INSTITUTO SUPERIOR TECNOLÓGICO

JAPÓN

Amor al conocimiento

GUÍA METODOLÓGICA

AUDITORÍA INFORMÁTICA

DESARROLLO DE SOFTWARE

COMPILADOR: MSC. DIANA MONCAYO

2019

INSTITUTO TECNOLÓGICO SUPERIOR JAPÓN
GUIA DE APRENDIZAJE

1. IDENTIFICACIÓN DE

Nombre de la Asignatura: AUDITORÍA INFORMÁTICA	**Componentes del Aprendizaje**	COGNOSCITIVOS

Resultado del Aprendizaje:

- Aplicar el análisis de riesgos, en auditorías informáticas así como determinar las áreas críticas de las TIC a ser controladas y auditadas mediante la elaboración de un informe de auditoría informática.
- Dominio de los conceptos sobre TIC y la Auditoría Informática fundamentados en los valores y bajo una base legal a fin de contrarrestar los delitos informáticos.
- Comprender la importancia de la Auditoría de Sistemas Informáticos en el contexto global de la auditoría integral.
- Aplica en la práctica el proceso de auditoría informática. Determinar las áreas críticas de las TIC a ser controladas y auditadas.
- Aplica las herramientas metodológicas para ejecutar una auditoría informática. Elaboración de un informe de auditoría informática.
- Organiza sus contenidos en las siguientes unidades de aprendizaje: I. Planteamiento de Problema , Planteamiento de propuesta, Desarrollo de metodología .
- Comprende los alcances de las TICs, y cómo influye la auditoria informática en su implementación.
- Utiliza las herramientas para realizar trabajos colaborativos cooperativos y compartidos.

OBJETIVOS:

- Capacitar sobre el correcto levantamiento de información en una organización, a fin de proponer una metodología práctica para la aplicación de un control de calidad en los sistemas de información,
- Se espera que el estudiante sea capaz de comunicar las TICs con el estilo adecuado y de analizar, sintetizar y gestionar la información.
- Identificar los roles que un Auditor de Sistemas.
- Conocer las herramientas, controles y Estándares que pueden ser aplicados en una auditoria informática.
- Determinar los riesgos, Control Interno y metodologías que proponen las buenas prácticas y regulación de información por medio de estándares.
- Manejar las normas y estándares más aceptados a nivel internacional para la gestión de seguridad, gobierno y gestión de tecnologías de información

COMPETENCIAS

- Conocer las herramientas, espacios y recursos del Aula Virtual.
- Adquirir habilidades de trabajo en equipo en un entorno virtual de aprendizaje.
- Reconoce, analiza y aplica técnicas bajo el enfoque de la auditoria de sistemas.
- Identifica metodologías o métodos formales para regularizar las funcionalidades de control en una organización.
- Diseña y aplica algunos instrumentos de diagnóstico para recabar información contextual que enriquezca posteriormente su plan de intervención de auditoria informática.
- Elabora y sustenta informes de diagnóstico sobre la identificación de riesgos o anomalías encontradas, aplicando una correcta práctica de evaluación de sistemas de información.
- Valora la responsabilidad de la ejecución de un proyecto, tiene de forma clara la identificación del proyecto y la solución propuesta.
- Valora y argumenta sobre la importancia de mantener una frecuencia auditoria a fin de disminuir el grado de riesgo encontrado.
- Sustenta el plan de intervención fundamentando la viabilidad de su ejecución.
- Entender la importancia del uso de nuevas metodologías tecnológicas para poder promocionar un programa de aprendizaje.

INSTITUTO TECNOLÓGICO SUPERIOR JAPÓN
GUIA DE APRENDIZAJE

Docente de Implementación: Msc. Diana Moncayo	
	Duración: 40 horas

Unidades	Competencia	Resultados de Aprendizaje	Actividades	Tiempo de Ejecución
UNIDAD I Auditoría Informática y las TICs	1.1 Conceptos TICS relacionados con la Auditoría Informática. 1.2 Normas Ético Moral que regulan la actuación del Auditor 1.3 Conceptos de Auditoría Informática 1.4 Delitos Informáticos .	Comprender la importancia de la Auditoría de Sistemas Informáticos en el contexto global de la auditoría integral..	Trabajos de Conocimiento semanal con los temas de: Levantamiento de información , identificación de riesgos. En grupos de trabajo identificar que es y que no es Auditoría Informática Preparar una presentación sobre que es un delito informático.	**5 horas**

UNIDAD II Identificación de riesgos y el control interno	2.1 Conceptos Control Interno Informático COSO y NIA 2.2 Conceptos fundamentales en: a) Análisis de Riesgos	Elabora herramientas de desarrollo o proporciona modelos de aplicación para regularizar una problemática empresarial, realiza un diagnóstico situacional y valida sus efectos y aplicación.	Proyecto Elaborado en Microsoft Word , teniendo iniciativa de la aplicación de las normas APA , el proyecto identifica la necesidad de crear una herramienta de carrera apoyado en las Tic´s y que debe ser un aporte empresarial de como identificar las vulnerabilidades a nivel de empresa.	**5 horas**
UNIDAD III Metodologías de Análisis de Riesgos.	3.1 Conceptos básicos de COBIT 3.2 Aplicación del sistema COBIT en los procesos de auditoría 3.3 Conceptos básicos de ITIL 3.4 Mejores prácticas de la auditoría en informática.	Entender y comprender las metodologías de desarrollo de software a fin de estructurar de mejor manera el problema y solución	Prácticas en Clase Aplicar técnicas de las metodologías revisadas en clase. Investigar software libre referente a Auditoría Informática	**5 horas**

UNIDAD IV Normas ISO y Estándares de Control	4.1 Conceptos básicos de SGSI 4.2 ISO 27001 4.3 ISO 27007-Guia para auditar	Comprende los lineamientos de las normativas y aplica correctamente en un caso de estudio de auditoria informática	Práctica en clase que se incluye en el proyecto final la aplicación de estándar para formalizar procesos de empresa.	**5 Horas**
UNIDAD V Planeación de auditoria informáticas y sus procesos.	5.1 Planeación de la Auditoría Informática 5.2 Ejecución de la Auditoría Informática en: Normas, hardware, Sistemas Operativos, Software base, Sistemas de Información, Bases de Datos, Seguridad Física y lógica, Contratación y Adquisición, Procesos TIC, Comunicaciones, etc. 5.3 Elaboración de Informe 5.4 Comunicación de Resultados	El estudiante es capaz de valorar al riesgo en cualquier entidad que realice una valoración, de esta forma plantea las posibles salvaguardas a seguir.	Se desarrolla un proyecto investigando las áreas de afectación, y se establece ponderaciones y valor al riesgo. Lectura Libro **Técnicas de la auditoría informática** **Yann Derrien** Planificación de actividad Informática Cap2	**5 horas**
UNIDAD VI Herramientas Case para Auditoría	6.1 Conceptos básicos de herramientas CASE 6.2 Ciclo de vida de un sistema 6.3 Funcionalidad de las herramientas Case	Conoce y aplica los conceptos de herramientas case que pueden realizar una secuencia organizada del proceso de auditoria informática.	El estudiante debe aplicar herramientas Case en el proyecto final , aplicando el ciclo de vida de un software, basado en los lineamientos formales.	

UNIDAD VII Elaboración de informes planes de continuidad del negocio.	7.1 Conceptos básicos de Plan de acción , Plan de contingencia	Conoce adecuadamente las metodologías de auditoria informática y aplica adecuadamente para estructurar su propuesta de proyecto empresarial	Presenta un informe de plan de actuación y continuidad del negocio.	
UNIDAD VIII Auditoría Continua	8.1 Conceptos sobre la Auditoria Continua 8.2 Aplicación de un modelo de auditoria Continua	El estudiante puede apoyarse de las herramientas de Tics y presentar una propuesta de gestión de seguridad de información a través de las mismas.	Presentación del proyecto, con una demostración del caso de estudio empresarial	**5 horas**

2. CONOCIMIENTOS PREVIOS Y RELACIONADOS

Co-requisitos

1.-Identificar los conceptos básicos de auditoria informática y la importancia de su aplicación apoyado de las herramientas las TIC’s (Tecnologías de información y comunicaciones) en la educación y la aplicación en proyectos de carrera.

