en Internet de la siguiente forma:

- Conseguir accesos no autorizados a los recursos de Internet.
- Entorpecer el uso intencionalmente de Internet.
- Gasto de recursos en forma innecesaria.
- Destruir la integridad de la información basada en las computadoras.
- Comprometer la privacidad de los usuarios.

En lo que respecta al mundo jurídico, es obvio que las personas en ningún momento se encuentran sujetas a normas morales, la situación requiere de un ambiente de obligatoriedad especificada a través de disposiciones y sanciones, es decir: las normas jurídicas. La relación entre la Seguridad Informática y el Derecho (Galindo, 1998) se ciñe a las preocupaciones existentes en materia de implementación, todas ellas en torno de los siguientes cuestionamientos:

- ¿Qué pasa si los programas de cómputo utilizados en la organización no tienen una licencia de uso (piratería)?
- ¿Cómo puedo hacer responsable al personal de proteger la integridad de la información?
- ¿En qué forma, se pueda evitar que la información confidencial de la empresa no sea revelada a terceros?
- ¿Cómo proteger los secretos industriales?
- ¿Cómo responsabilizar al personal cuando se les entrega una computadora para que trabajen con ella?

La situación por resolver en los aspectos legales son sólo dos:

- Promover una cultura jurídica en materia de Tecnología de la Información (TI), que en consecuencia impacte en un robustecimiento de las normas jurídicas existentes al día de hoy.
- Fortalecer la normatividad interna de las empresas con apego siempre a derecho.

6.7.1 Ley Federal de protección de datos

En el mundo existen dos vertientes principales entorno a la protección de los datos personales: el modelo europeo que busca proteger la información y la propiedad de la misma, en aras de conservar la honorabilidad de la persona aun cuando ésta hubiese

fallecido; la motivación de este modelo tiene base en los derechos humanos de los individuos. El modelo estadounidense pretende proteger la información de las personas con el concepto de derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto; el modelo surge derivado de motivos comerciales, ya que las empresas utilizaban de manera indiscriminada esa información. Diversos países han promulgado leyes de protección de datos personales y en cada país se ha buscado adaptar, a sus propias condiciones culturales, económicas y políticas, las bases de alguno de los dos modelos de protección de datos personales existentes. A continuación, se mencionan algunos casos relevantes sobre las leyes de protección de datos personales de distintos países, organizaciones y regiones del mundo:

Organización de Naciones Unidas (ONU). En 1948, adopta el documento conocido como Declaración Universal de Derechos Humanos, en la que el artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.

Alemania. En 1970, fue aprobada la primera ley de protección de datos (Datenschutz). En 1977, el Parlamento Federal Alemán aprueba la *Ley Federal Bundesdatenschutzgesetz*. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada.

Suecia. En 1973, se publicó la que fue una de las primeras leyes de protección de datos en el mundo.

Estados Unidos de América. La protección de datos tiene su base en *The Privacy Act* de 1974.

Unión Europea. El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como "Convenio 108" o "Convenio de Estrasburgo". En los años 90, se establece una norma común que se denominó Directiva 95/46/CE. La directiva es referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos.

España. *La Ley Orgánica 15*, de 1999, establece la Protección de Datos de Carácter Personal. Esta ley ha sido importante para Latinoamérica, porque se ha utilizado como firme referente del modelo europeo.

Latinoamérica. En América Latina, las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las Tecnologías de la Información y de las Comunicaciones (TIC), y al aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan al modelo europeo: en Argentina la *Ley 25.326* (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008).

Rusia. En el 2006, fue aprobada una exhaustiva ley de protección de datos personales.

Perú. *La Ley 29.733* del 2 de julio del 2011 es la más reciente ley de protección de datos personales en el mundo.

México. *La Ley Federal de Protección de Datos Personales en Posesión de Particulares* fue publicada en el *Diario Oficial de la Federación* el 5 de julio del 2010, entró en vigor un día después, y tiene efecto a partir de enero del 2012.

Esta última ley pretende salvaguardar el respeto a la privacidad, dignidad e información de las personas; en ella, se establecen cuatro derechos fundamentales que tienen los

individuos sobre su información en posesión de cualquier persona física o empresa particular (aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etcétera), son los denominados derechos ARCO: acceso, rectificación, corrección y oposición. La ley también indica que los particulares deberán avisar a cada persona de la que obtengan información personal, sobre el tratamiento que planean dar a sus datos. Lo anterior se debe hacer mediante un aviso de privacidad, el cual deberá ser respetado por el particular, y cada persona notificada tendrá la libertad de otorgar o no su consentimiento respecto al procesamiento de su información.

6.7.2 Gobernanza de Internet

Por gobernanza se entiende el conjunto de mecanismos, acuerdos y estructuras por medio de los cuales un grupo social coordina su acción. El concepto incluye desde luego a todas las estructuras formales de los gobiernos nacionales, pero también las excede.

Hay formas de gobernanza desde las más elementales normas de convivencia social hasta los sofisticados acuerdos multisectoriales e internacionales que rigen el manejo del medio ambiente natural para la humanidad. En las últimas décadas, las formas tradicionales de gobernanza internacional, como son las organizaciones intergubernamentales y los tratados, se han visto complementados cada vez más activamente, por la participación de los ciudadanos, las organizaciones sociales y las empresas, que en muchos casos, han rebasado o antecedido a la acción gubernamental nacional y a la intergubernamental en el plano internacional.

El medio ambiente, motivo de atención creciente, da muestras de este tipo de acción. Las organizaciones no gubernamentales (ONG) se anticiparon a los gobiernos, en las décadas de la Postguerra, en la identificación de los graves problemas antropogénicos del medio ambiente y en la acción contra sus causantes, especialmente cuando éstos son empresas privadas o públicas que producen contaminación severa e identificable.

Los gobiernos y las empresas han creado mecanismos para la gobernanza del medio ambiente que dan amplio espacio a la sociedad civil y a los expertos; estos últimos constituyen una fuerza por sí mismos, independientemente del hecho de que en instancias específicas no logren acuerdos ni tengan una posición unificada. El impacto de estas formas de gobernanza ha sido amplio. Si bien las organizaciones internacionales que rigen los acuerdos entre naciones en materia de medio ambiente siguen siendo intergubernamentales, han tenido que dar entrada desde el establecimiento de la agenda, hasta el seguimiento de los acuerdos, a los nuevos actores no gubernamentales.

Como se sabe, Internet es una red de redes; un sistema de interconexión de redes de cómputo, que se ha extendido a una sexta parte de la población mundial. Las redes que se interconectan en Internet son redes que conectan computadoras y otros dispositivos en sitios tan diversos como los hogares, las oficinas, los laboratorios y las fábricas. El salto cualitativo que dio lugar a Internet fue un conjunto de ideas concebidas y puestas a prueba de manera experimental en los años de las décadas de 1960 y 1970, a saber, la conmutación por paquetes, el principio "punta a punta" o *End Gobernanza de Internet* y los principios *Multistakeholder to End*, la "inteligencia en la orilla", y la estandarización de las comunicaciones no al interior de todas las redes, sino en la comunicación entre ellas.

Los desarrollos tecnológicos fundamentales para el crecimiento de Internet se basaron en un principio también fundamental: la estandarización en la interfaz y la interoperabilidad de las tecnologías. Para que la estandarización se diera de manera ágil y no interfiriera con el desarrollo de la tecnología, a diferencia de los procesos de la Unión

Internacional de Telecomunicaciones (UIT) y de la Organización Internacional de Estándares (ISO), los ingenieros productores de la tecnología se agruparon en la IETF3 y dieron lugar al proceso de los RFC (Krechmer, 2006).

Éstas fueron las primeras formas de gobernanza propias de Internet. Se orientaron a la solución de un problema específico: la estandarización para la interoperabilidad, y crearon mecanismos originales, distinguidos por la apertura en la discusión, la meritocracia, la importancia de las soluciones funcionales y la evolución constante tanto de las tecnologías como de los modos de gobernanza. La *Internet Engineering Task Force* (IETF) se volvió paradigmática de una amplia forma de conducir los asuntos de la comunidad, que fue reconocida como la "Comunidad Internet". En la IETF no hay autoridad sino coordinación; no hay una estructura permanente constituida jurídicamente, sino una conjunción de voluntades.

La IETF se describe a sí misma bajo el lema: "*Rough Consensus and Running Code*", (en español significa: "*Consenso aproximado y programas que funcionan*"), con los cuales ha llegado a agrupar hasta poco más de 15 000 especialistas, y a través de sus reuniones presenciales y sus interacciones a distancia, sobre todo por correo electrónico; producir una panoplia (una panoplia es una armadura completa con todas sus piezas) de tecnologías ya reconocida, como una de las veinte tecnologías de uso general más transformadoras de la historia (Lipsey; Kenneth y Clifford, 2005).

Los participantes de la IETF lo son a título individual y pertenecen a toda suerte de organizaciones: empresas, laboratorios de investigación públicos o privados, instituciones académicas, gobiernos, etcétera. Si bien en la IETF se expresan conflictos entre estas entidades en diversas formas (una de ellas son las "guerras de estándares"), la participación multisectorial no le da mayor peso a ninguno de estos tipos de organizaciones por sí mismo.

Hacia 1995, la evolución de la IETF exigió la creación de *The Internet Society* (ISOC), para contar con un paraguas corporativo que se hiciera cargo de operaciones como la organización de reuniones y publicaciones de la IETF; diera alojamiento formal a la función de editor de los RFC, y protegiera los estándares contenidos en éstos, del riesgo de apropiación privada (desde un principio, y a diferencia de muchos otros procesos de estandarización, los estándares de la IETF han sido abiertos y gratuitos, para su libre adopción). De manera adicional, ISOC se estableció como una sociedad profesional para los especialistas dedicados a Internet, como principal campo de acción, y como una sociedad para la promoción de Internet, su difusión global, y el conocimiento técnico necesario para expandirla.

6.8 Conclusiones

Los adelantos en ciencia y tecnología, el uso intensivo de las TIC y la dependencia de las organizaciones en los sistemas de información como estrategia para establecer ventajas competitivas más duraderas y difíciles de imitar, así como el apoyo para la toma de decisiones, obliga a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías. Mantener los procesos principales de las organizaciones y de las actividades operativas enfatizan la importancia de implementar sistemas de administración de seguridad de la información que proporcionen esquemas esenciales para soportar procesos críticos en las organizaciones.

Los sistemas de administración de seguridad de la información están conformados por elementos como: estándares, políticas, procedimientos, análisis de riesgos y auditorías de sistemas. La implementación de ISMS (*Information Security Management System*) es una decisión estratégica de la organización; y por lo tanto, debe ser apoyada desde los altos mandos hasta el personal de mandos medios; el diseño, desarrollo e implementación del ISMS debe cumplir con los objetivos organizacionales y cumplir con las expectativas de las áreas involucradas.

Por otro lado, la definición del perímetro de seguridad debe ser establecido como un control interno de la organización. Las políticas de seguridad deben estar alineadas a los objetivos organizacionales, ser flexibles y adecuados para cada una de las áreas donde se van aplicar. La creación del ISMS considera el diseño, la implementación, el monitoreo y el mantenimiento de los sistemas de seguridad y las estrategias en la elaboración de políticas, procedimientos, planes y grupos de trabajo. La ejecución de un análisis de riesgos consiste en la identificación de los activos, amenazas y vulnerabilidades. Es una metodología que busca maximizar los recursos escasos de la organización a través de una valoración de los riesgos y la tolerancia de la empresa a éstos.

El uso intensivo de las TIC en las economías más desarrolladas del mundo como herramienta para crear ventajas competitivas durables es innegable. Sin embargo, hay que reconocer que ésta debe estar soportada por un sistema de administración de seguridad de la información diseñada en capas que garanticen la operatividad de los servicios principales en la organización, a través de la correcta identificación de los activos, buscando el apoyo de los integrantes de la empresa y estableciendo claramente los objetivos de contar con una arquitectura de seguridad de la información. Hoy se dice que la gestión del talento humano junto con la información son los activos más importantes en las organizaciones. En un entorno de red, siempre debe asegurarse la privacidad de los datos sensibles.

Finalmente, no sólo es importante proteger de daños no intencionados o deliberados la información más preciada, sino también las operaciones de la red. El mantenimiento de la seguridad de ésta requiere un equilibrio entre facilitar un acceso fácil a los datos por parte de los usuarios autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad del administrador crear y garantizar este equilibrio, pues incluso en redes que controlan datos sensibles y financieros la seguridad a veces se considera medida tardía (Lokhart, 2007).

Las cuatro amenazas principales que afectan la seguridad de los datos en una red son: los accesos no autorizados, los sobornos electrónicos, los robos y el daño intencionados o no; sin embargo, hay que ser sinceros: la seguridad de los datos no siempre se imple-

menta de forma apropiada, precisamente por la seriedad de estas amenazas. La tarea del administrador es asegurar que la red se mantenga confiable, segura y, en definitiva, libre de aquéllas.

La magnitud y el nivel requerido de seguridad en un sistema de red depende del tipo de entorno en el que trabaja la red; por ejemplo, una que almacena datos para un banco importante requiere una mayor seguridad que una LAN que enlaza equipos en una pequeña organización de voluntarios.

Generar la seguridad en una red de computadoras del siglo XXI precisa establecer un conjunto de reglas, regulaciones y políticas que no dejan nada al azar: el primer paso para garantizar la seguridad de los datos es implementar las políticas que establecen los matices de la seguridad y que ayudan al administrador y a los usuarios a actuar cuando se producen modificaciones esperadas como las no planificadas tanto en el desarrollo como en el uso real de la red (Stallings, 2004).

PRÁCTICAS

Para realizar estas prácticas es requisito indispensable que descargue del sitio web: www.cisco.com el simulador Packet Tracer 7.0.

Después para familiarizarse con el uso de este simulador, busque en Internet, descargue y lea los tutoriales, vea los videos que existen sobre dicha aplicación informática.

PRÁCTICA 6.1

Técnicas de seguridad inalámbrica para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Configurar WPA2 en Linksys WRT300N.
- ☑ Ajustar el filtrado MAC en Linksys WRT300N.
- ☑ Establecer el reenvío de puerto único en Linksys WRT300N.

Introducción

En esta actividad se configurará el router inalámbrico Linksys WRT300N para utilizar el modo WPA2 personal como método de seguridad, buscando confiar en el filtrado MAC con el fin de mejorar la seguridad y de admitir el reenvío de puerto único.

Procedimiento

Primera Parte. Conexión al router inalámbrico

Para iniciar sesión en el *router* inalámbrico es necesario llevar a cabo los siguientes pasos:

- ☑ En la ficha "*Desktop*" en PC0 elija "*Web Browser*".
- ☑ Escriba la dirección IP del router inalámbrico: 192.168.0.1.
- ☑ Cuando se le solicite nombre de usuario y contraseña utilice "admin" para ambos, que son los predeterminados para todos los productos Linksys.
- ☑ Una vez cargada la página de configuración basada en la web WRS1, continúe con la parte 2.

Segunda Parte. Adición de funciones de seguridad a WRS1

Con el objetivo de configurar WPA2+AES en WRS1 siga los pasos presentados a continuación:

- ☑ En la página web de configuración WRS1 (a la que se accede desde un explorador web en PC0) vaya a "*Wireless*" > "*Wireless Security*" y cambie el "*Security Mode*" de "*Disabled*" a "*WPA2 Personal*". AES se considera un protocolo de encriptación de alta seguridad, por lo que se debe mantener seleccionado.
- ☑ La contraseña para esta red inalámbrica se configura en el campo "*Passphrase*", en éste escriba "aCompWiFi" como contraseña, tomando en cuenta que ésta distingue entre mayúsculas y minúsculas.
- ☑ Posteriormente, desplácese hacia abajo de la página y haga clic en "*Save Settings*" para guardar los cambios.
- ☑ WRS1 ahora está configurado para utilizar WPA2.

Nota: Laptop0 no podrá asociarse a WSPR1 porque aún no se ha configurado, esto se llevará a cabo en la tercera parte del procedimiento.

Tercera Parte. Configuración del cliente inalámbrico para Laptop0

- ☑ Haga clic en "*Laptop0*" para que aparezca la ventana de configuración y después en la ficha "*Desktop*"; en ésta seleccione "*PC Wireless*", tras ello debe ver el mensaje "*No Association with Access Point*".
- ☑ Oprima "*Connect*" y espere unos segundos para que aparezca el SSID difundido por WRS1, que debe ser "aCompany" enumerado en la columna "*Wireless Network Name*", y haga clic para seleccionarlo. Luego haga clic en "*Connect*".
- ☑ En el campo "*Security*" elija WPA2-Personal.
- ☑ Ingrese la contraseña para la red inalámbrica: "aCompWiFi" y luego haga clic en "Connect". Ahora debe asociarse *Laptop0* a WRS1.
- ☑ Tome nota de la dirección IP de *Laptop0* (adquirida a través de DHCP desde WRS1) y de la dirección MAC. Cierre la ventana "*PC Wireless*" y en la ficha "*Desktop*" seleccione "*Command Prompt*".
- ☑ Escriba "ipconfig /all" y tome nota de las direcciones IP y MAC de *Laptop0*.

Cuarta Parte. Configuración WRS1 para que admita el filtrado MAC

- ☑ Cierre la ventana de configuración de Laptop0.
- ☑ Haga clic en PC0 y abra un explorador web: para hacerlo vaya a "*PC0*" > "*Desktop*" > "*Web Browser*".
- ☑ Después ingrese la dirección IP de WRS1 para abrir la página web de configuración. Cuando se le solicite, ingrese "admin" como nombre de usuario y contraseña.
- ☑ Vaya a "*Wireless*" > "*Wireless MAC Filter*" y seleccione "*Enabled*"; observará el mensaje "*Permit PC Listed Below to Access Wireless Network*".
- ☑ Ingrese la dirección MAC de Laptop0 (descrita en la Parte 3) en *MAC 01*: campo. Tenga en cuenta el formato de dirección MAC que solicita WRS1 (debe respetar el formato XX:XX:XX:XX:XX:XX).
- ☑ Desplácese hacia abajo de la página y haga clic en "*Save Settings*". Debido a que la dirección MAC de Laptop0 es una dirección especificada, Laptop0 es el único dispositivo inalámbrico que actualmente puede asociarse a WRS1.

Quinta Parte. Prueba de conectividad

- ☑ Haga clic en PC0 y vaya a "*Desktop*" > "*Command Prompt*".
- ☑ Para realizar *ping* a RemotePC introduzca "*ping 200.100.50.10*". Los pings deben ser correctos.
- ☑ Cierre la ventana de configuración de PC0 y haga clic en "*Laptop0*" y, luego, en la ventana de configuración de ésta vaya a "*Desktop*" > "*Command Prompt*".
- ☑ Para realizar *ping* de RemotePC introduzca "*ping 200.100.50.10*". Los pings deben ser correctos. Posteriormente, cierre la ventana de configuración de Laptop0.
- ☑ Haga clic en RemotePC para que aparezca la ventana de configuración, en ésta vaya a "*Desktop*" > "*Command Prompt*".
- ☑ Para realizar *ping* a *Server0* desde RemotePC introduzca "*ping 192.168.0.20*". Los *pings* no deben tener éxito.
- ☑ En RemotePC abra un explorador web ("*Desktop*" > "*Web Browser*") e ingrese la dirección de la página web interna hospedada en Server0 (www.acompany.com). No debe aparecer la página.

- ☑ Cierre todas las ventanas de configuración de los dispositivos que puedan estar abiertas y continúe con la sexta parte.

Las solicitudes de *ping* y/o HTTP desde RemotePC a Server0 (o a cualquier otro dispositivo interno) no tienen éxito debido a que WRS1 no sabe qué dispositivo interno debe recibirlos. Para lograr esto, se debe configurar el reenvío de puertos en WRS1.

Sexta Parte. Configuración del reenvío de puerto único en WRS1

- ☑ Haga clic en PC0 para que aparezca la ventana de configuración.
- ☑ Vaya a "*Desktop*" > "*Web Browser*" y conéctese a WRS1.
- ☑ Desde la página web de configuración de WRS1 vaya a "*Application & Gaming*" > "*Single Port Forwarding*".
- ☑ En el menú de la derecha elija HTTP del primer cuadro combinado.
- ☑ En la parte central de la ventana ubique la primera fila y cambie la dirección IP para que coincida con la del Server0 (192.168.0.20). También seleccione la casilla de verificación "*Enabled*" al final de la misma fila.
- ☑ Desplácese hacia abajo de la página y haga clic en "*Save Settings*". Ahora debería tener acceso a la página web hospedada en Server0.
- ☑ Abra un explorador web en RemotePC y en la barra de dirección ingrese 121.120.119.100, que es la dirección IP asignada al puerto de Internet del WRS1.
- ☑ Ahora debe ver la página web hospedada en Server0.

Cuestionario

6.1.1 Explique a detalle, cómo configurar WPA2 en Linksys WRT300N.

6.1.2 Establezca cómo se debe ajustar el filtrado MAC en Linksys WRT300N.

6.1.3 Explique a detalle, cómo debe establecerse y mantenerse el reenvío de puerto único, en Linksys WRT300N.

PRÁCTICA 6.2

Administración del sistema operativo y de los archivos de configuración de un conmutador para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Crear y guardar una configuración básica de conmutador.
- ☑ Configurar un servidor TFTP en la red.
- ☑ Realizar una copia de respaldo del *software* IOS de Cisco en un servidor TFTP para después restaurarlo.
- ☑ Llevar a cabo una copia de respaldo de la configuración del switch a un servidor TFTP.
- ☑ Configurar un switch para cargar una configuración desde un servidor TFTP.
- ☑ Actualizar el *software* IOS de Cisco desde un servidor TFTP.
- ☑ Recuperar la contraseña para un switch Cisco 2960 (serie 2900).

Introducción

Un conmutador (*switch*) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del Modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

Procedimiento

Diagrama de la topología

La figura 6.3 muestra el diagrama de la topología a utilizar en el desarrollo de la presente práctica.

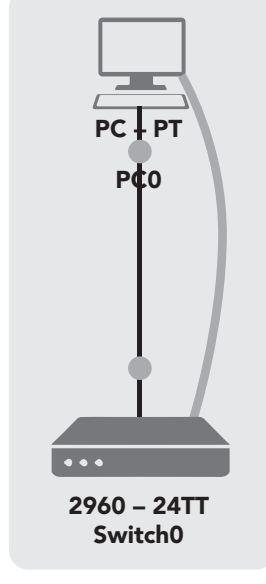


Figura 6.3 Diagrama de la topología

Tabla de direccionamiento

La tabla 6.10 muestra el direccionamiento de los equipos utilizados en la práctica.

Tabla 6.10 Direccionamiento de los dispositivos utilizados en esta práctica

Dispositivo	Nombre del *host*/ Interfaz	Dirección IP	Máscara de subred	*Gateway* de salida determinada
PC1	Host-A	172.17.99.21	255.255.255.0	172.17.99.1
Switch1	VLAN99	172.17.99.11	255.255.255.0	172.17.99.1

Escenario

En esta práctica se explorará la administración de archivos y los procedimientos para recuperar contraseñas en un *switch* Cisco Catalyst.

Nota: el resultado que arroja esta práctica es para un switch 2960. Si utiliza otros, el producto final y las descripciones de la interfaz podrían aparecer diferentes.

Primera Parte. Cableado e inicialización de la red

- ☑ Cablee una red de manera similar al diagrama de topología que se muestra en la figura 6.3.
- ☑ Luego, cree una conexión de consola al *switch*. El resultado que arroja esta práctica es para un conmutador (*switch*) 2960. Si utiliza otros conmutadores (*switches*), el resultado del conmutador (*switch*) y las descripciones de la interfaz podrían aparecer diferentes.
- ☑ Posteriormente, establezca una conexión de la consola al *switch* y borre la configuración en el conmutador.
- ☑ Para crear una configuración básica, ajuste el *switch* con el nombre de *host* y las contraseñas de acceso que se muestran en la tabla 6.11. Luego, establezca la contraseña "*enable secret*" en éste.

Tabla 6.11 Nombre del *host* y contraseñas para el conmutador utilizado en la práctica

Nombre del *host*/	Contraseña de la consola	Contraseña Telnet	Contraseña de comando
ALSwitch	Cisco	Cisco	Class

- ☑ Cree la VLAN 99: proporcione la dirección IP 172.17.99.11 para esta interfaz y asigne el puerto Fast Ethernet 0/18 a la VLAN.

- ☑ Configure el *host* para utilizar la dirección IP, la máscara y el *gateway* predeterminado identificado en la tabla 6.10 de direccionamiento. En esta práctica, dicho *host* actuará como el servidor TFTP.
- ☑ Para verificar que el *host* y el *switch* estén configurados correctamente haga *ping* a la dirección IP del *switch* desde el *host*.

Nota: si el *ping* no fue exitoso, realice el diagnóstico de fallas en la configuración de los *hosts* y del *switch*.

Segunda Parte. Inicio y configuración del servidor TFTP

- ☑ El servidor TFTP utilizado en el desarrollo de esta práctica es el Solar Wind, disponible en www.solarwindssoftware.com/toolsets/tools/tftp-server.aspx, el cual debe iniciar en el servidor en el host mediante "Inicio" > "Todos los programas" > "SolarWinds 2003 Standard Edition" > "TFTP Server".
- ☑ El servidor debe iniciarse y obtener la dirección IP de la interfaz Ethernet, que utiliza el directorio C:\TFTP-Root predeterminado.
- ☑ Luego verifique que el servidor TFTP está en funcionamiento y que es posible hacer *ping* a éste desde el *switch*.
- ☑ Determine el nombre exacto del archivo de imagen que debe guardarse. Observe que si éste se encuentra en un subdirectorio (como en el resultado anterior), al principio no puede ver el nombre de archivo de IOS de Cisco. Para hacerlo, primero cambie el directorio activo del *switch* por el directorio IOS de Cisco.
- ☑ Una vez realizado el paso anterior, examine el resultado desde el *switch* y responda las siguientes preguntas:
  - ➲ ¿Cuáles son el nombre y la longitud de la imagen IOS de Cisco almacenados en la memoria *flash*?
  - ➲ ¿Qué atributos se pueden identificar a partir de los códigos en el nombre de archivo IOS Cisco?

Tercera Parte. Copiado del archivo de imagen en el servidor TFTP en modo EXEC privilegiado

- ☑ Verifique la transferencia al servidor TFTP observando el archivo de registro. Con el servidor TFTP Solar Wind, puede revisar la transferencia desde la ventana de comandos o desde el archivo de registro del servidor en C:\Archivos de programa\SolarWinds\2003 Standard Edition\TFTP-Server.log.
- ☑ Compruebe que el tamaño de la imagen flash se encuentre en el directorio raíz del servidor. La ruta de éste se muestra en la ventana de comandos del servidor: C:\TFTP-root.
- ☑ Utilice el "Administrador de archivos" para buscar este directorio en el servidor y observe el listado detallado del archivo. La longitud que muestra el comando "*show flash*" debe ser igual al tamaño del archivo almacenado en el servidor TFTP. Si los tamaños de archivo no son idénticos, consulte su proyecto.

Cuarta Parte. Restauración del archivo IOS de Cisco en el switch desde un servidor TFTP

- ☑ Verifique que el servidor TFTP esté activo y haga ping a la dirección IP del servidor TFTP desde el switch. Si no puede hacer ping, realice el diagnóstico de fallas de las configuraciones del switch y del servidor. Luego, responda las siguientes preguntas:
  - ➲ ¿Cuál es el nombre del archivo en el directorio raíz del servidor TFTP que se copiará al *switch*?
  - ➲ ¿Cuál es el nombre de ruta del destino para el archivo IOS en el *switch*?
  - ➲ ¿Cuál es la dirección IP del servidor TFTP?

Nota: es importante que este proceso no se interrumpa.

