Auditoría Informática

Willian Geovanny Yanza Chávez
Johana Katerine Montoya Lunavictoria

2022

Alberto Patricio Robalino
Escuela Superior Politécnica de Chimborazo (ESPOCH)

Willian Geovanny Yanza Chávez
Escuela Superior Politécnica de Chimborazo (ESPOCH)

Johana Katerine Montoya Lunavictoria
Universidad Nacional de Chimborazo (UNACH)

Riobamba – Ecuador

2022
Publicado por acuerdo con los autores.
Este libro se sometió a arbitraje bajo el sistema de doble ciego *(peer review)*

Corrección y Diseño:
Índice Científico Editorial

Respaldado por:
La Caracola Editores

Auditoría Informática
Riobamba, Ecuador
Dirección de Publicaciones Científicas, 2022
ISBN: 978-9942-42-606-2
Fecha de Publicación: 2022-08-26

PRÓLOGO

La Auditoría Informática es un proceso donde la valoración de los sistemas informáticos de una empresa u organización puede ser esta pública o privada debe ser realizado por profesionales especialmente capacitados y preparados para el efecto, donde se deben recoger, agrupar, evaluar y examinar evidencias para determinar si un Sistema de Información tiene los niveles de seguridad exigidos para salvaguarda el activo más importante de la empresa, permitiendo conocer si se mantiene los principios de la seguridad informática como son la integridad, confidencialidad y disponibilidad de los datos y si se está llevando a cabo eficazmente por los responsables de la organización, de esta manera establecer la forma en la que se está llevando el manejo del recursos tecnológicos que dispone la empresa lo hacen de una forma eficiente cumpliendo con las leyes y regulaciones establecidas.

El presente texto consta de seis capítulos; el primer concepto generales la Auditoría; el capítulo dos una Introducción a la Informática; el capítulo tres sobre las afectaciones a los sistemas informáticos; cuarto capitulo los delitos informáticos en la legislación ecuatoriana; quito capítulo antecedentes de la Auditoria Informática y el sexto capitulo un ejercicio práctico de Auditoría Informática.

Finalmente, aspiramos a que el libro sea una guía que logre satisfacer las expectativas de sus lectores en lo referente a la Auditoria de Informática y cada uno de los procesos que se deben tener en cuenta para su respectivo análisis y evaluación.

INTRODUCCIÓN

Los cambios profundos en los últimos años son una verdadera revolución tecnológica que involucra de una sociedad industrial hacia una sociedad de información, por lo tanto las empresas y organizaciones deben adaptarse a estos cambios, de modo que la calidad, los controles sobre la seguridad de la información se convierten en el activo más preciado, que de hecho los profesionales hagamos eco de estas tendencias y acoplarnos a los estándares internacionales como el cobiT (Control Objetives For Information and Related Technology), como un sistema de control de la información.

La auditoría informática aparece como un aporte a la solución de los problemas que se generan en las empresas, organizaciones e instituciones, por lo que este texto constituirá en un verdadero aporte a nivel de estudiantes profesores y profesionales del quehacer de la contaduría pública. Actualmente la auditoria informática comprende un componente importante dentro de la evaluación, control y seguridad de programas, aplicaciones y tecnología que permiten a las Instituciones llevar a cabo de manera eficaz y eficiente sus operaciones.

En ese sentido, el presente trabajo funciona como herramienta de instrucción y conocimiento de algunos temas importantes relacionados con los sistemas informáticos y la auditoria informática, los cuales se desarrollarán en cinco capítulos como se describe a continuación:

En el primer capítulo se presenta el génesis de la auditoría, es decir, su historia, conceptos generales y definiciones de auditoría, los tipos de auditoría conjuntamente con los objetivos de cada tipo de auditoría, a su vez, los principios de auditoría.

En el segundo capítulo se detalla la introducción a la informática, definición de un sistema informático, funcionamiento de un sistema informático, elementos de un sistema informático, hardware, software, seguridad física, seguridad lógica, y cómo último punto los niveles de seguridad informática.

El tercer capítulo, trata acerca de las afectaciones a los sistemas informáticos, lo que engloba a: tipos de virus, tipos de ataques informáticos, vulnerabilidades a los sistemas Informáticos, privilegios excesivos, el abuso de

privilegios, la inyección de SQL, denegación del servicio DoS, vulnerabilidades en los protocolos de las bases de datos y la exposición de los datos de Back-Up.

En el cuarto capítulo, se presenta a los delitos informáticos en la legislación ecuatoriana, por lo cual es necesario presentar a las Normas de Control Interno de la Contraloría General del Estado, a su vez la penalización de los delitos informáticos en el Código Orgánico Integral Penal,

En el quinto capítulo se hace mención a los antecedentes de la Auditoría Informática, introducción a la Auditoría Informática, definición de Auditoría Informática, a su vez el marco esquemático de la auditoría de sistemas computacionales; enfoques, objetivos y características de la Auditoría Informática. Por su parte, la diferencia entre auditoría; informática, financiera y gestión. Así como se presenta a los métodos, técnicas, herramientas y procedimientos de la auditoría Informática, lo que engloba a: pruebas de cumplimiento y sustantiva, herramientas informáticas para la auditoría, entrevista y muestreo. Del mismo modo se detalla las fases de la Auditoría Informática, planificación, ejecución, comunicación de Resultados.

El sexto capítulo, trata sobre la Auditoría Informática y el riesgo, presentando a la valoración y componentes del riesgo, el Control Interno y los objetivos del Control Interno Informático, teniendo en cuenta también a los tipos de control interno informático y los controles internos aplicados por áreas funcionales y el COBIT. A su vez, se encuentra desglosado el COSO y sus componentes; ambiente interno, la asignación de autoridad y responsabilidades, evaluación del riesgo, actividades de control, información y comunicación, monitoreo e ITIL.

CONTENIDO

FIGURAS Y TABLAS

CAPÍTULO 1

Para Hablar de la práctica de la auditoría tenemos que remontarnos varios años atrás para ver los orígenes de la Auditoria, es así que en varios Autores indican que nació en Gran Bretaña durante la segunda mitad del siglo XIX y se extendió a otros países de cultura empresarial anglosajona, el mayor empuje a la Auditoria se da sobre todo en los Estados Unidos, llegando a consolidarse en las tres últimas décadas finales del siglo II, como una alternativa de proporcionar información contable y financiera que permita una información confiable y más transparente al inversor el mercado de valores, sobre todo después del precedente que supuso en denominado Crack de 1.929.

Con el crecimiento de las empresa e industrias y la necesidad de evaluar otros aspectos importantes que aparecen con la llegada de las computadoras, los softwares de aplicación, paquetes utilitarios, etc., para guardar información es como aparece la auditoría de sistemas informáticos que tiene como objetivo evaluar, examinar y analizar la eficiencia de los Sistemas Informáticos, verificando además su cumplimiento en lo referentes a la normativa en este ámbito Informático. Tiene por objeto también revisar la eficiencia y eficacia sobre la gestión de los recursos informáticos, Para finalmente emitir una opinión independiente, profesional y apegada a la verdad sobre la gestión informática.

Bajo todos estos aspectos mencionados anteriormente, la auditoría se configura como una herramienta fundamental en el proceso de control, proporcionando la confianza necesaria en la citada información e imponiéndose como exigencia social hasta el punto de que los poderes públicos, antes desconocedores del tema, asumen su establecimiento obligatorio como mecanismo necesario para la protección de los intereses de terceros y en beneficio también de la economía nacional.

1. Conceptos Generales

1.1. Inicios de la Auditoría

El comercio en sus inicios se manejaba con el conocido trueque, que consistía en el intercambio de productos como una forma de pago, a medida que este se incrementaba, se implementaron mecanismos rudimentarios que

permitían llevar un control sobre las operaciones que desarrollaban, este registro se inició a través de escribas, conforme esto avanzo se implementó la teneduría de libros, fue el uso de esta técnica la que impulso el inicio de la contabilidad, registro de libros y de pólizas. Conforme estos registros iban evolucionando surgió la necesidad de evaluarlos a fin de corroborar su veracidad y el correcto uso de los recursos que manejaban, fue esta necesidad la que da origen a la auditoría a fin de comprobar si los resultados presentados en los registros era la correcta.

Un auditor era la persona encargada de escuchar las lecturas de los ingresos y gastos que se producían en los distintos comercios que se manejaban en esa época, es por eso por lo que su raíz latina surge del verbo **"audire",** que significa oír, escuchar; esta práctica fue empleada por las civilizaciones antiguas. Como se menciona la auditoria nació en el momento que surgió la necesidad de evaluar y rendir cuentas respecto a los recursos que se manejaban dentro de los establecimientos dedicados al comercio, la función que desempeñaba la auditoría creció y evoluciono conforme iba creciendo las actividades mercantiles. Además, es importante mencionar que el nacimiento de la auditoría se le atribuye al siglo XV mucho antes de se implementará la teneduría de libros la misma que se fue personalizando en el tiempo hasta obtener en la actualidad los distintos tipos de auditoría y sus funciones.