2.Determinar los riesgos, Control Interno y Metodologías que proponen las buenas prácticas / estándares

3. Conocer metodologías de tecnología, para que el estudiante comprenda lo que requiere para iniciar un proyecto, identificando las fases a fin de estructurar de mejor manera el proyecto.

4. Propone alternativas para brindar soluciones al proceso de auditoría tecnológica

3. UNIDADES TEÓRICAS

- **Desarrollo de las Unidades de Aprendizaje (contenidos)**

A. Base Teórica

UNIDAD I

TEMA 1: Auditoría Informática y las TICs

1.1 Conceptos TICS relacionados con la Auditoría Informática.

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos.

Este enfoque es totalmente compatible con las prácticas y controles contenidos en COBIT, ITIL, estándares o normativa que relaciona el enfoque COSO, SAC, NIAS, Estándares de Seguridad de la Información (ISO 27000) entre otros, que hacen referencia a las pistas de auditoría en los sistemas informáticos, controles de acceso a los sistemas, bases de datos, Áreas de Tecnología de la Información y Comunicaciones (TIC´s) área de servidores, codificación de la información, prevención de virus, fraude, detección y mitigación de intrusos, entre otros; estos estándares no proporcionan un criterio legal aplicable si no han sido adoptados por la entidad, pero sí procedimientos de auditoría para examinar la gestión tecnológica en las diferentes organizaciones del sector público.

El departamento o equipo del área involucrada que dentro de una organización ejerce las funciones de Tecnologías de Información se encarga de estudiar, diseñar, desarrollar,

implementar y administrar los sistemas de información utilizados para el manejo de datos e información de toda la organización. Estos sistemas, a su vez, comprenden aplicaciones o software, y equipos o hardware.

Llevar a cabo las tareas de la organización apoyándose en las Tecnologías de Información, generalmente redunda en un procesamiento más rápido y confiable de sus datos. La información resultante tiene mayor movilidad y accesibilidad, y cuenta con mayor integridad, que cuando se procesa en forma manual. Igualmente, las computadoras relevan a los empleados de numerosas actividades repetitivas y aburridas, permitiéndoles aprovechar mejor su tiempo en actividades que agregan más valor.

A medida que los precios de los equipos de computación bajan, su capacidad aumenta, y se hacen más fáciles de usar, las TI se utilizan en nuevas y variadas formas. En las empresas, sus aplicaciones son diversas. Hoy en día, la mayoría de las empresas medianas y grandes (y cada día más pequeñas y micro-empresas) utilizan las TI para gestionar casi todos los aspectos del negocio, especialmente el manejo de los registros financieros y transaccionales de las organizaciones, registros de empleados, facturación, cobranza, pagos, compras, y mucho más.

¨Yann Derrien Planificación de actividad Informática Cap1"

1.2 Normas Ético Moral que regulan la actuación del Auditor

Proveer a los auditores tecnológicos lineamientos para la realización de una auditoría de gestión a las tecnologías de información y comunicaciones que coadyuven a la buena gestión de la disponibilidad de los servicios sistematizados prestado a la población en general, con el uso de la tecnología proporcionando seguridad, disponibilidad, confiabilidad y oportunidad de la información procesada y resguardada dentro de la entidad.

1.3 Conceptos de Auditoría Informática

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.

1.3.1 Objetivo de la auditoria informática

El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

1.3.2 Marco esquemático de la auditoría de sistemas Hardware

Evaluación a:

- Hardware: Plataforma de hardware. Tarjeta madre. Procesadores. Dispositivos periféricos. Arquitectura del sistema. Instalaciones eléctricas, de datos y de telecomunicaciones. Innovaciones tecnológicas de hardware y periféricos.

- Software: Plataforma del software. Sistema operativo. Lenguajes y programas de desarrollo. Programas, paqueterías de aplicación bases de datos. Utilerías, bibliotecas y aplicaciones. Software de telecomunicación. Juegos y otros tipos de software.

- Gestión informática: Actividad administrativa del área de sistemas. Operación del sistema de cómputo. Planeación y control de actividades. Presupuestos y gastos de los recursos informáticos. Gestión de la actividad informática. Capacitación y desarrollo del personal informático. Administración de estándares de operación, programación y desarrollo.

- Información : Administración, seguridad y control de la información. Salvaguarda, protección y custodia de la información. Cumplimiento de las características de la información.

- Diseño de sistemas: Metodologías de desarrollo de sistemas. Estándares de programación y desarrollo. Documentación de sistemas.

- Bases de datos: Administración de bases de datos. Diseño de bases de datos. Metodología para el diseño y programación de bases de datos. Seguridad, salvaguarda y protección de las bases de datos.

- Seguridad : Seguridad del área de sistema. Seguridad física. Seguridad lógica. Seguridad de las instalaciones eléctricas, de datos y de telecomunicaciones.

Seguridad de la información, redes y bases de datos. Administración y control de las bases de datos. Seguridad del personal informático.

- Redes de cómputo : Plataformas y configuración de las redes. Protocolos de comunicaciones. Sistemas operativos y software. Administración de las redes de cómputo. Administración de la seguridad de las redes. Administración de las bases de datos de las redes.

- Especialidades : Outsourcing. Helpdesk. Ergonomía en sistemas computacionales. ISO-9000. Internet/Intranet. Sistemas multimedia.

1.4 Delitos Informáticos

Son todas aquellas acciones antijurídicas que se ejecutan mediante vías informáticas. Se consideran delitos informáticos aquellos en los que las nuevas tecnologías intervienen, no solo como medio, sino también como objeto o como bien jurídico protegido.

Figura 1: Representación de delitos informáticos

1.4.1 Tipo de delitos informáticos:

- Fraudes cometidos mediante la manipulación de equipos informáticos.
- Falsificaciones informáticas, ya sea como objeto o como instrumento.
- Daños o modificaciones de programas o bases de datos, como sabotajes, virus o gusanos.

1.4.2 Ejemplos de delitos

- Delitos de estafa, especialmente el fraude informático.
- Delitos de acoso: ciberacoso o grooming
- Delitos de suplantación de la identidad.
- Delitos de daños, como el sabotaje informático, de forma que se borran, deterioran o alteran datos o programas electrónicos.
- Delitos relativos al mercado y a los consumidores.
- Delitos informáticos contra la propiedad intelectual, más comúnmente conocidos como “pirateo informático”.
- Delitos de intrusismo informático.
- Delitos de descubrimiento y relevación de secretos, de forma que se vulnera la intimidad de una persona o se interceptan comunicaciones y transmisiones de datos informáticos.

UNIDAD II
TEMA 1: Identificación de riesgos y el control interno

2.1 Conceptos Control Interno Informático COSO y NIA

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO ITIL e NIA.

Los modelos de control interno como COSO y COBIT son los dos modelos más difundidos en la actualidad, COSO está enfocado a toda la organización, contempla políticas, procedimientos y estructuras organizativas además de procesos para definir el modelo de control interno.

Mientras que COBIT (Control Objectives for Information and Related Technology, Objetivos de Control para Tecnología de Información y Tecnologías relacionadas) se centra en el entorno IT, contempla de forma específica la seguridad de la información

como uno de sus objetivos, cosa que COSO no hace. Además el modelo de control interno que presenta COBIT es más completo, dentro de su ámbito.

2.1.1 Objetivos del Control Interno COSO.

- Eficiencia y eficacia de las operaciones
- Fiabilidad de la información financiera
- Cumplimientos de leyes y normas aplicables.

2.1.2 Ventajas de COSO

- Permite a la dirección de la empresa poseer una visión global del riesgo y accionar los planes para su correcta gestión.

- Posibilita la priorización de los objetivos, riesgos clave del negocio, y de los controles implantados, lo que permite su adecuada gestión. toma de decisiones más segura, facilitando la asignación del capital.
- Alinea los objetivos del grupo, con los objetivos de las diferentes unidades de negocio, así como los riesgos asumidos y los controles puestos en acción.

- Permite dar soporte a las actividades de planificación estratégica y control interno.