- ☑ En modo EXEC privilegiado copie el archivo desde el servidor TFTP a la memoria *flash* y responda la siguiente pregunta:
  - ➲ ¿El tamaño del archivo cargado es similar al tamaño del archivo guardado en el directorio raíz del TFTP?
- ☑ Verifique que la imagen del *switch* es correcta. Para hacer esto, cárguela nuevamente y observe el proceso de inicio.
- ☑ Confirme que no haya errores de *flash*; de ser así, entonces el *software* IOS de Cisco del *switch* se habrá iniciado correctamente. Para una verificación posterior de la imagen de IOS de Cisco en la memoria *flash* ejecute el comando que muestra la versión de IOS de Cisco.

Quinta Parte. Elaboración de una copia de respaldo y restauración de un archivo de configuración desde un servidor TFTP

- ☑ Verifique que el servidor TFTP esté en funcionamiento y que es posible hacer ping a éste desde el *switch* y guarde la configuración activa.
- ☑ Haga una copia de respaldo del archivo de configuración en el servidor TFTP.
- ☑ Compruebe la transferencia al servidor TFTP observando la ventana de comandos de éste.

El resultado debe ser similar a lo siguiente:

Received alswitch-confg from (172.17.99.11), 1452 bytes

- ☑ Verifique que el archivo "*alswitch-config*" se encuentre en el directorio C:\TFTP-root del servidor TFTP.

Sexta Parte. Restauración del archivo de configuración inicial desde el servidor TFTP

- ☑ Para restaurar el archivo de configuración inicial, primero borre el existente y luego vuelva a cargar el *switch*.
- ☑ Después, debe volver a establecer la conectividad entre el *switch* y el servidor TFTP antes de que la configuración pueda restaurarse; para ello, vuelva a configurar la VLAN 99 con la dirección IP correcta y asígnele un puerto Fast Ethernet 0/18 como se estableció en la primera parte.
- ☑ Después de que la VLAN 99 esté activa, verifique la conectividad haciendo ping al servidor desde el *switch*. Si éste no tiene éxito, realice el diagnóstico de fallas de las configuraciones del *switch* y del servidor.
- ☑ Restaure la configuración desde el servidor TFTP copiando el archivo "*alswitch-confg*" desde el servidor al *switch*.

Nota: es importante que este proceso no se interrumpa.

- ☑ En modo EXEC privilegiado cargue nuevamente el *router*. Después de hacerlo, el *switch* debe mostrar el indicador "*ALSwitch*".
- ☑ Analice la configuración activa para verificar que la configuración restaurada se encuentra completa, incluyendo las contraseñas "*enable secret*" y de *vty*.

Séptima Parte. Actualización del *software* del *switch* IOS de Cisco

En esta práctica se requiere una combinación de la imagen IOS de Cisco y del archivo HTML (tar) ubicados de manera predeterminada en el directorio del servidor TFTP. El lector debe descargarlo del centro de *software* Cisco Connection online.

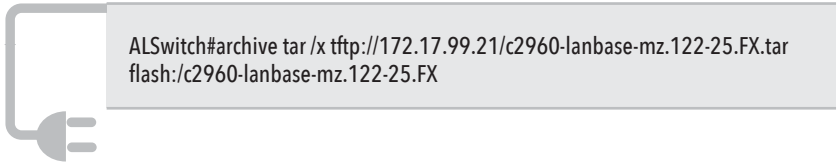
Aquí se hace referencia al archivo *c2960-lanbase-mz.122-25.FX.tar* para fines de instrucción solamente, el cual tiene la misma raíz de nombre de archivo que la imagen actual; sin embargo, suponga que éste es una actualización.

La actualización de versión del *software* IOS de Cisco incluye la imagen binaria y nuevos archivos HTML que admiten cambios en la interfaz web. Esta práctica también requiere que haya una copia guardada del archivo de configuración actual como respaldo; luego, lleve a cabo el siguiente procedimiento:

- ☑ Determine la secuencia de arranque actual del *switch* y verifique la disponibilidad de memoria.
- ☑ Establezca si hay suficiente memoria para múltiples archivos de imagen. Posteriormente, asuma que los nuevos archivos requieren tanto espacio como los archivos actuales en la memoria *flash*. Ahora, responda la siguiente pregunta:
- ☑ ¿Hay suficiente capacidad de memoria para almacenar archivos adicionales de Cisco y de HTML?

Octava Parte. Preparación para la nueva imagen

- ☑ Si el *switch* cuenta con suficiente memoria disponible como la que se describe en el último paso de la parte anterior, cambie el nombre del archivo IOS de Cisco para que tenga la extensión *.old*.
- ☑ Verifique que la asignación del nuevo nombre haya sido exitosa. Como medida de precaución deshabilite el acceso a las páginas HTML del *switch* y luego elimine los archivos HTML existentes de la memoria *flash*.
- ☑ Escriba lo siguiente, para ubicar la nueva imagen de IOS de Cisco y los archivos HTML en el directorio destino de la memoria *flash*:



- ☑ Vuelva a habilitar el servidor HTTP en el *switch*.

Introduzca el comando "*boot system*" con el nombre de archivo de la nueva imagen en la petición de entrada del modo de configuración; luego, guarde la configuración.

Novena Parte. Reinicio del *switch*

- ☑ Reinicie el switch por medio del comando "*reload*" para ver si el nuevo *software* IOS de Cisco se ha cargado.

Utilice el comando "*show version*" para ver el nombre del archivo IOS de Cisco. Luego, responda las siguientes preguntas:

- ➲ ¿Cuál es el nombre del archivo de IOS de Cisco desde el cual arrancó el *switch*?
- ➲ ¿Es éste el nombre de archivo correcto?

- ☑ Si el nombre de archivo IOS de Cisco es correcto, elimine el archivo de respaldo (con la extensión .old) de la memoria *flash*.

Décima Parte. Recuperación de las contraseñas en Catalyst 2960

Para reconfigurar la contraseña de consola cambie "*vty*" y "*enable secret*" del *switch*.

- ☑ Guarde los cambios en el archivo "*startup-config*" y vuelva a cargar el *switch*. Entonces, sin conocer las contraseñas, trate de acceder al modo EXEC privilegiado del *switch*.

Undécima Parte. Recuperación de las contraseñas en Catalyst 2960

Los procedimientos detallados para recuperar contraseñas se encuentran disponibles en la documentación de asistencia en línea de Cisco. En este caso, se pueden hallar en la sección de diagnóstico de fallas de la *Guía de configuración del software del switch* Catalyst 2960.

Siga los procedimientos para restaurar el acceso al *switch* y, al completarlos, desconéctese escribiendo "*exit*" y apague todos los dispositivos.

Cuestionario

6.2.1 Explique a detalle cómo crear y guardar una configuración básica de conmutador.

6.2.2 Establezca cómo se configurar un servidor TFTP en la red.

6.2.3 Explique a detalle cómo realizar una copia de respaldo del *software* IOS de Cisco en un servidor TFTP, para después restaurarlo.

6.2.4 Establezca cómo llevar a cabo una copia de respaldo de la configuración del conmutador (*switch*) a un servidor TFTP.

6.2.5 Establezca cómo configurar un conmutador (*switch*) para cargar una configuración desde un servidor TFTP.

6.2.6 Explique a detalle cómo actualizar el software IOS de Cisco desde un servidor TFTP.

6.2.7 Explique a detalle cómo recuperar la contraseña para un conmutador (*switch*) Cisco 2960 (serie 2900).

PRÁCTICA 6.3 Configuración básica inalámbrica para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Configurar opciones en la ficha de configuración inalámbrica de administración y de seguridad Linksys.
- ☑ Agregar conectividad inalámbrica a una computadora personal (PC).
- ☑ Probar la conectividad.

Introducción

La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa. WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales, y 5 o 13 dígitos alfanuméricos.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad, y debería estar activado como nivel de seguridad mínimo.

En esta actividad configurará un ***router*** Linksys inalámbrico permitiendo el acceso remoto tanto desde una PC, como desde la conectividad inalámbrica con seguridad WEP.

Procedimiento

Diagrama de topología

La figura 6.4 muestra la topología que debe configurar para realizar la práctica sugerida.

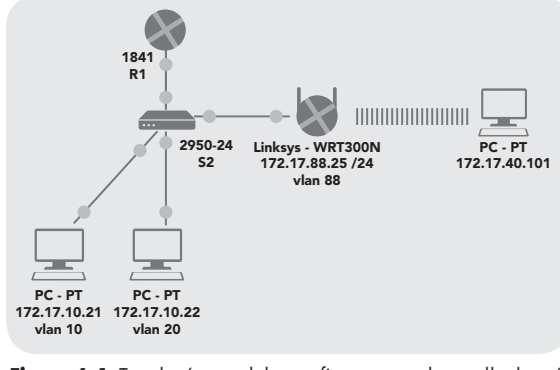


Figura 6.4 Topología que debe configurar para desarrollar la práctica

Primera Parte. Carga de las configuraciones de inicio

```
hostname R1
!
interface FastEthernet0/0
ip address 172.17.50.1 255.255.255.0
no shutdown
!
interface FastEthernet0/1
no ip address no shutdown
!
interface FastEthernet0/1,10
encapsulation dot1Q 10
ip address 172.17.10.1 255.255.255.0
!
interface FastEthernet0/1,20 encapsulation dot1Q 20
ip address 172.17.20.1 255.255.255.0
!
interface FastEthernet0/1,88
encapsulation dot1Q 88
ip address 172.17.88.1 255.255.255.0
!
```

Segunda Parte. Cargar las configuraciones de S2

Lleve a cabo las configuraciones de S2 mediante los siguientes códigos:

```
hostname S2
!
interface FastEthernet0/5
switchport trunk encapsulation dot1q switchport mode trunk
no shutdown
!
interface FastEthernet0/7
switchport access vlan 88 switchport mode access
no shutdown
!
interface FastEthernet0/11
switchport access vlan 10 switchport mode access
no shutdown
!
```

```
interface FastEthernet0/18
switchport access vlan 20 switchport mode access
no shutdown
!
```

Tercera Parte. Conexión e inicio de sesión en el *router* inalámbrico

- ☑ Para configurar los valores en el router inalámbrico se empleará su utilidad web *Graphical User Interface* (GUI). Puede accederse a ésta por medio de la dirección IP de LAN/inalámbrica del *router* con un navegador web. La dirección predeterminada es 192.168.1.1.
- ☑ Para establecer conectividad física utilice un cable de conexión directa desde la PC a uno de los puertos LAN del *router* inalámbrico. Éste proporcionará una dirección IP a la PC utilizando configuraciones DHCP predeterminadas.
- ☑ Abra un navegador web.
- ☑ Para navegar a la utilidad web del *router* inalámbrico establezca la URL del navegador en http://192.168.1.1. Las credenciales *login* predeterminadas son un nombre y una contraseña de usuario en blanco de "admin". Tenga presente que esto es muy inseguro, ya que es la configuración predeterminada de fábrica y se proporciona públicamente. Establezca su propia contraseña más adelante como medida inicial de administración y de seguridad de la topología propuesta.
- ☑ Para iniciar sesión, deje el nombre de usuario en blanco y establezca la contraseña como "admin".

Cuarta Parte. Configuración de opciones

Para establecer el tipo de conexión de Internet a IP estático tome en cuenta los siguientes puntos:

- ☑ De manera predeterminada, la página de inicio es la pantalla "*Setup*". En los menús superiores se encuentra la sección "Configuración" y debajo la ficha "Configuración básica".
- ☑ En la pantalla "Configuración" para el *router* Linksys ubique la opción "Tipo de conexión a Internet" en la sección "Configuración de Internet" de esta página. Haga clic en el menú desplegable y seleccione "IP estático" de la lista.
- ☑ Para configurar la dirección IP de VLAN 88, máscara de subred y el *gateway* predeterminado para WRS2 establezca la dirección IP de Internet en 172.17.88.25, la máscara de subred en 255.255.255.0 y el *gateway* predeterminado en 172.17.88.1.

Nota: por lo general en una red doméstica o una empresa pequeña esta dirección IP de Internet se asigna por el ISP mediante DHCP o PPPoE (los detalles específicos de PPPoE están fuera del ámbito de esta práctica).

Quinta Parte. Configuración de los parámetros IP del *router*

- ☑ En esta página desplácese hacia abajo a "Configuración de red" para los campos "IP de *router*"; luego, establezca la dirección IP en 172.17.40.1 y la máscara subred en 255.255.255.0.
- ☑ En "Configuración del Servidor DHCP" asegúrese de que éste se encuentre habilitado.
- ☑ Haga clic en el botón "Guardar configuración" en la parte inferior de la pantalla "Configuración". Tenga en cuenta que el rango de la dirección IP para el conjunto DHCP se ajusta a un rango de direcciones para coincidir con los parámetros IP del *router*. Estas direcciones se usan para clientes inalámbricos y clientes que se conectan al *switch* interno del *router* inalámbrico. Los clientes reciben una dirección y máscara IP y se les da la IP del *router* para que la utilicen como *gateway*.
- ☑ Una vez que se ha cambiado la dirección IP del *router* y el conjunto DHCP, se tendrá que reconectar utilizando la nueva dirección, configurada previamente; para ello se necesitará readquirir una dirección IP del *router* vía DHCP o establecer su propia dirección manualmente.
- ☑ Reconéctese a la configuración GUI del *router* utilizando una dirección IP de 172.17.88.1.

Sexta Parte. Configuración de opciones en la ficha inalámbrica Linksys

- ☑ Para establecer el nombre de la red (SSID) haga clic en la ficha "Inalámbrica".
- ☑ En "Nombre de red (SSID)" vuelva a nombrar la red desde "Predeterminada" a WRS_LAN.
- ☑ Haga clic en "Guardar configuraciones".
- ☑ Para establecer el modo de seguridad haga clic en "Seguridad inalámbrica", que está ubicada junto a "Configuraciones inalámbricas básicas" en la ficha principal "Inalámbrica".
- ☑ Cambie de "Modo de seguridad de desactivado" a "WEP".
- ☑ Usando la "Encriptación predeterminada" de 40/64-Bit establezca la "Clave1" en "1234567890".
- ☑ Haga clic en "Guardar configuraciones".

Séptima Parte. Configuración de opciones en la ficha de administración Linksys

- ☑ Para establecer la contraseña del *router* haga clic en la ficha "Administración".
- ☑ En "Acceso al *router*" cambie la contraseña a "Cisco123" e ingrese la misma contraseña para confirmar.
- ☑ En "Acceso remoto" habilite "Administración remota".
- ☑ Haga clic en "Guardar configuraciones".
- ☑ Puede que se le solicite que inicie sesión otra vez. Utilice la nueva contraseña "cisco123" y continúe manteniendo el nombre de usuario en blanco.

Octava Parte. Configuración de opciones en la ficha de seguridad Linksys

- ☑ De manera predeterminada, las peticiones a la interfaz LAN/Inalámbrica (172.17.40.1) de WRS2 desde fuentes en su interfaz WAN (por ejemplo PC1 y PC2) se bloquearán por razones de seguridad implementadas por el *router* inalámbrico. Con el propósito de verificar la conectividad en esta práctica, hay que permitirlas. Para ello, haga clic en la ficha "Seguridad".
- ☑ Luego, seleccione "Filtro de Internet" y desmarque "Filtrar solicitudes anónimas de Internet".

Novena Parte. Adición de conectividad inalámbrica a una PC

- ☑ Desconecte la conexión Ethernet desde la PC3 a WRS2.
- ☑ Utilice su versión instalada de Windows para conectarse al *router* inalámbrico:
  - ➲ Ubique el ícono de "Conexión a la red inalámbrica" en su barra de tareas o vaya a "Inicio" > "Panel de control" > "Conexiones de red".
  - ➲ Luego, seleccione "Conexión de red inalámbrica".
  - ➲ Navegue al menú "Archivo" y seleccione "Estado".
  - ➲ Haga clic en "Ver redes inalámbricas", localice "SSID WRS_LAN" en la lista de redes disponibles y conéctese a él.
  - ➲ Cuando se le solicite la clave WEP ingrese "1234567890", como se estableció anteriormente, y haga clic en "Conectar".
  - ➲ Para verificar la conexión, en la ventana "Estado" seleccione la ficha "Soporte".
  - ➲ Verifique que la PC3 haya recibido una dirección IP del conjunto de direcciones DHCP de WRS2 o que haya sido configurada manualmente.

La figura 6.5 muestra la pantalla que debe observar en el "Estado de Conexiones de red inalámbricas".

Figura 6.5 Estado de Conexiones de red inalámbricas

Cuestionario

6.3.1 Explique a detalle cómo configurar opciones en la ficha de configuración inalámbrica de administración y de seguridad Linksys.

6.3.2 Establezca el procedimiento para agregar conectividad inalámbrica a una computadora personal (PC).

6.3.3 Explique a detalle cómo se prueba la conectividad en un arreglo inalámbrico.

[5] En Informática, la difusión amplia, difusión ancha o broadcast, es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

PRÁCTICA 6.4 Configuración básica de una VLAN para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Cablear una red según el diagrama de la topología mostrada.
- ☑ Borrar la configuración inicial y volver a cargar un conmutador (*switch*) al estado predeterminado.
- ☑ Realizar las tareas de configuración básicas en un conmutador (*switch*).
- ☑ Asignar puertos de un conmutador (*switch*) a una VLAN.
- ☑ Verificar la configuración de la VLAN.
- ☑ Habilitar el enlace troncal en conexiones entre conmutadores (*switches*).

Introducción

Una red de área local virtual (VLAN, *Virtual Local Area Network*) es un grupo flexible de dispositivos que se encuentran en cualquier ubicación de una red de área local, pero que se comunican como si estuvieran en el mismo segmento físico. Con las VLAN se puede segmentar la red sin restringirse a las ubicaciones o conexiones físicas. Las ventajas que pueden aportar las VLAN son, entre muchas otras:

- ☑ Mayor flexibilidad y mejor gestión de recursos, al facilitar el cambio y el movimiento de los dispositivos en la red.
- ☑ Facilidad de localización y aislamiento de averías.
- ☑ Mejora en cuanto a seguridad, debido a la separación de dispositivos en distintas VLAN.
- ☑ Control de tráfico de *broadcast*.[5]
- ☑ Separación de protocolos.

Se pueden implementar atendiendo a diversos criterios como puertos de un conmutador (*switch*), a los que se conectan los ordenadores, direcciones MAC, etc.

Procedimiento

Diagrama de la configuración

La figura 6.6 muestra la topología que debe desarrollarse en esta práctica.

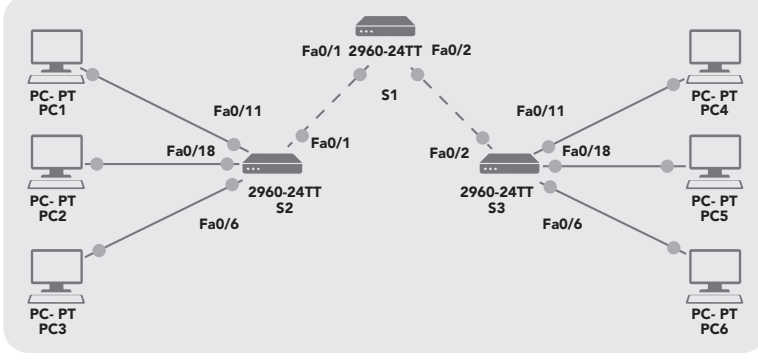


Figura 6.6 Diagrama de la topología a desarrollar durante la práctica

Por su parte, la tabla 6.12 muestra el direccionamiento que debe realizarse para la configuración de la figura 6.6.

Tabla 6.12 Direccionamiento para los dispositivos de la topología para la práctica

Dispositivo Nombre del *host*	Interfaz	Dirección IP	Máscara de subred	Puerta de salida predeterminada (*gateway*)
S1	VLAN56	192.168.56.11	255.255.255.0	No aplicable
S2	VLAN56	192.168.56.12	255.255.255.0	No aplicable
S3	VLAN56	192.168.56.13	255.255.255.0	No aplicable
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
PC4	NIC	192.168.10.24	255.255.255.0	192.168.10.1
PC5	NIC	192.168.20.25	255.255.255.0	192.168.20.1
PC6	NIC	192.168.30.26	255.255.255.0	192.168.30.1

Aplicaciones iniciales de puertos

La tabla 6.13 muestra las aplicaciones iniciales de los puertos utilizados en el desarrollo de la práctica.

Tabla 6.13 Aplicaciones iniciales de los puertos utilizados en el desarrollo de la práctica

Puertos	Asignación	Red
Fa0/1-0/5	Enlaces troncales 802.1q (VLAN 56 nativa)	192.168.56.0 /24
Fa0/6-0/10	VLAN 30: Guest (predeterminada)	192.168.30.0 /24
Fa0/11-0/17	VLAN 10: Cuerpo docente/personal	192.168.10.0 /24
Fa0/18-0/24	VLAN 20: Estudiantes	192.168.20.0 /24

Primera Parte. Preparación de la red

- ☑ Cablee una red de manera similar al diagrama de la topología.
- ☑ Borre configuraciones existentes en los *switches* e inicialice todos los puertos en estado desactivado.

Segunda Parte. Ajuste de las configuraciones básicas del *switch*

Configure los *switches* de acuerdo con la siguiente guía:

- ☑ Configure el nombre de *host* del *switch*
- ☑ Deshabilite la búsqueda DNS.
- ☑ Determine una contraseña de modo EXE, para ello utilice “clase”.

- ☑ Configure la contraseña "cisco" para las conexiones de consola y para las conexiones de *vty*.
- ☑ Vuelva a habilitar los puertos de usuario en S2 y S3.

Tercera Parte. Ajuste de las configuraciones básicas del *switch*

Configure los *switches* de acuerdo con la siguiente guía:

- ☑ Configure el nombre de *host* del *switch*.
- ☑ Deshabilite la búsqueda DNS.
- ☑ Determine una contraseña de modo EXE, para ello utilice "clase".
- ☑ Configure la contraseña "cisco" para las conexiones de consola y para las conexiones de *vty*.
- ☑ Vuelva a habilitar los puertos de usuario en S2 y S3.

Cuarta Parte. Configure y active las interfaces Ethernet

Configure las interfaces Ethernet de las seis PC con las direcciones IP y los gateways predeterminados desde la tabla 6.13 de direccionamiento.

Quinta Parte. Configuración de las VLAN en el *switch*

- ☑ Cree las VLAN en el *switch* S1.
- ☑ Configure, asigne un nombre y verifique las VLAN en los *switches* S2 y S3.
- ☑ Asigne puertos de *switch* a las VLAN en S2 y S3.
- ☑ Determine qué puertos se han añadido a la VLAN 10 en S2.
- ☑ Configure la VLAN 56 de administración en cada uno de los *switches*.
- ☑ Configure y verifique los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en los tres conmutadores *switches*.
- ☑ Cerciórese de que S1, S2 y S3 se pueden comunicar.
- ☑ Haga *ping* a varios *hosts* desde la PC2. ¿Cuál es el resultado?
- ☑ Ubique la PC1 en la misma VLAN que la PC2. ¿PC1 puede hacer ping satisfactoriamente a PC2?
- ☑ Asigne 192.168.20.22 como dirección IP de PC1. La máscara de subred y el *gateway* predeterminado pueden seguir siendo las mismas. ¿PC1 puede hacer ping satisfactoriamente a PC2?
- ☑ Una vez más haga *ping* desde el *host* PC2 al *host* PC1 utilizando la dirección IP recién asignada. ¿El intento de hacer *ping* fue exitoso?, ¿por qué?

Sexta Parte. Documentación de las configuraciones de los *switches*

En cada *switch* capture la configuración activa en un archivo de texto y consérvela para futuras referencias.

Séptima Parte. Limpieza

- ☑ Borre las configuraciones y vuelva a cargar los switches.
- ☑ Desconecte y guarde el cableado. En caso de PC hosts que están normalmente conectadas a otras redes (tales como la LAN de la organización o de Internet), vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Cuestionario

6.4.1 Explique cómo se borra la configuración inicial, y cómo se puede volver a cargar un conmutador (switch) al estado predeterminado.

6.4.2 Establezca como realizar las tareas de configuración básicas en un conmutador (*switch*).

6.4.3 Explique a detalle cómo se asignan los puertos de un conmutador (*switch*) a una VLAN.

6.4.4 Establezca cómo verificar la configuración de la VLAN en la realidad.

6.4.5 Explique a detalle cómo habilitar el enlace troncal en conexiones, entre conmutadores (*switches*).

PRÁCTICA 6.5

Configuración básica del protocolo VLAN *Trunking* (VTP) para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Crear las VLAN en el servidor VTP y distribuir la información de éstas a los *switches* en la red.
- ☑ Explicar las diferencias en operación entre el modo VTP transparente, el modo servidor y el modo cliente.
- ☑ Presentar de qué manera la depuración reduce el tráfico de *broadcast* innecesario en la LAN.

Introducción

El VLAN Trunk Protocol (VTP) reduce la administración en una red de conmutador (*switch*). Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los conmutadores (*switches*) del dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es un protocolo de propiedad de Cisco que está disponible en la mayoría de los productos de la serie Cisco Catalyst.

VTP es un protocolo de mensajería de capa 2, que mantiene la coherencia de la configuración de VLAN al administrar la adición, eliminación y/o cambio de nombre de VLAN, dentro de un dominio VTP. Un dominio VTP (también denominado dominio de gestión VLAN) está compuesto por uno o más dispositivos de red que comparten el mismo nombre de dominio VTP, y que están interconectados con los troncos. VTP minimiza las configuraciones erróneas y las inconsistencias de configuración que pueden resultar en una serie de problemas, como nombres de VLAN duplicados, especificaciones de tipo VLAN incorrectas, y ciertas violaciones de seguridad. Antes de crear una VLAN debe decidir si se desea utilizar VTP en una red. Con VTP, pueden realizarse cambios de configuración de forma centralizada en uno o más dispositivos de red, y hacer que dichos cambios se comuniquen automáticamente a todos los demás dispositivos de red, de la red.

Procedimiento

Diagrama de la topología

La figura 6.7 muestra el diagrama de la topología a desarrollar en la práctica.

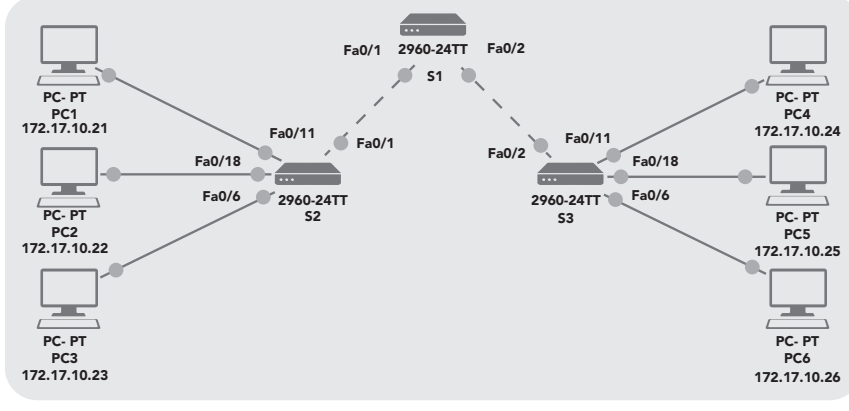


Figura 6.7. Diagrama de la topología utilizada en el desarrollo de la práctica

La tabla 6.14 muestra el direccionamiento que debe realizarse para la configuración de la figura 6.7.

Tabla 6.14 Direccionamiento para los dispositivos de la topología para la práctica

Dispositivo Nombre del *host*	Interfaz	Dirección IP	Máscara de subred	Puerta de salida predeterminada (*gateway*)
S1	VLAN99	172.17.99.11	255.255.255.0	No aplicable
S2	VLAN99	172.17.99.12	255.255.255.0	No aplicable
S3	VLAN99	172.17.99.13	255.255.255.0	No aplicable
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Aplicaciones iniciales de puertos

La tabla 6.15 muestra las aplicaciones iniciales de los equipos utilizados en el desarrollo de la práctica.