Por otro lado, es importante mencionar los conceptos de algunos autores importantes que hablan de la Auditoría como es Muñoz Razo en su libro titulado Auditoría en sistemas computacionales que expresa antecedentes históricos de la auditoría de la siguiente forma:

"Los orígenes de la auditoría vienen desde hace los tiempos más remotos muchos siglos atrás es en donde la auditoría se creó en base a una actividad de aplicación como eran los principios de contabilidad, basada en la verificación de los registros patrimoniales de las haciendas, para observar su exactitud. Por ejemplo, su existencia radica desde la época de la civilización Sumeria y el pueblo Azteca. La auditoría, en su forma más primitiva y simple, surge cuando un pueblo o núcleo social, sojuzga o domina a otro, por medio de la política, religión, economía, ciencias, o como antiguamente era la manera más común, por la fuerza. Así, el pueblo o la comunidad social eran obligadas a pagar un tributo a quien lo domina. Este tributo hoy se conoce como contribución, el gobernante requiere que los tributos que impuso sean pagados correctamente en el tiempo requerido para estar seguros de que dicho pago se realizará, se designaban revisores, quienes realizaban una actividad de fiscalización."

En 1942 que se refiere al descubrimiento de América y con la llegada de los españoles se incrementó la actividad de la auditoría, los Reyes de España enviaron visitadores América donde su trabajo era revisar como se estaban llevando las cuentas, resultados y novedades que existían en cada una de sus colonias; estos visitadores eran los encargados de revisar los registro y manejo de las cuentas que sus movimientos sean los más fueran correctos y emitían una opinión sobre la actuación de los Responsables.

Con la aparición de la Revolución Industrial en 1800, muchas Instituciones habían alcanzado la cúspide en las actividades fabriles y mercantiles, lo cual trajo consigo un notable crecimiento en sus operaciones; con estas actividades aumentó también la necesidad de registrar las operaciones contables, es así que se hizo indispensable la existencia de la profesión de un contador para satisfacer esa creciente necesidad. Esto provocó una gran demanda de ejercer un mayor control, vigilancia sobre los registros de las operaciones financieras y la emisión de resultados que realizaban estos nuevos profesionales, de esta manera el dictamen emitido por el contador independiente se consideraba totalmente confiable. De esta manera creció la popularidad del auditor y se destacó como una actividad preponderante en la administración de las Instituciones de ese entonces.

En un inicio, a la auditoría se consideraba como una rama complementaria de la contaduría pública, y que únicamente se dedicaba a evaluar los registros contables y la correcta presentación de los estados financieros de las Empresas. Posteriormente, dicha aplicación se extendió a otros campos profesionales para ampliar su revisión; primero a los de carácter administrativo, después a los asociados a otras actividades de la Institución, luego se extendió a las ramas de ingeniería, medicina, sistemas y así sucesivamente, hasta que su práctica alcanzó a casi todas las disciplinas del quehacer humano.

Aunque la revisión de registros y cuentas se pueden considerar como el inicio de la auditoría, su reconocimiento como profesión se inició en los albores del presente siglo. No obstante, también hay evidencias de que, a mediados del siglo pasado, los británicos, españoles, estadounidenses, e incluso los mexicanos, iniciaron la actividad formal de la auditoría. Debido a la abundancia de literatura sobre la auditoría financiera, y a la profundidad con que numerosos autores han realizado el análisis a la auditoría de los estados financieros, sólo nos enfocaremos en conocer los antecedentes generales de la auditoría de carácter administrativo y operacional, ya que de la conjugación de esos tipos de auditoría

nacieron otros más especializados, entre ellos la auditoría de sistemas computacionales o Informática.

Como se puede anotar según varios autores hablan de que la auditoria existió desde tiempos antiguos, en distintas formas, métodos y técnicas, de las cuales con el pasar de los tiempos y el avance de las tecnologías ha ido evolucionando conforme se incrementaban los registros de las operaciones mercantiles el crecimiento de las empresas, áreas de trabajo, logrando en la actualidad un sistema de auditoría tanto interno como externa que permite evaluar y controlar el manejo de los todos los recursos de una organización, así como también de los objetivos de estas y el grado de cumplimiento en un periodo determinado; con el tiempo se han sumado distintos tipos de auditoría especializadas en distintas áreas, mismas que permiten una evaluación completa de las distintas áreas de la Institución.

1.2. Definición de Auditoría

Para hablar de auditoria se han tomado referencias de varios autores que han construido una definición respecto a la auditoría para lo cual existe una variedad de definiciones sobre este concepto, muchas de estas son similares o coinciden en ciertos criterios que este tema desarrolla, de estas definiciones se ha tomado las más acertadas respecto al tema que se desarrolla en el presente texto, concluyendo con una definición propia.

Figura 1. *Auditoría.*

Fuente: *Auditest (s/f). Figura de auditoría. [Figura]. Recuperado de: https://auditest.es/auditorias- por-que-son-importantes-para-mi-Institución/*

Arens, Randal y Mark autores del libro Auditoría un enfoque integral mencionan una definición respecto a un concepto sobre la auditoría que menciona que la Auditoria:

"Auditoría es la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente."

Otro Autor importante es Sánchez Curiel donde en su texto que lleva como título Auditoría de estados financieros práctica moderna integral emite la siguiente definición sobre el término auditoría es:

"El examen integral sobre la estructura, las transacciones y el desempeño de una entidad económica para contribuir a la oportuna prevención de riesgos, la productividad en la utilización de los recursos y el acatamiento permanente de los mecanismos de control implantados por la administración".

Considerando las distintas definiciones del término auditoria escrita por varios Autores entendidos en la rama de la Auditoria, se puede aportar la siguiente conceptualización de este:

La auditoría es una evaluación que se realiza no solo a la parte financiera, económica o administrativa de una organización, sino que puede aplicarse a cada una de las áreas que esta posea, con el fin de tener clara la situación de la Institución y a la vez controlar el cumplimiento de objetivos y garantizar la adecuada utilización de los recursos organizacionales, en caso de existir anomalías permite tomar medidas correctivas a fin de mejorar la eficiencia y eficacia de la organización en el desempeño de sus actividades optimizando sus recursos.

1.3. Clasificación de los Tipos de Auditorías

Para poder establecer un correcto análisis, evaluación, examen, verificación existen una gran clasificación de Auditorias que tiene el propósito de identificar diferentes criterios y puntos de vista para cada una de las actividades que se realicen dentro de una Institución, con este objeto vamos a describir una clasificación de auditorías en el siguiente cuadro

Auditorías por su aplicación:	**Auditoría Externa. –** Esta auditoria se caracteriza porque es ejecutada por una persona externa alejada de la organización, esto permite eliminar los conflictos de intereses y de libertad en la realización de actividades por parte del auditor.
	Auditoría Interna. – La auditoría Interna a lo contrario de la Auditoría externa señala que el auditor interno deberá desarrolla sus actividades bajo relación de dependencia en la misma Institución, la auditoría interna también se trata de una revisión, evaluación o examen que lo debe realizar dentro de la Institución y que también es realizada por un profesional formado en Auditoría.
Auditorías por su área de aplicación:	**Auditoría Financiera. –** en esta auditoría la principal función tiene como finalidad evaluar la correcta y oportuna aplicación de los registros contables, tributarios de las Instituciones.
	Auditoria Administrativa. – Es la evaluación que se realiza a la parte administrativa de una Institución, en esta se evalúa su organización, el área de talento humano, cumplimiento de funciones; esto con el fin de evaluar el desempeño administrativo de cada una de las áreas que conforman la organización.
	Auditoría Operacional. – encargada de la revisión absoluta, metodológica y concreta que se realiza a las actividades de una Institución, con el objetivo de valorar la eficiencia, suficiencia, eficacia del correcto desarrollo de sus operaciones en el establecimiento y cumplimiento delos métodos, técnicas y procedimientos de trabajo necesarios para el buen desarrollo de sus operaciones.
	Auditoría Integral. – Esta auditoría se encarga de la revisión global a todas las actividades y operaciones que se desarrollan en una Institución en un determinado periodo de tiempo, esta auditoría comprende la evaluación al área administrativa, financiera, contable, legal.

	Auditoría Gubernamental. – Esta auditoría es la evaluación que se realiza a las entidades que forman parte del estado, es un proceso sistemático que permite revisar las actividades y operaciones de las entidades, organizaciones e Instituciones que conforman el Estado.
	Auditoría de sistemas. – La Auditoria de sistemas es aquella que se encarga de la revisión, evaluación y examen de los métodos y procedimientos de uso en una Institución, con el propósito de determinar su diseño, aplicación y buen uso de los sistemas informáticos.