- Permite cumplir con los nuevos marcos regulatorios y demanda de nuevas prácticas de gobierno corporativo.

- Fomenta que la gestión de riesgos pase a formar parte de la cultura del grupo.

2.1.3 Normas Internacionales De Auditoria (NIA)

Las Normas Internacionales de Auditoría y Aseguramiento son un conjunto de principios, reglas o procedimientos que necesariamente debe aplicar un profesional que se dedique a labores de auditoría de estados financieros, con la finalidad de evaluar de una manera razonable y confiable la situación financiera de la empresa o ente por él auditados, y en

base de aquello le permita emitir su opinión en forma independiente con criterio y juicio profesionales acertados. Estas normativas tienen un rango superior al haberse introducido el acápite del Aseguramiento, con el fin de proporcionar un alto nivel de seguridad ya que el riesgo de auditoría, da inicio desde los aspectos previos a la contratación, siguiendo con la Planeación hasta concluir con el Informe, proporcionado de esta manera un alto índice de confianza a los diferentes usuarios de los estados financieros, y por consiguiente la correspondiente credibilidad de sus contenidos.

2.1.4 Normativas NIA

- NIA-ES 200. Objetivos globales del auditor independiente y realización de la Auditoría de conformidad con las Normas Internacionales de Auditoría.
- NIA-ES 210. Acuerdos de los términos del encargo de auditoría.
- NIA-ES 220. Control de Calidad de la Auditoría de Estados Financieros.
- NIA-ES 230. Documentación de Auditoría.
- NIA-ES 240. Responsabilidades del Auditor en la Auditoría de Estados Financieros con respecto al Fraude.
- NIA-ES 250.Consideración de las Disposiciones Legales y Reglamentarias en la Auditoría de Estados Financieros.
- NIA-ES 260. Comunicación con los responsables del gobierno de la Entidad.

2.2 Conceptos fundamentales en análisis de riesgos :

2.2.1 Análisis de Riesgos

El proceso de análisis de riesgos involucra tres subprocesos fundamentales:

1) análisis de los riesgos donde se identifica y detalla las causas que originan los riesgos, quienes se ven involucrados y como se presentan.
2) Evaluación de riesgos en cuanto a probabilidad e impacto, donde se definen las escalas de medición de los riesgos para medir la probabilidad de ocurrencia de riesgos en un periodo de tiempo y el impacto que esos riesgos pueden ocasionar deteriorando parcial o completamente los activos impactados o los servicios que se prestan a través de los sistemas que los soportan. Y 3) Gestión de los riesgos donde una vez que se identifican las causas del riesgo, se propone los controles para mitigar esos riesgos.

2.2.1.1 Riesgos Iniciales

Para la identificación de los riesgos iniciales en una empresa, cada estudiante de acuerdo al proceso que está evaluando, debe mirar que riesgos son los que están relacionados directamente con el proceso evaluado y deben listarse como riesgos.

- Incumplimiento en el cronograma de copias de seguridad de equipos de cómputo de usuarios y servidores
- Funcionamiento inadecuado de las aplicaciones de software institucionales
- Indisponibilidad del servidor o equipos de computo
- Funcionamiento inadecuado del almacenamiento
- Fallas en las telecomunicaciones y/o fluido eléctrico

2.2.1.2 Riesgos con la aplicación de instrumentos

Posteriormente, al aplicar los instrumentos como entrevistas se descubrieron nuevos riesgos, al aplicar la lista de chequeo se descubre que faltan algunos controles en el proceso evaluado de acuerdo a la norma, y en el cuestionario están prácticamente, todos los riesgos detectados en el proceso evaluado y se hace una lista de ellos.

- Desactualización Software
- Perdida de información por virus informáticos
- Incumplimiento en el reporte re la información
- Uso indebido de la información
- Inadecuada utilización del portal Web institucional
- Desconocimiento de los avances del Plan Estratégico
- Accesos no autorizados a las instalaciones del área tecnológica

MATRIZ PARA MEDICIÓN DE PROBABILIDAD E IMPACTO DE RIESGOS

iMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**

1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Tabla 1: Niveles para la medición del riesgo

PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir sólo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Se ha presentado al menos 1 vez en los últimos 5 años
3	Posible	El evento puede ocurrir en algún momento	Se ha presentado al menos de 1 vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Se ha presentado al menos 1 vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Se ha presentado

Tabla 2: Probabilidad de que el riesgo se materialice.

Con las escalas de medición se construye la matriz de riesgos general que se aplica para cualquiera de los procesos, teniendo en cuenta los riesgos encontrados.

EVALUACIÓN Y MEDIDAS DE RESPUESTA					
PROBABILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

Tabla 3: Matriz que identifica la medición del riesgo.

IMPACTO
Insignificante = 1
Menor = 2
Moderado = 3
Mayor = 4
Catastrófico = 5

Tabla 4: Lista de Impactos

PROBABILIDAD
Raro = 1
Improbable = 2
Posible = 3
Probable = 4
Casi Seguro = 5

Tabla 5: Lista de Probabilidades

Teniendo en cuenta los insumos anteriores se procede a hacer el proceso de evaluación de los riesgos encontrados en cada uno de los procesos evaluados, teniendo en cuenta los riesgos en cuanto a la probabilidad de ocurrencia de los mismos y el impacto que pueden causar en la empresa.

ANALISIS Y EVALUACIÓN DE RIESGOS

N°	Descripción	Impacto	Probabilidad
R1	Incumplimiento en el cronograma de copias de seguridad de equipos de cómputo de usuarios y servidores	5	3
R2	Funcionamiento inadecuado de las aplicaciones de software institucionales	4	3
R3	Indisponibilidad del servidor o equipos de computo	4	4
R4	Funcionamiento inadecuado del almacenamiento	3	2
R5	Fallas en las telecomunicaciones y/o fluido eléctrico	3	3

R6	Desactualización Software	2	2
R7	Perdida de información por virus informáticos	5	3
R8	Incumplimiento en el reporte re la información	4	3
R9	Uso indebido de la información	3	2
R10	Inadecuada utilización del portal Web institucional	3	3
R11	Desconocimiento de los avances del Plan Estratégico	3	2
R12	Accesos no autorizados a las instalaciones del área tecnológica	3	3

Tabla 6: Análisis y evaluación de riesgos

RESULTADO MATRIZ DE RIESGOS

EVALUACIÓN Y MEDIDAS DE RESPUESTA					
PROBABILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)					
Improbable (2)		R7	R4, R10		
Posible (3)			R6, R11	R2, R9	R1, R5, R8
Probable (4)				R3	
Casi Seguro (5)					

Tabla 7: Matriz Resultante

Una vez se tiene la matriz de riesgos aplicada a cada uno de los procesos se indica las acciones que pueden realizarse para el tratamiento de los riesgos de acuerdo a la siguiente tabla donde se indica por cada color, el tratamiento que se puede aplicar en cada caso.

B	Zona de riesgo Baja: Asumir el riesgo
M	Zona de riesgo Moderada: Asumir el riesgo, reducir el riesgo
A	Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E	Zona de riesgo Extremo: Reducir el riesgo, evitar, compartir o transferir

Tabla 8: Tratamiento del Riesgo

Fuente: http://auditordesistemas.blogspot.com/2012/02/guias-de-auditoria-para-aplicacion.html

UNIDAD III
TEMA 1: Metodologías de Análisis de Riesgos.

3.1 Conceptos básicos de COBIT

Control (Objectives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI).

COBIT es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

3.1.1 Objetivos de COBIT

- Mejor alineación basada en una focalización sobre el negocio.
- Visión comprensible de TI para su administración.
- Clara definición de propiedad y responsabilidades.
- Aceptabilidad general con terceros y entes reguladores.
- Entendimiento compartido entre todos los interesados basados en un lenguaje común.
- Cumplimiento global de los requerimientos de TI planteados en el Marco de Control Interno de Negocio COSO.