Tabla 6.15 Aplicaciones iniciales de los equipos utilizados en el desarrollo de la práctica

Puertos	Asignación	Red
Fa0/1-0/5	Enlaces troncales 802.1q (VLAN 56 nativa)	192.168.56.0 /24
Fa0/6-0/10	VLAN 30: Guest (predeterminada)	192.168.30.0 /24
Fa0/11-0/17	VLAN 10: Cuerpo docente/personal	192.168.10.0 /24
Fa0/18-0/24	VLAN 20: Estudiantes	192.168.20.0 /24

Nota: se puede utilizar cualquier *switch* actual en su práctica, siempre y cuando éste tenga las interfaces necesarias que se presentan en la topología. El resultado que se muestra en esta práctica está basado en los *switches* de la serie y familia 2960 de Cisco Sys. El uso de cualquier otro tipo de *switch* puede producir resultados distintos. Si va a usar *switches* más antiguos, algunos comandos pueden ser diferentes o ya no estar disponibles.

Primera Parte. Preparación de la red

- ☑ Cablee una red de manera similar al diagrama de la topología mostrada en la figura 6.7.
- ☑ Observe en la tabla 6.14 de direccionamiento de las PC que se han configurado con una dirección de IP predeterminada del gateway, la cual sería la del *router* local que no se incluye en este escenario de la práctica.
- ☑ El *gateway* predeterminado del router será necesario para las PC en diferentes VLAN para poder comunicarse. Establezca conexiones de consola en los tres *switches*.
- ☑ Borre toda configuración existente en los *switches*.
- ☑ Utilice el comando "*show vlan*" para verificar que sólo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN1:

```
S1#show vlan
Nombre de la VLAN                Estado              Puertos
–
1    default                     active              Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                     Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                     Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                     Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                     Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                     Gig1/1, Gig1/2
1002 fddi-default                active
1003 token-ring-default          active
1004 fddinet-default             active
1005 trnet-default               active
```

- ☑ Deshabilite todos los puertos con el comando "*shutdown*".

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown
S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown
S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

- ☑ Vuelva a habilitar los puertos de usuario en S2 y S3.
- ☑ Configure los puertos de usuario en modo de acceso y consulte el diagrama de topología para determinar cuáles puertos están conectados a dispositivos de usuario final.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S3(config)#interface fa0/6
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/11
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
S3(config-if)#interface fa0/18
S3(config-if)#switchport mode access
S3(config-if)#no shutdown
```

Segunda Parte. Realización de las configuraciones básicas del *switch*

- ☑ Configure los *switches* S1, S2 y S3 según las siguientes pautas y guarde todas sus configuraciones:
  - ➔ Configure el nombre de *host* del *switch* según lo indicado en la topología.
  - ➔ Deshabilite la búsqueda DNS.
  - ➔ Ajuste una contraseña de modo EXEC como "*class*".
  - ➔ Configure la contraseña "cisco" para las conexiones de consola.
  - ➔ Establezca la contraseña "cisco" para las conexiones de vty. A continuación, se muestran los resultados para S1:

```
Switch>enable

Switch#configure terminal
Enter configuration commands, one per line. Finalice con CNTL/Z. Switch(config)#hostname
S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
```

```
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]? Building configuration...
[OK]
```

Tercera Parte. Configuración de las interfaces Ethernet en las PC *Host*

- ☑ Configure las interfaces Ethernet de PC1, PC2, PC3, PC4, PC5 y PC6 con las direcciones IP y los *gateways* predeterminados que se indican en la tabla 6.14.
- ☑ Verifique que la PC1 pueda hacer *ping* a PC4, que la PC2 pueda hacer *ping* a la PC5 y que la PC3 pueda hacer ping a la PC6.

Cuarta Parte. Configuración VTP en los *switches*

VTP permite al administrador de redes controlar las instancias de las VLAN en la red creando dominios VTP, dentro de los cuales se configuran uno o más *switches* con servidores VTP.

Las VLAN se crean en el servidor VTP e informan a los otros *switches* en el dominio. Las tareas comunes de configuración VTP son la configuración del modo operativo, del dominio y de la contraseña.

A continuación, se utilizará S1 como el servidor VTP, con S2 y S3 configurados como clientes o en el modo transparente de VTP.

- ☑ Verifique las configuraciones VTP actuales en los tres switches:

```
S1#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode               : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest                      : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

```
S2#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally: 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest: 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD Configuration last modified by
0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S3#show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally: 255
Number of existing VLANs        : 5
VTP Operating Mode              : Servidor
VTP Domain Name                 :
VTP Pruning Mode                : Deshabilitado
VTP V2 Mode                     : Deshabilitado
VTP Traps Generation            : Deshabilitado
MD5 digest: 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

☑ Observe que los tres *switches* se encuentran en modo servidor, que es el modo VTP predeterminado para la mayoría de los *switches* Catalyst.

Quinta Parte. Configuración del modo operativo, el nombre de dominio y la contraseña de VTP en los tres *switches*

☑ Establezca "Lab4" como nombre de dominio VTP y "cisco" como contraseña en los tres *switches*. Configure S1 en modo servidor, S2 en modo cliente y S3 en modo transparente por medio de los siguientes comandos:

Tabla 6.16 Direccionamiento para los dispositivos de la topología para la práctica	
Comando	**Descripción**
S1(config)#vtp mode server	Configurar el dispositivo en modo servidor VTP
S1(config)#vtp domain Lab4	Cambiar el nombre del dominio VTP de NULL a "Lab4"
S1(config)#vtp password cisco	Configurar la contraseña de la base de datos VLAN del dispositivo en "cisco"
S1(config)#end	S1(config)#end
	Término
S2(config)#vtp mode client	Configurar el dispositivo en modo CLIENTE VTP
S2(config)#vtp domain Lab4	Cambiar el nombre del dominio VTP de NULL a Lab4
S2(config)#vtp password cisco	Configurar la contraseña de la base de datos VLAN del dispositivo en "cisco"
S2(config)#end	Término
S3(config)#vtp mode transparent	Configurar el dispositivo en modo TRANPARENT VTP
S3(config)#vtp domain Lab4	Cambiar el nombre del dominio VTP de NULL a Lab4
S3(config)#vtp password cisco	Configurar la contraseña de la base de datos VLAN del dispositivo en "cisco"
S3(config)#end	Término

Nota: el nombre del dominio VTP puede ser aprendido por un *switch* de cliente desde uno de los servidores, pero solamente si el dominio del *switch* de cliente se encuentra en estado nulo. No puede aprender un nombre nuevo si un nombre fue establecido anteriormente; por esta razón, es una buena práctica configurar el nombre de dominio manualmente en todos los *switches* para asegurar que sea configurado correctamente. Los switches en diferentes dominios VTP no intercambian información de VLAN.

- ☑ Configure los enlaces troncales y la VLAN nativa para los puertos de enlace troncales en los tres switches.
- ☑ Simplifique esta tarea con el comando interface "range" en el modo de configuración global:

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
```

```
S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

- ☑ Configure la seguridad de puerto en los *switches* de la capa de acceso S2 y S3.
- ☑ Ajuste los puertos fa0/6, fa0/11 y fa0/18 de modo tal que sólo permitan un solo *host* y se aprenda la dirección MAC de éste de manera dinámica.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end

S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Sexta Parte. Configuración de las VLAN en el servidor VTP

Hay cuatro VLAN adicionales que se requieren en esta práctica:

- VLAN 99 (administración).
- VLAN 10 (cuerpo docente/personal).
- VLAN 20 (estudiantes).
- VLAN 30 (guest).

☑ Configúrelas en el servidor VTP

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

☑ Verifique que se hayan creado las VLAN en S1 con el comando "*show vlan brief*".

☑ Utilice nuevamente el comando "*show vlan brief*" en S2 y S3 para determinar si el servidor VTP ha pulsado su configuración VLAN a todos los *switches*.

```
S2#show vlan brief

Nombre de la VLAN                Estado    Puertos
–
1    default                     active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                                   Gig0/2
10   faculty-staff               active
20   token-ring-default          active
30   fddinet-default             active
99   trnet-default               active
```

```
S3#show vlan brief
Nombre de la VLAN                Estado          Puertos
–
1       default                  active          Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                                 Gig0/2
1002    fddi-default             act/unsup
1003    token-ring-default       act/unsup
1004    fddinet-default          act/unsup
1005    trnet-default            act/unsup
```

- ☑ Responda las siguientes preguntas:
  - ➔ ¿Están configuradas las mismas VLAN en todos los *switches*?
  - ➔ Explique por qué S2 y S3 tienen diferentes configuraciones de VLAN en este momento.
- ☑ Cree una nueva VLAN en los *switches* 2 y 3:

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.
S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

Por qué no se permite crear una nueva VLAN en S2, pero sí en S3?

- ☑ Borre la VLAN 88 de S3:

```
S3(config)#no vlan 88
```

- ☑ Para configurar las VLAN en forma manual ajuste las cuatro VLAN identificadas anteriormente en el *switch* S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
```

```
S3(config)#vlan 10
S3(config-vlan)#name faculty/staff
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name students
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name guest
S3(config-vlan)#exit
```

Aquí se aprecia una de las ventajas del VTP. La configuración manual es tediosa y puede suscitar fallas, por lo que cualquier error introducido aquí puede evitar la comunicación entre VLAN. Además, puede resultar difícil diagnosticar este tipo de problemas.

- ☑ Configure la dirección de la interfaz de administración en los tres switches:

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

- ☑ Verifique que todos los *switches* estén correctamente configurados haciendo *ping* entre ellos: desde S1 haga *ping* a la interfaz de administración en S2 y S3. Desde S2 haga *ping* a la interfaz de administración en S3.
- ☑ ¿Los *pings* son exitosos? De no ser así realice el diagnóstico de fallas de las configuraciones de los *switches* e inténtelo nuevamente.

Séptima Parte. Asignación de puertos de switch a las VLAN

- ☑ Consulte la tabla 6.15 para asignar puertos a las VLAN.
- ☑ Simplifique esta tarea con el comando "*interface range*".
- ☑ Las asignaciones de puertos no se configuran a través del VTP, sino que deben ser configuradas en cada *switch* manual o dinámicamente utilizando un servidor VMPS. Los comandos sólo se muestran para S3, pero los *switches* S2 y S1 deben ser configurados de manera similar. Cuando termine, guarde la configuración.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#end
S3#copy running-config startup-config Destination filename [startup-config]? [intro] Building configuration
[OK] S3#
```

Octava Parte. Configuración de la depuración VTP en los *switches*

La depuración VTP permite a un servidor VTP suprimir tráfico de *broadcast* IP para VLAN específicas a *switches* que no tienen ningún puerto en esa VLAN. De manera predeterminada, todos los *multicasts* y *broadcasts* en una VLAN se saturan en toda la VLAN. Todos los *switches* en la red reciben todos los *broadcasts*, incluso en situaciones en las que unos pocos usuarios están conectados a ésta. La depuración del VTP se utiliza para eliminar o depurar este tráfico innecesario y para ahorrar banda ancha LAN porque los *broadcasts* no tienen que ser enviados a los *switches* que no los necesitan.

La depuración se establece en el *switch* del servidor mediante el comando "*vtp pruning*" en modo de configuración global. La configuración se dirige a los *switches* de clientes; sin embargo, puesto que S3 está en modo transparente, la depuración de VTP debe configurarse localmente en ese *switch*.

☑ Confirme la configuración de depuración VTP en cada *switch* utilizando el comando "*show vtp status*":

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 17
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Servidor
VTP Domain Name                 : Lab4
VTP Pruning Mode                : Habilitado
```

Novena Parte. Limpieza

Borre las configuraciones y vuelva a cargar los *switches*. En caso de PC *hosts* que están normalmente conectadas a otras redes (como la LAN de una organización o de Internet), vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Cuestionario

6.5.1 Explicar a detalle cómo crear las VLAN en el servidor VTP, y cómo distribuir la información de éstas, a los conmutadores (*switches*) en la red.

6.5.2 Establezca ejemplos de uso exitosos de dicha creación de VPN en el servidor de red.

6.5.3 Explicar a detalle las diferencias en operación entre el modo VTP transparente, el modo servidor y el modo cliente.

6.5.4 Establezca ejemplos de uso de cada uno de ellos.

6.5.5 Establezca cómo presentar la depuración que reduce el tráfico de *broadcast* innecesario en la LAN.

6.5.6 Proporcione ejemplos de uso exitosos de dicha depuración.

PRÁCTICA 6.6 Enrutamiento inter VLAN para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Llevar a cabo las tareas básicas de configuración en una LAN conmutada y un *router*.
- ☑ Configurar las VLAN y el protocolo VLAN Trunking (VTP) en todos los *switches*.
- ☑ Configurar un *router* para admitir el enlace 802.1q en una interfaz Fast Ethernet o con subinterfaces que correspondan a las VLAN configuradas.

Introducción

El enrutamiento tradicional requiere de ruteadores (*routers*), que tengan interfaces físicas múltiples, para facilitar el enrutamiento inter VLAN. El ruteador realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz está configurada con una dirección IP para la subred asociada con la VLAN conectada a ésta. Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN, pueden comunicarse con el ruteador utilizando la interfaz física conectada a la misma VLAN. En esta configuración, los dispositivos de red pueden utilizar el ruteador como una pasarela (*gateway*), para acceder a los dispositivos conectados a las otras VLAN.

Un dominio VTP (también denominado dominio de gestión VLAN) está compuesto por uno o más dispositivos de red interconectados que comparten el mismo nombre de dominio VTP. Un dispositivo de red se puede configurar para que esté en uno y sólo un dominio VTP. Realiza cambios de configuración de VLAN globales para el dominio utilizando la interfaz de línea de comandos (CLI), o el protocolo SNMP (*Simple Network Management Protocol*).

El modo de servidor VTP es el predeterminado, y el conmutador se encuentra en el estado de dominio sin administración, hasta que recibe un anuncio para un dominio a través de un enlace troncal o configura un dominio de administración. Si el conmutador recibe un anuncio de VTP sobre un enlace troncal, hereda el nombre de dominio de administración y el número de revisión de configuración de VTP. El modificador ignora los anuncios con un nombre de dominio de administración diferente, o un número de revisión de configuración anterior.

Procedimiento

Diagrama de la topología

Desarrolle la topología inter VLAN mostrada en la figura 6.8.

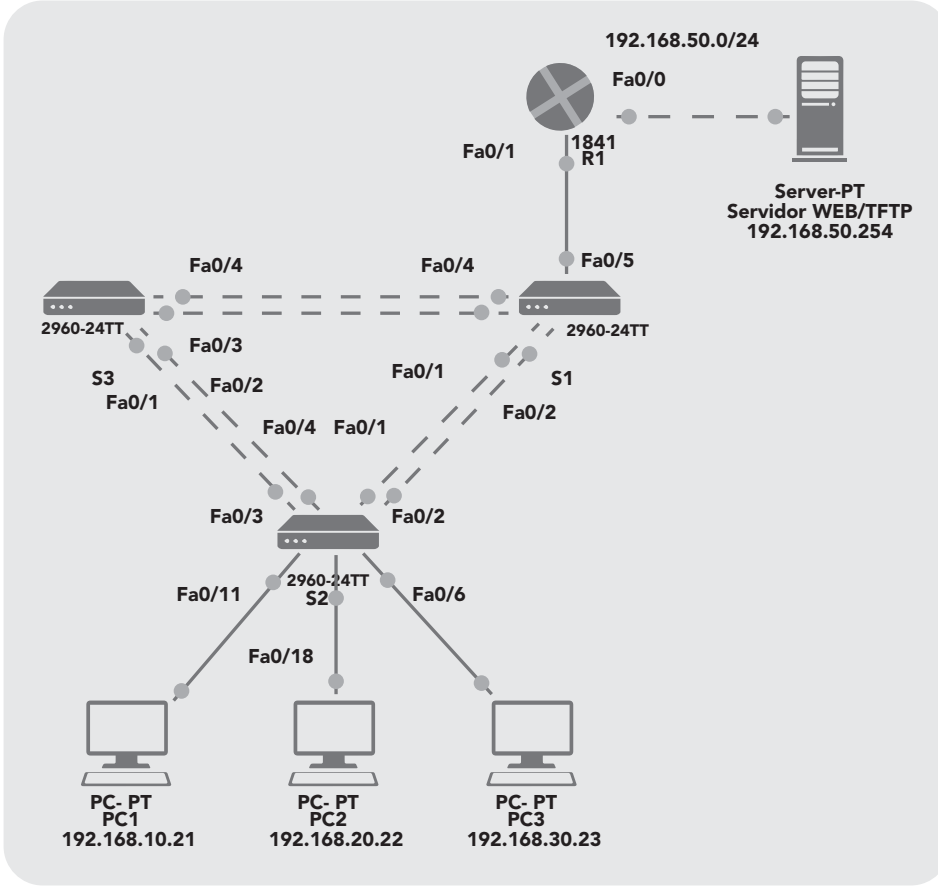


Figura 6.8 Topología inter VLAN para el desarrollo de la práctica

Por su parte, la tabla 6.17 muestra el direccionamiento de los equipos requeridos para la realización de la práctica.

Tabla 6.17 Configuración y direccionamiento de los equipos

Dispositivo Nombre del *host*	Interfaz	Dirección IP	Máscara de subred	Puerta de salida predeterminada (*gateway*)
S1	VLAN99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN99	192.168.99.13	255.255.255.0	192.168.99.1
R1	Fa 0/0	192.168.50.1	255.255.255.0	No aplicable
R2	Fa 0/1	Ver tabla de configuración de subinterfaz	Ver tabla de configuración de subinterfaz	No aplicable

continúa

PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.10.23	255.255.255.0	192.168.30.1
Servidor	NIC	192.168.50.254	255.255.255.0	192.168.50.1

Además, la tabla 6.18 muestra las asignaciones para configurar y conectar el puerto para el conmutador 2.

Tabla 6.18 Asignaciones para configurar y conectar el puerto para el *switch 2*

Puertos	Asignación	Red
Fa0/1-0/4	Enlaces troncales 802.1q (LAN 99 nativa)	192.168.99.0 /24
Fa0/5-0/10	VLAN 30: Sales	192.168.30.0 /24
Fa0/11-0/17	VLAN 10: R&D	192.168.10.0 /24
Fa0/18-0/24	VLAN 20: Engineering	192.168.20.0 /24

Por otro lado, la tabla 6.19 muestra la configuración para hacer la conexión del *router* 1 en la topología de red propuesta para la práctica.

Tabla 6.19 Configuración para hacer la conexión del *router* 1 en la topología de red

Interfaz del *router*	Asignación	Dirección IP
Fa0/0,1	VLAN 1	192.168.1.1
Fa0/0,10	VLAN 10	192.168.10.1
Fa0/0,20	VLAN 20	192.168.20.1
Fa0/0,30	VLAN 30	192.168.30.1
Fa0/0,99	VLAN 99	192.168.99.1

Nota: el resultado que se muestra en esta práctica se encuentra basado en los *switches* de la familia 2960 y en un *router* de la familia 1841. Puede utilizarse cualquier *switch* actual, siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de la topología ya mencionada. El uso de cualquier otro tipo de dispositivo posiblemente produzca resultados distintos.

Se debe observar que las interfaces LAN (10Mb) en los *routers* no admiten enlaces troncales y el *software* IOS de Cisco anterior a la versión 12.3 tal vez no admita enlaces troncales en interfaces de *router* Fast Ethernet.

Primera Parte. Preparación de la red

- ☑ Cablee una red de manera similar al diagrama de la topología mostrado en la figura 6.8.
- ☑ Establezca conexiones de consola en los tres *switches* y en el *router*.
- ☑ Borre la NVRAM y el archivo "*vlan.dat*" y reinicie los *switches*. Después de que la recarga se haya completado, utilice el comando "*show vlan*" para verificar que sólo existan VLAN predeterminadas y que todos los puertos se asignen a la VLAN 1.
- ☑ Deshabilite todos los puertos usando el comando "*shutdown*".
- ☑ Asegúrese de que los estados del puerto de switch estén inactivos deshabilitando todos los puertos. Simplifique esta tarea con el comando "*interface range*".

Segunda Parte. Rehabilitación de los puertos de usuario activos en S2 en el modo de acceso

Habilite los puertos Fa0/6, Fa0/11 y Fa0/18 en S2 usando el comando no "shutdown" y configúrelos como puertos de acceso.

Tercera Parte. Realización de las configuraciones básicas del *switch*

Configure los *switches* S1, S2 y S3 según los valores establecidos en la tabla 6.16 y de acuerdo con las siguientes pautas:

- ☑ Configure el nombre de *host* del *switch*.
- ☑ Deshabilite la búsqueda DNS.
- ☑ Configure una contraseña de modo EXEC: "*class*".
- ☑ Establezca la contraseña "cisco" para las conexiones de consola y para las conexiones de *vty*.
- ☑ Determine el *gateway* predeterminado en cada *switch*.

Cuarta Parte. Configuración de las interfaces Ethernet en el servidor y las PC Host

- ☑ Configure las interfaces Ethernet de PC1, PC2, PC3 y el Servidor TFTP/*Web remote* con las direcciones IP de la tabla 6.16.
- ☑ Conecte estos dispositivos utilizando los cables e interfaces correctos.

Quinta Parte. Configuración VTP en los *switches*

Utilice los valores de la tabla 6.20 para configurar los *switches*. Recuerde que las contraseñas y los nombres de dominios VTP distinguen entre letras mayúsculas y minúsculas.

Tabla 6.20 Configuración VTP de los *switches*			
Nombre del *switch*	**Modo de operación VTF**	**Dominio del VTP**	**Contraseña de VTP**
S1	Servidor	Lab6	Cisco
S2	Cliente	Lab6	Cisco
S3	Cliente	Lab6	Cisco

Sexta Parte. Configuración de los puertos de enlace troncales y designación de la VLAN nativa para estos

- ☑ Configure Fa0/1 a Fa0/5 como puertos de enlace y designe la VLAN 99 como la VLAN nativa para los enlaces troncales. Simplifique esta tarea con el comando "*interface range*" en el modo de configuración global.
- ☑ Posteriormente, configure las siguientes VLAN en el Servidor VTP, tal como se muestran en la tabla 6.21.

Tabla 6.21 Configuración de VLAN en el servidor VTP	
VLAN	**Nombre de la VLAN**
VLAN 99	Administración
VLAN 10	R & D
VLAN 20	Ingeniería
VLAN 30	Ventas

- ☑ Verifique que se hayan creado las VLAN en S1 con el comando "*show vlan brief*".
- ☑ Cerciórese de que las VLAN creadas en S1 se hayan distribuido a S2 y S3 adecuadamente; para ello use el comando "*show vlan brief*" en S2 y S3.

Séptima Parte. Configuración de la dirección de la interfaz de administración en los tres *switches*

- ☑ Consulte la tabla 6.16 para asignar la dirección IP de administración en los tres *switches*.
- ☑ Verifique que todos los *switches* estén correctamente configurados haciendo *ping* entre ellos. Desde S1 haga *ping* a la interfaz de administración en S2 y S3; desde S2 haga *ping* a la interfaz de administración en S3.
- ☑ En caso de que los *pings* no sean exitosos realice el diagnóstico de fallas de las configuraciones de los *switches* y solucione el problema.

Octava Parte. Asignación de puertos de *switch* a las VLAN en S2

- ☑ Consulte la tabla 6.16 para asignar puertos a las VLAN.
- ☑ Luego abra las ventanas de comandos en los tres *hosts* conectados a S2.
- ☑ Haga *ping* desde la PC1 (192.168.10.21) a la PC2 (192.168.20.22) y desde la PC2 a la PC3 (192.168.30.23).
- ☑ ¿Los *pings* fueron exitosos? De no ser así, ¿por qué fallaron?

Novena Parte. Configuración del *router*

- ☑ Borre la configuración en el *router* y vuelva a cargarla.
- ☑ Configure el router con el nombre de *host* R1.
- ☑ Deshabilite la búsqueda DNS.
- ☑ Configure una contraseña de modo EXEC: "*class*".
- ☑ Establezca la contraseña "cisco" para las conexiones de consola y de *vty*.

Décima Parte. Configuración de la interfaz de enlaces troncales en R1

- ☑ Configure la interfaz Fa0/1 en R1 con cinco subinterfaces, una para cada VLAN identificada en la tabla 6.18. Configúrelas con encapsulamiento dot1q y utilice la primera dirección en cada subred de VLAN en la interfaz del *router*.
- ☑ Especifique la VLAN 99 como la VLAN nativa en su subinterfaz. No asigne una dirección IP a la interfaz física, pero asegúrese de habilitarla.
- ☑ Documente sus subinterfaces y sus respectivas direcciones IP en la tabla de subinterfaces.

Undécima Parte. Configuración de la interfaz de servidor LAN en R1

Consulte la tabla 6.18 y configure Fa0/0 con la dirección IP y máscara correctas.

Duodécima Parte. Verificación de la configuración de enrutamiento

En este momento debe haber seis redes configuradas en R1. Verifique que pueda enrutar paquetes a las seis redes viendo la tabla de enrutamiento en R1. Si ésta no muestra las seis redes, realice el diagnóstico de fallas de su configuración y resuelva el problema antes de proceder.

Decimotercera Parte. Verificación del enrutamiento entre las VLAN

Desde la PC1 verifique que pueda hacer *ping* en el servidor remoto (192.168.50.254) y en los otros dos *hosts* (192.168.20.22 and 192.168.30.23). Puede que tome un par de pings antes de que se establezca la ruta de extremo a extremo.

Si los *pings* no son exitosos, haga el diagnóstico de fallas de su configuración. Verifique que los *gateways* predeterminados se han establecido en todas las PC y en todos los *switches*. Si alguno de los *hosts* ha entrado en hibernación, la interfaz conectada puede desactivarse.

En este momento usted puede hacer *ping* a cualquier nodo en cualquiera de las seis redes configuradas en su LAN, incluyendo las interfaces del *switch* de administración.

Decimocuarta Parte. Limpieza

- ☑ Borre las configuraciones y vuelva a cargar los *switches*.
- ☑ Desconecte y guarde el cableado. En caso de PC *hosts* que están normalmente conectadas a otras redes (tales como la LAN de la escuela o de Internet), vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Cuestionario

6.6.1 Explique a detalle, cómo llevar a cabo las tareas básicas de configuración en una LAN conmutada y un ruteador.

6.6.2 Establezca cómo se configuran las VLAN, y el protocolo VLAN *Trunking* (VTP) en todos los conmutadores (*switches*).

6.6.3 Explique a detalle cómo configurar un ruteador para admitir el enlace 802.1q, en una interfaz *Fast Ethernet*, o con subinterfases que correspondan a las VLAN configuradas.

PRÁCTICA 6.7

Protocolo *Spanning Tree* para transmitir datos utilizando Packet Tracer 7.0 de Cisco Systems

Objetivos de aprendizaje

- ☑ Borrar la configuración de inicio y volver a cargar la configuración predeterminada configurando un *switch* al estado inicial.
- ☑ Observar y explicar el comportamiento predeterminado del protocolo *Spanning Tree* (STP, 802.1D).
- ☑ Explicar las limitaciones de 802.1D STP para soportar la continuidad de servicio.
- ☑ Observar las mejoras ofrecidas por *Rapad STP.*

Introducción

S*panning Tree Protocol* (STP) es un protocolo de capa 2 que se ejecuta en los puentes (*bridges*) y en los conmutadores (*switches*). La especificación para STP es IEEE 802.1D. El propósito principal de STP es garantizar que no se creen ciclos anidados (*loops*) cuando se tengan trayectorias redundantes en la red. Los ciclos redundantes (*loops*) son fatales para una red.

Hay diferentes tipos de STP, pero 802.1D es el más popular, y el que más se ha implementado. Se implementa STP en los puentes (*bridges*) y en los conmutadores (*switches*) para prevenir los ciclos anidados (*loops*) en la red. Debe utilizarse STP en situaciones donde se deseen enlaces redundantes, pero no ciclos anidados (*loops*). Los enlaces redundantes (*links*) son tan importantes como los de respaldo, en el caso de una falla severa en una red. Una falla en un enlace primario activa los enlaces de respaldo, para que los usuarios puedan continuar utilizando la red. Sin STP en los puentes (*bridges*) y los conmutadores (*switches*), dicha falla podría generar un ciclo anidado (*loop*). Si dos conmutadores (*switches*) conectados ejecutan diferentes tipos de STP, requieren diferentes tiempos (*timings*) para la convergencia. El uso de diferentes tipos en los conmutadores (*switches*) crea problemas de temporización (*timing*) entre los estados de Bloqueo y Reenvío. Por lo tanto, se recomienda utilizar los mismos tipos de STP.