Existen también otras Auditorias que están definidas como auditorías que tienen un alcance definido y concreto estableciendo el área a auditar, surgiendo de la necesidad o preocupación patente del cliente por los incidentes o anomalías detectadas en el ámbito solicitado.

Auditorías especializadas en áreas específicas:	**Auditoría al área médica. –** Para este tipo de Auditorias se debe realizar una evaluación sistemática, exhaustiva y especializada que se realiza a las ciencias médicas y de la salud, la misma debe ser aplicada por especialistas en disciplinas médicas o similares.
	Auditoría al desarrollo de obras y construcciones. – En este tipo de Auditoria también se debe realizar una revisión técnica especializada por un profesional de la construcción que se dedique a la edificación de construcciones, cimientos, obranegra, acabados y servicios urbanísticos complementarios de casas, edificios, puentes, caminos, presas y cualquier otro tipo de construcción, ya sea de tipo civil y/o arquitectónico.
	Auditoría fiscal. – La Auditoría Fiscal esta encargada de la revisión exhaustiva, pormenorizada y completa que se realizan a todos a los registros y operaciones contables de una Institución, así como la evaluación exhaustiva de una correcta elaboración de los resultados financieros de un ejercicio fiscal.

	Auditoría laboral. – Esta auditoria se encarga de la revisión y evaluación de las actividades que realiza la Empresa, sus funciones, el recurso y humano y la correcta aplicación de las prestaciones personales, económica de seguridad e higiene.
	Auditoría Ambiental. - Está auditoria hace relación a la evaluación relacionada a la calidad atmosférica, medio ambiente, ríos, lagos y océanos, así como también a la conservación de la flora y fauna silvestre con la finalidad de realizar un dictamen preventivo y correctivo que permita disminuir la contaminación provocada por el hombre, empresas, vehículos, etc.

Auditoría de sistemas computacionales:

Esta Auditoría es la encargada del control, verificación del procesamiento de la Información, en el desarrollo de sistemas y sus instalaciones. Se esta Auditoría se deprende algunas otras como son:

- **Auditoría informática**
  Es un examen y evaluación que se realiza al software, hardware, sistemas e información utilizadas por una organización con el fin de mejorar sus procesos, para poder medir la eficiencia y eficacia con la que se están utilizando los recursos informáticos de las Instituciones, evaluar su uso adecuado y los resultados que aportan a la organización.

- **Auditoría a la gestión informática**
  Este tipo de auditoría es especial porque se enfoca en la revisión y control de las funciones y actividades que cumple el personal a cargo del área informática, además es la encargada de evalúa las actividades administrativas que se llevan a cabo en la Empresa, así como la revisión de las instalaciones, mantenimientos y el correcto desarrollo de los sistemas.

- **Auditoría de la seguridad de sistemas computacionales**
  Esta auditoría se aplica a todo lo que se encuentre directamente relacionado con la seguridad de un sistema de cómputo dentro de la Empresa, departamentos, áreas, personal, así como también a las actividades, funciones y acciones preventivas, correctivas y detectivas que

contribuyen a proteger y mejorar el funcionamiento adecuado de los sistemas informáticos de la Institución.

- **Auditoría a los sistemas de redes**
  Esta Auditoria está enfocada en todos los sistemas de comunicación y de redes informáticas que utiliza diariamente la Institución para un adecuado desempeño de sus actividades, además con esta evaluación también se revisa el software institucional, y todo sistema o programa relacionado que permita acceder a las bases de datos que esta maneje.

- **Auditoría integral a los centros de cómputo**
  La Auditoria Integral es la encargada de realizar una revisión exhaustiva, sistemática y global por medio de un equipo multidisciplinario de auditores, de todas las actividades y operaciones de un centro de sistematización, a fin de evaluar, en forma integral, el uso adecuado de sus sistemas de cómputo como son equipos periféricos y de apoyo para el procesamiento de información de la Institución, así también la red de servicios de una Institución y el desarrollo correcto de las funciones de sus áreas, personal y usuarios.

- **Auditoría ergonómica de sistemas computacionales**
  Esta auditoría evalúa tres entornos que son: hombre- maquina- medio ambiente a fin de que está posea calidad, eficiencia y utilidad, esto en el entorno de los sistemas computacionales de cada organización, en esta también se evalúa que la Institución posea el mobiliario, equipo y sistemas adecuados y necesarios que proporcionen el ambiente de trabajo adecuado para que el personal pueda desempeñar sus funciones sin que estén expuestos a daños en su salud a corto o largo plazo dentro de la Institución.

1.4. Objetivos Generales de Auditoría

Para la escuela de negocios de EAE Business School el principal objetivo de una auditoría es:

- *"La elaboración de un documento en el que se recopilen los resultados obtenidos del proceso de auditoría y que, a la vez, estos insumos sirvan de referencia para terceros agentes, estos pueden ser miembros integrantes de*

la propia Institución o de algún otro organismo o institución oficial que ha solicitado la puesta en marcha de la auditoría."

Por otro lado, entre muchos otros autores como es el caso de Carlos Muñoz Razo en su texto auditoría en sistemas computacionales hace referencia a los siguientes objetivos generales de auditoría:

- *"Realizar una revisión independiente de todas las actividades, áreas o funciones especiales de una institución, a fin de poder emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados apegados a la realidad."*

- *"Hacer una revisión especializada, desde un punto de vista profesional y autónomo del Auditor, del aspecto contable, financiero y operacional de las áreas de una Institución que se está Auditando."*

- *"Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulen el comportamiento de los empleados y funcionarios de una institución, así como evaluar todas las actividades que se desarrollan en cada una de sus áreas y unidades administrativas en la Institución."*

- *"Dictaminar de manera profesional e independiente sobre los resultados obtenidos de la Auditoria por la Institución y sus áreas, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones."*

En este contexto se debe señalar que todos los criterios que los Auditores hacen con respecto al objetivo de la son generales respecto a la auditoría, sin embargo, estos pueden ser aplicados a los distintos tipos de auditoría existentes, para dar inicio a un trabajo de auditoría es esencial establecer los objetivos de cada trabajo de auditoría que se pretende desempeñar, esto se debe realizar con cada una de las áreas de la Institución que se pretenden evaluar. Los objetivos deben dejar claro lo que se pretende lograr con la revisión de cada área, para al finalizar este trabajo se tenga certeza respecto al cumplimiento del trabajo de auditoría alcanzado.

1.5. Objetivos de cada tipo de Auditoría

Así como existen objetivos generales de auditoría Informática, también

existen los objetivos por cada tipo de auditoría que se describen a continuación en las distintas Auditorias según se indica a continuación:

Auditoría externa

- Realizar una evaluación, de manera profesional e independiente, a una institución con la cual el Auditor no este subordinado a la misma, con el fin emitir un dictamen externo sobre la razonabilidad de sus actividades, operaciones y resultados.

- Hacer una revisión independiente profesional sobre el aspecto contable y las finanzas de las áreas de una Institución, emitiendo un dictamen autónomo apegado a la realidad de la Institución.

- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan las funciones de una institución, así como evaluar las actividades de sus áreas y unidades administrativas, utilizando un enfoque ajeno a la institución.

Auditoría interna

- Realizar una evaluación independiente y profesional dentro de la institución donde el Auditor presta sus servicios, en tal virtud cuenta con un mayor entendimiento de sus actividades y operaciones de la Institución, esto con el fin de ayudar a evaluar de mejor manera la actuación de la gestión administrativa de la Institución.

- Hacer una revisión interna del área contable, financiera y del control interno de las áreas de una Institución, a fin de evaluar su correcto funcionamiento desde un punto de vista interno.

- Evaluar internamente el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de cada uno de los integrantes de una institución, así como de sus áreas administrativas.

- Dictaminar en forma interna sobre las actividades, operaciones y funciones que se realizan en una Institución, contando con un mayor conocimiento de las actividades del personal que labora en ella, así como de sus funciones y tareas.

Auditoría Financiera

- Realizar una evaluación, de manera independiente, de las operaciones financieras de una institución, a fin de poder emitir un dictamen profesional sobre la razonabilidad de sus registros, operaciones y resultados financieros.

- Hacer una revisión, desde un punto de vista autónomo e independiente, de las actividades financieras y de las operaciones y registros contables de las áreas de una Institución.

- Evaluar el buen cumplimiento de los planes, programas, políticas, lineamientos y normas que regulan las actividades financieras de una institución, así como de sus áreas presupuestales y unidades administrativas.

- Vigilar el ejercicio y cumplimiento de los planes, presupuestos y programas de inversión de la Institución, así como sus bienes e inventarios.

- Revisar los estados financieros que se presentan ante las autoridades fiscales y terceros, con el propósito de evaluar su correcta elaboración, los pagos de impuestos y utilidades de una Institución, así como emitir una opinión sobre el comportamiento de ésta.

Auditoría administrativa

- Realizar una evaluación, de manera independiente, de las actividades, operaciones, estructura organizacional y funciones de una institución, con el fin de emitir un dictamen sobre la razonabilidad de su gestión administrativa.

- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la gestión directiva de las áreas y unidades administrativas de una institución.

- Evaluar la actividad administrativa de los directivos y demás empleados de una Institución, así como dictaminar sobre el cumplimiento de sus funciones y actividades.

- Analizar todo lo relacionado con la gestión administrativa de una Institución.

Auditoría operativa

- Realizar una evaluación, de manera independiente, de las actividades, operaciones, estructura organizacional y funciones de una institución, a fin de emitir un dictamen sobre la razonabilidad de sus operaciones fundamentales.

- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la realización de las operaciones de una institución, así como evaluar sus áreas y unidades operacionales.

- Evaluar la actividad operativa de los directivos y demás empleados de una Institución.

- Evaluar los cambios y mejoras en los sistemas de operación, los métodos, procedimientos de trabajo y las técnicas específicas que regulan las operaciones y las actividades de los funcionarios y demás empleados de una Institución.

- Mejorar el uso de los recursos de la Institución en el desarrollo de sus operaciones y actividades.

- Evaluar el volumen, frecuencia y periodicidad de las operaciones y actividades de las diferentes unidades administrativas de una Institución, en función de su objetivo institucional.

Auditoría integral

- Realizar una evaluación global, multidisciplinaria e independiente sobre las actividades, operaciones, estructura organizacional y funciones de todas y cada una de las áreas y unidades de trabajo de una institución, con el fin de emitir un dictamen global sobre la razonabilidad de sus funciones y operaciones.

- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan las áreas y unidades de trabajo de una

Institución, así como de la correlación e integración de sus funciones y actividades.

- Dictaminar, en forma integral y multidisciplinaria, sobre los resultados e interrelación de las actividades de cada una de las áreas y unidades administrativas de una Institución, utilizando siempre las mismas herramientas de evaluación para hacer una valoración sistemática y emitir un dictamen veraz.

- Mejorar los sistemas de operación, los métodos y procedimientos de trabajo, las técnicas específicas y los controles que regulan las operaciones y actividades de todas las áreas de una institución, a través de una evaluación global y multidisciplinaria de las mismas.

- Aprovechar los recursos de las múltiples disciplinas de la auditoría, para hacer evaluaciones conjuntas de las operaciones y actividades de todas las unidades de trabajo de una Institución.

Auditoría gubernamental

- Realizar una evaluación, de manera independiente, sobre las actividades, operaciones, estructura de organización y funciones de las Instituciones de la administración pública federal, a fin de emitir un dictamen sobre la razonabilidad de su gestión administrativa y del uso de los recursos públicos.

- Evaluar el adecuado cumplimiento de los planes globales de desarrollo, de los presupuestos y programas de inversión, y el uso correcto de los recursos públicos por parte de cada entidad de las administraciones públicas federal, estatal o municipal.

- Evaluar la actualización y correcta aplicación de las leyes, normas, políticas y procedimientos que regulan las actividades de una institución gubernamental, así como sus relaciones con otras dependencias y los ciudadanos.

- Dictaminar sobre los resultados de la gestión administrativa de directivos, empleados y trabajadores de cada una de las Instituciones y dependencias de las administraciones públicas federal, estatal y municipal, así como

sobre el cumplimiento de sus actividades y funciones.

Auditoría de sistemas

- Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.

- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.

- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.

- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.

- Realizar la evaluación de las áreas, actividades y funciones de una Institución, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio de la computadora.

Cabe señalar que cada uno de los objetivos descritos anteriormente son importantes porque el propósito es dar a conocer las características y principales fines que posee cada uno de los tipos de auditoría y que puedan servir como base para la realización de trabajos de auditoría en las distintas áreas que conforman la Institución y que pretendan evaluar mediante un trabajo de auditoría.

1.6. Principios de Auditoría

Hay seis principios de auditoría, sobre los cuales se basa la auditoría, de acuerdo con lo que establecen las normas ISO:

- **La Integridad**: toda auditoría debe basarse en la profesionalidad.

- **La Presentación justa:** cada auditoría tiene la responsabilidad de informar sus hallazgos de manera no solo precisa sino también veraz.

- **Cuidado profesional:** cada auditoría debe realizarse de tal manera que se apliquen el buen juicio y la debida diligencia al proceso.

- **La Confidencialidad:** mucha de la información que se recopila y comparte durante una auditoría es de naturaleza confidencial. Su seguridad debe, por lo tanto, ser asegurada apropiadamente.

- **La Independencia:** la auditoría, ya sea que la lleve a cabo un auditor interno o externo, debe ser imparcial y las conclusiones deben ser objetivas, sin verse influidas por ningún miembro de la gerencia de la organización.

- **El enfoque basado en la evidencia:** las conclusiones de la auditoría se deben llegar de manera racional y no solo deben ser confiables sino también reproducibles. La única forma en que esto es posible es que el proceso de auditoría sea sistemático y se base en evidencia un trabajo profesional e independiente a los criterios que emita el Auditor en la Institución.

CAPÍTULO 2

2. Introducción a la Informática

2.1. Definición de un Sistema Informático

Existen muchas definiciones de muchos expertos en el Área de los Sistemas Informáticos con donde manifiestan que un sistema informático está conformado por un conjunto de elementos y procesos que tiene por objetivo el de almacenar y procesar la información para obtener nuevos resultados. Para procesar la información es necesario que exista la entrada o datos que den como resultado nueva información o salida de datos. Por lo tanto, el sistema informático se encuentra conformado por dos componentes, el primero es la parte central del sistema que da lugar al procesamiento de datos, la segunda parte, está conformada por los instrumentos externos o periféricos que facilitan la entrada y salida de datos que han resultado del procesamiento de la información.

Otra definición de un sistema informático se establece como un conjunto de dispositivos, con al menos una CPU o unidad central de proceso, que estarán física y lógicamente conectados entre sí a través de canales, lo que se denomina modo local, o se comunicarán por medio de diversos dispositivos o medios de transporte, en el llamado modo remoto. Dichos elementos se integran por medio de una serie de componentes lógicos o software con los que pueden llegar a interaccionar uno o varios agentes externos, entre ellos el hombre.

En este contexto se puede mencionar que un sistema informático corresponde al conjunto de todos los componentes físicos e intangibles que interactúan entre sí, a través del almacenamiento, procesamiento y recolección de datos, con el propósito de procesar información que, mediante el uso de periféricos de entrada y salida se logra obtener una nueva información como resultado del proceso de datos. Así como un sistema informático se convierte en una herramienta electrónica que lleva a cabo operaciones tecnológicas.

Con estas consideraciones sobre el Sistema Informático podemos manifestar que para que este funcione adecuadamente es necesario tener en cuenta tres aspectos necesarios:

- **Aspecto Físico:** está conformado por todos los periféricos que integran o conforman el computador.

- **Aspecto Lógico:** se refiere a los programas y aplicaciones que permiten la funcionalidad del computador.

- **Aspecto Humano:** está conformado por las personas que trabajan el equipo informático y son los encargados de crean nuevas aplicaciones para mejorar el procesamiento de datos.

Figura 2. *Componentes del Sistema Informático.*

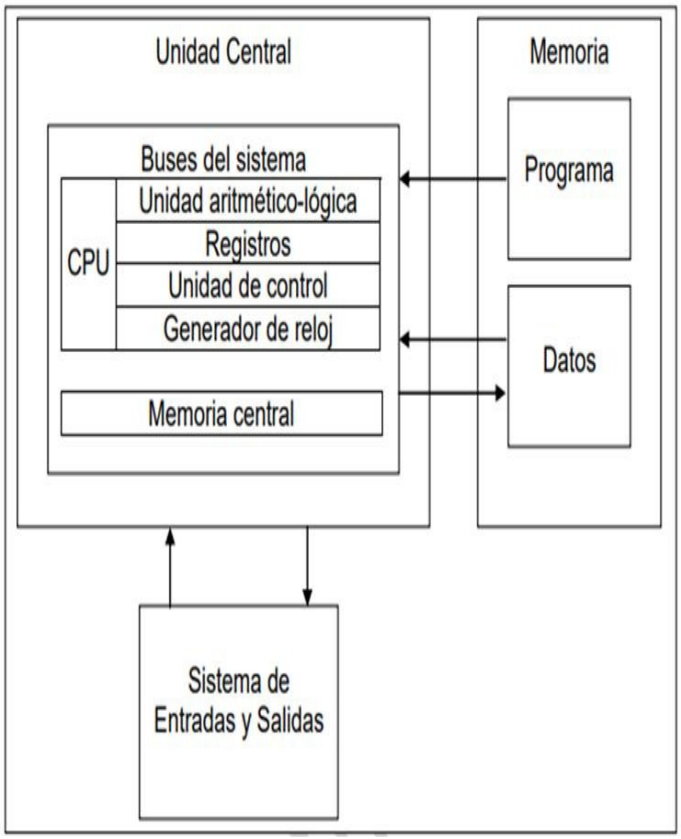
Fuente: *MORENO, J. & SERRANO, J. (2014). Figura de los componentes de un sistema informático. [Figura]. Recuperado de: https://elibro.net/es/ereader/espoch/62457?fs_q=hardware y software&prev=fs (p. 29).*

En la figura No.2 se puede apreciar los componentes que conforman el sistema informático, tanto la parte lógica como la parte física que trabajan conjuntamente para procesar la información y obtener nuevos resultados. Si uno

de estos componentes no funcionaría de manera adecuada, difícilmente se puede obtener información favorable que contribuya a la toma de decisiones de un sistema informático.