3.1.2 Requerimientos del negocio

Con la implementación de COBIT se realizan requerimientos de información del negocio los cuales son:

- La efectividad: información que se proporciona oportuna, veraz que se puede utilizar en el negocio siendo importante y pertinente.
- La eficiencia: la información llegue haciendo un uso óptimo de los recursos.
- La confidencialidad: la información solo sea visible por el personal autorizado.
- La integridad: la información solo sea modificada por el personal autorizado en la empresa.
- La disponibilidad: la información esté disponible y a tiempo cuando sea requerida en cualquier momento.
- El cumplimiento: Establecimiento de políticas internas y externas para acatar las leyes inmersas en las actividades del negocio.
- La confiabilidad: información apropiada que ayude a la toma de decisiones a la alta gerencia.

3.1.3 División de Cobit

- Dominios: Es una agrupación de procesos con una responsabilidad dentro de la organización.
- Procesos: Conjuntos de actividades.
- Actividades: Acciones para lograr un resultado.

Cobit Tiene procesos agrupados en dominios como lo muestra la siguiente imagen:

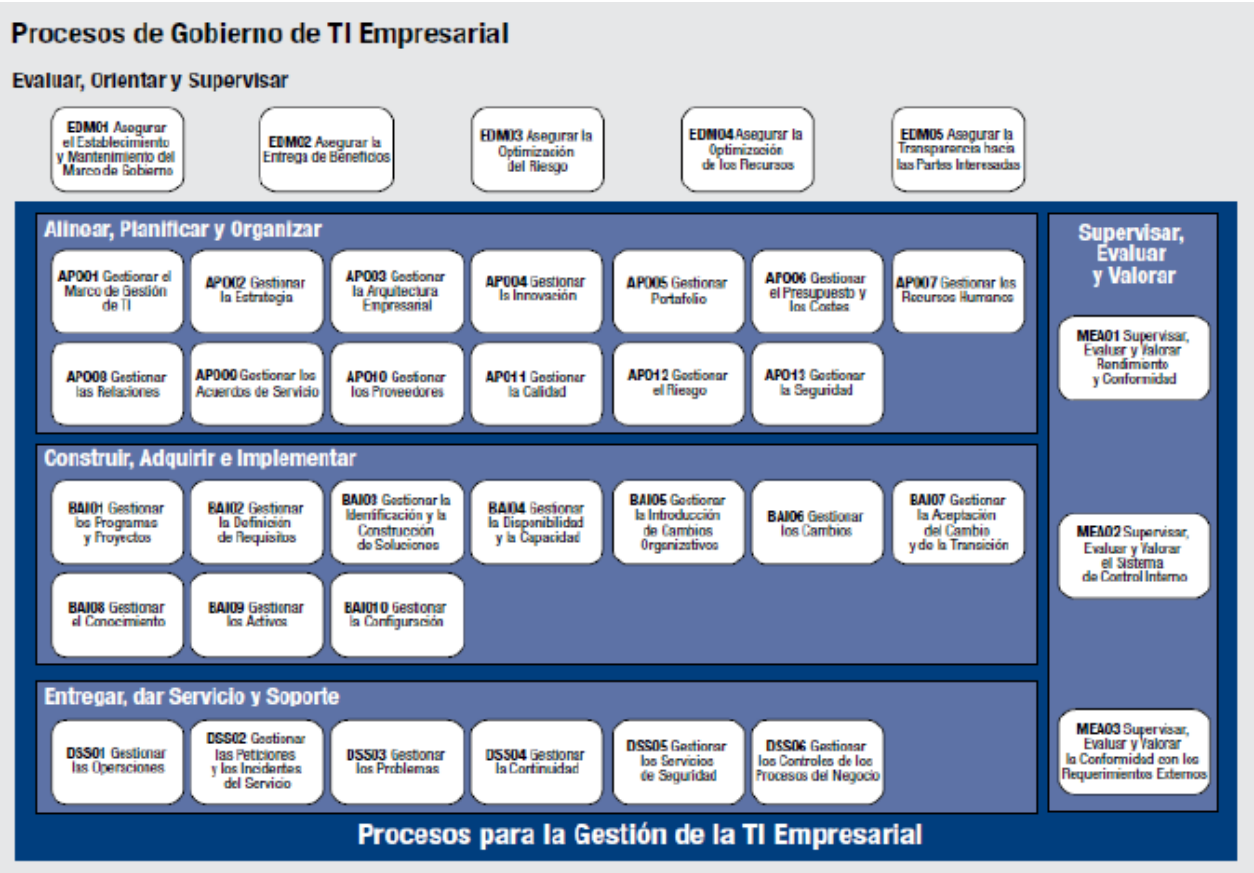


Figura 2: Modelo de Referencia Procesos Cobit5
Fuente : ISACA-COBIT 5, 2012

La mayor prioridad para las organizaciones en el trascurso de los años, es mantener la seguridad informática, la cual ayuda a mejorar la prestación de servicios, implementando políticas, procedimientos y métodos, para mantener la confidencialidad, integridad y disponibilidad de la información, garantizando que mantenga segura. Debido a ello es necesario establecer Sistemas de Gestión de Seguridad Informática para tener claros lineamientos, políticas, normas, procesos, que ayudaran a manejar, controlar e implementarlos; para garantizar un correcto funcionamiento de la seguridad informática, pero todo esto se logra con el apoyo constante de la alta gerencia, lo que ayuda a incentivar a los involucrados al buen manejo y aplicación de los sistemas para contrarrestar la vulnerabilidad de la información

Dentro del mismo es necesario realizar el proceso de la identificación de riesgos, para poder tratarlos y gestionarlos de tal manera que no genere un impacto negativo para la organización, para ello se debe tener una metodología clara para gestión de los tipos de riesgos que se puedan

presentar en materia de seguridad, la auditoría permite realizar evaluación de los sistemas que le permitan minimizar los riesgos.

3.2 Aplicación del sistema COBIT en los procesos de auditoría

3.2.1 Principios de COBIT

La estructura del modelo COBIT propone un marco de acción, donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros; y, finalmente, se realiza una evaluación sobre los procesos involucrados en la organización. Este modelo define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios principales, a saber:

- Planificación y organización
- Adquisición e implantación
- Soporte y servicio
- Monitoreo

Figura 3: Principios de Cobit5
Fuente : ISACA-COBIT 5, 2012

Las empresas existen para crear valor para sus accionistas. En consecuencia, cualquier empresa, comercial o no, tendrá la creación de valor como un objetivo de Gobierno. Creación de valor, significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo.

Figura 4: Objetivos de Govierno
Fuente : ISACA-COBIT 5, 2012

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT, es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y, por supuesto, a los auditores involucrados en el proceso.

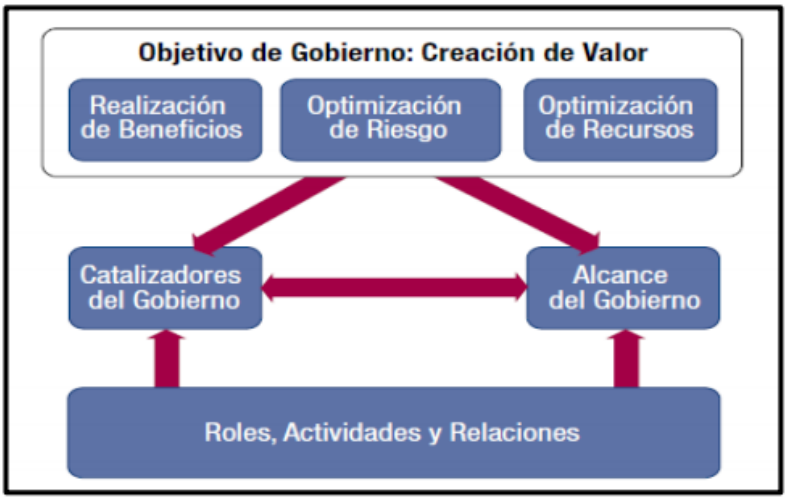


Figura 5: Objetivos de Gobierno de Cobit5
Fuente : ISACA-COBIT 5, 2012

En el desarrollo de la investigación se ha utilizado una encuesta aplicada a las organizaciones sobre como evalúan los sistemas de información en las organizaciones, a continuación se detallan los aspectos más relevantes:

Criterio	Frecuencia	Impacto Porcentual
Siempre	16	27%
Frecuentemente	32	53%
A veces	12	20%
Rara vez	0	0%
Nunca	0	0%
Total	**60**	**100%**

Tabla 9: Frecuencia de práctica de auditoria

Según la tabla 9, la mayoría de las empresas realizan la revisión de sus sistemas informáticos a fin de conocer sus debilidades y superarlas a futuro, para lo cual, deben implementar acciones que se encaminen al logro de los objetivos organizacionales planteados por la gerencia.