Procedimiento

Diagrama de la topología

Desarrolle la topología que se presenta en la figura 6.9 y que hace referencia al protocolo *Spanning Tree*.

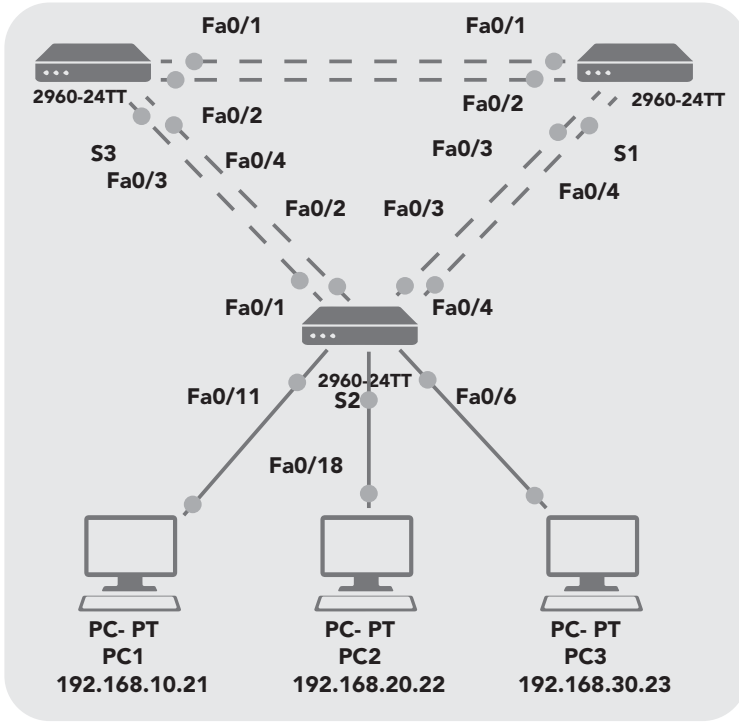


Figura 6.9 Topología que muestra la configuración al protocolo *Spanning Tree*

Por otro lado, la tabla 6.22 muestra el direccionamiento de los dispositivos que se establecen en la figura 6.9.

Tabla 6.22 Direccionamiento de los dispositivos

Dispositivo Nombre del *host*	Interfaz	Dirección IP	Máscara de subred	Puerta de salida predeterminada (*gateway*)
S1	VLAN99	172.17.99.11	255.255.255.0	No aplica
S2	VLAN99	172.17.99.12	255.255.255.0	No aplica
S3	VLAN99	172.17.99.13	255.255.255.0	No aplica
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.12
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.12
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.12

Además, la tabla 6.23 muestra las asignaciones para configurar y conectar el puerto para el *switch* 2.

Tabla 6.23 Asignaciones para configurar y conectar el puerto para el *switch 2*		
Puertos	**Asignación**	**Red**
Fa0/1-0/4	Enlaces troncales 802.1q (LAN 99 nativa)	172.17.99.0 /24
Fa0/5-0/10	VLAN 30: Guest (pre-determinada)	172.17.30.0 /24
Fa0/11-0/17	VLAN 10: Cuerpo docente/personal	172.17.10.0 /24
Fa0/18-0/24	VLAN 20: Estudiantes	172.17.20.0 /24

Nota: puede utilizar cualquier *switch* actual en su práctica, siempre y cuando éste tenga las interfaces necesarias que se muestran en el diagrama de la topología de la figura 6.7.

El resultado que se muestra en esta práctica está basado en los *switches* de la familia 2960. El uso de cualquier otro modelo puede producir resultados distintos. Establezca conexiones de consola en los tres *switches*.

Primera Parte. Preparación de la red

- ☑ Cablee una red de manera similar al diagrama de la topología de la figura 6.7.
- ☑ Borre la NVRAM, así como archivo "vlan.dat", y reinicie los *switches*. Después de que la recarga se haya completado, utilice el comando privilegiado EXEC "*show vlan*" para verificar que sólo existan VLAN predeterminadas y que todos los puertos se asignen a VLAN 1.

```
S1#show vlan

Nombre de la VLAN                Estado    Puertos
1    default                     active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
1002 fddi-default                active
1003 token-ring-default          active
1004 fddinet-default             active
1005 trnet-default               active
```

- ☑ Asegúrese de que los estados del puerto de switch estén inactivos con el comando "shutdown" o simplifique esta tarea con el comando "*interface range*":

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown
S2(config)#interface range fa0/1-24
S2(config-if-range)#shutdown
S2(config-if-range)#interface range gi0/1-2
S2(config-if-range)#shutdown
S3(config)#interface range fa0/1-24
S3(config-if-range)#shutdown
S3(config-if-range)#interface range gi0/1-2
S3(config-if-range)#shutdown
```

Segunda Parte. Rehabilitación de los puertos de usuario en S2 en modo de acceso

Consulte el diagrama de topología para determinar qué puertos de *switch* en S2 están activados para acceso por el dispositivo de usuario final. Estos se configurarán para modo de acceso y se habilitarán con el comando "*no shutdown*".

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
```

Tercera Parte. Configuraciones básicas del *switch*

Configure los *switches* S1, S2 y S3 según las siguientes pautas:

- ☑ Configure el nombre de *host* del *switch*.
- ☑ Deshabilite la búsqueda DNS.
- ☑ Configure una contraseña de modo EXEC: "*class*".
- ☑ Establezca la contraseña "cisco" para las conexiones de consola y para las conexiones de *vty*.

A continuación, se muestran los resultados para S1. Ingrese los comandos de configuración, uno por línea y finalice con CTRL+Z.

```
Switch>enable
Switch#configure terminal
Switch(config)# hostname S1
S1(config)#enable secret class
```

```
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Buildin configuration
[OK]
```

Cuarta Parte. Configuración de las PC *host*

Configure las interfaces Ethernet para PC1, PC2 y PC3 con la dirección IP de la máscara de subred y la puerta de salida (*gateway*) indicadas en la tabla 6.21.

Quinta Parte. Configuración de las VLAN

Configure los *switches* S1, S2 y S3 según las siguientes pautas:

Configure VTP en los tres *switches* utilizando la tabla 6.24. Recuerde que las contraseñas y los nombres de dominios VTP distinguen entre letras mayúsculas y minúsculas. El modo operativo predeterminado es servidor.

Tabla 6.24 Configuración de una VTP

Nombre del *switch*	Modo de operación VTF	Dominio del VTP	Contraseña de VTP
S1	Servidor	Práctica de Lab5	cisco
S2	Cliente	Práctica de Lab5	cisco
S3	Cliente	Práctica de Lab5	cisco

También tome en cuenta los siguientes comandos:

Comando en código	Descripción
S1(config)#vtp mode server	Modo dispositivo ya es SERVIDOR VTP.
S1(config)#vtp domain Lab5	Cambiar el nombre del dominio VTP de NULL a Lab5.
S1(config)#vtp password cisco	Configurar la contraseña de la base de datos VLAN del dispositivo en "cisco".
S1(config)#end	Término
S2(config)#vtp mode client	Configurar el dispositivo a modo CLIENTE VTP.
S2(config)#vtp domain Lab5	Cambiar el nombre del dominio VTP de NULL a Lab5.

continúa

S2(config)#vtp password cisco	Configurar la contraseña de la base de datos VLAN del dispositivo en "cisco".
S2(config)#end	Término.
S3(config)#vtp mode client	Configurar el dispositivo a modo CLIENTE VTP.
S3(config)#vtp domain Lab5	Cambiar el nombre del dominio VTP de NULL a Lab5.
S3(config)#vtp password cisco	Configurar la contraseña de la base de datos VLAN del dispositivo en "cisco".
S3(config)#end	Término.

Sexta Parte. Configuración de los enlaces troncales y la VLAN nativa

- ☑ Para cada *switch*, configure los puertos de Fa0/1 a Fa0/4 como puertos de enlace troncal.
- ☑ Designe a VLAN 99 como la VLAN nativa para estos enlaces troncales.
- ☑ Simplifique esta tarea con el comando "*interface range*" en el modo de configuración global. Recuerde que estos puertos fueron deshabilitados en un paso anterior y deben rehabilitarse con el comando "*no shutdown*".

```
S1(config)#interface range fa0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end
S2(config)#interface range fa0/1-4
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)#interface range fa0/1-4
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end
```

Séptima Parte. Configuración del servidor VTP con las VLAN

VTP permite configurar y probar las VLAN en el servidor VTP cliente en el dominio. Esto asegura la consistencia en la configuración de VLAN en toda la red.

- ☑ Configure las siguientes VLAN en el servidor VTP de acuerdo con lo que se establece en la tabla 6.25.

Tabla 6.25 Datos para la configuración de las VLAN en el servidor VTP

VLAN	Nombre de la VLAN
VLAN 99	Administración
VLAN 10	cuerpo docente-personal
VLAN 20	estudiantes
VLAN 30	*guest*

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#exit
```

- ☑ Use el comando "*show vlan brief*" en S2 y S3 para verificar que las cuatro VLAN se hayan distribuido a los *switches* clientes.

```
S2#show vlan brief

Nombre de la VLAN                Estado          Puertos
–
1       default                  active          Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                                 Gig1/1, Gig1/2
10      faculty/staff            active
20      students                 active
30      guest                    active
99      management               active
```

```
S3#show vlan brief

Nombre de la VLAN                Estado          Puertos
–
1       default                  active          Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10      faculty/staff            active
20      students                 active
30      guest                    active
99      management               active
```

Octava Parte. Configuración de la dirección de la interfaz de administración en los tres *switches*

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown

S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown

S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Verifique que todos los *switches* estén correctamente configurados haciendo *ping* entre ellos. Desde S1 haga *ping* a la interfaz de administración en S2 y S3, y de S2 a la interfaz de administración en S3.

En caso de que los *pings* no sean exitosos, realice el diagnóstico de fallas de las configuraciones de los *switches* e inténtelo nuevamente.

Novena Parte. Asignación de puertos de *switch* a las VLAN

Asigne puertos a las VLAN en S2, para ello consulte la tabla 6.21:

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Creando la configuración
[OK]
S2#
```

Décima Parte. Configuración de *Spanning Tree*

Examine la configuración predeterminada de 802.1D STP; para ello, en cada *switch* muestre la tabla de *Spanning Tree* con el comando "*show spanning-tree*". El resultado se presenta para S1 solamente. La selección de la raíz varía según el BID de cada *switch*.

```
S1#show spanning-tree

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0019.068d.6980
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface        Role          Sts           Cost          Prio.Nbr      Type
–
Fa0/1            Desg          FWD           19            128.3         P2p
Fa0/2            Desg          FWD           19            128.4         P2p
Fa0/3            Desg          FWD           19            128.5         P2p
Fa0/4            Desg          FWD           19            128.6         P2p

VLAN0010
Spanning tree enabled protocol ieee
Root ID Priority 32778
```

```
        Address 0019.068d.6980
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
  Address 0019.068d.6980
  Hello Time 2 sec Max Age 20 sec
  Forward Delay 15 sec
  Aging 300

Interface        Role          Sts          Cost          Prio.Nbr      Type
–
Fa0/1            Desg          FWD          19            128.3         P2p
Fa0/2            Desg          FWD          19            128.4         P2p
Fa0/3            Desg          FWD          19            128.5         P2p
Fa0/4            Desg          FWD          19            128.6         P2p

  VLAN0020
  Spanning tree enabled protocol ieee
  Root ID Priority 32788
        Address 0019.068d.6980
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID Priority 32788 (priority 32768 sys-id-ext 20)
  Address 0019.068d.6980
  Hello Time 2 sec Max Age 20 sec
  Forward Delay 15 sec
  Aging Time 300

Interface        Role          Sts          Cost          Prio.Nbr      Type
–
Fa0/1            Desg          FWD          19            128.3         P2p
Fa0/2            Desg          FWD          19            128.4         P2p
Fa0/3            Desg          FWD          19            128.5         P2p
Fa0/4            Desg          FWD          19            128.6         P2p

  VLAN0030
  Spanning tree enabled protocol ieee
  Root ID Priority 32798
        Address 0019.068d.6980
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32798 (priority 32768 sys-id-ext 30)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface        Role          Sts           Cost          Prio.Nbr      Type
–
Fa0/1            Desg          FWD           19            128.3         P2p
Fa0/2            Desg          FWD           19            128.4         P2p
Fa0/3            Desg          FWD           19            128.5         P2p
Fa0/4            Desg          FWD           19            128.6         P2p

VLAN0099
Spanning tree enabled protocol ieee
Root ID Priority 32867
        Address 0019.068d.6980
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface        Role          Sts           Cost          Prio.Nbr      Type
–
Fa0/1            Desg          FWD           19            128.3         P2p
Fa0/2            Desg          FWD           19            128.4         P2p
Fa0/3            Desg          FWD           19            128.5         P2p
Fa0/4            Desg          FWD           19            128.6         P2p
```

Observe que hay cinco instancias del *Spanning Tree* en cada *switch*. La configuración predeterminada del STP en los *switches* Cisco es Per-VLAN *Spanning Tree* (PVST+), que crea un *Spanning Tree* individual para cada VLAN (VLAN 1 y cualquier VLAN configurada a nivel de usuario).

Examine el *Spanning Tree* de VLAN 99 para los tres *switches*:

```
S1#show spanning-tree vlan 99 priority?

VLAN0099
Spanning tree enabled protocol ieee
Root ID Priority 32867
```

```
        Address 0019.068d.6980
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)
Address 0019.068d.6980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface        Role          Sts          Cost          Prio.Nbr      Type
---------------- ------------- ------------ ------------- ------------- ----------
Fa0/1            Desg          FWD          19            128.3         P2p
Fa0/2            Desg          FWD          19            128.4         P2p
Fa0/3            Desg          FWD          19            128.5         P2p
Fa0/4            Desg          FWD          19            128.6         P2p

S2#show spanning-tree vlan 99

VLAN0099
Spanning tree enabled protocol ieee
Root ID Priority 32867
        Address 0019.068d.6980
        Cost    19
        Port    3 (FastEthernet0/3)
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)
Address 001b.0c68.2080
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface        Role          Sts          Cost          Prio.Nbr      Type
---------------- ------------- ------------ ------------- ------------- ----------
Fa0/1            Desg          FWD          19            128.3         P2p
Fa0/2            Desg          FWD          19            128.4         P2p
Fa0/3            Root          FWD          19            128.5         P2p
Fa0/4            Altn          BLK          19            128.6         P2p

S3#show spanning-tree vlan 99

VLAN0099
Spanning tree enabled protocol ieee
Root ID Priority 32867
```

```
        Address 0019.068d.6980
        Cost 19
        Port 1 (FastEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)
Address 001b.5303.1700
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface        Role          Sts           Cost          Prio.Nbr      Type
–
Fa0/1            Root          FWD           19            128.3         P2p
Fa0/2            Altn          FWD           19            128.4         P2p
Fa0/3            Altn          FWD           19            128.5         P2p
Fa0/4            Altn          BLK           19            128.6         P2p
```

Undécima Parte. Examine el resultado

Responda las siguientes preguntas con base en el resultado:

1. ¿Cuál es la prioridad ID de puente para los *switches* S1, S2 y S3 en VLAN 99?

a) S1
b) S2
c) S3

2. ¿Cuál es la prioridad ID de puente para los *switches* S1, S2 y S3 en las VLAN 10, 20, 30 y 99?

a) VLAN 10
b) VLAN 20
c) VLAN 30
d) dVLAN 99

3. ¿Qué switch es la raíz para el *Spanning Tree* de VLAN 99?

_____

4. En la VLAN 99, ¿qué puertos del *Spanning Tree* están en estado de bloqueo en el *switch* raíz?

_____

5. En la VLAN 99, ¿qué puertos del *Spanning Tree* están en estado de bloqueo en los *switches* que no son raíz?

_____

6. ¿Cómo elige el STP el *switch* raíz?

_____

7. Ya que las prioridades de puente son las mismas, ¿qué más usa el *switch* para determinar la raíz?

_____

Duodécima Parte. Optimización de STP

Dado que hay una instancia separada de *Spanning Tree* para cada VLAN activa, se realiza una elección de raíz separada para cada una. Como se ha visto, si se usan las prioridades predeterminadas del *switch* en la selección de raíz, ésta se elige para cada *Spanning Tree*, lo cual podría llevar a un diseño inferior.

Algunas de las razones para controlar la selección del *switch* raíz incluyen:

- ☑ Éste es responsable de generar las BPDU en STP 802.1D y es el punto focal del control de tráfico de *Spanning Tree*. Además, debe manejar esta carga de procesamiento adicional.
- ☑ La ubicación de la raíz define las rutas activas conmutadas en la red y la ubicación aleatoria posiblemente lleve a rutas que no sean las óptimas. Lo ideal es que la raíz se encuentre en la capa de distribución.

Considere la topología empleada en esta práctica: de los seis enlaces troncales configurados solamente dos transportan tráfico; aunque esto evita los bucles, es una pérdida de recursos. Ya que la raíz puede definirse con base en la VLAN, puede haber algunos puertos que bloqueen ésta y envíen a otra.

En este ejemplo se ha determinado que la selección de raíz utilizando valores predeterminados ha llevado a la subutilización de los enlaces troncales disponibles del *switch*. Por lo tanto, es necesario obligar a otro *switch* a que se transforme en el raíz para la VLAN 99 con la finalidad de compartir algo de la carga en los enlaces troncales.

La selección del *switch* raíz se logra cambiando la prioridad del *Spanning Tree* para la VLAN. Dado que variar en el entorno de su práctica se configurará S1 y S3 para que sean los *switches* raíz para las VLAN específicas. La prioridad predeterminada, como puede haber observado, es 32 768 más el ID de VLAN. El número más bajo indica una prioridad más alta para la selección de raíz.

- ☑ Establezca la prioridad para la VLAN 99 en S3 en 4 096:

```
S3(config)#spanning-tree vlan 99 ?
```

Tome en cuenta los siguientes comandos:

Comando	Descripción
forward-time	Establece el retardo de envío para el *Spanning Tree*.
forward-time	Establece el intervalo de saludo para el *Spanning Tree*.
max-age	Establece el intervalo de antigüedad máxima para el *Spanning Tree*.
Priority	Establece la prioridad de puente para el *Spanning Tree*.
Root	Configura el *switch* como raíz.

```
S3(config)#spanning-tree vlan 99 ?
<0-61440> prioridad de Puente en incrementos de 4096
S3(config)#spanning-tree vlan 99 priority 4096
S3(config)#exit
```

- ☑ A continuación, se establece la prioridad para las VLAN 1, 10, 20 y 30 en S1 en 4 096. Una vez más, el número más bajo indica una prioridad más alta para la selección de raíz:

```
S1(config)#spanning-tree vlan 1 priority 4096
S1(config)#spanning-tree vlan 10 priority 4096
S1(config)#spanning-tree vlan 20 priority 4096
S1(config)#spanning-tree vlan 30 priority 4096
S1(config)#exit
```

- ☑ Proporcione un tiempo a los switches para recalcular el *Spanning Tree* y luego verifique el árbol para VLAN 99 en el *switch* S1 y el *switch* S3:

```
S1#show spanning-tree vlan 99

VLAN0099
Spanning tree enabled protocol ieee
Root ID Priority 4195
        Address 001b.5303.1700
        Cost 19
        Port 3 (FastEthernet0/1)
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)
        Address 0019.068d.6980
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300

Interface        Role          Sts          Cost          Prio.Nbr      Type
–
Fa0/1            Root          FWD          19            128.3         P2p
Fa0/2            Altn          BLK          19            128.4         P2p
Fa0/3            Desg          FWD          19            128.5         P2p
Fa0/4            Desg          FWD          19            128.6         P2p

        S3#show spanning-tree vlan 99
```

```
VLAN0099

Spanning tree enabled protocol ieee
Root ID Priority 4195
        Address 001b.5303.1700
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 4195 (priority 4096 sys-id-ext 99)
        Address 001b.5303.1700
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
–					
Fa0/1	Desgt	FWD	19	128.3	P2p
Fa0/2	Desg	FWD	19	128.4	P2p
Fa0/3	Desg	FWD	19	128.5	P2p
Fa0/4	Desg	FWD	19	128.6	P2p

- ☑ A continuación, responda los siguientes cuestionamientos:
  - ➲ ¿Qué *switch* es la raíz para VLAN 99?
  - ➲ En la VLAN 99, ¿qué puertos del *Spanning Tree* están en estado de bloqueo en el nuevo *switch* raíz?
  - ➲ En la VLAN 99, ¿qué puertos del *Spanning Tree* están en estado de bloqueo en el *switch* raíz antiguo?
- ☑ Luego, compare el *Spanning Tree* de la VLAN 99 de S3 arriba, con el *Spanning Tree* de la VLAN 10 de S3:

```
S3#show spanning-tree vlan 10

VLAN0010

Spanning tree enabled protocol ieee
Root ID Priority 4106
        Address 0019.068d.6980
        Cost 19
        Port 1 (FastEthernet0/1)
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
        Address 001b.5303.1700
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
–					
Fa0/1	Root	FWD	19	128.3	P2p
Fa0/2	Altn	BLK	19	128.4	P2p
Fa0/3	Altn	BLK	19	128.5	P2p
Fa0/4	Altn	BLK	19	128.6	P2p

Observe que S3 puede ahora usar los cuatro puertos para el tráfico de la VLAN 99, siempre y cuando no estén bloqueados al otro extremo del enlace troncal. No obstante, la topología original del *Spanning Tree*, con tres de cuatro puertos de S3 en el modo de bloqueo, todavía está instalada para las otras cuatro VLAN activas. Al configurar grupos de VLAN para usar diversos enlaces troncales como la ruta primaria de envío, se mantiene la redundancia de éstos contra fallas, sin tener que dejar enlaces troncales totalmente sin usar.

Decimotercera Parte. Observación de la respuesta al cambio de topología en 802.1D STP

☑ Para observar la continuidad a través de la LAN durante un cambio de topología, primero reconfigure PC3, que está conectada al puerto S2 Fa0/6 con la dirección IP 172.17.99.23 255.255.255.0. Luego, reasigne el Puerto fa0/6 de S2 a la VLAN 99. Esto le permite hacer *ping* continuamente a través de la LAN desde el host.

```
S2(config)#interface fa0/6
S2(config-if)#switchport access vlan 99
```

☑ Verifique que los *switches* puedan hacer *ping* al *host*.

☑ S2#*ping* 172.17.99.23

☑ Escriba "*escape sequence*" para abortar.

```
Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms

S1#ping 172.17.99.23
```

☑ Escriba "*escape sequence*" para abortar.

```
Sending 5, 100-byte ICMP Echos to 172.17.99.23, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1007 ms
```

- ☑ •Ponga S1 en modo *debug* de evento del *Spanning Tree* para monitorear los cambios durante el cambio de topología.

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
```

- ☑ Abra una ventana de comandos en PC3 y comience a hacer un *ping* continuo a la interfaz de administración de S1 con el comando *ping* –t 172.17.99.11.
- ☑ Ahora desconecte los enlaces troncales en S1 Fa0/1 y Fa0/3.
- ☑ Monitoree los pings. Éstos comenzarán a expirar a medida de que la conectividad en la LAN se interrumpa.
- ☑ Apenas la conectividad se haya restablecido, finalice los *pings* presionando "Ctrl + C".
- ☑ A continuación, encontrará una versión abreviada del resultado de la depuración que verá en S1 (varios TCN están omitidos para mayor brevedad).

```
S1#debug spanning-tree events
Spanning Tree event debugging is on
S1#
6d08h: STP: VLAN0099 new root port Fa0/2, cost 19 6d08h: STP: VLAN0099 Fa0/2 -> listening
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2
6d08h: STP: VLAN0030 Topology Change rcvd on Fa0/2
6d08h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
6d08h: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to down
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4 6d08h: STP: VLAN0099 Fa0/2 -> learning
6d08h: STP: VLAN0099 sent Topology Change Notice on Fa0/2 6d08h: STP: VLAN0099 Fa0/2 -> forwarding
6d08h: STP: VLAN0001 Topology Change rcvd on Fa0/4
```

Recuerde que cuando los puertos se encuentran en modo "escuchar y aprender", no están enviando tramas y la LAN está esencialmente desactivada. El recálculo del Spanning Tree puede tomar hasta 50 segundos para completarse, una interrupción significativa en los servicios de red.

El resultado de los *ping* continuos muestra el tiempo real de interrupción. En este caso, fue de aproximadamente 30 segundos. Aunque el STP 802.1D impide la formación de bucles de conmutación, este largo tiempo de restauración es considerado una seria desventaja en las LAN de alta disponibilidad de la actualidad.

La figura 6.8 muestra *pings* que se recalculan cada 30 segundos.

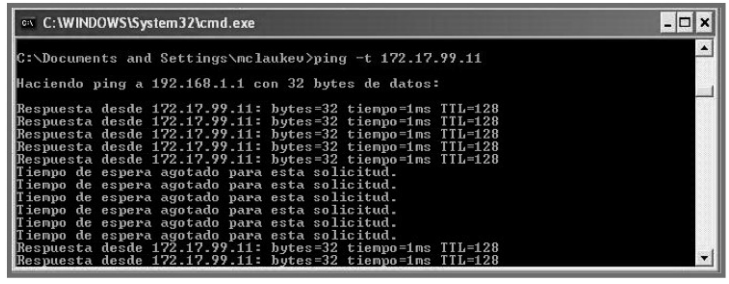


Figura 6.8 Pings que muestran un lapso de 30 segundos en la conectividad

Decimocuarta Parte. Configuración del protocolo *Rapid Spanning Tree* (PVST)

Cisco Systems ha desarrollado varias opciones para tratar los tiempos lentos de convergencia asociados al STP estándar. *PortFast*, *UplinkFast* y *BackboneFast* son opciones que, cuando se configuran correctamente, pueden reducir drásticamente el tiempo requerido para restaurar la conectividad. Incorporarlas requiere de configuración manual, y se debe tener cuidado para hacerlo siempre de la manera adecuada. La solución a largo plazo es Rapid STP (RSTP) 802.1w, que incorpora dichas características, entre otras. RSTP-PVST está configurado como sigue:

```
S1(config)#spanning-tree mode rapid-pvst
```

Configure los tres *switches* de esta manera:

- ☑ Use el comando "*show spanning-tree summary*" para verificar que RSTP esté habilitado

Decimoquinta Parte. Observación del tiempo de convergencia de RSTP

- ☑ Comience restaurando los enlaces troncales que desconectó anteriormente si es que aún no lo ha hecho (puertos Fa0/1 y Fa0/3 en S1).
- ☑ Configure el *host* PC3 para que haga ping continuamente a toda la red.
- ☑ Habilite la depuración de eventos de *Spanning Tree* en el *switch* 1.
- ☑ Desconecte los cables a los puertos Fa0/1 y Fa0/3.
- ☑ Observe el tiempo requerido para restablecer un *Spanning Tree* estable. A continuación, se muestra el resultado parcial de depuración:

```
S1#debug spanning-tree events Spanning Tree event debugging is on
S1#
6d10h: RSTP(99): updt rolesroot port Fa0/3 is going down 6d10h: RSTP(99): Fa0/2 is now root port
6d10h: RSTP(99): syncing port Fa0/1
6d10h: RSTP(99): syncing port Fa0/4
6d10h: RSTP(99): transmitting a proposal on Fa0/1
6d10h: RSTP(99): transmitting a proposal on Fa0/4
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
6d10h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
```

El tiempo de restauración con RSTP habilitado fue menos de un segundo y no se descartó ningún *ping*.

Decimosexta Parte. Limpieza

- ☑ Borre las configuraciones y recargue las opciones predeterminadas de los *switches*.
- ☑ Desconecte y guarde el cableado. En caso de PC *hosts* que están normalmente conectadas a otras redes (tales como la LAN de la institución o de Internet), vuelva a conectar el cableado apropiado y restaure la configuración de TCP/IP.

Decimoséptima Parte. Configuraciones finales

Switch S1