Generalmente, para poder optimizar los resultados, las Instituciones establecen normas, reglamentos o políticas que permitan el uso correcto de estos componentes, por ello, el ser humano juega un papel fundamental en el sistema informático debido a que, dentro de una Institución tienen la responsabilidad de seguir los planes de capacitación para el uso de los sistemas, así como también los programas y aplicaciones necesarios para el desarrollo de la Institución.

Figura 3. *Procesamientos de datos.*



Fuente: *CHCACÓN, F. (2014). Figura del procesamiento de datos con las respectivas entradas y salidas de información. [Figura]. Recuperado de: https://www.preparadores.eu/temamuestra/PTecnicos/PComerciales.pdf*

Como se observa en la figura No.3 anterior presentada existe un ordenador que se encarga de recibir la información entregada por un periférico externo de entrada, posteriormente esta información es almacenada por una memoria Interna con el fin de enviar a la unidad central de procesos para que esta, continúe con el procesamiento de la información con el fin de obtener resultados y presentarlos al exterior.

Es muy común que en las actividades Institucionales se utilicen los sistemas informáticos, generalmente en Instituciones grandes, por tal motivo se puede decir que, esas actividades operacionales dan lugar a los sistemas informáticos, por ejemplo, dentro de una Institución comercializadora es necesario recurrir a sistemas que permitan procesar la información de manera lógica, coherente y rápida, por ejemplo cuando se realiza una compra, venta, un cobro o pago, se deben registrar las operaciones en sistemas informáticos, con el fin de obtener los resultados financieros al final del periodo contable.

Cabe mencionar que existen diferentes tipos de sistemas informáticos que utilizan las Instituciones:

Sistemas Informáticos que contribuyen al procesamiento de transacciones, son todos aquellos que permiten el registro de las actividades económicas que realiza una Institución como por ejemplo el registro de los inventarios, transacciones de adquisición de activos fijos, registro de nómina de sueldos y salarios.

Sistema Informáticos para la automatización de oficinas, funciona como un procesador de texto, intervienen cuando la Institución requiere que una aplicación sea utilizada para colaborar en el trabajo administrativo. Por ejemplo, dentro de este sistema se encuentran las hojas de cálculo, los sistemas contables, los correos electrónicos que son exclusivamente para clientes, etc.

Sistemas Informáticos para información: este tipo de sistemas se maneja con base y almacenamiento de datos que el cual al procesar la información contable se obtiene una visión clara de la realidad de la situación de a la Institución, por tal motivo se puede tomar decisiones para mejorar las falencias detectadas en este perfil.

2.2. Funcionamiento de un Sistema Informático

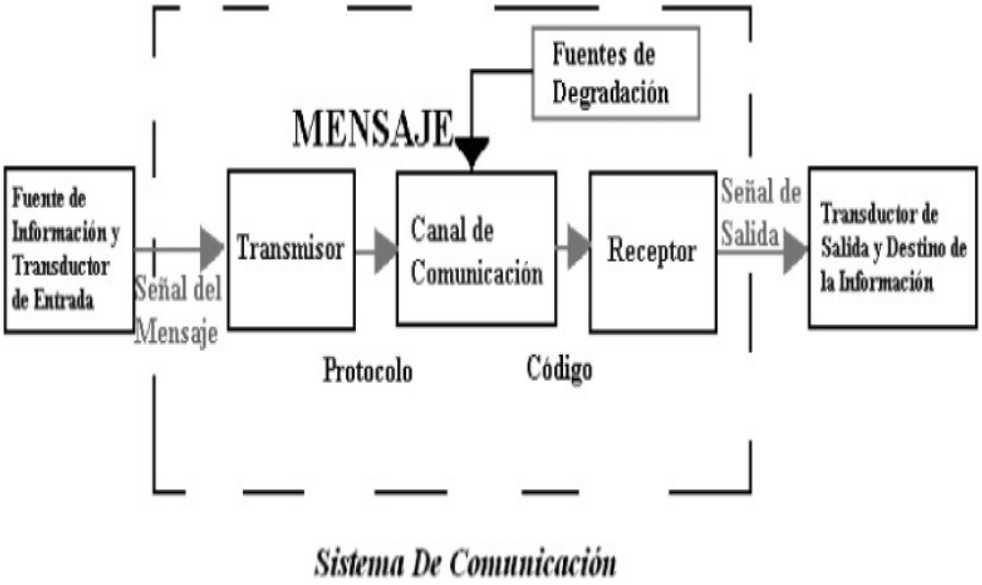
El sistema informático tiene varias especificaciones entre una de ellas y la más importante es el procesamiento de datos, esto datos se vuelven información importante para cualquier Institución una vez que se procesan los datos dentro del disco duro y memoria del ordenador. Por tal motivo estos datos deben estar contenidos en soportes accesibles al sistema informático, es decir que los datos deben almacenarse en soportes que permitan el procesamiento de datos de forma ágil y coherente.

Figura 4. *Actividades que conforma un Sistema Informático.*

Fuente*: PINTO, M. (2019). Figura del funcionamiento el sistema informático. [Figura]. Recuperado de: http://www.mariapinto.es/alfineees/sistemas/como.htm*

Como se observa en la figura No.5 y de acuerdo con Pinto manifiesta que el funcionamiento de los sistemas informáticos está compuesto de tres actividades que permiten el procesamiento de la información para la toma de decisiones y el control de las operaciones. Las actividades que se dividen en la Gráfica son tres: entrada, procesamiento y salida. Estas actividades producen información convirtiendo la entrada de datos de forma significativa para posteriormente transferir la información (salida) a las personas que la usarán para tomar decisiones. Para corregir desviaciones en las entradas de información es necesario realizar una retroalimentación que corresponde a la salida de la información para que las personas puedan evaluar la entrada de datos con el fin de obtener resultados favorables.

Figura 5. *Comunicación del Sistema Informático*



Fuente: *MORENO, J. & SERRANO, J. (2014). Figura de la comunicación de un sistema informático. [Figura]. Recuperado de: https://elibro.net/es/ereader/espoch/62457?fs_q=hardware y software&prev=fs (p. 16).*

En la figura No. 5 se explica como es el funcionamiento del Sistema Informático los mensajes inician con una fuente de información de entrada que

ingresa mediante un protocolo de comunicación que viene siendo el transmisor del mensaje, el mismo pasa por un canal de comunicación que llega mediante un código al Receptor que recibe la información logrando de esta manera llegar al destinatario del mensaje.

2.3. Elementos de un Sistema Informático

2.3.1. Hardware

Con respecto a un concepto técnico podemos decir que el Hardware son todos los elementos que constituyen la parte física de un sistema informático, es decir, los computadores. Además, incluye los componentes mecánicos, eléctricos y electrónicos. En otras palabras, el hardware es la parte que se puede visualizar en un sistema informático, se conoce también como la parte tangible o materializada del sistema operativo.

Tipos de computadores

Un ordenador o computador está conformado por un conjunto de programas y elementos de carácter electrónico que se encargan del procesamiento de la información, es la parte física del sistema informático que también costa de una parte intangible denominada software, el conjunto de dichos componentes dan como resultado el sistema informático. Existen varios tipos de ordenadores, sin embargo, se consideran como importantes a los siguientes:

Superordenador: son considerados como computadores de alto rendimiento, generalmente se usan para actividades específicas y tiene la función de potencias el procesamiento de datos.

Computadoras de Escritorio: estas computadoras cuanta con elementos o periféricos que están adheridos al equipo como el mouse, teclado, monitor, etc., una de sus grandes características es que tiene gran capacidad de almacenamiento. Los computadores de escritorio son parecidos a los computadores portátiles con la diferencia de que todo el sistema de información está compactado y conforma una sola pieza electrónica.

PDA: es un ordenador de bolsillo que se utiliza como herramienta

personal en la que se puede agendar lista de contactos, las Instituciones lo usan como operador de logística ya que en él se pueden almacenar pedidos, devoluciones y realizar envíos.