Criterio	Frecuencia	Impacto Porcentual
Alto	15	25%
Medio	40	67%
Bajo	5	8%
Total	**60**	**100%**

Tabla 10: Nivel de definición de objetivos

Según la tabla 10, un alto porcentaje de empresas tiene un nivel medio respecto a la definición de los objetivos, por tal razón, deben empezar por reforzar esta debilidad, para poder fortalecer los sistemas informáticos y alinearlos a los objetivos empresariales correctamente definidos.

COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo a extremo, es decir, todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

3.3 Conceptos básicos de ITIL

ITIL (IT Infraestructure Library) Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de tecnologías de información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado que se apoyan en herramientas de evaluación e implementación

3.3.1 Objetivo ITIL

ITIL como metodología propone el establecimiento de estándares que ayudan al control, operación y administración de los recursos. Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua. Otra de las cosas que propone es que para cada actividad que se realice, se debe de hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda los usuarios estén al tanto de los cambios y no se tome a nadie por sorpresa.

3.4 Mejores prácticas de la auditoría en informática.

3.4.1 Libros ITIL

ITIL v3 consta de 5 libros basados en el ciclo de vida del servicio:

a) Estrategia del Servicio
b) Diseño del Servicio
c) Transición del Servicio
d) Operación del Servicio
e) Mejora Continua del Servicio

a) Estrategia del Servicio

Se enfoca en el estudio de mercado y posibilidades mediante la búsqueda de servicios innovadores que satisfagan al cliente tomando en cuenta la real factibilidad de su puesta en

marcha. Así mismo se analizan posibles mejoras para servicios ya existentes. Se verifican los contratos con base en las nuevas ofertas de proveedores antiguos y posibles nuevos proveedores, lo que incluye la renovación o revocación de los contratos vigentes.

b) Diseño del Servicio

Una vez identificado un posible servicio el siguiente paso consiste en analizar su viabilidad. Para ello se toman factores tales como infraestructura disponible, capacitación del personal y se planifican aspectos como seguridad y prevención ante desastres. Para la puesta en marcha se toman en consideración la reasignación de cargos (contratación, despidos, ascensos, jubilaciones, etc), la infraestructura y software a implementar.

Procesos

- ✓ Gestión del Catálogo de Servicios
- ✓ Gestión de Niveles de Servicios
- ✓ Gestión de la Disponibilidad
- ✓ Gestión de la Capacidad
- ✓ Gestión de la Continuidad de los Servicios de TI
- ✓ Gestión de Proveedores
- ✓ Gestión de la Seguridad de Información
- ✓ Coordinación del Diseño (nuevo en la versión 2011)

c) Transición del Servicio

Antes de poner en marcha el servicio se deben realizar pruebas. Para ello se analiza la información disponible acerca del nivel real de capacitación de los usuarios, estado de la infraestructura, recursos IT disponibles, entre otros. Luego se prepara un escenario para realizar pruebas; se replican las bases de datos, se preparan planes de rollback (reversión) y se realizan las pruebas. Luego de ello se limpia el escenario hasta el punto de partida y se analizan los resultados, de los cuales dependerá la implementación del servicio. En la evaluación se comparan las expectativas con los resultados reales.

Procesos

- ✓ Gestión de la Configuración y Activos
- ✓ Gestión del Cambio
- ✓ Gestión del Conocimiento
- ✓ Planificación y Apoyo a la Transición
- ✓ Gestión de Release y Despliegue
- ✓ Gestión Validación y Pruebas
- ✓ Evaluación (Evaluación del cambio)

d) Operación del Servicio

En este punto se monitoriza activa y pasivamente el funcionamiento del servicio, se registran eventos, incidencias, problemas, peticiones y accesos al servicio.

Procesos

- ✓ Gestión de Incidentes
- ✓ Gestión de Problemas
- ✓ Cumplimiento de Solicitudes
- ✓ Gestión de Eventos
- ✓ Gestión de Accesos

e) Mejora Continua del Servicio

Se utilizan herramientas de medición y feedback para documentar la información referente al funcionamiento del servicio, los resultados obtenidos, problemas ocasionados, soluciones implementadas, etc. Para ello se debe verificar el nivel de conocimiento de los usuarios respecto al nuevo servicio, fomentar el registro e investigación referentes al servicio y disponer de la información al resto de los usuarios.

UNIDAD IV

TEMA 1: Normas ISO y Estándares de Control

4.1 Conceptos básicos de SGSI

El **SGSI** es la abreviatura usada para referirse al **Sistema de Gestión de la Seguridad de la Información** e ISMS son las siglas equivalentes en ingles a Information Security Management System.

Podemos entender por información todo el conjunto de datos que se organizan en una organización y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

El Sistema de Gestión de Seguridad de la Información, según **ISO 27001** consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

Fundamentos:

Para garantizar que el **Sistema de Gestión de Seguridad de la Información** gestionado de forma correcta se tiene que identificar el **ciclo de vida** y los aspectos relevantes adoptados para garantizar su:

- Confidencialidad: la información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizados.
- Integridad: mantener de forma completa y exacta la información y los métodos de proceso.
- Disponibilidad: acceder y utilizar la información y los sistemas de tratamiento de la misma parte de los individuos, entidades o proceso autorizados cuando lo requieran.

  Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un **SGSI**.

4.2 ISO 27001

La norma ISO 27001 refiere, a un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

4.3 ISO 27007-Guia para auditar

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la comisión electrotécnica internacional que se encargan de establecer estándares y guías llevadas a cabo con sistemas de gestión y son aplicables a cualquier tipo de empresa internacional y mundial, con el fin de facilitar el comercio, facilitar el intercambio de información y contribuir a la trasferencia de tecnologías.

La norma ISO 27007 se basa en gran medida en ISO 19011, el estándar para auditar sistemas de gestión, que ofrece orientación específica para el Sistema de Gestión de Seguridad de la Información.

El estándar cubre todos los aspectos específicos del Sistema de Gestión de Seguridad de la Información de la auditoría de cumplimiento:

- Administración del programa de auditoría del Sistema de Gestión de Seguridad de la Información para determinar que se debe auditar, cuando y como, además de asignar los auditores apropiados, administrar todos los riesgos, mantener registros de auditoría, mejorar de forma continua el proceso, etc.
- Realización de una auditoría, con los que se debe realizar una planificación, establecer una conducta, llevar a cabo las actividades clave de auditoría, incluyendo el trabajo de campo, realizar el análisis, los informes y el seguimiento.

- Gestión de auditores del Sistema de Gestión de Seguridad de la Información, como puede ser competencias, habilidades, atributos y evaluación.

El Software ISO 27001 para la Seguridad de la Información se encuentra compuesta por diferentes aplicaciones que, al unirlas, trabajan para que la información que manejan las empresas no pierda ninguna de sus propiedades más importantes: disponibilidad, integridad y confidencialidad.

4.3.1 Marco de referencia.

La norma ISO 27001 se ha elaborado tomando en consideración el enfoque orientado a procesos y sigue el modelo PDCA para estructurar todos los procesos del SGSI de forma que resulta compatible con las normas ISO 9001 e ISO 14001. Así mismo se contemplan los principios definidos en las Directrices de la OCDE para la Seguridad de los Sistemas y Redes de Información (2002).

El modelo PDCA (Plan-Do-Check-Act) propuesto por Deming (1986) es una estrategia de mejora continua de la calidad en cuatro pasos. Se trata de un proceso cíclico (también conocido como espiral de Deming) que consta de cuatro fases:

- ✓ PLAN (Planificar): Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado. Al tomar como foco el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora. o

- ✓ DO (Hacer). Implementar los nuevos procesos. Si es posible, en una pequeña escala.

- ✓ CHECK (Verificar): o Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada. o Documentar las conclusiones.