```
hostname S1
!
enable secret class
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 4096
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 4096
!
interface FastEthernet0/1
switchport trunk native vlan 99
```

```
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6 shutdown
!
interface FastEthernet0/7 shutdown
!
(remaining port configuration ommitted - all non-used ports are shutdown)
!
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan1
ip address 219,170,1000,1 255.255.255.0
no ip route-cache
!
line con 0
password cisco login
line vty 0 4 password cisco login
line vty 5 15 password cisco login
!
end
```

Switch S2

```
hostname S2
!
enable secret class
!
no ip domain-lookup
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 30
!
interface FastEthernet0/6
switchport access vlan 30
!
interface FastEthernet0/7
switchport access vlan 30
!
interface FastEthernet0/8
switchport access vlan 30
!
interface FastEthernet0/9
switchport access vlan 30
!
interface FastEthernet0/10
switchport access vlan 30
```

```
!
interface FastEthernet0/11
switchport access vlan 10
!
interface FastEthernet0/12
switchport access vlan 10
!
interface FastEthernet0/13
switchport access vlan 10
!
interface FastEthernet0/14
switchport access vlan 10
!
interface FastEthernet0/15
switchport access vlan 10
!
interface FastEthernet0/16
switchport access vlan 10
!
interface FastEthernet0/17
switchport access vlan 10
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 20
!
interface FastEthernet0/20
switchport access vlan 20
!
interface FastEthernet0/21
switchport access vlan 20
!
interface FastEthernet0/22
switchport access vlan 20
!
interface FastEthernet0/23
switchport access vlan 20
!
```

```
interface FastEthernet0/24
switchport access vlan 20
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan1
ip address 172.17.99.12 255.255.255.0
no ip route-cache
!
line con 0
line vty 0 4 password cisco login
line vty 5 15
password cisco
login
!
end
```

Switch S3:

```
hostname S3
!
enable secret class
!
no ip domain-lookup
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 99 priority 4096
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/2
```