Workstation portátiles: es un ordenador de alto rendimiento construido para ejecutar aplicaciones intensivas que impulsan objetivos personales o empresariales clave dentro de la Institución, se utilizan para aplicaciones de alta gama como diseño gráfico, edición de vídeo, diseño 3D, diseño CAD u otros programas que exigen mucha CPU y RAM

Mainframe: son macrocomputadoras capaces de tener un control de diferentes usuarios de manera simultánea, se utiliza en grandes organizaciones que requieren el procesamiento de datos masivos como por ejemplo censo y estadísticas a gran escala, otra funcionalidad que se asigna es que permite la planificación de recursos Institucionales y procesar transacciones con grandes datos informáticos.

Tipos de periféricos de entrada

Los periféricos de entrada son aquellos que permiten ingresar la información a los computadores. Los periféricos logran la comunicación con los computadores mediante la tarjeta de memoria.

Mouse: conocido en español como ratón cumple la función de controlar el puntero que aparece en la pantalla del ordenador, este dispositivo permite la movilización del puntero a fin manipular la información presente en la pantalla.

Teclado: cumple la función de ingresar datos en forma de caracteres utilizando un le guaje binario.

Cámara web: es un dispositivo que permite grabar y capturar imágenes para luego emitirlas de manera directa haciendo uso del internet.

Escáner: tiene la funcionalidad de capturar la imagen de un documento para digitalizarlo e introducir la imagen como un archivo dentro del ordenador. Está compuesta por lámparas que permiten reconocer la longitud del documento que se dese escanear. Existen diferentes tipos de escáner dependiendo de las necesidades de cada entidad de sutilizan como periféricos de entrada.

Micrófono: este dispositivo permite la entrada de audio que se conecta a la computadora para grabar los sonidos o comunicar a personas a través del internet.

Tipos de periféricos de salida

Monitor: este dispositivo es considerado como un interfaz que cumple la funcionalidad de mostrar las imágenes, datos y todo tipo de información proceda al usuario.

Parlantes: son dispositivos que permiten escuchar sonidos pueden ser sonidos de videos o música.

Impresora: cumple la funcionalidad de imprimir imágenes, documentos, etc., en papel con el fin de proporcionar información física al usurario. Dependiendo de las necesidades de las Instituciones las impresoras pueden ser Led, de inyección a tinta, matriciales, laser, multifunción, etc.

Plotter: son impresoras profesionales que se utilizan en el campo de la ingeniería, diseño, arquitectura, etc. Con el fin de representar físicamente gráficos vectoriales en papel, se diferencia de la impresora debido a que los plotters son más lentos al imprimir, esto como consecuencia de los movimientos con mayor precisión que las impresoras comunes.

Proyector de video: tiene la funcionalidad de mostrar imágenes o videos a través de un sistema de lentes electrónicos, para ello debe recibir una señal eléctrica que dará paso a la proyección de la información que se requiera en ese momento.

2.3.2. Software

Se considera como el componente intangible debido a que no se puede tocar físicamente, se conoce también como un componente lógico. En otras palabras, el software está representado por los programas de aplicación y sistemas operativos que permiten al ordenador realizar diversas funciones haciendo uso de programas, hojas de cálculo, sistemas contables, aplicaciones, etc.

Tipos de sistemas operativos

Los sistemas operativos representan el conjunto de computadores y programas que cumplen con la función de controlar los procesos que realizan los computadores para emitir nueva información procesada.

Los sistemas operativos más utilizados son Windows, Linux y Mac Os, Android, Web Os en televisores inteligentes Smartv.

Sistema operativo multitarea: tiene la función de procesar información de distintas tareas de forma simultánea. Esto con el objetivo de mejorar el rendimiento de los computadores y hacer más fácil las labores al usuario.

Sistema operativo mono tarea: son los sistemas más antiguos que permiten procesar información únicamente en ese momento es decir que solo puede centrarse en una sola tarea por lo que no logra optimizar el tiempo.

Sistema operativo multiusuario: son sistemas que tratan de satisfacer las necesidades de dos o más usuarios de forma simultánea, por motivos de la secuencialidad de procesos los procesadores son mejor utilizados.

Sistemas operativos por lotes: procesan información con características similares de forma simultánea además no requieren de la interacción de usuarios o programas que contribuyen a la ejecución del procesamiento de información.

Sistema operativo de tiempo real: este sistema centra sus esfuerzos en el procesamiento de información, generalmente este tipo de sistemas se utilizan en el procesamiento de datos con grandes sucesos o eventos.

Tipos de bases de datos

Las bases de datos son aquella que está en la capacidad de almacenar una gran cantidad de información, todos los dispositivos electrónicos utilizan bases de datos ya que sin este elemento no se lograría guardar información en los dispositivos y tampoco se tendría acceso a la información.

Existen también muchos conceptos de base de datos que dicen: una base

de datos es considerado como un almacén que tiene como finalidad guardar grandes cantidades de información de manera ordenada, cronológica y sistemática para cuando el usuario requiera de la información la pueda encontrar fácilmente.

Los tipos de bases de datos se clasifican de distintas maneras; las bases de datos más utilizadas sin SQL Server, Oracle, PostgreSQL y Microsoft Access.

Base de datos estáticas: se caracterizan por almacenar datos históricos con el fin de poder analizar esos datos posteriormente y realizar proyecciones para tomar decisiones.

Base de datos dinámicas: va cambiando con el pasar del tiempo, es decir que constantemente se encuentra actualizando su información, por ejemplo, un almacén de ropa que por cada temporada debe actualizar su base de datos.

Base de texto completo: son aquellas bases de datos que proporcionan de manera online textos completos como libros, revistas, etc., son bases de datos de fuentes primarias.

Base de datos de red: son similares a las bases de datos jerárquicas, que se encuentran compuestas por una serie de registros en lanzados entre si formando una red. Este tipo de base de datos son utilizados por las Instituciones para establecer una conexión entre un tipo de registro con otro tipo de registro.

2.4. Seguridad Física

La seguridad física en los sistemas informáticos está sujetos a diferentes amenazas externas que intentan perjudicar el correcto funcionamiento de estos sistemas, estas amenazas están dadas por dos factores ajenos a los sistemas informáticos, uno de ellos son los accidentes intencionales producto de desastres naturales como tormentas de lluvia, terremotos, inundaciones, temperaturas altas y bajas que tiene como consecuencias fenómenos catastróficos. El otro factor es el ser humano que puede crear disturbios, sabotajes, falsificaciones, etc.

Al hablar de la seguridad física, se debe tener en cuenta el levantamiento de datos que conlleven a tomar decisiones acerca del hardware, centros

informáticos, interconexión del cableado electrónico, métodos de base de datos, verificación de todas las operaciones que se realizan diariamente en los sistemas informáticos, etc.

Toda Institución debe tomar medidas específicas de seguridad donde deben incluirse políticas, normas o reglamentos que permitan desarrollar las bases con que se requiere asegurar o proteger las instalaciones tomando en cuenta los siguientes factores: grado de clasificación de la información, tipo de información, cantidad de información, amenazas y vulnerabilidades, medios de almacenamiento de información.

Por lo tanto, la seguridad física es establecer parámetros de protección hacia los sistemas que sean vulnerables a amenazas físicas. Es decir que, la seguridad física permite crear barreras y procedimientos de control como medida se prevención ante ciertas amenazas, pueden ser amenazas causadas por el hombre o la naturaleza, como por ejemplo un sabotaje o un incendio natural.

Algunas recomendaciones para mantener la seguridad física son:

- Las computadoras deben estar constantemente actualizadas y seguras.
- Personal técnico con capacidad para manejar los sistemas informáticos
- Tomar muy en cuenta las vulnerabilidades de los sistemas Informáticos
- Control de acceso adecuado
- Restricción de acceso a personal No autorizado
- Gestión de riesgo ante la vulnerabilidad de los equipos informáticos

2.5. Seguridad Lógica

Generalmente en este tipo de seguridades lógicas debe combatir amenazas relacionadas con el software del sistema informático, es decir con la parte intangible que son los programas, aplicaciones, etc. En todo tipo de Institución la seguridad lógica es vulnerable debido a la cantidad de información que manejan, por tal motivo se debe tener en cuenta tanto los ataques o virus informáticos, así como los fallos en los procesos que pueden llevar al fracaso a las entidades. Esto hace referencia a que las aplicaciones, programas o sistemas contables que utiliza la Institución pueden tener fallas ocultas de fabricación que pueden ocasionar problemas graves en el procesamiento de datos de la Institución.

En este sentido la importancia de la seguridad lógica está orientada a proteger el uso del software dentro de una Institución, este tipo de resguardo tiene la función de asegurar que las aplicaciones obtengan una medida de seguridad con el objetivo de resguardar el sistema informático de accesos no autorizados desde la red, programas o actualizaciones no autorizadas ni realizadas por los trabajadores encargados de la seguridad del software.

En ese sentido la seguridad lógica trata de crear mecanismos de seguridad y protección para el uso del software que utiliza una Institución. De esa manera el uso de los procesos, aplicaciones y programas generaran confianza al momento de procesar la información y obtener información confidencial.