- ✓ ACT (Actuar): o Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario. o Aplicar nuevas mejoras, si se han detectado errores en el paso anterior. o Documentar el proceso.

A continuación se muestra la adaptación del modelo de Deming al caso de un SGSI:

Figura 6: Modelo PDCA aplicado a procesos SGSI
Fuente : ISACA-COBIT 5, 2012

Planificar (Plan) Crear el SGSI	Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer (Do) Implementar y operar	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (Check) Supervisar y revisar	Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.
Actuar (Act) Mantener y mejorar	Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la Dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.

Tabla 11: adaptación del modelo de Deming al caso de un SGSI

UNIDAD V

TEMA 1: Planeación de auditoria informáticas y sus procesos.

5.1 Planeación de la Auditoría Informática

Para el desarrollo de una auditoría de gestión a las TIC´s, es muy importante que el auditor, conozca el entorno de la entidad y del Área de Tecnología de la Información, procesos sistematizados, organización del área de tecnología de información y comunicaciones, planes estratégicos de TIC, planes operativos, planes de contingencia y/o continuidad del negocio relacionado con la tecnología de la información, planes de mantenimiento preventivo y correctivo de la plataforma tecnológica con la que cuenta la entidad, de manera que le permita una adecuada planificación de su trabajo, pues ese conocimiento le brinda un marco conceptual, que le permite evaluar si la organización sigue un enfoque estructurado de gestión informática y si el mismo es adecuado.

5.2 Ejecución de la Auditoría Informática en: Normas, hardware, Sistemas Operativos, Software base, Sistemas de Información, Bases de Datos, Seguridad Física y lógica, Contratación y Adquisición, Procesos TIC, Comunicaciones, etc.

5.2.1 Organización de área TIC.

El auditor debe de conocer, comprender y analizar la arquitectura organizacional de la Entidad de manera general, identificando las ideas rectoras, organización, instrumentos administrativos, recursos humanos (principales funcionarios), productos y servicios de la entidad, así como la relación que mantiene con otras organizaciones y del conocimiento de la función del área de Tecnología de Información y Comunicaciones principalmente en aspectos como: Arquitectura Organizacional, Ideas Rectoras, Objetivos y metas operativas, Instrumentos Administrativos, Organización y función, Procesos, Productos y/o Servicios, Insumos y el entorno de la función de Tecnología de Información y Comunicaciones (clientes), aplicando procedimientos generales tales como:

- ✓ Revisar y evaluar si la función de TIC está alineada con la misión, visión, valores, objetivos y estrategias de la organización y deberá revisar el desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.
- ✓ Revisar y evaluar la eficacia de los recursos de TIC y el desempeño de los procesos administrativos. Se debe utilizar un enfoque basado en riesgos para evaluar la función de TIC. Se deberá revisar y evaluar el ambiente de control de la organización.
- ✓ Se deberá de revisar las áreas físicas de TIC´s, con el propósito si está en condiciones para la operatividad de las Tecnologías de la Información y Comunicaciones.
- ✓ Se deberá de revisar las funciones de cada uno de los técnicos para comprobar si estos cuentan con herramientas y condiciones necesarias para realizar su trabajo y de la optimización de los recursos tecnológicos.
- ✓ Se deberá de verificar y analizar el Manual de funciones sea aplicable y acorde a la realidad de las funciones desarrolladas por el capital humano del Área de Tecnología de Información y Comunicaciones.

5.2.2 Infraestructura Tecnológica de la entidad auditada.

El auditor debe conocer, comprender y analizar de forma general la Gestión en Tecnología de la Información, la infraestructura o plataforma tecnológica y los sistemas de información aplicados a la entidad, tales como:

- ✓ Granja de Servidores y sus características
- ✓ Seguridad Perimetral
- ✓ Estructura de redes
- ✓ Sistemas Operativos
- ✓ Software y hardware de seguridad
- ✓ El inventario de Hardware y Software con el propósito de establecer el nivel de obsolescencia o actualización.
- ✓ Servicios tercerizados contratados por la entidad y vinculados con la tecnología de la información y comunicaciones.
- ✓ Adquisiciones (Inversiones) en recursos de Tecnología de la información.
- ✓ Infraestructura eléctrica, entre otras.

5.2.3 Sistemas de Información (Aplicaciones)

- ✓ Procesos y/o funciones (sustantivos, apoyo y administrativos) de la entidad, que están soportados con tecnología de información y comunicaciones.
- ✓ La Administración de Sistemas y Bases de Datos.
- ✓ Adopción de Metodologías de Análisis y desarrollo de Sistemas.
- ✓ Lenguajes de programación
- ✓ Aplicaciones en producción y desarrollo
- ✓ Gestores de bases de datos.

5.3 Elaboración de Informe

Como producto del proceso de gestión, el área de tecnología de información y comunicaciones debe elaborar un plan maestro, definido como un documento a largo plazo que contenga la

estrategia de proyectos de modernización de los procesos institucionales a través de los recursos tecnológicos, con el objetivo de brindar con calidad el servicio ofrecido a los usuarios (Clientes) de la entidad, entre los aspectos mínimos que conforman dicho plan se encuentran los siguientes:

- ✓ Objetivos estratégicos institucionales
- ✓ Misión
- ✓ Visión
- ✓ Acciones estratégicas
- ✓ Procesos que serán automatizados
- ✓ Usuarios que intervienen en el proceso
- ✓ Recursos humanos, materiales, financieros y técnicos
- ✓ Cronograma de implementación de proyectos

5.3.1 Planes Operativos Los planes operativos son un instrumento de control a corto plazo que el auditor debe revisar, y que éstos contengan el desglose de las actividades y acciones a desarrollar que conforman cada línea estratégica del plan maestro, plasmándose lo siguiente:

- ✓ Objetivo general
- ✓ Objetivos específicos
- ✓ Líneas estratégicas y acciones a corto plazo
- ✓ Responsables de los proyectos a desarrollar.
- ✓ Recursos humanos, materiales, financieros y técnicos
- ✓ Cronogramas de actividades a desarrollar en el periodo.

5.4 Comunicación de Resultados

5.4.1 Resultados Preliminares de Auditoría (Informe Previo).

Esta etapa finaliza con los procedimientos de auditoría de la fase de ejecución, y comienza con la elaboración del Informe previo de Auditoría de resultados preliminares (en algunos países se le conocen como: informe previo, pre-informe, borrador de informe, entre otros), el jefe de equipo agrupa todos los asuntos de importancia (condiciones, deficiencias, observaciones) que incumplieron las disposiciones relacionadas con aspectos de control interno y/o de cumplimiento

con leyes, reglamentos legales y técnicos u otras disposiciones aplicables que dieron origen a la condición (Criterio), con la documentación que los respaldan y que los auditores determinaron al aplicar sus procedimientos de auditoría y se comunicarán a la máxima autoridad de la entidad y a los funcionarios actuantes responsables, esto se hace para garantizarse que dichos funcionarios tuvieron la oportunidad de defensa y convocándolos a una lectura de los resultados obtenidos y previos de auditoría para que emitan sus comentarios de defensa respectivos. Para que un asunto de importancia (condiciones, deficiencias, observaciones), sea incluido en el Informe previo de Auditoría de resultados preliminares e Informe de Auditoría deberá estar estructurado con todos sus atributos (Condición, Criterio, Causa, Efecto, Comentarios de la Administración, Comentarios del Auditor y Recomendaciones).

Las recomendaciones y conclusiones hechas por los auditores deberán ser viables y factibles para que éstas sean atendidas por la administración y que sean de fácil comprensión y análisis para terceras personas y auditores que verificarán el cumplimiento en auditorias recurrentes.

El informe previo de Auditoría de resultados preliminares deberá tener un formato uniforme y estar dividido por secciones para facilitar al funcionario lector una rápida comprensión del contenido del informe, y contendrán los principios y estructuras descrita en el Informe de Auditoría.