```
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
(remaining port configuration omitted-all non-used ports are shutdown)
!
interface Vlan1 no ip address
no ip route-cache
shutdown
!
interface Vlan1
ip address 172.17.99.13 255.255.255.0
no ip route-cache
!
line con 0
password cisco login
line vty 0 4
password cisco login
line vty 5 15 password cisco login
!
end
```

Cuestionario

6.7.1 Explique a detalle cómo borrar la configuración de inicio y volver a cargar la configuración predeterminada, configurando un conmutador (*switch*) al estado inicial.

6.7.2 Explique a detalle cómo se explica el comportamiento predeterminado del protocolo *Spanning Tree* (STP, 802.1D). Establezca estudios de caso exitosos de uso.

6.7.3 Explique detalladamente las limitaciones de 802.1D STP para soportar la continuidad del servicio.

6.7.4 Establezca en qué consisten las mejoras ofrecidas por Rapad STP.

Referencias

3GPP (s.f.). *3rd Generation Partnership Project* (3GPP). Disponible en http://www.3gpp.org/specs/releases-contents.htm

3GPP (2006a). *3rd Generation Partnership Project TS 23.228:* IP Multimedia Subsystem.

3GPP (2006b). *The Internet Engineering Task Force. RFC 4566: SDP: Session Description Protocol*. Disponible en http://www.ietf.org/rfc/rfc4566.txt?number=4566

Abramson, N. (2000). "Internet access using VSAT" in *IEEE Community Magazine*, (38): pp. 60-68.

Academia de Networking de Cisco Systems (2004). *Serie Cisco Systems CCNA*. EUA: Cisco Press, 3ª ed.

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems.* New York: John Wiley & Sons.

Barrios Garrido, G. (1988). *Internet y Derecho en México*. México: McGraw-Hill.

Berghel, H. L. (2001). "Cyber privacy in the new millennium" in *IEEE Computer*, (34): pp. 132-134.

Berners-Lee, T. (1990). *Inventing the Web: Christmas Baby. Seeing the Picture*.

_____ (2009). Pre-W3C Web and Internet Background. *World Wide Web Consortium*.

Berners-Lee, T.; Cailliau, A.; Loutonen, A.; Nielsen, H. F. and Secret, A. (1994). "The World Wide Web" in *Community of the ACM*, (37): pp. 76-82.

Berners-Lee, T. *et al.* (2004). *Architecture of the World Wide Web, Volume One*. Version 20041215. W3C.

Bertsekas, D. and Gallager, R. (1992). *Data networks*. Englewood Cliffs, New Jersey: Prentice-Hall.

Bhatti, S. N. and Crowcroft, J. (2000). "QOS sentitive flows: Issues in IP packet handling" in *IEEE Internet Computing*, (4): pp. 48-57.

Black, U. (1997). *Redes de computadoras. Protocolos, normas e interfaces*. México: Alfaomega Grupo Editor, 2ª ed.

Boggs, D.; Mogul, J. and Kent, C. (1988). Measured capacity of an Ethernet: Myths and reality. *Procedures SIGCOMM ´88 Conference*, pp. 222-234.

Bounoure, Francois, *et al*., (2006). *Laboratorio de redes: Session Initiation Protocol*. Argentina: Universidad de Buenos Aires. Disponible en http://www.fiuba6662.com.ar/6648/presentaciones/2006/Informe%20SIP.pdf

Braden, R. (1989). Requirements for Internet hosts-communications layers. *RFC 1 122*.

Bray, T.; Paoli, J.; Sperberg-McQueen, C.; Maler, E.; Yergeau, F. and Cowan, J. (2006). Extensible Markup Language (XLM) 1.1. *Recommendation of the W3C*.

Burleigh, S.; Hooke, A.; Torgerson, L.; Fall, K.; Cerf, V.; Durst, B.; Scott, K. and Weiss, H. (2003). "Delay-tolerant networking: An approach to interplanetary Internet" in *IEEE Community Magazine*, (41): pp. 128-136.

Cisco Sys. (2010a). *Cisco visual networking index: Forecast and methodology*. USA: Cisco Systems.

_____ (2010b). *Resource Reservation Protocol*. Disponible en http://www.cisco.com/en/US/docs/internetworking/technology/handbook/RSVP.pdf

Clark, D. D. (1988). The design philosophy of the DARPA Internet protocols. *Procedures SIGCOMM ´88 Conference*, ACM, pp. 106-114.

Clark, D. D.; Jacobson, V.; Romkey, J. and Salwen, H. (1989). "An analysis of TCP processing over-head" in *IEEE Community Magazine*, (27): pp. 23-29.

Clark, D. D.; Shenker, S. and Zhang, L. (1992). Supporting real-time applications in an integrated services packet network. *Procedures SIGCOMM ´92 Conference ACM*, pp. 14-26.

Comer, D. E. (2005). *Internetworking with TCP/IP*. Englewood Cliffs, New Jersey: Prentice-Hall, 5th ed.

_____ (2007). *The Internet book*. Englewood Cliffs, New Jersey: Prentice-Hall, 4th ed.Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública en Argentina (s.f.). *Manual de Seguridad en Redes (ArCERT)*. Disponible en http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

Correa, C. M. *et al*. (1987). *Derecho informático*. Buenos Aires, Argentina: De Palma Editores.

Croft, B. (2005). *RFC 951: Bootstrap Protocol*. USA: FRC.

Crovella, M. and Krishnamurty, B. (2006). *Internet measurement*. New York: John Wiley & Sons.

Chase, J. S.; Gallatin, A. J. and Yocum, K. G. (2001). End system optimization for high-speed TCP. *IEEE Community Magazine*, (39): pp. 68-75.

Chen, S. and Nahrstedt, K. (1998). An overview of QOS routing for next-generation networks. *IEEE Network Magazine*, (2): pp. 64-69.

Davara Rodríguez, M. Á. (1993). *Derecho informático*. Pamplona, España: Aranzadi Editores.

Davie, B. and Farrel, A. (2008). *MPLS: Next generation*. San Francisco, California: Morgan Kaufmann.

Davie, B. and Rekhter, Y. (2000). *MPLS technology and applications*. San Francisco, California: Morgan Kaufmann.

Davies, J. (2008). *Understanding IPv6*. Redmon, WA: Microsoft Press.

Day, J. D. and Zimmermann, H. (1983). "The OSI Reference Model" in *Procedures of the IEEE*, (71): pp. 1334-1340.

Deering, S. E. (1993). "SIP: Simple Internet Protocol" in *IEEE Network Magazine*, (7): pp. 16-28.

Deering, S. E. and Cheriton, D. (1990). "Multicast routing in datagram networks and extended LAN" in *ACM Transactions on Computer Systems*, (8): pp. 85-110.

Demers, A.; Keshav, S. and Shenker, S. (1990). "Analysis and simulation of a fair queueing algorithm" in *Internetworking: Research and Experience*, (1): pp. 3-26.

Devarapalli, V.; Wakikawa, R.; Petrescu, A. and Thubert, P. (2005). Network mobility (NEMO) basic support protocol. *RFC 3 963*.

Donahoo, M. and Calvert, K. (2009). *TCP/IP sockets in C*. San Francisco, California: Morgan Kaufmann, 2nd ed.

_____ (2008). *TCP/IP sockets in Java*. San Francisco, California: Morgan Kaufmann, 2nd ed.

Donaldson, G. and Jones, D. (2001). "Cable TV broadband network architectures" in *IEEE Community Magazine*, (39): 122-126.

Ericsson (2007). I*ntroduction to IMS, White Paper*. Disponible en http://www.ericsson.com/technology/whitepapers/8123_Intro_to_ims_a.pdf

Fall, K. (2003). A delay-tolerant network architecture for challenged Internets. *Procedures SIGCOMM 2003 Conference ACM*, pp. 27-34.

Faloutsos, M.; Faloutsos, P. and Faloutsos, C. (1999). On power-law relationships of the Internet topology. P*rocedures SIGCOMM ´99 Conference ACM*, pp. 251-262.

Farrell, S. and Cahill, V. (2007). *Delay and disruption tolerant networking*. London: Artech House.

Fenner, B.; Handley, M.; Holbrook, H. and Kouvelas, I. (2006). Protocol Independent Multicast-Sparse Mode (PIM-SM). *RFC 4 601*.

Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Berners-Lee's, T. (1999). *Hypertext Transfer Protocol-HTTP/1.1. Request for comments 2616*. USA: Information Sciences Institute.

Ford, W. and Baum, M. S. (2000). *Secure electronic commerce*. Upper Saddle River, New Jersey: Prentice-Hall.

Fouli, K. and Maler, M. (2009). "The road to carrier-grade Ethernet" in *IEEE Community Magazine*, S30-S38.

Galindo, F. (1998). *Derecho e informática*. Madrid, España: Editorial La Ley-Actualidad.

García, T. (2001). *Redes para proceso distribuido*. México: Alfaomega Grupo Editor, 2ª ed.

Gast, M. (2005). *802.11 Wireless networks: The definitive guide*. Sebastopol, California: O'Reilly.

Gershenfeld, N.; Krikorian, R. and Cohen, D. (2004). "The Internet of things" in *Scientific American*, (291): pp. 76-81.

Goode, B. (2002). "Voice over Internet Protocol" in *Procedures of the IEEE*, (90): 1495-1517.

Grayson, M.; Shatzkamer, K, and Wainner, S. (2009). *IP design for mobile networks*. Indianapolis: Cisco Press.

Ha, S.; Rhee, I. and Lisong, X. (2008). "CUBIC: A new TCP friendly high speed TCP variant" in SIGOPS *Operating Systems Review*, (42): pp. 64-74.

Hallivuori, V. (2000). *Real Time Transport Protocol (RTP) Security*. Helsinki, Finlandia: University of Technology. Disponible en http://kotiweb.kotiportti.fi/vhallivu/files/rtp_security.pdf

Halsall, F. (1988). *Comunicación de datos, redes de computadoras y sistemas abiertos*. México: Pearson Education, 4ª ed.

Harte, L.; Kellogg, S.; Dreher, R. and Schaffnit, T. (2000). *The comprehensive guide to wireless technology*. Fuquay-Varina, NC: APDG Publishing.

Hecht, J. (2005). *Understanding fiber optics*. Upper Saddle River, New Jersey: Prentice-Hall.

Held, G. (2010). *A practical guide to content delivery networks*. Boca Ratón, Florida: CRC Press.

Hiertz, G.; Denteneer, D.; Stibor, L; Zang, Y.; Costa, X. and Walke, B. (2010). "The IEEE 802.11 universe" in *IEEE Community Magazine*, (48): pp. 62-70.

Hoe, J. (1996). Improving the start-up behavior of a congestion control scheme for TCP. *Procedures SIGCOMM '96 Conference ACM*, pp. 270-280.

Hu, Y. and Li, V. O. K. (2001). "Satellite-based Internet: A tutorial" in *IEEE Community Magazine*, (30): pp. 154-162.

Huitema, C. (1999). *Routing in the Internet*. Englewood Cliffs, New Jersey: Prentice Hall, 2nd ed.

International Telecommunications Union (ITU) (2005a). *ITU Internet reports 2005: The Internet of things*. Ginebra, Switzerland: ITU.

_____ (2005b). *Measuring the information society: The ICT development index*. Ginebra, Switzerland: ITU.

Jacobson, V. (1990). Compressing TCP/IP headers for low speed serial links. *RFC 1 144*.

Jain, R. and Routhier, S. (1986). "Packet trains-measurements and a new model for computer network traffic" in *IEEE Journal on Select Areas in Communications*, (6): pp. 986-995.

Joel, A. (2002). "Telecommunications and the IEEE communications society" in *IEEE Community Magazine, 50th Anniversary Issue*, pp. 6-14, 162-167.

Jalercom (s.f.). *Infraestructura y equipos de VOIP*. Disponible en http://www.jalercom.com/Brochures/brochure_infraestructura%20%20equipo%20de%20voip.pdf

Johnson, D.; Perkins, C. and Arkko, J. (2004). Mobility support in IPv6. *RFC 3 775*.

Kaufman, C.; Perlman, R. and Speciner, M. (2002). *Network security*. Englewood Cliffs, New Jersey: Prentice-Hall, 2nd ed.

Koodli, R. and Perkins, C. E. (2007). *Mobile internetworking with IPv6*. New York: John Wiley & Sons.

Krishnamurti, B. and Rexford, J. (2001). *Web protocols and practice*. Boston, Massachusetts: Addison-Wesley.

Kurose, J. F. and Keith, W. R. (2005). *Computer Networking: A top-Down Approach Featuring the Internet*. USA: Addison Wesley, 3th ed.

Labovitz, C.; Ahuja, A.; Bose, A. and Jahanian, F. (2001). "Delayed Internet routing convergence" in I*EEE/ACM Transactions on Networking*, (9): pp. 293-306.

Le Point (2010). *Le Web a até inventé en France*.

Lewis, M. (2006). *Comparing, designing and deploying VPN*. Indianapolis, IN: Cisco Press.

Long, T. (2012). Aug. 7, 1991: L*adies and Gentlemen, the World Wide Web*. Disponible en https://www.wired.com/2012/08/aug-7-1991-ladies-and-gentlemen-the-world-wide-web/

Lin, S. and Costello, D. (2004). *Error control coding*. Upper Saddle River, New Jersey: Pearson Education.

Lubacz, J.; Mazurczyk, W. and Szczypiorski, K. (2010). "Voice over IP" in *IEEE Spectrum*, pp. 42-47.

Mani, M. and Crespi, N. (2007). *Adopting IMS in Wi-Fi Technology*. Disponible en http://portal.acm.org/citation.cfm?id=1378117

Maufer, T. A. (1999). *IP fundamentals*. Upper Saddle River, New Jersey: Prentice-Hall.

Metz, C. (2001). "Interconnecting ISP networks" in *IEEE Internet Computing*, (5): pp. 74-80.

Munasighe, K. and Jamalipour, A. (2008). *Interworking of WLAN-UMTS Netwoks: An IMS based Pltaform for Session Mobility*. USA: IEEE.

Neuman, C. and Ts´O, T. (1994). "Kerberos: An authentications service for computer networks" in *IEEE Community Magazine*, (32): pp. 33-38.

Palais, J. C. (2004). *Fiber optic communications*. Englewoods Cliffs, New Jersey: Prentice-Hall.

Parameswaran, M.; Susarla, A. and Whinston, A. B. (2001). "P2P networking: An information sharing alternative" in *IEEE Computer*, (34): pp. 31-38.

Pechuán, Luis Miralles (2010). *El nuevo sistema multimedia conocido como IMS que adoptarán las redes UMTS*. Universidad de Valencia. Disponible en http://www.uv.es/montanan/redes/trabajos/index.html

Perkins, C. E. (1998). *Mobile IP design principles and practices*. Upper Saddle River, New Jersey: Prentice-Hall.

_____ (ed) (2001). *Ad hoc networking*. Boston, Massachusetts: Addison-Wesley.

_____ (2002). IP mobility support for IPv4. *RFC 3 344*.

_____ (2003). *Audio and video for the Internet*. Boston, Massachusetts: Addison-Wesley.

Perlman, R. (1985). "An algorithm for the distributed computation of a spanning tree in an extended LAN" in *Procedures SIGCOMM ´85 Conference ACM*, pp. 44-53.

_____ (2000). InterConnections. Boston, Massachusetts: Addison-Wesley.

Pieprzyk, J.; Hardjono, T. and Seberry, J. (2004). *Fundamentals of computer security*. USA: Prentice-Hall.

Piscitello, D. M. and Chapin, A. L. (1993). *Open systems networking: TCP/IP and OSI*. Boston, Massachusetts: Addison-Wesley.

Poikselka, Miikka, et. al., (2006). *The IMS IP multimedia concepts and services*. USA: John Wiley & Sons Ltd, 2nd.

Polo, L. (2003). *World Wide Web technology architecture: A conceptual analysis*. USA: New Devices.

Postel, J. (1981). Internet control message protocols. *RFC 792*.

Quittner, J. (2010). Tim Berners-Lee. Time 100 People of the Century. *Time Magazine*.

Rabin, J. and McCathienevile, C. (2008). Mobile web best practices 1.0. *Recommendation of the W3C*.

Ramaswami, R.; Kumar, S. and Sasaki, G. (2009). *Optical networks: A practical perspective*. San Francisco, California: Morgan Kaufmann, 3th ed.

Real Academia Uruguaya (s.f.). *Introducción al IPv6*. Disponible en http://www.rau.edu.uy/ipv6/queesipv6.htm

Ronan, John, Sasitharan Balasubramaniam, Adnan K Kiani, Wenbing Yao. (s/a). *On the use of SHIM6 for mobility support in IMS Networks*.

Salazar, J. E., et al., (2002). *Diffserv como solución a la provisión de Q_0S en la Internet*. España: Universidad Carlos III de Madrid. Disponible en http://www.ist-mobydick.org/publications/cita2002.pdf

Simpson, W. (2008). *Video over IP*. Burlington, Massachusetts: Focal Press.

Spurgeon, C. E. (2000). *Ethernet: The definitive guide*. Sebastopol, California: O´Reilly.

Stallings, W. (2010). *Comunicaciones y redes de computadoras*. México: Pearson Educación, 9ª ed.

Stevens, W. R. (1994). *TCP/IP illustrated: The protocols*. Boston, Massachusetts: Addison-Wesley.

Tanenbaum, A. S. (2007). *Modern operating systems*. Upper Saddle River, New Jersey: Prentice-Hall, 3rd ed.

Tanenbaum, A. S. and Van Steen, M. (2007). *Distributed systems: Principles and paradigms*. Upper Saddle River, New Jersey: Prentice-Hall.

Telefónica (s.f.). *Evolución al dominio IMS*. Disponible en http://www.telefonica.es/sociedaddelainformacion/pdf/publicaciones/movilidad/capitulo_12.pdf

Terán Pérez, D. M. (2010). *Redes convergentes. Diseño e implementación*. México: Alfaomega Grupo Editor.

_____ (2012). *Introducción a la computación cuántica para ingenieros*. México: Alfaomega Grupo Editor.

_____ (2014). *Administración estratégica de la función informática*. México: Alfaomega Grupo Editor.

_____ (2016). *Introducción a la ingeniería*. México: Alfaomega Grupo Editor.

The Internet Engineering Task Force (s.f.). RFC 2 205. *Resource ReSerVation Protocol (RSVP)*. Disponible en http://www.ietf.org/rfc/rfc2205.txt?number=2205

_____ (s.f.). RFC 2 748. *The COPS (Common Open Policy Service) Protocol*. Disponible en http://www.ietf.org/rfc/rfc2748.txt?number=2748

_____ (s.f.). RFC 3 550. *RTP: A Transport Protocol for Real-Time Applications*. Disponible en http://www.ietf.org/rfc/rfc3550.txt

Tompros, S. and Denazis, S. (2007). *Interworking of heterogeneous access networks and QoS provisioning via IP multimedia core networks*. Universidad de Patras. Disponible en http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VRG-4PMJK6C-5-N&_cdi=6234&_user=2620291&_orig=search&_coverDate=01%2F18%2F2008&_sk=999479998&view=c&wchp=dGLzVtz-zSkWA&md5=23bec3e813019432ac5fc4e1f6fabd00&ie=/sdarticle.pdf

Wittenburg, N. (2009). *Understanding voice over IP technology*. Clifton Park, New York: Delmar Cengage Learning.

World Wide Web (2009). *Proposal for a hypertexts Project*.

_____ (2010). *Proposal for a Hyper Text Project*.

Znaty, S.; Dauphin, J. L. and Geldwerth, R. (s.f.). *IP Multimedia Subsystem: Principios y arquitectura. EFORT*. Disponible en http://www.efort.com/media_pdf/IMS_ESP.pdf

Znaty, Simon, Dauphin, Jean Louis and Geldwerth, Roland. (s/a). *SIP: Session Initiation Protocol effort.* Disponible en http://www.efort.com/media_pdf/IMS_ESP.pdf

Capítulo

Situación actual de las redes de computadoras

Si vas a hacer el mal, por favor, hazlo bien.

David Moisés Terán Pérez

Reflexione y responda las siguientes preguntas:

- Qué es el estado del arte?
- ¿Qué es el estado del conocimiento?
- ¿Por qué es importante conocer el estado del arte sobre redes de computadoras?
- ¿Qué es el Internet de las cosas, cómo funciona y qué aplicaciones tiene?
- ¿Qué es la realidad aumentada, cómo funciona y qué aplicaciones tiene?
- ¿Qué es la web 3.0, cómo funciona y qué aplicaciones tiene?
- ¿Qué es la web 4.0, cómo funciona y qué aplicaciones tiene?
- ¿Qué son los drones, cómo funcionan y qué aplicaciones tienen?

Después de estudiar este capítulo, el lector será capaz de:

- Entender qué es el estado del arte de una disciplina específica.
- Comprender qué es el estado del conocimiento de una disciplina específica.
- Establecer qué es el estado del arte sobre redes de computadoras.
- Explicar qué es el Internet de las cosas, cómo funciona y qué aplicaciones reales tiene en la actualidad.
- Explicar qué es la realidad aumentada cómo funciona y qué aplicaciones reales tiene actualmente.
- Explicar qué es la web 3.0, cómo funciona y qué aplicaciones reales tiene actualmente.
- Explicar qué es la web 4.0, cómo funciona y qué aplicaciones reales tiene actualmente.
- Explicar qué son los drones, cómo funcionan y qué aplicaciones reales tienen en la actualidad.

Para cumplir con los objetivos planteados, el siguiente diagrama de flujo presenta la forma de acceder a los contenidos:

7.1 Introducción

En el estudio del estado del arte sobre redes de computadoras destacan las que abarcan las redes móviles *ad hoc* (MANET, *Mobile ad hoc Network*) y su seguridad, el DNS seguro (DNSSEC, *Domain Name System Security Extensions*), el DNSCurve, las nuevas tendencias en el cableado estructurado, la simulación y la virtualización aplicadas a la enseñanza de redes, entre muchos otros temas. Adicionalmente, se tratan temas de aplicación de las redes de computadoras, en aspectos como el Internet de las cosas, la realidad aumentada, la web 3.0 y la 4.0, así como los drones. No son los únicos temas, pero sí los más representativos en estas nuevas tendencias y líneas de investigación sobre el diseño, implementación, uso, mantenimiento y desarrollo de las nuevas redes de computadoras.

7.2 El inventario y la clasificación de activos de la seguridad informática

El término "estado del arte" es un anglicismo derivado de la expresión "*state of the art*" (S_OA), utilizado para la investigación-acción. La expresión inglesa se puede traducir al español también como: "puntero", "lo último" o "lo más avanzado"; por ejemplo, *state of the art technology* se traduce literalmente como "tecnología de punta", "lo último en tecnología" o "tecnología de vanguardia".

En el ámbito de la investigación científica, el S_OA hace completa referencia al estado último de la materia u objeto de estudio, en términos de I+D+I (Investigación+Desarrollo +Innovación), refiriéndose incluso al límite de conocimiento humano público sobre la materia objeto de estudio. Dentro del ambiente tecnológico industrial se entienden como "estado del arte", "estado de la técnica" o "estado de la cuestión" todos aquellos desarrollos de última tecnología realizados a un producto que han sido probados en la industria y acogidos y aceptados por diferentes fabricantes.

Hablando específicamente acerca del estado del arte sobre redes de computadoras, a continuación se presentan las más innovadoras líneas de investigación y de desarrollo.

7.2.1 Integración segura de MANET[1] a redes de infraestructura

Motivación

Una de las principales ventajas de una MANET es la posibilidad de integrarla a una red de infraestructura con diferentes objetivos, tales como el acceso a Internet o a sistemas de información de una organización desde un dispositivo móvil, además de la opción de transportar información a lugares sin cobertura de red. La seguridad y el rendimiento son factores importantes para el éxito de esta integración (Ozan, 2016); sin embargo, se encuentran expuestas a posibles ataques o accesos no autorizados, además de que la mayoría de todos los dispositivos móviles de la MANET tienen capacidad de procesamiento limitada, ancho de banda reducido y son alimentados por baterías con energía limitada (figura 7.1). En este contexto, se propone investigar sobre diferentes protocolos y mecanismos de seguridad, que permitan realizar una integración y/o comunicación segura entre redes móviles de este tipo y redes de infraestructura GPRS o LAN/WAN) bajo dos premisas:

- Garantizar el cumplimiento de confidencialidad, integridad y autenticación.
- La implementación de la seguridad, en lo posible, no debe comprometer el rendimiento del dispositivo móvil, la utilización del ancho de banda, de los recursos físicos y el consumo de energía.

[1] Una *Mobile Ad Hoc Network,* en algunas ocasiones denominada también como malla de nodos móviles (*Mobile Mesh Network*), se trata de una red de dispositivos conectados inalámbricamente y que poseen propiedades de autoconfiguración, además de tener cierta movilidad; es decir, se encuentran montados en plataformas móviles.

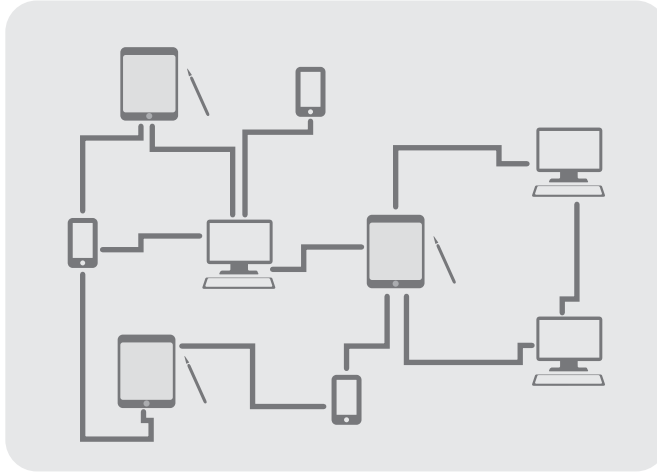


Figura 7.1 Representación de una red MANET

Resultados y objetivos

Los resultados de esta línea de investigación están dirigidos a organizaciones que requieran integrar tecnologías móviles a su red de infraestructura (Toh, 2012). Se busca concientizar a los distintos niveles jerárquicos de la organización sobre los riesgos que implica una integración no segura, evitando así las posibles pérdidas económicas que pueden generarse por un ataque o acceso no autorizado a la información; para lograrlo se plantean los siguientes objetivos (Carlton, 2006):

- Presentar una revisión del estado del arte de seguridad en redes móviles *ad hoc*.
- Efectuar un análisis de alternativas para realizar comunicaciones seguras entre redes de infraestructura y redes móviles *ad hoc*.
- Presentar una propuesta de comunicaciones seguras para MANET que incluya un conjunto de recomendaciones y una guía de buenas prácticas para incorporar mecanismos de seguridad en los dispositivos móviles, teniendo en cuenta las características especiales de este tipo de redes e intentando minimizar el impacto de la seguridad en el rendimiento del dispositivo.

La revisión del estado del arte de seguridad en redes móviles *ad hoc* servirá como guía para profesionales informáticos que requieran implementar políticas de seguridad en una organización, lo que facilitará al administrador de redes y a los programadores de aplicaciones móviles la elección de la alternativa que mejor se adapte a los requerimientos de seguridad de su organización. La propuesta de comunicaciones seguras para MANET servirá como referencia para futuras implementaciones de seguridad en entornos móviles (Bayya; Gupte; Shukla y Garikapati, 2007).

7.2.2 Evaluación de extensiones de seguridad para DNS

Motivación

Cuando el protocolo DNS fue diseñado, los principales objetivos se basaron en proporcionar un mecanismo de comunicación que fuera rápido, efectivo, escalable y de alta disponibilidad, omitiendo aspectos como la integridad y autenticidad de los datos.

En la actualidad, estas omisiones han permitido un incremento significante de actividades maliciosas, tales como suplantación de identidad, distribución de *malware*, falsificación de respuestas DNS, entre otras.

Tomando conciencia de estas fallas en el diseño original del protocolo DNS, es que las organizaciones y los particulares han puesto especial énfasis en la implementación de políticas y de prácticas destinadas a dotar de seguridad al servicio proporcionado por el DNS (RFC-4 033, 2005). En consecuencia, a escala global, se viene trabajando en la implementación de lo que se conoce como DNSSEC, destinado a proteger el flujo de datos en el esquema DNS tradicional (figura 7.2). DNSSEC se presenta como un conjunto de extensiones para el sistema tradicional de DNS, diseñado para autenticar y proteger la integridad de sus respuestas a través del uso de firmas digitales basadas en clave pública. La información necesaria para autenticar las respuestas es almacenada en un nuevo conjunto de registros de recursos (RFC-4 034, 2005):

RRSIG (*Resource Record Digital Signature*). Contiene la firma digital para un conjunto de registros de recursos (RRSet, *Resource Record set*) que tiene un RRSIG asociado.

DNSKEY (DNS, *Domain Name System Key*). Contiene la clave pública asociada a un RRSIG. Una zona puede contener múltiples registros DNSKEY.

DS (*Domain Services*). Almacena un elemento de la clave pública de una "zona hija" asociada a una "zona padre". A través de un proceso de delegación permite posteriormente la validación de una cadena de confianza.

NSEC (*Next Secure*). Permite la autenticación de respuestas negativas; es decir, verificar si una respuesta del tipo NXDOMAIN (*Non-Existent Domain*) fue recibida del host consultado.

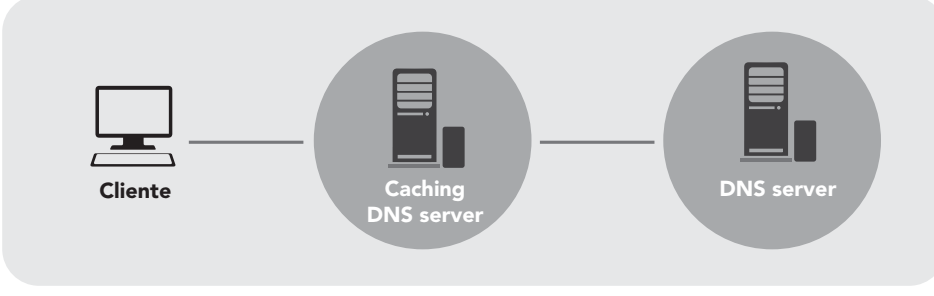


Figura 7.2 Evaluación de extensiones de seguridad para DNS

Resultados y objetivos

Como se ha especificado anteriormente, la implementación de DNSSEC implica contar con un mayor poder de procesamiento necesario para la generación y verificación de registros. Se observa también que dada la necesidad del intercambio de estos nuevos registros en un proceso de solicitud/respuesta, el recurso que se ve más comprometido es el del ancho de banda, ya que se requiere de un aumento significativo de éste. Por otra parte, un aspecto importante es que en el proceso de validación de la cadena de confianza, el protocolo DNSSEC debe estar implementado en toda la jerarquía, siendo este último aspecto quizás el que demore una implementación a nivel global, dado que a la fecha no todos los dominios lo han implementado aún (DNSCurve, s.f.). Por todo lo anterior, es que actualmente los investigadores se encuentran realizando tareas vinculadas con:

- La recopilación de las formas más frecuentes de ataque al sistema DNS.
- Impacto de la adopción de las extensiones de seguridad para DNS en el ámbito universitario.
- Integración de DNSSEC con otros mecanismos de seguridad tales como IPSEC y DNSCurve.

7.2.3 Virtualización de redes

Motivación

Las redes de computadoras son complejas y contienen múltiples dispositivos (routers, servidores, entre muchos otros), interfaces, protocolos e interconexiones físicas que crean topologías complejas. Comprender las redes de computadoras sin realizar experimentos prácticos es dificultoso, por no decir que casi imposible. Desafortunadamente, disponer y configurar un laboratorio de redes puede ser de un costo muy elevado y en muchos casos impracticable (Virtual Box, s.f.).

Por otro lado, realizar experimentos en una red en producción puede ser inviable (servicios críticos para los usuarios, coordinación entre departamentos, etcétera). Como solución alternativa, existe la posibilidad de poner en marcha *software* que emule un dispositivo de red de la forma más realista posible para, de esta manera, construir la infraestructura de red necesaria de forma virtual sin necesidad de incurrir en los gastos de tener los dispositivos físicos.

Las herramientas de virtualización permiten orquestar la creación de dichos dispositivos virtuales, así como interconectarlos para obtener la infraestructura de red necesaria. De esta manera, es posible solucionar los problemas planteados anteriormente de forma eficiente y económica. Además, la virtualización muestra, a diferencia de los simuladores, un comportamiento real del sistema; por lo tanto, permite disponer y configurar infraestructuras de *networking* con costos muy bajos, facilitando la implementación de entornos de experimentación y de enseñanza. Mediante el uso de la virtualización, los conceptos fundamentales de las redes de datos pueden aplicarse de forma práctica en ambientes casi reales (figura 7.3).

Figura 7.3 Virtualización en redes

Resultados y objetivos

Se plantea por un lado una investigación tendiente a exponer la evolución y estado actual de la virtualización aplicada a las redes de datos; así como a la búsqueda, la selección y la prueba de las herramientas más difundidas de *software* libre de virtualización de redes.

◉ 7.2.4 Cableado estructurado, estándares y nuevos componentes

Motivación

En la actualidad, los diseños de las redes locales de datos deben proveer calidad, flexibilidad, valor y funcionalidad, no sólo para cubrir las necesidades actuales, sino también para soportar los requerimientos futuros (figura 7.4).

La supervivencia de las organizaciones actuales depende de la confiabilidad y efectividad del intercambio de información y éste a su vez de la confiabilidad y efectividad del diseño de su infraestructura de red (ANSI/TIA/EIA-606A, 2002). Mediante la instalación de cableado estructurado se busca crear una infraestructura que sea altamente confiable con capacidad de ofrecer servicios de telecomunicaciones de acuerdo con los nuevos requerimientos para el manejo de la información.

De manera tradicional, la infraestructura de cableado de un edificio corporativo es en lo último en lo que se piensa; de hecho, los cables no son contemplados en el presupuesto de construcción inicial, por lo que su planeación e instalación se realiza cuando el edificio está listo para ocuparse y, por lo general, se utilizan varios tipos de cables para distintas funciones (ANSI/TIA/EIA-568-B.1, 2001). Es posible entonces afirmar que el cable ocupa una de las últimas jerarquías en las preocupaciones de los propietarios, los ingenieros y los arquitectos; por lo tanto, considerando que existe una demanda permanente de este tipo de redes, y que en cualquier edificación nueva se debe instalar una red de cableado confiable para el transporte y distribución de los servicios de telecomunicaciones, lo ideal es esclarecer el tema de cableado estructurado propuesto en cuanto a las

normativas internacionales vigentes, normas en el país si es que existen y nuevos componentes desarrollados, a fin de que se constituya un material de referencia para las futuras obras de cableado estructurado en una organización (ANSI/TIA/EIA-568-B.1-1, 2001).

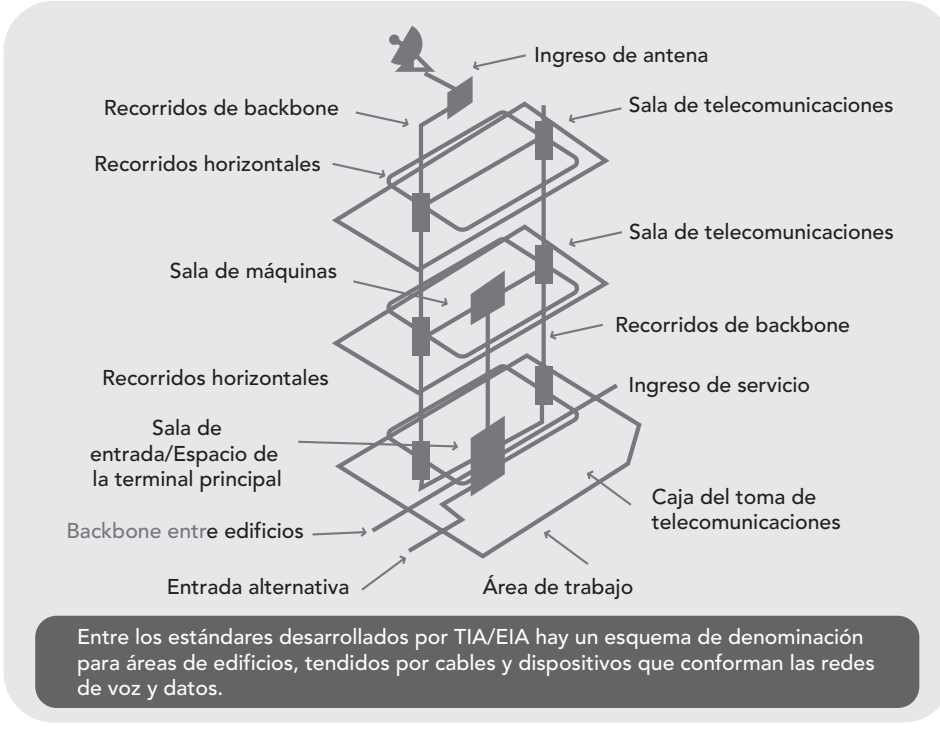


Figura 7.4 Cableado estructurado, estándares y nuevos componentes

Resultado y objetivos

Es de suma importancia realizar una investigación tendiente a exponer la normativa vigente de cableado estructurado y las nuevas tendencias en cuanto a la utilización de nuevos componentes, tal como las unidades de "parcheo" inteligentes.

7.3 Últimas tendencias en redes

Los últimos doce meses provocaron en el mundo sacudidas en aspectos políticos, económicos, sociales y tecnológicos. Pero a diferencia de los dos primeros, la tecnología trajo muchas buenas noticias que se pueden sintetizar de la siguiente forma: 2016 fue un año en el que el avance tecnológico fue tan grande, que en varios aspectos no habrá vuelta atrás.

Cada día se crean aproximadamente 2.5 quintillones de bytes en el mundo, cuyo almacenamiento requeriría 10 millones de discos *Blu-Ray*. Es tanta la información que el 90 % de los datos en la historia de la humanidad, se han recolectado o creado en los últimos dos años. Así, con un optimismo -llamado "de idealismo radical" (que no se veía desde el Siglo de la Ilustración), los tecnólogos han globalizado las ideas del Valle del Silicio (*Silicon Valley*), y están realizando innovaciones que esperan beneficien considerablemente a la población mundial.

Así, con el optimismo de que una persona que tiene acceso a Internet en un país como México, Bangladesh o Turquía tiene acceso a más información y educación que la que tenía George W. Bush cuando era presidente, la pregunta es: ¿qué está pasando en el mundo, y cómo pueden tomar ventaja los emprendedores, los empresarios y los líderes mexicanos?, ¿qué tendencias influirán en los emprendimientos del 2017, y de los años siguientes?

1) La realidad mixta llegará a las masas:

Durante el 2016, se vio la masificación de las tecnologías de Realidad Aumentada (representación del mundo físico aumentado con información digital), y de realidad virtual (simulación inmersiva de un ambiente real), con videojuegos como *Pokemon Go*, y dispositivos como el *Oculus Rift* de *Facebook*. Pero el 2017, es el año en que la realidad mixta se populariza en el mercado. La realidad mixta se puede entender como la poderosa combinación de lo mejor de dos realidades: la virtual y la aumentada. Para crear la realidad mixta, un visor superpone elementos virtuales interactivos sobre objetos reales, con tan alta precisión que le crea al usuario la ilusión de que los objetos virtuales son reales. Por ahora, Magic Leap se podría considerar como la empresa pionera de la realidad mixta, gracias al desarrollo de un visor de realidad mixta supuestamente revolucionario que saldrá al mercado este año. Con inversiones de gigantes como Google, Qualcomm y Alibaba; Magic Leap, se ha convertido en una de las *start-ups* tecnológicas más prometedoras. Microsoft es otro importante jugador en esta arena, quien anunció recientemente que, con colaboración de sus socios comerciales, lanzará en 2017 al mercado: Windows Holographic, su tecnología de realidad mixta. Cabe destacar que Holographic está detrás del innovador pero costoso dispositivo HoloLens, que se lanzó a la comunidad de desarrolladores por $3 000 USD.