Algunas recomendaciones para mantener la seguridad lógica son:

- Delimitar el acceso a los programas y archivos, es decir está información debe ser confidencial.
- Los Empleados deben tener en cuenta los reglamentos en cuanto a programación y uso de aplicaciones que no se encuentran como uso en alguna normativa interna.
- Asegurarse de que la información enviada le corresponde al destinatario correcto y no a otra persona.
- Asesorarse de que la información que el destinario está recibiendo es la misma que fue solicitada por él.

2.5.1. Niveles de Seguridad Informática

Dentro de los niveles de seguridad existen algunos niveles que van a permitir la protección de la información la misma que se ha vuelto un factor muy importante dentro del desarrollo de las Instituciones que tiene el objetivo de proteger la infraestructura de los sistemas de cómputo y a su vez gestionar la información de manera adecuada para mitigar las amenazas que vuelven vulnerable a los sistemas de información. Los niveles de seguridad son los parámetros asignados para determinar cuál es el grado de confianza que tiene el software.

Para la seguridad informática se establecen varios niveles de seguridad estos deben ser vigilados para evitar pérdidas de datos y prestigio, por lo tanto, debe ser tratado como uno de los temas más importantes, debido a que la

información Institucional está sujeta a muchos ataques informáticos, por eso es necesario asegurar el contenido de la red Institucional, así como también las comunicaciones; los niveles de seguridad deben certificar que los recursos del sistema de información de una organización sean utilizados de manera adecuada y correcta para que el acceso a la información así como su modificación solo esté disponible para el personal autorizado y que se encuentre acreditado y dentro de los límites de su autorización.

Existen 4 niveles de seguridad informática

NIVEL D: este sistema está diseñado para sistemas poco confiables, es decir, sistemas que no cumplen con ninguna norma específica de seguridad. Además, no cuentan con protección para el hardware, generalmente los sistemas operativos son inestables. Es decir, este nivel está dirigido para los sistemas informáticos con una mínima protección.

NIVEL C: este nivel está destinado para que cada usuario tenga acceso únicamente a ese tipo de información. Dentro de este nivel están dos subniveles:

- **SUBNIVEL C1:** se trata de la protección de seguridad discrecional, en la que las bases de datos de cada usuario tienen acceso a la información asignada por lo tanto tiene la responsabilidad de seguir todos los procedimientos para asegurar dicha información.

- **SUBNIVEL C2:** se trata de la protección de acceso controlado, en donde el administrador debe implementar procedimientos que cumplan la función de crear accesos seguros con el fin de monitorear todas las actividades que realiza el usuario.

NIVEL B: en este tipo de sistemas se utilizan normas o reglas necesarias para el control de acceso, por tal motivo la información que se encuentra almacenada en los computadores son archivos de carácter secreto y privado. Existen tres subniveles:

- **SUBNIVEL B1:** se denomina seguridad etiquetada, debido a que asigna una etiqueta reconociendo cuál es el nivel de seguridad jerárquico que pueden ser considerados como altos, secretos, reservados, confidenciales, etc. De esa manera la personas que desee adquirir la información deberá obtener el permiso respectivo.

- **SUBNIVEL B2:** se denomina seguridad estructurada, en donde todos los usuarios deben tener permiso para acceder a los datos. Este nivel permite conocer la información de manera estructurada en donde su primer componente empieza a referirse del problema desde un nivel elevado de seguridad para comunicar a otro nivel más inferior.

- **SUBNIVEL B3:** se refiere a los dominios de seguridad en donde el hardware, se usa para proteger el dominio de seguridad de acceso a las personas que no ha sido autorizadas para acceder a la información contenida en ese sistema. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido

NIVEL A: es considera como el nivel de seguridad más elevado debido a que, conocida como nivel de protección verificada.

Para tener confianza en el procesamiento de información hay que tener en cuenta la fiabilidad, confidencialidad, integridad y disponibilidad, por tal motivo. Generalmente tiene que existir los 3 aspectos descritos para que haya seguridad. Dependiendo del entorno en el que trabaje un sistema, a sus responsables les interesara dar prioridad a un cierto aspecto de la seguridad.

CAPÍTULO 3

3. Afectaciones a los Sistemas Informáticos

3.1. Tipos de Virus

En los últimos tiempos y con el avance de la tecnología, internet, redes sociales, etc., han aparecido virus más sofisticados y complejos de detectar, esto hace que las redes y los sistemas informáticos se vuelvan vulnerables. En ese sentido se debe asegurar los sistemas informáticos para evitar que un programa externo entre al software y lo destruya.

Buscando diferentes conceptos que se da a los virus informáticos podemos indicar que un virus informático es un programa o código malicioso y autor replicante que se introduce en cualquier dispositivo tecnológico sin su conocimiento ni permiso provocando daños, problemas o molestias al sistema informático y, por ende, al usuario.

También hablando del virus informático podemos indicar que es un programa con una codificación diseñada con el objetivo de causar daños a un equipo informático, generalmente los virus se propagan sin el consentimiento del usuario corrompiendo archivos del sistema, malgastando recursos, destruyendo datos o alterando el funcionamiento de los sistemas informáticos.

Entre los virus más conocidos tenemos:

Virus residentes en la memoria: este virus se aloja en la memoria del ordenador y funciona cuando el sistema operativo ejecuta alguna acción de esa manera infecta a todos los archivos impidiendo que los mismo se abran y se pierda toda la información.

Virus de acción directa: funciona cuando se cumple una acción específica y afecta directamente al directorio, se ubica en la raíz del disco duro para activarse cuando este arranca. A medida que el tiempo avanza este virus se dirige a otras partes del sistema operativo con el objetivo de infectar otros archivos.

Virus Sobreescritura: tiene la funcionalidad de borrar toda información de los archivos y reemplazar la información sin cambiar el tamaño del archivo original. Es muy fácil de detectar puesto que el programa que está siendo infectado se vuelve inútil enseguida.

Virus polimórfico: este tipo de virus tienen un codificado especial debido a que utilizan diferentes algoritmos y claves de cifrado cada vez que infectan el sistema, por esa razón, no son de fácil detección por los programas de antivirus.

Virus de la macro: se consideran los más peligrosos debido a que tiene la función de sustituir a una macro y reemplazando las funciones de esta, dependiendo de la magnitud de daños que pueda causar este virus, incluso algunos pueden cambiar la configuración de Windows, borrar archivos del disco duro, enviar correos malignos sin que el usuario se dé cuenta.

Virus en el sector de arranque: Este tipo de virus se encarga de afecta al sector de arranque del disco duro. Esta es una parte crucial del disco porque es donde se encuentra la información que hace posible arrancar el ordenador desde disco.

Virus de secuencias de comandos Web: Muchas páginas web incluyen código complejo para crear contenido interesante e interactivo. Este código es a menudo explotado por estos tipos de virus informáticos para producir ciertas acciones indeseables.

3.2. Tipos de ataques informáticos

En estos tiempos es común escuchar sobre los ataques informáticos que son una irrupción a los sistemas que son provocados por maniobras planeadas, se la puede considerar como un intento de violación a la seguridad del sistema que constantemente es vulnerable por los diferentes virus que cada día con desarrollados con mayor grado de complejidad.

Un ataque informático desde el punto de vista de la informática se define como el aprovechamiento de alguna vulnerabilidad o debilidad que presenta el software o en el hardware, este ataque principalmente tiene el objetivo de obtener algún beneficio económico. Normalmente los ciberataques tienden a ser realizados por individuos solitarios.

Los ataques informáticos están en constante desarrollo, sin embargo, a través de planes de contingencia se permite controlar los riesgos a fin de proteger los sistemas operativos. Del tema de los ataques informáticos se desprende el término de seguridad informática que dice "La **seguridad informática** es una disciplina o rama de la Tecnología de la información, encargada del estudio de las amenazas y vulnerabilidades de los sistemas informáticos especialmente en la red como, por ejemplo, virus, gusanos, caballos de troya, ciber-ataques, ataques de invasión, robo de identidad, robo de datos.

Entre los ataques más comunes a los sistemas informáticos tenemos:

Troyano: es un tipo de programa pequeño maligno que cumple la funcionalidad de simular ser un software legitimo para después activarse y convertirse en un programa que permite el acceso a la información a terceras personas con el fin de robar información confidencial y tener acceso al sistema informático. Su objetivo principal pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo "huésped", así queda activo en el sistema y abre un puerto de entrada a esa computadora

Spyware: este programa tiene la funcionalidad de recopilar toda la información de un ordenador y pasar toda la información de un dispositivo a otro para que el segundo dispositivo tenga acceso a la información. De esa manera, es que este virus guarda las contraseñas, datos de tarjetas de crédito y otro tipo de datos personales para enviarlos a terceras personas.