5.4.2 Informe de Auditoria

Posterior a la lectura del informe previo de Auditoría de resultados preliminares (Pre Informe, Borrador de Informe) se analizan los comentarios y documentación presentada por la administración, y se elabora el Informe de Auditoría que contiene los resultados finales de la auditoría que no fuesen superados. Se comunicarán los resultados al máximo nivel de dirección de la entidad auditada y otras instancias administrativas, así como a los funcionarios involucrados en los asuntos de importancia relativa (observaciones) que correspondan, cuando esto proceda. El informe de Auditoría debe tener un formato uniforme y estar dividido por secciones para facilitar al funcionario lector una rápida comprensión del contenido del informe. El informe de Auditoría debe cumplir con los principios siguientes:

- Que se emita por el jefe de grupo de los auditores actuantes.
- Por escrito.

• Oportuno.

• Que sea completo, exacto, objetivo y convincente, así como claro, conciso y fácil de entender.

El hecho de que un Informe sea Conciso, no significa que su contenido sea corto, lo que se quiere es que su contenido sea breve, ya que muchos informes pueden ser amplios porque las circunstancias así lo requieren; sin embargo no deben incluir hechos impertinentes, superfluos o insignificantes.

- ✓ Que todo lo que se consigna esté reflejado en los papeles de trabajo y que responden a hallazgos relevantes con evidencias suficientes y competentes.
- ✓ Que refleje una actitud independiente.
- ✓ Que muestre la conclusión u opinión de los resultados o evaluación de la Auditoría. • Distribución rápida y adecuada.

- ✓ El informe de auditoría deberá ser estructurado y tendrá como mínimo requerido lo siguiente:
- ✓ Nombre de la organización
- ✓ Destinatario del Informe
- ✓ Alcance de la Auditoría
- ✓ Objetivos de la Auditoría
- ✓ Período auditado
- ✓ Naturaleza, plazo y extensión de las labores de auditoría
- ✓ Hallazgos
- ✓ Conclusiones
- ✓ Recomendaciones
- ✓ Seguimiento Recomendaciones de Informes de auditorías anteriores (acciones implementadas)
- ✓ Firma
- ✓ Fecha
- ✓ Distribución del Informe de acuerdo a los mecanismos de cada Contraloría

UNIDAD VI
TEMA 1: Herramientas Case para Auditoría
6.1 Conceptos básicos de herramientas CASE

Se puede definir a las Herramientas CASE como un conjunto de programas y ayudas que dan asistencia a los analistas, ingenieros de software y desarrolladores, durante todos los pasos del Ciclo de Vida de desarrollo de un Software. Los estados en el Ciclo de Vida de desarrollo de un Software son: Investigación Preliminar, Análisis, Diseño, Implementación e Instalación.

6.1.1 Herramientas CASE en las Organizaciones.

Históricamente, las organizaciones han experimentado problemas con la adopción de Herramientas CASE. Dado que las organizaciones no conocen aún los beneficios de esta tecnología, se desea que el uso de un bien fundamentado proceso de adopción de CASE, ayude a incrementar la sucesiva adopción de estas herramientas. Es importante ampliar el rango de organizaciones que adquieran tecnologías de computación y desarrollen estándares para el desarrollo de software, diseño de métodos, metodologías y técnicas para llevar adelante el ciclo de vida de los sistemas.

Para ello, se recomienda:

- ✓ Identificar los factores críticos en los procesos.
- ✓ Proponer un conjunto de procesos a adoptar.
- ✓ Guiar satisfactoriamente esta adopción teniendo en consideración la organización y su entorno cultural.

Apoyo de la Administración: Extender la participación activa de la alta gerencia para alentar la adopción de CASE, sin limitar la buena voluntad para obtener los recursos que sean necesarios.
$ Uso estratégico de herramientas: Definir una estrategia clara para el uso adecuado de las herramientas.
$ Desarrollo del Plan para el proceso total de adopción: Un plan y diseño para el proceso total de posicionar estas herramientas al interior de cada componente de la organización.

$ Compromiso: Propiciar que las personas se involucren en el esfuerzo de adopción en forma activa, motivando a los participantes.

Metodología ajustable: La buena disposición y factibilidad técnica de ajustar, cuando sea necesario, los métodos de la organización y los métodos típicos de usar herramientas CASE, de tal forma que permitan llegar a un conjunto consistente de métodos.

Entrenamiento:

- ✓ Proveer el entrenamiento e información necesarios y apropiados en cada paso a cada persona envuelta en el proceso de adopción
- ✓ Ayuda de expertos: Provisión de ayuda experta en el uso de estas herramientas durante el proyecto piloto y continuamente tal como las herramientas se utilicen entre los componentes de la organización.
- ✓ Proyecto piloto: Los resultados de una prueba piloto controlada son prioritarios al tomar una decisión final.
- ✓ Capacidad de la herramienta: La capacidad técnica de la herramienta, en cuanto al entorno de hardware y software, de modo que satisfaga los objetivos definidos en el contexto del alcance esperado.
- ✓ Cambiado moderado: Asegurar la viabilidad que la organización pueda operar simultáneamente entre el viejo y nuevo métodos, hasta que los componentes de la organización hayan cambiado totalmente hacia el nuevo método.

6.2 Ciclo de vida de un sistema

La participación de la Auditoría de Sistemas en el desarrollo de una aplicación, se debería realizar desde el principio hasta el fin del proyecto, sin que esto requiera una participación de tiempo completo. Las etapas de mayor criticidad y donde se requiere una mayor participación por parte de la Auditoría de Sistemas son las etapas de análisis e implementación.

El auditor de Sistemas, en el desarrollo de una aplicación, debe asumir el rol de asesor y no comprometerse con la ejecución del diseño y construcción de la aplicación. El Auditor debe facilitar a los miembros del grupo de desarrollo, elementos y criterios para que tomen una mejor decisión (alternativas y no solución particular).

En el desarrollo de un sistema de información se han considerado cuatro etapas básicas: análisis, diseño, construcción e implementación.

ETAPA		PRODUCTO FINAL
Análisis	→	Lista de requerimientos de los usuarios, informática y de auditoria
Diseño	→	Diseño de la base de datos, de las entradas y salidas del sistema de información
Construcción	→	Aplicación teminada con manuales de usuario, técnico y de procedimientos
Implementación	→	Aplicación lista para empezar a operar efectivamente

Tabla 12: Etapas de un ciclo de vida

6.3 Funcionalidad de las herramientas Case

Estrategias de Implantación de una Herramienta CASE

1. Identificar la magnitud de problemas a resolver en la Institución.
2. Identificar el nivel estratégico que deben tener los sistemas.
3. Evaluar los recursos de hardware y software disponibles en la Institución y el medio.
4. Evaluar el nivel del personal.
5. Efectuar un estudio de costo-beneficio definiendo metas a lograr.
6. Elegir las herramientas apropiadas para la Institución.
7. Establecer un programa de capacitación de personal de sistemas y usuarios.
8. Elegir una aplicación que reúna la mayor parte de los siguientes requisitos: Gran impacto de resultados, Disponibilidad de recursos, Mínimo nivel de riesgos, Máxima colaboración de usuarios, Tamaño reducido de solución.
9. Se establecerán interfaces de compatibilidad de los nuevos sistemas que deben convivir con los sistemas anteriores.
10. Al elegir una herramienta es importante diseñar los procesos de auditoria informática, ejemplo BIzagi, Power Designer

UNIDAD VII

TEMA 1: Elaboración de informes planes de continuidad del negocio.

7.1 Conceptos básicos de Plan de acción , Plan de contingencia

El Área de TIC´s debe establecer un plan de continuidad o contingencia, viable donde se detallen acciones, procedimientos y recursos financieros, humanos y tecnológicos que considere los riesgos posibles, que afecten de forma parcial o total la operativa normal de los servicios de TIC´s categorizando el tipo de acción a realizar en cuanto a la medición en tiempo y recurso financiero para el restablecimiento de las operaciones tecnológicas. Este plan deberá ser autorizado por la máxima autoridad de la entidad y ser comunicado a los niveles pertinentes. Además, este plan debe probarse y actualizarse atendiendo la realidad tecnológica de la entidad al menos una vez al año.

El Área de TIC´s debe contar con una infraestructura tecnológica adecuada, que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red eléctrica.

La entidad debe contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones que permita mitigar el riesgo provocado ante cualquier tipo de contingencia y desastre natural (incendio, impacto de rayo, explosión, explosión, humo, gases o líquidos corrosivos, corto circuito, variaciones de voltaje, huelga, motín, robo, asalto y fenómenos naturales).