2) *Chatbots* inundarán mensajería instantánea:

Llegamos al 2016 con las plataformas de mensajería (Messenger, WhatsApp, Telegram, Slack), como el tipo de aplicaciones más populares del mundo. El 2017 es el año en que los *chatbots* comenzarán a reemplazar a muchas aplicaciones móviles tradicionales y se popularizarán. Los *chatbots* o *bots* conversacionales, son programas informáticos que utilizan inteligencia artificial para mantener una conversación natural con los usuarios, por medio de alguna plataforma de mensajería. Los *chatbots* pueden servir como asistentes y facilitadores de tareas cotidianas, como pedir un taxi, consultar las noticias, o reservar una cita con el médico. Se han vuelto más prácticos que las *apps*, ya que se usan a través de aplicaciones de mensajería, por lo que no necesitan instalarse, y realizan diferentes actividades únicamente en comandos por texto. Entre los *chatbots* más utilizados se encuentran los de: CNN, Uber y WholeFoods desarrollados para Facebook Messenger, así como el "SlackBot" de Slack. Las tiendas de *chatbots* tendrán una enorme expansión en sus catálogos, y se convertirán en serios rivales de las *apps stores* convencionales. Microsoft, que durante el 2016 lanzó su Bot Framework, logró atraer ya a aproximadamente 67 000 desarrolladores y la plataforma de Facebook Messenger ya cuenta con más de 30 000 *bots*.

3) Más presencia de asistentes virtuales controlados por voz:

Los grandes avances en tecnologías de inteligencia artificial, aprendizaje automático ("*machine learning*") y procesamiento de voz han llevado a que los asistentes virtuales por voz sean cada vez más precisos, y por lo tanto, más utilizados. Siri de Apple fue el primer asistente virtual por voz en llegar a las masas, y para mediados del 2015 ya manejaba más de 1 000 millones de solicitudes de voz semanales. Luego Amazon puso a Alexa en el mercado, seguido por Microsoft con Cortana, y Google con Now y Assistant. En 2017, los asistentes virtuales controlados por voz se integran más al ecosistema del hogar inteligente a través de altavoces inteligentes como Amazon Echo, Amazon Echo Dot, y Google Home. Éstos se convierten en compañeros de hogar que apoyan en tareas rutinarias, como por ejemplo encontrar una receta para preparar la comida, revisar el correo electrónico (*e-mail*), controlar las luces de la casa, escuchar recordatorios, y otras 3 000 habilidades distintas. De hecho, Echo y Echo Dot fueron los productos más vendidos por Amazon en 2016. Sabiendo que es más fácil hablar que teclear, o hacer *click*, los gigantes de tecnología quieren llevar sus asistentes virtuales por voz al mayor número de hogares posible, por lo que están abriendo sus plataformas para fabricantes de *hardware*, y desarrolladores de las *apps*.

4) Taxis autónomos circulan por las calles:

En 2016, 70 000 personas recorrieron 1 255 millones de kilómetros en el modo autopiloto de los vehículos semiautónomos Tesla. Google completó otro año más con 60 vehículos semiautónomos rodando por las calles. El saldo fue notable: un accidente por compañía atribuible al vehículo y, sobre todo, una cantidad brutal de información recolectada para ayudar a mejorar la ingeniería y el marco normativo global de esta tecnología. Además, Uber comenzó a experimentar con automóviles en Pittsburgh y San Francisco. El 2017 es decisivo para la industria, pues ya se ven más alianzas entre compañías de *software*, de manufactura de *chips*, y de automóviles. Las marcas tradicionales de automóviles anunciaron que comercializarán sus vehículos entre el 2018 y 2021. A este ritmo exponencial, se esperaría que los automóviles totalmente autónomos lleguen entre 2022 y 2023, y que estarían en todo el mundo para el 2025. Para esa época, los automóviles autónomos estarán circulando todo el tiempo, y permitirán prescindir de 80 % de los automóviles convencionales, ganando el espacio que ocupan por estacionarse. Más aún, quedará en el pasado el número de percances por conducción humana de automóvil, que en 2016 llegó a 1.1 millones de fallecimientos alrededor del mundo, y a 31 millones de lesionados. La principal preocupación actual de los tecnólogos es demostrar que la tecnología es segura. Esto ayudará a que la regulación sea más amigable a sus intereses, sabiendo que la mayoría de países no tienen regulación al respecto. Otros debates futuros incluirán el papel de la privacidad, el riesgo de *hackeo*, y la baja significativa de empleos como chofer de taxi, tráiler o autobús.

5) Nuevas colaboraciones entre humano y máquina:

La inteligencia artificial (IA) permite juntar los mejores atributos intelectuales y de raciocinio de los seres humanos con la capacidad de procesamiento de las computadoras. Así, humano y máquina se han unido por medio de la IA para alcanzar nuevos niveles en el ajedrez, en el diagnóstico médico, en la selección de contenido(s), y la elección de compras. A través del aprendizaje automático (*machine learning*) y del aprendizaje profundo (*deep learning*), la inteligencia artificial se usará en aplicaciones como el diagnóstico y la monitorización de enfermedades, el descubrimiento y sugerencia de medicamentos y tratamientos, y la mejora del estilo de vida, dietas y programas de nutrición. Se espera que la telemedicina por fin despunte a través de aplicaciones como consultas vía teleconferencia, discusiones entre grupos de médicos a distancia, transmisión de fotografías, o procesamiento de análisis clínicos en línea (*online*), el conserje médico, y una gestión digital de prescripciones. Estos sistemas están migrando la filosofía "misma solución para todos los padecimientos" a una más personalizada, pues los pacientes tienen reacciones distintas. Las nuevas soluciones se distribuirán vía tiendas minoristas (*retail*), aplicaciones *one-click*, y clínicas de cuidados paliativos.

6) La corroboración de datos y de hechos (*fact-checking*) entrará en medios sociales y buscadores:

Las redes sociales y los sitios web de noticias se convirtieron en las principales fuentes de noticias, con efectos colaterales como la rápida propagación de noticias falsas. Como resultado de esto, los sitios de corroboración de datos y de hechos (*fact-checking*) se han fortalecido. Por ejemplo, durante la intensa jornada electoral estadounidense del 2016, los votantes tuvieron la opción de usar 47 sitios activos de corroboración de datos y de hechos (fact-checking) para verificar las declaraciones públicas de los candidatos. Donald Trump fue el campeón de este rubro, pues de acuerdo con PolitiFact, 76 % de sus declaraciones eran falsas, o tenían un manejo incorrecto de la información. En 2017, herramientas como Snopes, FactCheck.org y PolitiFact, se han expandido en medios sociales, buscadores y agregadores de noticias. Igualmente, los gigantes tecnológicos irán a la guerra contra sitios de noticias falsas. *Google News* (en idioma inglés), ya facilita a sus lectores comprobar la veracidad de las noticias. Además, Facebook, anunció que próximamente permitirá a los usuarios reportar contenido engañoso y usará sitios externos de corroboración de datos y de hechos (*fact-checking*) para identificar noticias falsas en su red, y etiquetarlas como de dudosa veracidad.

7) La mayoría de los bancos comenzarán a usar transacciones seguras (*blockchain*):

En 2016, 15 % de los grandes bancos del mundo comenzaron a experimentar con el uso de las transacciones seguras (blockchain); pero 66 % ya tiene planes concretos para implementarla. Los bancos le dan especial importancia a las transacciones seguras (blockchain), por ser una base de datos de registro de transacciones seguras compartida por todos los nodos de una red de computadoras. Como registra y almacena todas las transacciones de la red, ya no requiere de terceros "*de confianza*" que las dé por válidas. En 2017, la persona promedio comienza a entender que las transacciones seguras (*blockchains*) son herramientas para hacer una rearquitectura de los sistemas financiero, político y social, pues su implementación obliga a los bancos, los contadores, los notarios, los custodios, los fideicomisarios y los asesores financieros a encontrar mejores propuestas de valor, que únicamente ser intermediarios "*de confianza*" de las transacciones. Los bancos se están enfocando en actualizar sus datos en tiempo real, y en reducir costos, eliminando a los intermediarios, y acelerando las transacciones electrónicas. Así, áreas como préstamos al consumo, pago a tiendas minoristas, y el intercambio en tiempo real de información de transacciones, son ya las grandes potenciaciones de la banca (https://www.forbes.com.mx/las-7-tendencias-tecnologicas-del-2017/) [termina nota de revista].

7.3.1 El Internet de las cosas

Al igual que con varios conceptos novedosos, las raíces del Internet de las cosas (IOT, *Internet of Things*,) se pueden remontar al Instituto de Tecnología de Massachusetts (MIT), hasta llegar al trabajo del Auto-ID Center. Este grupo, fundado en 1999, realizaba investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y las tecnologías de sensores emergentes. Los laboratorios de investigación estaban conformados por siete universidades ubicadas en cuatro continentes, seleccionadas por Auto-ID Center para diseñar la arquitectura del Internet de las cosas.

Antes de analizar minuciosamente el estado actual del Internet de las cosas es importante ponerse de acuerdo en una definición: según el grupo de soluciones empresariales basadas en Internet (IBSG, *Internet Business Solutions Group*) de Cisco: "La Internet de las cosas […] es sencillamente el punto en el tiempo en el que se conectaron a la Internet, más 'cosas u objetos' que personas" (Cisco IBSG, 2011).

En el 2003 había aproximadamente 6.3 mil millones de personas en el planeta y 500 millones de dispositivos conectados a Internet. Si se divide la cantidad de dispositivos conectados por la población mundial, el resultado indica que había menos de un dispositivo (0.8) por persona. Según la IBSG, la Internet de las cosas aún no existía en 2003 porque la cantidad de cosas conectadas era relativamente escasa, dado que apenas comenzaba la invasión de los dispositivos omnipresentes, como los teléfonos inteligentes (*smartphones*). Por ejemplo, el director general de Apple, Steve Jobs, no presentó el iPhone sino hasta el 9 de enero de 2007 en la conferencia *Macworld*. Por su parte, el crecimiento explosivo de los teléfonos inteligentes y las tabletas elevó a 12.5 mil millones en 2010 la cantidad de dispositivos conectados a Internet, en tanto que la población mundial aumentó a 6.8 mil millones, por lo que el número de dispositivos conectados por persona llegó a 1.84 por primera vez en la historia (Cisco IBSG, 2010).

Entonces, en cuanto a su estado del arte, actualmente el Internet de las cosas está compuesto por una colección dispersa de redes diferentes y con distintos objetivos y aplicaciones. Por ejemplo, los automóviles actuales tienen múltiples redes para controlar el funcionamiento del motor, las medidas de seguridad, los sistemas de comunicación, los frenos, etcétera. De manera similar, los edificios comerciales y residenciales tienen distintos sistemas de control para la calefacción, la ventilación, el aire acondicionado, la telefonía, la seguridad y la iluminación. A medida que el Internet de las cosas evoluciona, estas redes y muchas otras estarán conectadas con la incorporación de capacidades de seguridad, análisis y administración (figura 7.5), lo que permitirá que sea una herramienta aún más poderosa.

Resulta interesante señalar que esta situación refleja lo que el sector de la tecnología experimentó en los primeros días de la red. Por ejemplo, a finales de la década de 1980 y a comienzos de 1990, Cisco entró en el mercado aunando redes dispares con ruteo multiprotocolo, lo que luego condujo al establecimiento de IP como la norma de redes común. Con el Internet de las cosas, la historia se repite, aunque en una escala drásticamente más grande, con más involucrados y con mucho mejores resultados.

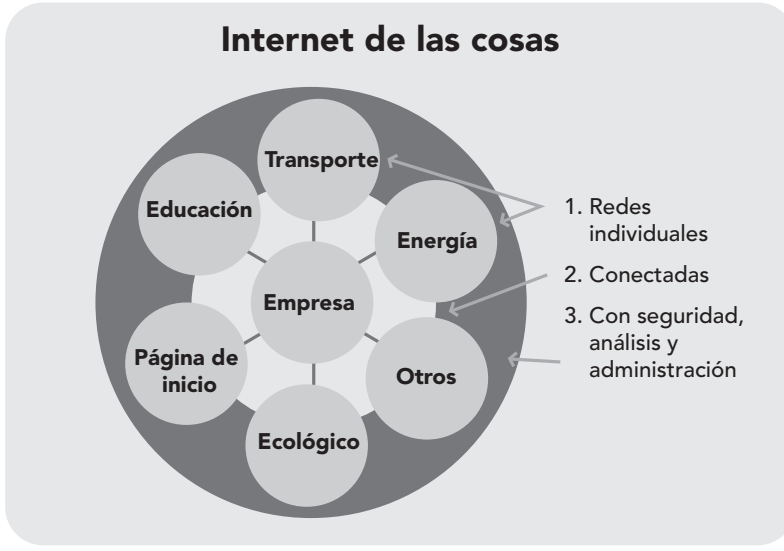


Figura 7.5 Aplicaciones del Internet de las cosas

Hace veinticinco años, cuando nació la primera conexión entre redes dispersas geográficamente, nadie hubiese imaginado el rotundo cambio que el desarrollo de lo que hoy se conoce como Internet iba a producir. Como se sabe, en la actualidad, Internet reinventa de forma continua la manera en la que las personas trabajan, aprenden, viven y juegan.

Por su lado, el Internet de las cosas generará un cambio aún mayor al vivido en los últimos 25 años; esto de forma más rápida, más crítica y con un impacto social infinitamente mayor.

El Internet de las cosas no es un producto, no es una tecnología, no es algo que se pueda comprar o tomar de una estantería ni algo que no existía en el pasado; pero la madurez de las tecnologías, el desarrollo de las aplicaciones y la manera en que actualmente se vive hace que este concepto tome forma y se haga realidad.

Para comprender cabalmente lo que es el Internet de las cosas debe recorrerse y recordarse la evolución que como sociedad se ha vivido y tenido en los últimos 25 años, lo que hoy puede confirmar lo mucho que ha cambiado la vida de las personas en apenas un periodo generacional: se acepta y se convive con la tecnología, lo cual ha representado un profundo cambio de hábitos de la vida cotidiana que, a veces, no se es capaz de analizar o dar el valor que corresponde en retrospectiva. El cambio fue principalmente generado por la llegada del Internet a las casas, escuelas y trabajos (Cazila y Junco, 2015).

De hecho, se puede decir que gran parte de la sociedad aceptó el cambio, se adecuó a él y no hay dudas de que lo que se vive hasta ahora no es más que el punto de partida de un cambio mayor, habiendo sido Internet tan solo un detonador de los nuevos paradigmas que regirán los hábitos en el futuro. Habrá que reflexionar bastante para darse cuenta de lo mucho que se han facilitado las cosas en los diversos entornos como el trabajo, el estudio, el ocio, el aprendizaje, el turismo, las compras, etc.

Aunque en un mundo globalizado es difícil que el paradigma del Internet de las cosas se vea demorado por razones de entorno particulares a un mercado concreto, en la actualidad, variables como el tiempo de adaptación del usuario no parecen un problema

como sí lo fueron en el pasado, incluso en transiciones menos disruptivas que ésta, lo que quiere decir que el Internet de las cosas (algunas veces denominado "Internet de los objetos") lo cambia todo, incluso a los propios usuarios.

Ahora se debe tener en cuenta que el Internet de las cosas representa claramente la próxima evolución de Internet, que será un enorme salto en su capacidad para reunir, analizar y distribuir datos que se puedan convertir en información, luego en conocimiento y, en última instancia, en sabiduría. En este contexto, el Internet de las cosas se vuelve inmensamente importante; por ejemplo, ya están en marcha proyectos de esta nueva tecnología que prometen cerrar la brecha entre ricos y pobres, así como mejorar la distribución de los recursos del mundo para quienes más los necesitan y ayudar a comprender mucho mejor al planeta para ser proactivos y no reactivos (figura 7.6).

Figura 7.6 Representación del uso del Internet de las cosas

El tiempo hizo posible validar las mejoras tecnológicas introducidas como reales: actualmente, por lo general, no se lleva una cámara fotográfica cuando se visita un lugar o se celebra un cumpleaños; no se requiere disponer de un GPS como dispositivo independiente; han caído en desuso los teléfonos públicos o los mapas en papel.

Hoy, al salir de casa, se toma la billetera, el *smartphone*, las llaves, y se anda con la relativa seguridad y certeza de que se porta todo lo necesario. Lo resultante de esta dinámica de cambio permanente es que muchas organizaciones importantes han desaparecido, pues no pudieron adaptarse a la nueva constante que invade el rubro de la tecnología y que rige el cambio de hábitos de vida. Sin duda, toda innovación, por pequeña que haya sido, ha dejado algo en el día a día de forma directa o indirecta, uniéndose al proceso natural de transformación constante y de cambio permanente que gobierna en estos tiempos, lo cual hace que las personas estén entrenadas para una dinámica más rápida en la adopción, adaptación, implementación y estandarización de nuevas soluciones y tecnologías.

7.3.2 La realidad aumentada

"Realidad Aumentada" (RA) es el término que se usa para definir una visión a través de un dispositivo tecnológico, directa o indirectamente, de un entorno físico del mundo real, cuyos elementos se combinan con objetos virtuales para la creación de una realidad mixta pero en tiempo real. Consiste en un conjunto de dispositivos que añaden información virtual a la información física ya existente; es decir, agregar una parte sintética virtual a lo real es la principal diferencia con la realidad virtual, puesto que no sustituye la realidad física, sino que sobreimprime los datos informáticos al mundo real. Con la ayuda de la tecnología, la información sobre el mundo real alrededor del usuario se convierte en interactiva y digital, además de que puede ser almacenada y recuperada como una capa de información en la parte superior de la visión del mundo real (Woodrow y Caudell, 2001).

La realidad aumentada de investigación explora la aplicación de imágenes generadas por computadora en tiempo real a secuencias de video como una forma de ampliar el mundo real. La investigación incluye el uso de pantallas colocadas en la cabeza, un display virtual en la retina (para mejorar la visualización) y la construcción de ambientes controlados a partir sensores y actuadores.

Recientemente, el término "realidad aumentada" se ha difundido por el creciente interés del público en general (figura 7.7). En cuanto a las diversas definiciones que sobre la realidad aumentada existen, se tiene que una de ellas fue dada por Ronald Azuma (1997), quien establece para ésta las siguientes características:

- Combina elementos reales y virtuales.
- Es interactiva en tiempo real.
- Está registrada en 3D.

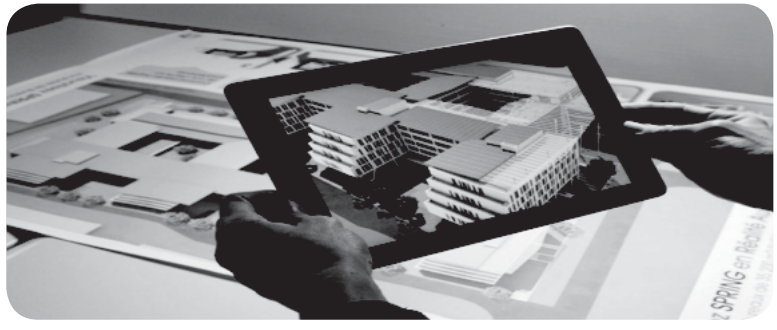


Figura 7.7 Aplicación de la realidad aumentada

La realidad aumentada también es la incorporación de datos e información digital en un entorno real por medio del reconocimiento de patrones, la cual se realiza mediante un *software* especial; en otras palabras, es una herramienta interactiva que está dando sus primeros pasos alrededor del mundo y que en unos años será observada en todas partes: los videojuegos, los medios masivos de comunicación, la arquitectura, la educación e incluso en la medicina, trayendo realmente un mundo digital hasta hoy inimaginable y desconocido; pero lleno de posibilidades en el entorno real. Su gran diferencia con la realidad virtual es que ésta extrae de su contexto a las personas para llevarlas a una realidad objetiva.

Los sistemas de realidad aumentada modernos utilizan una o más de las siguientes tecnologías: cámaras digitales, sensores ópticos, acelerómetros, GPS, giroscopios, brújulas de estado sólido, RFID, etcétera. La combinación de todos estos elementos se da frecuentemente en los teléfonos inteligentes de última generación, convirtiéndose en una posible plataforma para la realidad aumentada (figura 7.8) (Nister; Naroditsky yBergen, 2004).

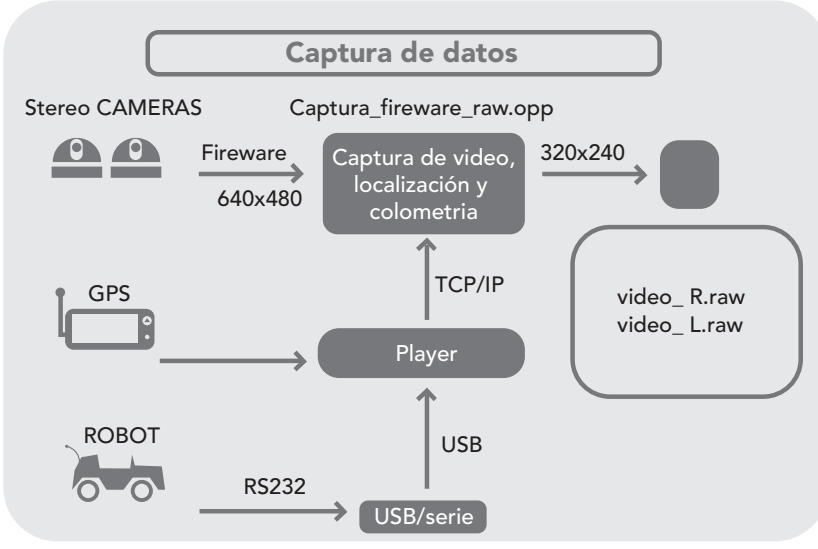


Figura 7.8 Ejemplos de herramientas utilizadas para la realidad aumentada

Existen tres técnicas principales para mostrar la realidad aumentada:

Display en la cabeza. Esta pantalla instalada en la cabeza (HMD, *Head-Mounted Display*) muestra tanto las imágenes de los lugares del mundo físico y social donde las personas se encuentran, como los objetos virtuales sobre la vista actual del usuario. Los HMD son dispositivos ópticos que permiten al usuario ver el mundo físico a través de la lente y superponer información gráfica que se refleja en los ojos del usuario. El HMD debe ser rastreado con un sensor. La información gráfica está condicionada a la vista de los usuarios.

Display de mano. El dispositivo manual con realidad aumentada cuenta con un dispositivo informático que incorpora una pantalla pequeña que cabe en la mano de un usuario. Todas las soluciones utilizadas hasta la fecha por los diferentes dispositivos de mano han empleado técnicas de superposición sobre el video con la información gráfica. Inicialmente, los dispositivos de mano empleaban sensores de seguimiento tales como las brújulas digitales y el GPS que añadían marcadores al video. Más tarde, el uso de sistemas como *ARToolKit*, permitían agregar información digital a las secuencias de video en tiempo real. Hoy, los sistemas de visión como SLAM o PTAM son empleados para el seguimiento. El *display* de mano promete ser el primer éxito comercial de las tecnologías de la realidad aumentada. Sus dos principales ventajas son el carácter portátil de los dispositivos de mano y la posibilidad de ser aplicada en los teléfonos con cámara.

Display espacial. La realidad aumentada espacial (SAR, *Spatial Augmented Reality*) hace uso de proyectores digitales para mostrar información gráfica sobre los objetos físicos. La diferencia clave es que la pantalla está separada de los usuarios del sistema debido a que no se encuentra asociada a cada usuario. La SAR tiene varias ventajas sobre el tradicional *display* colocado en la cabeza y sobre los dispositivos de mano: el usuario no está obligado a llevar el equipo encima ni a someterse al desgaste de la pantalla sobre los ojos; esto hace del display espacial un buen candidato para el trabajo colaborativo, ya que los usuarios pueden verse las caras. Éste no se halla limitado por la resolución de la pantalla, que sí afecta a los dispositivos anteriores. Los dispositivos portátiles tienen una pequeña ventana al mundo para representar la información virtual, en cambio, en un sistema SAR se puede mostrar un mayor número de superficies virtuales a la vez en un entorno interior. Es una herramienta útil para el diseño, ya que permite visualizar una realidad que es tangible de forma pasiva.

Por otro lado, según Prendes Espinosa (2015), los denominados "niveles de la realidad aumentada" pueden definirse como los distintos grados de complejidad que presentan las aplicaciones basadas en la realidad aumentada según las tecnologías que implementan; en consecuencia, cuanto mayor sea el nivel de una aplicación, más ricas y avanzadas serán sus funcionalidades y sus prestaciones. En este sentido, Fitzgerald (2009), uno de los navegadores de realidad aumentada más extendidos en la actualidad, propone una clasificación en cuatro niveles (de 0 a 3):

Nivel 0 (*Physical world hyper linking*). En este nivel, las aplicaciones hiperenlazan el mundo físico mediante el uso de códigos de barras y 2D (por ejemplo, los códigos QR) sin registro alguno en 3D ni seguimiento de algún tipo de marcadores.

Nivel 1 (*Marker Based AR*). Las aplicaciones utilizan marcadores (imágenes en blanco y negro, cuadrangulares y con dibujos esquemáticos), habitualmente para el reconocimiento de patrones 2D. La forma más avanzada de este nivel también permite el reconocimiento de objetos 3D.

Nivel 2 (*Markerless AR*). Las aplicaciones sustituyen el uso de los marcadores por el GPS y la brújula de los dispositivos móviles para determinar la localización y orientación del usuario y superponer "puntos de interés" sobre las imágenes del mundo real.

Nivel 3 (*Augmented Vision*). Se representa por dispositivos como *Google Glass*, lentes de contacto de alta tecnología u otros que, en el futuro, serán capaces de ofrecer una experiencia completamente contextualizada, inmersiva y personal.

Entre las actuales aplicaciones, la realidad aumentada ofrece infinidad de nuevas posibilidades de interacción que provocan que esté presente en muchos y muy variados ámbitos, tales como la arquitectura, el entretenimiento, la educación, el arte, la medicina o las comunidades virtuales. A continuación, se desarrollan y explican algunas de las aplicaciones que se tienen para la realidad aumentada:

Proyectos educativos. En la actualidad, la mayoría de aplicaciones de realidad aumentada para proyectos educativos se usan en museos, exhibiciones y parques de atracciones temáticos, puesto que su costo todavía no es suficientemente bajo para que puedan ser empleadas en el ámbito doméstico. Estos lugares aprovechan las conexiones inalámbricas para mostrar información sobre

objetos o lugares, así como imágenes virtuales; por ejemplo, ruinas reconstruidas o paisajes tal y como eran en el pasado, además de escenarios completos en realidad aumentada, donde se pueden apreciar e interactuar con los diferentes elementos en 3D. Una de las primeras aplicaciones en formación es un sistema de realidad aumentada para aprender a soldar sin riesgos y realizando todas las horas de prácticas necesarias sin costo añadido. También se han desarrollado aplicaciones de realidad aumentada para la educación infantil, que interaccionan con juguetes físicos como un globo terráqueo.

Televisión. La realidad aumentada se ha vuelto común en la teledifusión de deportes. La línea amarilla del "primero y diez" vista en las transmisiones de los partidos de futbol americano muestra la marca que la ofensiva del equipo debe cruzar para recibir dicha jugada. Los elementos del mundo real son el campo de futbol y los jugadores, y el elemento virtual es la línea amarilla electrónica, que aumenta la imagen en tiempo real. La realidad aumentada también se utiliza en las transmisiones de futbol para mostrar el resultado en el círculo central o para exponer las situaciones de fuera de juego. Del mismo modo, en los partidos de *hockey* sobre hielo se colorea en realidad aumentada la ubicación y dirección de la pastilla (*puck*), aunque esto fue rechazado por los puristas del *hockey*. Por otro lado, las transmisiones de natación suelen añadir una línea a través de los carriles para indicar la posición del poseedor del récord actual y compararla con la carrera.

Entretenimiento. En consideración de que los juegos son un mercado que mueve aproximadamente unos 30 000 millones de dólares al año en los Estados Unidos de América, es comprensible que se esté apostando mucho por la realidad aumentada en dicho campo, puesto que posibilita aportar nuevas opciones a la manera de jugar. Una de las puestas en escena más representativas de la realidad aumentada es el *Can You See Me Now de Blast Theory*, que es un juego en línea de persecución por las calles, donde los jugadores empiezan en localizaciones aleatorias de una ciudad, llevan una computadora portátil y están conectados a un receptor de GPS. El objetivo del juego es procurar que otro corredor no llegue a menos de 5 metros de ellos, puesto que, en este caso, se les hace una foto y pierden. Otro de los proyectos con más éxito es el *ARQuake Project*, donde se puede jugar *Quake* en exteriores disparando contra monstruos virtuales. A pesar de estas aproximaciones, todavía es difícil obtener beneficios del mercado de los juegos, puesto que el *hardware* es muy costoso y se necesitaría mucho tiempo de uso para amortizarlo.

Simulación. Se puede aplicar la realidad aumentada para simular vuelos y trayectos terrestres.

Servicios de emergencia y en aplicaciones militares. En caso de emergencias, la realidad aumentada puede servir para mostrar instrucciones de evacuación de un lugar. En el campo militar, presenta información de mapas, la localización de los enemigos, la entrada y la salida de una zona de combate, etc.

Arquitectura. La realidad aumentada es muy útil a la hora de "resucitar" virtualmente edificios históricos destruidos, así como proyectos de construcción que todavía están bajo los planos para su posible edificación.

Apoyo en la realización de tareas complejas, difíciles y/o repetitivas. Las tareas complejas como el montaje, el mantenimiento y la cirugía pueden simplificarse mediante la inserción de información adicional en el campo de visión.

Por ejemplo, para un mecánico que está realizando el mantenimiento de un sistema, las etiquetas pueden mostrar las partes de éste para aclarar su funcionamiento.

La realidad aumentada posibilita incluir imágenes de los objetos ocultos que pueden ser especialmente eficaces para el diagnóstico médico o la cirugía. Esto se ejemplifica en una radiografía de rayos X vista virtualmente y basada en la tomografía previa o en las imágenes en tiempo real de los dispositivos de ultrasonido o de resonancia magnética nuclear abierta.

Dispositivos de navegación. La realidad aumentada mejora la efectividad de los dispositivos de navegación para una variedad de aplicaciones. Por ejemplo, la navegación dentro de un edificio puede ser mejorada con el fin de dar soporte al encargado del mantenimiento de instalaciones industriales. Por otro lado, los parabrisas de los automóviles pueden ser usados como pantallas de visualización para proporcionar indicaciones de navegación e información de tránsito.

Aplicaciones industriales. La realidad aumentada puede ser utilizada para comparar los datos digitales de las maquetas físicas con su referente real para encontrar de manera efectiva discrepancias entre las dos fuentes. Además, se puede emplear para salvaguardar los datos digitales en combinación con prototipos reales existentes y así ahorrar y/o reducir al mínimo la construcción de prototipos reales y mejorar la calidad del producto final. Por ejemplo, el Instituto Tecnológico Metalmecánico presentó recientemente los resultados del Proyecto ARMETAL, llamado *Viabilidad de la realidad aumentada aplicada a empresas*, mostrando las experiencias piloto desarrolladas en cooperación con empresas de diversos subsectores, como son los fabricantes de maquinaria, de joyería, de herrajes, de componentes electrónicos y de luminarias aplicadas a diversos procesos empresariales y a la vez sobre diversos dispositivos, recopilando dicha información en un documento llamado *Manual de buenas prácticas sobre aplicación de la realidad aumentada* (AIMME, 2016).

Prospección. En los campos de la hidrología, la ecología y la geología, la realidad aumentada puede ser utilizada para mostrar un análisis interactivo de las características del terreno. El usuario puede utilizar, modificar y analizar hasta tres mapas bidimensionales interactivos simultáneamente.

Colaboración. La realidad aumentada puede ayudar a facilitar la colaboración entre los integrantes de un equipo de trabajo a través de conferencias con los participantes reales y virtuales.

Publicidad. Hay diferentes campañas que utilizan la realidad aumentada para llamar la atención del usuario. La armadora de automóviles italiana Fiat ha lanzado una campaña en la que cualquier usuario puede crear su propio anuncio de televisión con el Fiat 500 como protagonista a través de su sitio web, para lo que el usuario solamente necesita tener una *webcam*. Por otro lado, la revista Esquire publicó en el 2014 diferentes códigos QR, los cuales, al ser reconocidos, ofrecen información extra sobre el producto.

Turismo. *Aplicaciones como La Ciudad de México en el Tiempo*, de ILLUTIO, han logrado llevar a los usuarios a recorrer la ciudad en sus diferentes épocas históricas a través de la realidad aumentada y la geolocalización (Ruíz Torres, 2011). Por otro lado, plataformas como *Junaio* o *Layar* permiten el desarrollo de aplicaciones a terceros, prácticamente sin conocimientos técnicos, a través

de sus servidores. Esto ha fomentado la publicación de miles de aplicaciones sobre turismo, *gincanas*,[2] exposiciones virtuales, etc.

Información. La empresa austriaca Mobilizy ha desarrollado *Wikitude*, la cual permite que, al apuntar la cámara del móvil hacia un edificio histórico, el GPS reconozca la localización y muestre información proveniente de *Wikipedia* sobre el monumento. En Japón, *Sekai Camera*, de la empresa Tonchidot añade al mundo real los comentarios de la gente acerca de direcciones, tiendas y restaurantes. También, Acrossair, disponible en siete ciudades, entre ellas Madrid y Barcelona, identifica en la imagen la estación de metro más cercana (*Bionic Eye y Yelp Monocle*, en los Estados Unidos de América, son ejemplos similares).

Networking y actividades. La empresa mexicana ILLUTIO ha desarrollado BIC (*Business Intelligent Card*), la cual reconoce la imagen o logo de una empresa en una tarjeta de presentación y muestra un video, animación o modelo 3D sobre ésta; además, guarda los datos de contacto en la nube sin necesidad de preocuparse por perder o guardar las tarjetas físicas.

Por último, en un futuro muy cercano, la realidad aumentada deberá tener modelos informáticos de lugares y sonidos relacionados con la realidad física, así como determinar la situación exacta de cada usuario y ser capaz de mostrarle una representación realista del entorno que se ha añadido virtualmente. Es muy importante precisar la orientación y posición exacta del usuario, sobre todo en las aplicaciones que así lo requieran: uno de los retos más importante que se tiene a la hora de desarrollar proyectos de realidad aumentada es que los elementos visuales estén coordinados a la perfección con los objetos reales, puesto que un pequeño error de orientación puede provocar un desalineamiento perceptible entre los objetos virtuales y los físicos. En zonas muy amplias, los sensores de orientación usan magnetómetros, inclinómetros, sensores inerciales, etcétera, que realmente pueden verse afectados de manera seria por campos magnéticos y, por lo tanto, se ha de intentar reducir al máximo este efecto.

Como reto a muy largo plazo, es posible sugerir el diseño de aplicaciones en los que la realidad aumentada fuera un poco más allá, lo que podría llamarse tentativamente "una realidad aumentada retroalimentada", esto es, que la "descoordinación" resultante del uso de los sensores de posición/orientación fuera corregida midiendo las desviaciones entre las medidas de los sensores y las del mundo real. Podría imaginarse un sistema de realidad aumentada que partiendo de pares de imágenes estéreo obtenidas de dos cámaras solidarias al usuario (*head-mounted*) fuera capaz de determinar la posición y orientación exacta del que mira.

Es importante señalar que la realidad aumentada es un desarrollo costoso de la tecnología, debido a ello, el futuro de ésta depende de si esos costos se pueden reducir de alguna manera, ya que si la tecnología de la realidad aumentada se hace asequible podría ser muy amplia, pero, por ahora, las principales industrias son los únicos compradores que tienen la oportunidad de utilizar este recurso.

[2] Prueba o concurso en que los participantes deben pasar por muchas pruebas y obstáculos antes de llegar a la meta.

7.3.3 Web 3.0

La web 3.0 es una expresión que se utiliza para describir la evolución del uso y la interacción de las personas en Internet a través de diferentes maneras, entre las que se incluyen la transformación de la red en una base de datos, un movimiento social con el objetivo de crear contenidos accesibles por múltiples aplicaciones sin navegador (*non-browser*), el empuje de las tecnologías de inteligencia artificial, la web semántica, la web geoespacial o la web 3D. La expresión apareció por primera vez en 2006 en un artículo de Jeffrey Zeldman, crítico de la web 2.0 y asociado a tecnologías como AJAX, y es utilizada por los mercados para promocionar las mejoras respecto a la web 2.0.

En la actualidad, existe un debate considerable en torno a lo que realmente significa la web 3.0 y cuál es su definición más adecuada, sin que aún se haya llegado a un acuerdo concreto; sin embargo, se ha hecho un esfuerzo importante por definir la idea, así como sus principales aplicaciones. Debe tomarse en cuenta, sin embargo, que la web 4.0 ya está en desarrollo (Wells, 2007). La figura 7.9 muestra las aplicaciones de la web 3.0.

Figura 7.9 Aplicaciones reales de la web 3.0

Las tecnologías de la web 3.0, como son los programas inteligentes que utilizan datos semánticos, se han implementado y usado a pequeña escala en ciertas organizaciones para conseguir una manipulación de datos más efectiva. En los últimos años; sin embargo, ha habido un mayor enfoque dirigido a trasladar estas tecnologías de inteligencia semántica[3] al público en general. A continuación, se presentan algunas de dichas aplicaciones:

[3] La inteligencia semántica es, básicamente, un tipo de tecnología que es capaz de "entender" el significado de las palabras por su contexto. Esto es muy relevante por dos motivos fundamentales: a medida que aumenta la cantidad de información digital, y sobre todo la información desestructurada, se hace más difícil filtrarla de forma efectiva. Por otra parte, la inteligencia semántica es capaz de analizar el "lenguaje natural" (las personas no hablan como máquinas, e incorporan errores gramaticales, licencias lingüísticas, expresiones, coloquialismos, ironías, etcétera). Por supuesto, no es una ciencia exacta. Se fundamenta en algoritmos avanzados que "aprenden" por sí mismos: cuanto mayor sea la cantidad de información analizada, más ajustados podrán ser los resultados. Es lo que hace posible, por ejemplo, que existan los asistentes virtuales, que se puedan realizar búsquedas inteligentes de información (que no sólo rastreen palabras clave), que se efectúen grandes análisis de texto multilingüe o que las empresas puedan realizar una segmentación de sus usuarios mucho más realista.

Bases de datos. El primer paso hacia la web 3.0 es el nacimiento de la *Data web*, ya que los formatos en que se publica la información en Internet son dispares, como XML, RDF y microformatos; el reciente crecimiento de la tecnología SPARQL permite un lenguaje estandarizado y API para la búsqueda a través de bases de datos en la red. La *Data web* permite un nuevo nivel de integración de datos y de aplicación interoperable, haciendo los datos tan accesibles y enlazables como las páginas web. La *Data web* es el primer paso hacia la completa web semántica y su objetivo es principalmente hacer que los datos estructurados sean accesibles utilizando RDF. El escenario de la web semántica ampliará su alcance en tanto que los datos estructurados e incluso lo que tradicionalmente se ha denominado contenido semiestructurado esté disponible en los formatos semánticos de RDF y OWL (Markoff, 2006).

Inteligencia artificial. La web 3.0 también ha sido utilizada para describir el camino evolutivo de la red que conduce a la inteligencia artificial. Algunos escépticos lo ven como una visión inalcanzable, empero, compañías como IBM y Google actualmente ya están implementando nuevas tecnologías que cosechan información sorprendente, como el hecho de hacer predicciones de canciones que serán un éxito, tomando como base de información las webs de música a nivel internacional. Existe también un debate sobre si la fuerza conductora tras web 3.0 serán los sistemas inteligentes, o si la inteligencia vendrá de una manera orgánica; es decir, a través de sistemas de inteligencia humana y de servicios colaborativos como del.icio.us, Flickr y Digg, que extraen el sentido y el orden de la red existente, y cómo la gente interactúa con dicha red.

La web semántica y arquitecturas orientadas a servicios (*SOA, Service Oriented Architecture*). En relación con la dirección de la inteligencia artificial, la web 3.0 podría ser la realización y extensión de la "web semántica". Las investigaciones académicas están dirigidas a desarrollar programas que puedan razonar, basados en descripciones lógicas y agentes inteligentes. Dichas aplicaciones pueden llevar a cabo razonamientos lógicos utilizando reglas que expresan relaciones lógicas entre conceptos y datos en la red (Wainewright, 2005). Mitra difiere con la idea de que la web semántica será la esencia de la nueva generación de Internet y propone una fórmula para encapsular la web 3.0 (Mitra, 2005). Este tipo de evoluciones se apoyan en tecnologías de llamadas asíncronas para recibir e incluir los datos dentro del visor de forma independiente. También permiten la utilización en dispositivos móviles o algunos accesibles para personas con algún tipo de discapacidad (visual, auditiva, motriz, lingüística, cognitiva, etcétera) o que utilizan diferentes idiomas para comunicarse sin transformar los datos.

Para los visores. En la web, xHTML, JavaScript, Comet, AJAX, etc.

Para los datos. Los lenguajes de programación interpretados, bases de datos relacionales y protocolos.

Evolución al 3D. Otro posible destino para la web 3.0 es la dirección hacia la visión 3D liderada por el Web3D Consortium. Esto implicaría la transformación de la web en una serie de espacios 3D, llevando más lejos el concepto propuesto por Second Life (Wallensteinn, 2007). Esto podría abrir nuevas formas de conectar y colaborar, utilizando espacios tridimensionales (Wells, 2007). En lo que a su aspecto semántico se refiere, la web 3.0 es una extensión de la *World Wide Web* en la que se puede expresar no sólo el lenguaje natural, sino

que se puede utilizar un lenguaje que se puede entender e interpretar por agentes bajo un *software* prestablecido, permitiendo de este modo encontrar, compartir e integrar la información más fácilmente.

La web 3.0 constituye y configura un nuevo tipo de web en la que se añade contenido semántico a los documentos que la conforman; lo que conlleva a que la ejecución de ésta sea realizada por máquinas que, basándose en ciertos perfiles en la red, descubren información para los usuarios o clientes. Un ejemplo claro es que en la web "tradicional" los usuarios, tras buscar información sobre el tema "gato" a través de Google, obtendrían todo tipo de felinos; por su lado, la propia web semántica presentaría diferentes alternativas de la búsqueda de "gato" pero desde una perspectiva mecánica.

"*La web 3.0 se encarga de definir el significado de las palabras y de esta manera facilitar que un contenido web pueda ser portador de un significado adicional que va más allá del propio significado textual de dicho contenido*". (Google Webmaster Central Blog, 2015).

Desde el punto de vista de la mercadotecnia, esta web 3.0 permite construir un mensaje publicitario que será difundido mediante una tecnología digital avanzada. La codificación semántica de dicho mensaje puede incluir información no presente a simple vista para el usuario. Efectivamente, las tecnologías de la web 3.0 que utilizan datos semánticos se han implementado y usado a pequeña escala en compañías para conseguir una acumulación y personalización de datos más efectiva.

En resumen, la web 3.0 marca los principios para crear una base de conocimiento e información semántica y cualitativa. Se pretende con ello almacenar las preferencias de los usuarios (gustos, costumbres, conectividad, interactividad, usabilidad, etcétera) y, al mismo tiempo, combinarlas con los contenidos existentes en redes sociales e Internet móvil, entre muchos otros, para así atender de forma más precisa las demandas de información y facilitar la accesibilidad a los contenidos digitales, proporcionando con ello una herramienta esencial para la aceptación, la adopción, el flujo y la funcionalidad de la publicidad de una organización con el objetivo de fidelizar al usuario con las marcas que se presentan en la red.

7.3.4 Web 4.0

La web 4.0 propone un nuevo modelo de interacción con el usuario más completo y personalizado, no limitándose simplemente a mostrar información, sino comportándose como un espejo mágico que ofrezca soluciones concretas a las necesidades del navegante. La web 4.0 es una capa de integración necesaria para la explotación de la web semántica y sus enormes posibilidades (figura 7.10).

La web 4.0 es un nuevo modelo de Internet que nace con el objetivo de resolver las limitaciones de la red al día de hoy. Actualmente, las formas que tiene un usuario de interactuar con la web son muy limitadas. Una parte fundamental de Internet son los buscadores; sin embargo, con el tiempo se ha ido aprendiendo sobre su funcionamiento y las personas que los utilizan se han adaptado a sus limitaciones, que principalmente consisten en que no hablan el lenguaje del usuario, por lo que no son capaces de responder a preguntas como "¿En qué año murió Kennedy?", ya que no son capaces de entenderla.

La web semántica promete mejorar este problema aplicando técnicas de procesado del lenguaje natural, pero la solución que propone no es suficiente. La web 3.0 será capaz de responder a la pregunta anterior, pero la novedad se limitará a obtener resultados

de búsqueda más precisos; esto significa que nunca podrá responder consultas del tipo: "Quiero que un taxi venga a buscarme", lo que sí podrá llevar a cabo la web 4.0 sin intervención directa del usuario, pues el teléfono móvil se comunicará automáticamente con la compañía de taxis más cercana. La web 4.0 se fundamenta en cuatro pilares principales:

Comprensión del lenguaje natural (NLU, Natural Language Understandig). Que incluye las técnicas de *Speech-to-Text*.

Nuevos modelos de comunicación máquina-máquina (M2M, *Machine to Machine*). La red estará formada por agentes inteligentes en la nube que serán capaces de comunicarse entre sí y de delegar la respuesta al agente adecuado.

Uso de información de contexto del usuario. *Sentimental analysis*, geolocalización, sensores, entre muchas otras posibilidades de aplicación.

Nuevo modelo de interacción con el usuario. Para que la web no se convierta en un mero almacén de información (*datawarehouse*), o en un simple receptáculo ocioso, son necesarios nuevos modelos de interacción , además de ejecutar acciones concretas que den respuesta a las necesidades de los usuarios haciendo hincapié en su uso sobre dispositivos móviles.

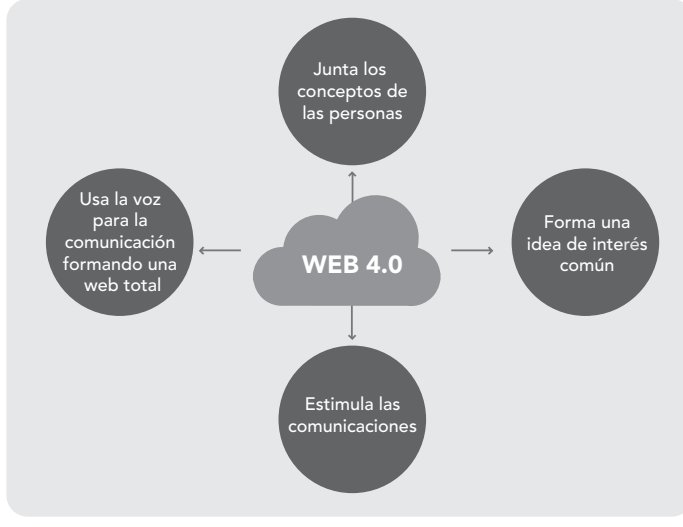


Figura 7.10 Aplicaciones reales de la web 4.0

La web 4.0 se empieza a plantear como una realidad futura en que los sistemas operativos y los programas locales dejarán de existir o coexistirán con los programas ubicados en los servidores. Si se tienen en cuenta los parámetros de la ley de Moore,[4] la velocidad de acceso será mucho más rápida, los componentes mucho más pequeños y los gadgets personales digitales tendrán una inteligencia casi humana (Kurzweil, 1999, 2005).

[4] Esta ley expresa que aproximadamente cada dos años se duplica el número de transistores en una computadora. Se trata de una ley empírica formulada por Gordon E. Moore en1965, la cual se ha podido constatar hasta la actualidad. Los principios que propone esta ley son los siguientes: 1) Cada 18 meses se duplica la potencia y sube 2 % del costo; 2) Cada 10 años se pasa a otro orden de magnitud y 3) La mejor computadora de la actualidad tiene 1 % de la potencia de la que tendrá dentro de 20 años.

En resumen, la web 4.0 es el avance más grande en las telecomunicaciones, ya que con esta tecnología se facilita la investigación a través de la creación de un sistema operativo tan rápido en respuesta como lo es el cerebro humano.

7.3.5 Drones

El término dron, recogido en la 23ª edición del *Diccionario de la Lengua Española*, derivado por asimilación del inglés drone, que literalmente significa "zángano", designa a diversos tipos de vehículos aéreos no tripulados. En una primera etapa, se aludía a aparatos básicamente de uso militar y con aspecto similar al de un avión, por lo que se extendió como alternativa al término procedente del inglés la expresión "avión no tripulado", que puede considerarse adecuada en muchos casos. No obstante, en los últimos tiempos han surgido otros vehículos que no guardan apenas semejanza con los aviones. Para ellos, pueden emplearse expresiones más genéricas como "vehículos aéreos no tripulados" o "robots voladores", según los casos.

Un vehículo aéreo no tripulado (VANT), UAV (*Unmanned Aerial Vehicle*), es una aeronave que vuela sin tripulación. Aunque hay VANT de uso civil, también son usados en aplicaciones militares, donde son denominados "vehículo aéreo de combate no tripulado" (UCAV, *Unmanned Combat Aerial Vehicle*). Un VANT se define como un vehículo sin tripulación reutilizable, capaz de mantener de manera autónoma un nivel de vuelo controlado y sostenido y propulsado por un motor de explosión o de reacción.

Hay una amplia variedad de formas, tamaños, configuraciones y características en el diseño de los drones. Históricamente, éstos eran simplemente aviones pilotados remotamente, pero cada vez se está empleando más su control autónomo. En este sentido, se han creado dos variantes: algunos son controlados desde una ubicación remota y otros vuelan de forma autónoma sobre la base de planes de vuelo preprogramados, usando sistemas más complejos de automatización dinámica.

Cabe destacar que las aeronaves controladas remotamente en realidad no califican para ser llamadas como VANT, ya que los vehículos aéreos pilotados remotamente (o por control remoto) se conocen como aeronaves radiocontroladas o aeronaves R/C; esto debido a que, precisamente, los VANT son también sistemas autónomos que pueden operar sin intervención humana alguna durante su funcionamiento en la misión a la que se hayan encomendado; es decir, pueden despegar, volar y aterrizar automáticamente. Sin embargo, con el paso de los años los drones han logrado otros tipos de usos que amplían el número de consumidores; desde los más pequeños hasta profesionales del sector (figura 7.11).

Figura 7.11 Ejemplo de dron

Su auge en el mercado ha sido tal, que cada vez hay un mayor número de empresas que emergen en este nicho de mercado, tales como Syma, DJI o Phantom, las cuales son tres de las más punteras en el ámbito de los drones. Actualmente, los VANT militares realizan tanto misiones de reconocimiento como de ataque (Axe, 2009). Si bien se ha informado de muchos ataques de drones con éxito, también son susceptibles de provocar daños colaterales y/o identificar objetivos erróneos, como con otros tipos de arma (*The New York Times,* 2015).

Los VANT también son utilizados en un pequeño pero creciente número de aplicaciones civiles, como en labores de lucha contra incendios o seguridad civil, como la vigilancia de los oleoductos. Los vehículos aéreos no tripulados suelen ser preferidos para misiones que son demasiado "aburridas, sucias o peligrosas" para los aviones tripulados. A continuación se presenta una clasificación de los drones dependiendo de su misión principal:

Blanco. Sirven para simular aviones o ataques enemigos en los sistemas de defensa de tierra o de aire.

Reconocimiento. Envían información; entre estos destacan los MUAV (*Micro Unmanned Aerial Vehicle*), tipo avión o helicóptero.

Combate. Sirven para combatir y llevar a cabo misiones que suelen ser muy peligrosas.

Logística. Diseñados para llevar carga.

Investigación y desarrollo. En ellos se prueban e investigan los sistemas en desarrollo.

UAV comerciales y civiles. Se han diseñado para propósitos civiles como realizar filmaciones, tomar imágenes y/o purificar el aire.

También pueden ser categorizados dependiendo de su alcance máximo:

Handheld. 2 000 pies de altitud, 600 metros y aproximadamente 2 km de alcance en vuelo.

Close. 5 000 pies de altitud, 3 000 metros y hasta 10 km de alcance.

NATO. 10 000 pies de altitud, hasta 50 km de alcance.

Tactical. 18 000 pies de altitud, hasta 160 km de alcance.

MALE (*Medium Altitude, Long Endurance*). Hasta 30 000 pies de altitud y un alcance de unos 200 km.

HALE (*High Altitude, Long Endurance*). 30 000 pies de techo y un alcance indeterminado.

Hypersonic. Alta velocidad, supersónico (de 1 a 5 Mach) o hipersónico (Mach 5+); 50 000 pies de altitud o altitud suborbital, alcance de 200 km.

Orbital. En órbitas bajas terrestres (Mach 25+).

CIS Lunar. Viaja entre la Luna y la Tierra.

Los UAV actualmente tienen múltiples y muy variadas aplicaciones, posibilidades y prestaciones en el mercado civil, militar y profesional; entre las más importantes destacan las siguientes:

- Distribución de señal gratuita de Internet (Geekdigital, 2014)
- Realización de ortofotomapas y de modelos de elevaciones del terreno en muy alta resolución
- Monitorización de instalaciones
- Transporte y entrega de mercancías
- Gestión de cultivos
- Cine y deportes extremos
- Seguimiento de las áreas boscosas o control de incendios
- Búsqueda, rescate y salvamento de personas
- Geología
- Hidrología
- Topografía
- Zoología
- Estado de la atmósfera
- Seguimiento de la planificación urbanística
- Gestión del patrimonio
- Seguridad y control fronterizo
- Auditoría de siniestros
- Purificar el aire mediante un proceso de filtrado

También se aprovecha la ventaja de que su duración máxima volando sólo es limitada por su combustible y por su sistema de vuelo sin tener las limitaciones correspondientes a tener tripulación (ABC, 2015).

Cabe destacar, por otro lado, que los UAV pueden estar controlados remotamente desde una estación de tierra por un operador o pueden ser autónomos y seguir una trayectoria ya predefinida.

7.4 Conclusiones

Semiconductores, electrónica digital, sistemas binarios, microchips, Internet, Intranet, protocolos, redes, bases de datos, información y comunicación o construcción del conocimiento, éstos son sólo algunos de los conceptos sobre los que versa nuestra sociedad tecnológica actual.

En el siglo XXI, la sociedad de la información se mueve en coordenadas que van desde la resolución de problemas en nanosegundos hasta el almacenamiento de información en gigabytes, terabytes y, muy pronto, en petabytes, según lo demanden los sistemas *Big-Data* o la fabricación de los nanocircuitos.

El impacto tecnológico es algo que afecta para bien a todas las facetas de la vida humana: la científica, la económica, la sanitaria, lo social; lo educativo o lo lúdico; por ejemplo, la máquina de vapor, el motor de explosión, la electricidad y la automatización de procesos en el campo y en las fábricas son los ejes a través de los cuales se forjó una nueva época y un nuevo modelo socioeconómico: el capitalismo financiero e industrial.

Por su parte, las nuevas tecnologías de la información y de las comunicaciones (NTIC) representan el catalizador de procesos de cambios estructurales, de nuevas maneras de relación y de comunicación, de nuevos retos y riesgos, y de nuevas pérdidas y ganancias. En los últimos 25 a 30 años, la incorporación generalizada de los microprocesadores y las PC, de los satélites y periféricos o de móviles, redes e Internet y la aparición de una ingente diversidad de fuentes de información en la investigación, la industria, la banca, el comercio o la educación universitaria, han provocado el comienzo de una nueva era, de una nueva revolución autoalimentada no sólo tecnológica, sino global (política, económica, comunicativa, creativa y cultural): la sociedad de la información (SI), que no son meros recursos instrumentales dados los cambios radicales y la construcción de nuevos estilos de vida, de trabajo, de estudio o de ocio.

Las NTIC no son el futuro, sino que ya son una realidad en ámbitos como la investigación, la banca, el comercio, las empresas de servicios, de ocio o de la educación universitaria. El mayor impacto visible de esta nueva sociedad se refiere a la globalización del flujo de capitales y a sus efectos sumamente nocivos.

Por todo ello, se hace necesario estudiar las computadoras no como un sistema aislado, sino como un elemento que forma parte de una red y que permite diversas formas de comunicación electrónica a grandes distancias.

Cuestionario

7.1 ¿Por qué es importante conocer el estado del arte sobre las redes de computadoras? Establezca estudios de caso exitosos de aplicación en el área de las nuevas tecnologías de las redes de computadoras.

7.2 ¿Qué es el Internet de las cosas, cómo funciona y qué aplicaciones tiene en la actualidad? Establezca estudios de caso exitosos de su aplicación.

7.3 ¿Qué es la realidad aumentada, cómo funciona y qué aplicaciones tiene en la actualidad? Establezca estudios de caso exitosos de su aplicación.

7.4 ¿Qué es la web 3.0, cómo funciona y qué aplicaciones tiene en la actualidad? Establezca estudios de caso exitosos de su aplicación.

7.5 ¿Qué es la web 4.0, cómo funciona y qué aplicaciones tiene en la actualidad? Establezca estudios de caso exitosos de su aplicación.

7.6 ¿Qué son los drones, cómo funcionan y qué aplicaciones tienen en la actualidad? Establezca estudios de caso exitosos de su aplicación.

Referencias

Adas, A. A. and Shawly, T. A. (2010). Simulation of IPSec protocol in ad-hoc networks. *Department of Electrical and Computer Engineering, Faculty of Engineering.* Saudi Arabia: King Abdul Aziz University.

ANSI/TIA/EIA-568-B.1. (2001). *Norma para cableado de Telecomunicaciones en edificios Comerciales, Parte 1: Requerimientos Generales*.

ANSI/TIA/EIA-568-B.1-1. (2001). *Norma para cableado de telecomunicaciones en edificios comerciales, Parte 1: Requerimientos Generales. Apéndice 1: Radios de curvatura mínimos de cables UTP de cuatro pares y STP de cuatro pares para cordones de parcheo*.

ANSI/TIA/EIA-568-B.2. (2001). *Norma para cableado de Telecomunicaciones en edificios comerciales, Parte 2: Componentes de cableado de par trenzado balanceado*.

ANSI/TIA/EIA-568-B.2-1. (2001). *Norma para cableado de Telecomunicaciones en edificios comerciales, Parte 2: Componentes de cableado de par trenzado balanceado*.

ANSI/TIA/EIA-606A. (2002). *Norma para la Administración de Infraestructura de Telecomunicaciones Comercial*.

Arends, R.; Austein, M.; Larson, D.; Massey, V. and Rose, S. (2005). *Internet Engineering Task Force*. USA: IETF.

Arreola, J. y J. C. Murillo (2017). "Las 7 tendencias tecnológicas del 2017" en *Forbes*. Disponible en https://www.forbes.com.mx/las-7-tendencias-tecnologicas-del-2017/

Axe, David. (2009). Strategist: Killer drones level extremists advantage. *Wired Review*.

Barfield, W. y Caudell, T. (eds). (2001). *Fundamentos de informática usable y realidad aumentada*. Mahwah, New Jersey: Lawrence Erlbaum.

Bayya, A. K.; Gupte, S.; Shukla, Y. K. and A Garikapati. (2007). Security in ad hoc networks. *Computer Science Department University of Kentucky*. USA: University of Kentucky.

Bernstein, D. J. *DNSCurve: Usable Security for DNS*.

Bimber, O. y Raskar, R. (2005). *Realidad aumentada espacial: Real fusión y los mundos virtuales*. UK: AK Peters.

Carlton, R. D. (2006). *Security protocols for mobile ad hoc networks*. Phd Thesis. McGill University, Montreal, QC, Canada.

Cawood, S. y Fiala, M. (2008). *Realidad aumentada: Una guía práctica*. México: McGraw-Hill.

Gligor, V. D. (2007). Security of emergent properties in ad-hoc networks. *Electrical and Computer Engineering Department University of Maryland*. USA: University of Maryland.

Hainich, R. R. (2009). *El fin de hardware: Un nuevo enfoque a la realidad aumentada*. USA: Booksurge, 3ª ed.

Haller, M.; Billinghurst, M. y Thomas, B. (2006). *Tecnologías emergentes de la realidad aumentada: Interfaces y diseño*. México: Idea Group Publishing.

Hekmat, R. (2006). Ad-hoc networks: Fundamental properties and network topologies. *Delft University of Technology*. The Netherlands.

Labiod, H.; Afifi, H. and De Santis, C. (2007). *Wi-Fi, Bluetooth, ZigBee and WiMAX*. Germany: Springer/Verlag.

Lens-Fitzgerald, M. (2009). *Augmented reality hype cycle*. SPRXmobile: Mobile service architects. Disponible en http://www.sprxmobile.com/the-augmented-reality-hype-cycle/

Markoff, J. (2006). "Entrepreneurs see a Web guided by common sense". *The New York Times*.

Nakhjiri, M. and Nakhjiri, M. (2005). *AAA and network security for mobile access*. USA: John Wiley & Sons.

Nister, D.; Naroditsky, O. and Bergen, J. (2004). "Visual Odometry" en *Computer Vision and Pattern Recognition*, CVPR, (1): 1, pp.652-659.

Ozan, K. and Tonguz, G. F. (2016). Ad hoc wireless networks: *A communication-theoretic perspective*. USA: John Wiley & Sons.

Prendes Espinosa, M. P. (2015). "Realidad aumentada y educación: Análisis de experiencias prácticas" en Píxel-Bit. *Revista de Medios y Educación,* (46): pp. 187-203. Disponible en http://acdc.sav.us.es/pixelbit/images/stories/p46/12.pdf

RFC 4 033 (2005). *DNS Security Introduction and Requirements*. Internet Engineering Task Force.

RFC 4 034 (2005). *Resource Records for the DNS Security Extensions*. Internet Engineering Task Force.

RFC 4 035 (2005). *Protocol Modifications for the DNS Security Extensions*. Internet Engineering Task Force.

Ruíz Torres, D. (2011). "Realidad aumentada, educación y museos" en *Revista Ícono*, 14, (2): pp. 212-226.

Scaramuzza, D. and Siegwart, R. (2008). Appearance-guided monocular omnidirectional visual odometry for outdoor ground vehicles. Robotics, *IEEE Transactions on, 5,* (24): pp. 1 015-1 026

Sramana, M. (2007). *Web 3.0 = (4C + P + VS)*.

Toh, C. K. (2012). *Ad hoc mobile wireless networks: Protocols and systems*. USA: Prentice Hall Publishers.

Wainewright, P. (2005). *Qué se espera de la web 3.0*.

Wallensteinn, A. (2007). *Hollywood hot for second life*. California, USA.

Glosario de términos

ACK: Acknowledgement

ACL: listas de control de acceso

ADF: Access Decision Facility

AEF: Access Enforcement Facility

ANSI: American National Standards Institute

APM: Application Performance Management o Desempeño de Aplicaciones

ARP: Adress Resolution Protocol

BBS: Bulletin Board System

BCP: Business Continuity Plan

BIC: Business Intelligent Card

BOOTP: Bootstrap

BSI: British Standard Institute

CA: Certification Authority

CBEFF: Common Biometric Exchange File Fomat

CER: Cross-Over Error Rate

CERN: Centro Europeo de Investigaciones Nucleares

CIA: Confidentiality, Integrity, Availability

CIFS: Common Internet File Systems

CMIP: Common Management Information Protocol

CMIS: Content Management Interoperability Services

CSMS-CD: Call Sense Multiple Access-Collision Detec

COOP: Continuity of Operations Planning

DAMA: Data Management Association International

DCHP: Dynamic Host Configuration Protocol

DES: Data Encryption Standard

DLCI: Data Link Connection Identifier

DMARC: Domain-Based Message Authentication, Reporting and Conformance

DNS: Domain Name System

DNSKEY: Domain Name System Key

DNSSEC: Domain Name System Security Extensions

DRII: Disaster Recovery institute International

DS: Domain Services

DTP: Dynamic Trunking Protocol

EDI: Electronic Data Interchange

EER: Equal Error Rate

FAR: False Acceptance Rate

FCAPS: Fault, Configuration, Accounting, Performance, Security

FDDI: Fiber Distributed Data Interface

FER: Failure-to-Enroll Rate

FNMR: False Nonatch Rate

FQDN: Fully Qualified Domain Name

FRR: False Rejection Rate

FTP: File Transfer Protocol

GA: gestión de amenazas

GIGO: Garbage In, Garbage Out

Google: motor de búsqueda web

Gopher: motor de búsqueda web

HALE: High Altitude, Long Endurance

Help Desk: Asistencia a usuarios

HMD: Head-Mounted Display

HMI: interfaz hombre-máquina

HTML: Hyper Text Markup Language

HTTP: Hypertext Transfer Protocol

IAM: Identity Access Management

IBSG: Internet Business Solutions Group

ICMP: ping o tracerouter

IDS: Intrusion Detection System

IEC: International Electrotechnical Commissioin

IETF: Internet Engineering Task Force o Grupo de Trabajo de Ingeniería Abierta

IMAP: Internet Message Access Protocol

INCITS: National Institute of Standards and Technology

IOS: Iphone Operating Systems

IP: Internet Protocol

IPX: Internetwork Packet Exchange

ISMS: Information Security Management System

ISO: Organización Internacional de Estándares
ISS: Internet Security Scanner
ITIL: Information Technology Infrastructure Library
KGC: Key Generator Center
L2TP: Layer 2 Tunneling Protocol
LAN: Local Area Network
LP: Least Privilege
M2M: Machine to Machine
MALE: Medium Altitude, Long Endurance
MANET: Mobile ad hoc Network
MBWA: Mobile broadband Wireless Access
MIB: Management Information Base
MIH: Media Independent Handoff
MIME: Multipurpose Internet Mail Extensions
MIT: Massachusetts Institute of Technology
MO: Management Object
MRTG: Multi Router Traffic Grapher
MSS: manejo de servicios de seguridad
MTU: Maximum Transmission Unit
MUAV: Micro Unmanned Aerial Vehicle
NFS: Network File System
NIC: Network Interface Card
NIS: Network Time Protocol
NIST: National Bureau of Standards and Technology o Insituto Nacional de Estandarización y Tecnología
NLU: Natural Language Understandig
NMS: Network Management Station
NSEC: Next Secure
NTIC: nuevas tecnologías de la información y de las comunicaciones
NTK: Need to Know
NTLM: NTLM Authentication Protocol and Security Support Provider
NTP: Network Time Protocol
NVRAM: Non-Volatile Random Access Memory
OCTAVE: Operationally Critical Threat Asset and Viulverability Evaluation
OSI: Open Systems Interconnection
PAC: Programmable Automation Controller
PBX: Private Branch eXchange
PDCA: Plan, Do, Check, Act
PDI: prevención y detección de intrusión
PETI: Plan Estratégico de Tecnología Informática
PGP: Pretty Good Privacy
PKG: Private Key Generator
PKI: Public Key Infrastructure
SoPLC: Programmable Logic Controller
POP: Post Office Protocol
POP1: Protocol Post Office
POP2: Protocol Post Office
POP3: Protocol Post Office
PPTP: Point to Point Tunneling Protocol
Protocolo SGMP: Simple Gateway Monitoring Protocol
Protocolo SNMP: Simple Network Management Protocol
PSI: proveedor de servicios de Internet
PSTN: Public Switched Telephone Network
Q_oS: Quality of Service
RAID: Redundant Array of Independent Disk
RARP: Reverse Address Resolution Protocol
RFID: radiofrecuencia en red
RMA: Reliability, Mantainability, Availabity
RRQ: Read Request
RRSet: Resource Record set
RRSIG: Resource Record Digital Signature
RSA: Rivest, Shamir and Adleman
RTU: Remote Transmission Unit
SANS: SysAdmin Audit, Networking and Security Institute
SAR: Spatial Augmented Reality
SASL: Simple Authentication and Security Layer
SATAN: Security Administrator Tool Analyzing Network
SCADA: Supervisory Control and Data Acquisition
SLA: Service Level Agreement

SMB: Server Message Block
SMF: Systems Management Functions
SMFA: System Management Funtional Area
SMTP: Simple Mail Transfer Protocol
SNI: Server Name Indication
SNMP: Simple Network Management Protocol
S_oA: state of the art
SOA: Service Oriented Architecture
SOC: Security Operation Center
SoD: Segregación de funciones
SPAN: Switch Port Analiser
SPF: Sender Policy Framework
SRI: Stanford Research Institute
SSH: Secure Shell
SSH: Communications Security
SSL: Secure Sockdts Layer
STP: Spanning Tree Protocol
TI: Tecnologías de la Información
TIC: Tecnologías de Información y de las Comunicaciones
TCP: Transmission Control Protocol
TDL: Top Level Domain
TDM: Multilexaje por División de Tiempo
Telnet: Telecommunication Network
TFTP: Trivial File Transfer Protocol
TI: Tecnología de la Información
TLS: Transport Layer Security o Seguridad en la Capa de Transporte
TMN: Telecommunication Management Network
TTS: Trouble Tickets Systems
UAV: Unmanned Aerial Vehicle
UCAV: Unmanned Combat Aerial Vehicle
UDP: User Datagram Protocol)
UIDL: Unique Identification Listing
URI: Uniform Resource Identifier
URL: Uniform Resource Locator
VLAN: red de área local virtual
VPN: Virtual Private Network
W3C: World Wide Web Consortium
WAN: Wide Area Network
WAP: Wireless Application Protocol
WINS: Windows Internet Naming Service
WQR: Write Request
WRAN: Wireless Regional Area Network
WTLS: Wireless Transport Layer Security
WWW: World Wide Web
XML: eXtensible Markup Language

Índice analítico