UNIDAD VIII

TEMA 1: Auditoría Continua

8.1 Conceptos sobre la Auditoria Continua

1. Auditoría Continua: evaluaciones permanentes de riesgos y controles mediante el uso de Tecnología por parte de la Gerencia de Auditoría Interna.

• 2. Monitoreo Continuo: evaluaciones permanentes de riesgos y controles mediante el uso de Tecnología por parte de la Gerencia de Línea.

• 3. Aseguramiento Continuo: Existencia concomitante de Auditoría Continua (1) y la función de Monitoreo Continuo (2) auditada.

La Auditoría Continua, una de las tecnologías más importantes para el desarrollo de la auditoría moderna, considerada por algunos autores, como el nuevo paradigma de la auditoría.

Es importante destacar que la Auditoría Continua no entra a reemplazar la auditoría tradicional, lo que hace es complementar una auditoría que mira retrospectivamente los hechos, con un modelo proactivo, que se fundamenta en una auditoría predictiva y preventiva, fundamentada en el uso intensivo de las TIC como herramientas que apalancan el proceso auditor.
La auditoría continua es un proceso comprensivo de auditoría que permite a los auditores dar cierto grado de seguridad en relación con información continua generada simultáneamente, o muy poco tiempo después de que dicha información sea revelada.

En definitiva, la auditoría continua puede centrarse en cualquier tipo de información para la toma de decisiones, no sólo la presentación de informes de los estados financieros o temas comunes de auditoría.

8.2 Aplicación de un modelo de auditoria Continua

De acuerdo a lo anterior y ante la importancia de poder contar con una clasificación de los modelos de Auditoría Continua, que sirvan de base para seleccionar aquellos que cumplen con ciertos criterios para su aplicación en un contexto específico, se ha construido una taxonomía, siguiendo para ello la siguiente metodología:

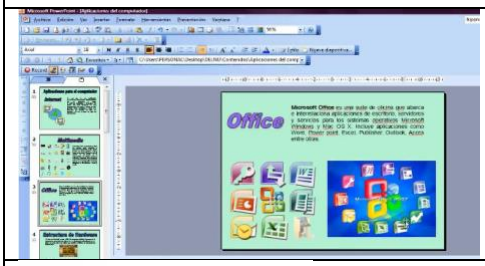
- Identificación del foco orientador de búsqueda y análisis
- Identificación de los esquemas sujetos de análisis• Análisis de la estructura metodológica de los esquemas
- Definición de categorías y propuesta taxonómica
- Explicación de cada una de las categorías taxonómicas.

B. Base de Consulta

TÍTULO	AUTOR	EDICIÓN	AÑO	IDIOMA	EDITORIAL
Auditoría en Informática	Hernández Hernández Enrique	1	1996	Español	México Cecsa
Auditoría de seguridad informática	Gómez Vieites /Alvaro	1	2013	Español	Bogotá Ediciones de la U
Auditoría Informática: Un enfoque Práctico	Piattini Mario G.	1	2001	Español	México ALFAOMEGA
Conceptos de la auditoria de sistemas	El Cid Editor	1	2009	Español	Argentina
Interfacing and adopting ITIL and COBIT	Hardy, Gary	1	2015	Español	Londres The Stationery Office
ITIL and the information lifecycle: integrating agile, devops and ITSM	Arcangel, Darren	1	2016	Español	Londres The Stationery Office
Reingeniería de la auditoría informática	Solís Montes, Gustavo Adolfo	1	2002	Español	México Trillas S.A.
Tecnologías de la información y la comunicación para la innovación educativa	Ruiz-Velasco Sánchez, Enrique, coord	1	2012	Español	México Consejo Nacional de Ciencia y Tecnología

http://repositorio.uned.ac.cr/reuned/bitstream/120809/380/1/GE3070%20Seguridad%20y%20Auditor%C3%ADa%20en%20las%20TIC%20-%202008%20-%20Inform%C3%A1tica.pdf

C. Base práctica con ilustraciones

TRABAJOS A PRESENTAR	DETALLE
	**2.- Presentación de un proyecto de auditoria informática aplicada a una empresa**
	3- Presentación del Proyecto Impreso Debe contener carátula, encabezado y pie de página , Índice, inicio a normas APA

4. ESTRATEGIAS DE APRENDIZAJE

ESTRATEGIA DE APRENDIZAJE 1: Análisis y Planeación
Descripción: • Discusión sobre las lecturas, artículos y videos. • Desarrollar, habilidades y destrezas, con los conocimientos desarrollados en la comunidad para identificar los factores de riesgo y su oportuna intervención. • Elaborar un proyecto, entendiendo conceptos de marco teórico, estado del arte, hipótesis, etc. • Implementar un proyecto de desarrollo social como respuesta a un problema previamente identificado en el ámbito comunitario, el cual sustenta con claridad y precisión. • Definir, analizar, implementar y gestionar las herramientas de TI, mostrando un conocimiento sólido respecto al uso de las Tecnologías de la Información y Comunicación y aplicando las técnicas elementales para buscar información en internet, procesarla y almacenarla.

• Realizar prácticas en clase, para comprender el desarrollo de un proyecto metodológico , apoyado en las tecnologías de información y que sean un aporte social comunitario • Crear debates de participación.
Ambiente(s) requerido: Aula amplia con buena iluminación, y laboratorios.
Material (es) requerido: ✓ Aula de clase ✓ Aulas virtuales ✓ Bibliotecas, páginas web ✓ Videos a fines al tema impartido ✓ Proyector Computador
Docente: Con conocimiento de la materia.

5. ACTIVIDADES

- Controles de lectura
- Exposiciones
- Presentación del Trabajo final
- CD con contenido del Proyecto
- Habilidad y esfuerzo en el proyecto entregado

6. EVIDENCIAS Y EVALUACIÓN

Tipo de Evidencia	**Descripción (de la evidencia)**
De conocimiento:	Creación de un Proyecto aplicando una metodología de desarrollo de software, que permita estructurar el proyecto y que siga los lineamientos de las normas APA , que permitirá al estudiante tener los elementos y lineamientos para trabajos

	colaborativos.
Desempeño:	Trabajo individual presentación del trabajo sobre la creación de una proyecto, usando herramientas de tecnologías de información que pueda dar un aporte significativo a la comunidad. Exposición individual del proyecto educacional
De Producto:	✓ Desarrollo de un proyecto innovador, que debe ser promocionado a un entorno social, utilizando medios para difundir la información, generando interés significativo y positivo. Intervención mediante una práctica de los estudiantes. ✓ Exposición oral sobre los temas de investigación individuales asignados a los estudiantes.
De Innovación	Se revisará la participación investigativa por parte del alumno en cuanto refiere a la innovación y desempeño al proyecto entregado el cual debe contener la difusión de las TICs Metodologías formales en su estructuración.
Criterios de Evaluación (Mínimo 5 Actividades por asignatura)	Identificar la metodología seleccionada, medios de difundir la información, herramienta tecnológica utilizada, Normas Apa establecidas en el proyecto, creatividad e investigación social.

+

ANEXO 1 EVIDENCIAS DE APRENDIZAJE

Msc. Diana Moncayo	**Alexis Benavides**	**Milton Altamirano**

Elaborado por:	Revisado Por:	Reportado Por:
(Docente)	(Coordinador)	(Vicerrector)

ANEXO 1

INSTITUTO SUPERIOR TECNOLÓGICO

JAPÓN

Amor al conocimiento

Guía metodológica de auditoría informática
Desarrollo de software
Msc. Diana Moncayo
2019

Coordinación editorial general:
Mgs. Milton Altamirano Pazmiño
Ing. Alexis Benavides Vinueza
Mgs. Lucía Begnini Dominguez

Diagramación: Sebastián Gallardo Ramírez
Corrección de estilo: Mgs. Lucía Begnini Dominguez
Diseño: Sebastián Gallardo Ramírez
Imprenta: JKIMPRIMA

Instituto Superior Tecnológico Japón
AMOR AL CONOCIMIENTO

ISBN: 978-9942-811-95-0