Gusanos: el objetivo de este tipo de virus es colapsar a los computadores y las redes informáticas lo que impide el correcto funcionamiento de los programas en el sistema operativo, este virus se aloja dentro del sistema sin ser detectado hasta cierto tiempo para luego paralizar el ordenador e impedir el trabajo del usuario.

Ransomware: este tipo de virus impide a los usuarios hacer uso de su información persona y pide a cambio una cierta cantidad de dinero para que el usuario pueda recuperar la información.

Adware: este virus tiene la funcionalidad de tomar el control del navegador mediante la exhibición de anuncios publicitarios de ese modo

el creador de este virus generar ganancias a partir de esas publicaciones.

Phishing: tipo de ataque informático es utilizado para obtener información a través del uso de correos electrónicos utilizando ingeniería social, generalmente este virus ataca a las Instituciones ya que mediante él envió de los correos electrónicos se puede obtener información de las víctimas. Por ejemplo, este ataque funciona cuando el sistema infectado envía correos electrónicos con información del nombre de un banco, adjunto a este correo va una nota en la que se advierte el retiro de dinero de la entidad bancaria.

Anonimato: Es la capacidad de acceder a una red y realizar cualquier actividad de modificación o publicación de información indeseada, no se puede identificar el punto de acceso o el autor causante del ataque.

3.3. Vulnerabilidades a los Sistemas Informáticos

Dentro de la seguridad ya se hablado de ataques, virus, pero no sé a topado el tema de Vulnerabilidades a los sistemas informáticos muy frecuentes en estos tiempos debido a la gran demanda de aplicaciones empresariales en la nube o en aplicaciones móviles.

Es de suma importancia analizar la seguridad de bases de datos almacenadas de las empresas o Instituciones, encontrándose las mismas sujetas a una amplia gama de ataques contra seguridad de su base de datos.

De esta manera a continuación se presentan un concepto relacionado a las vulnerabilidades que pueden sufrir los sistemas informáticos: Una vulnerabilidad es una debilidad o fallo que presenta un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas.

Entre las principales vulnerabilidades encontradas están las siguientes:

Los privilegios excesivos: esta vulnerabilidad se presenta cuando a los usuarios o aplicaciones se conceden privilegios de base de datos, que exceden los requerimientos de su función de trabajo, estos privilegios se pueden utilizar para obtener acceso a información confidencial.

Para solucionar esta vulnerabilidad la solución es el control de acceso a nivel de consulta. El control de acceso a nivel de consulta permite restringir los privilegios de las operaciones a solo utilizar los datos mínimos requeridos. A su vez, la mayoría de las plataformas de seguridad de bases de datos nativas, ofrecen algunas de estas capacidades como: Triggers, RLS, entre otros, aunque el diseño de estas herramientas manuales las hace impracticables en todo, excepto en las implementaciones más limitadas según experiencia de expertos de seguridad web.

El abuso de privilegios: esta vulnerabilidad aparece cuando los usuarios pueden abusar de los privilegios de acceso de datos legítimos para fines no autorizados o malintencionados, según los expertos de auditoría de base de datos y seguridad web.

La solución a este tipo de vulnerabilidad está en generar una política de control de acceso que se aplique, no sólo a lo que los datos son accesibles, pero ¿Cómo se accede a los datos? Al hacer cumplir las políticas de seguridad web, sobre cosas como la ubicación, el tiempo, el cliente de aplicación y el volumen de los datos recuperados, es posible identificar a los usuarios que están abusando de los privilegios de acceso.

Inyección de SQL: los Ataques de inyección SQL, implican a un usuario que se aprovecha de vulnerabilidades en aplicaciones web y procedimientos almacenados, para proceder a enviar consultas de bases de datos no autorizadas, a menudo con privilegios elevados.

Para solucionar esta vulnerabilidad de deberá realizar una seguridad de bases de datos, auditoría de base de datos, control de acceso a nivel de consulta detecta consultas no autorizadas inyectadas a través de aplicaciones web y / o procedimientos almacenados.

Denegación del servicio DoS: esta otra vulnerabilidad la denegación de servicio (DoS) puede ser invocada a través de muchas técnicas, las técnicas más comunes de DOS incluyen desbordamientos de búfer, corrupción de datos, la inundación de la red y el consumo de recursos.

La prevención de ataques DoS debería ocurrir en múltiples capas, incluyendo las de red, aplicaciones y bases de datos según recomendaciones de cursos de seguridad de bases de datos y seguridad web.

Recomendaciones sobre las bases de datos incluyen el despliegue de un IPS, y controles de la velocidad de conexión. Al abrir rápidamente un gran número de conexiones, los controles de velocidad de conexión pueden impedir que los usuarios individuales usan los recursos del servidor de base de datos.

Vulnerabilidades en los protocolos de las bases de datos: Las vulnerabilidades en los protocolos de bases de datos pueden permitir el acceso no autorizado a datos, la corrupción o la disponibilidad.

La solución que se puede implementar es que los protocolos de ataques pueden ser derrotados mediante el análisis y validación de las comunicaciones de SQL, para asegurarse de que no están malformados. Pueden aprender más sobre este ataque durante cursos de seguridad de bases de datos y seguridad web de cybersecurity.

La exposición de los datos de Back-Up: Algunos ataques recientes de alto perfil, han involucrado el robo de cintas de Back-up de base de datos y discos duros.

Para esta Vulnerabilidad todas las copias de seguridad deben ser cifradas, de hecho, algunos proveedores han sugerido que los futuros productos DBMS no deberían admitir la creación de copias de seguridad sin cifrar. El cifrado de base de datos en línea es un pobre sustituto de controles granulares de privilegios, acuerdo a expertos de seguridad de base de datos.

CAPÍTULO 4

4. Delitos informáticos en la legislación ecuatoriana

4.1. Normas de Control Interno de la Contraloría General del Estado

De acuerdo con Normas de Control Interno de la Contraloría General de Estado, (2014), en la norma 410 se menciona acerca del componente de tecnología de la información que consta de 17 normas sujetas al control interno de la TI. Es necesario conocer las funciones que desempeña la unidad de tecnología, así como la importancia de este departamento dentro de las entidades públicas.

410-01 Organización informática: esta norma habla que la unidad de tecnología de información conforma un nivel alto dentro de la estructura organizacional de las entidades públicas, de esa manera puede efectuar las actividades de asesoría y brindar apoyo a la alta dirección y demás unidades en el campo tecnológico, además, esta unidad juega un papel importante en la toma de decisiones para generar cambios informáticos y tecnológicos dentro de empresa.

410-02 Segregación de funciones: esta norma indica que las funciones y responsabilidades del personal encargado de la tecnología de información deben ser claras, definidas y comunicadas a los responsables con el fin de permitir el correcto desempeño de los roles y responsabilidades asignados.

Además, se deberá considerar la descripción grafica documentada de los respectivos puestos de trabajo que conforman la unidad de tecnología de la información. Esta descripción es elaborada con el objetivo de que los procedimientos sean independientes a las demás unidades.

410-03 Plan informático estratégico de tecnología: esta norma indica que la unidad tecnológica tendrá que elaborar un plan estratégico con el objetivo de administrar y dirigir los recursos tecnológicos, este plan deberá tener un nivel suficiente para permitir entender los objetivos estratégicos de la entidad, además deberá contar con un plan de mejoras el cual debe incluir la estructura

interna, procesos, infraestructura, comunicaciones, servicios a ofrecer, etc. También se debe considerar las estrategias, los riesgos y el presupuesto.

410-04 Políticas y procedimientos: para esta norma la unidad de tecnología tiene la responsabilidad documentar, elaborar y difundir los temas relacionados con las políticas, estándares y procedimientos que permitan regular las actividades relacionadas con la tecnología. A través de procedimientos que permitan la supervisión de funciones, revisión de indicadores de gestión, (eficiencia, eficacia y economía) y nivel de cumplimiento de las regulaciones y estándares definidos.

Entre los temas relacionados con esta norma están los de calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas, legalidad de software, etc.

410-05 Modelo de información organizacional: esta norma indica que la unidad de tecnología deberá definir un modelo de información que permita facilitar la creación, uso y compartición del modelo, la creación de este modelo debe incluir las reglas de validación y controles de integridad y consistencia. Además, se deberá crear procesos para clasificar a los datos y aplicar el nivel de seguridad correspondiente.

410-06 Administración de proyectos tecnológicos: en lo que se refiere a los proyectos esta norma indica que se deberán estar regulados por mecanismos creados por la unidad de información de esta manera, se permite facilitar la administración de todos los proyectos existentes en todas las unidades.

Los aspectos que se deberán considerar para elaborar los mecanismos son:

- Descripción de: naturaleza, objetivos y alcance del proyecto.
- Cronograma de actividades
- Formulación de proyectos
- Asegurar la ejecución del proyecto
- Cubrir con la planeación, ejecución, control, monitoreo y cierre.
- Incorporar análisis de riesgos
- Establecer plan de control

- El cierre del proyecto debe incluir pruebas que certifiquen la calidad y el cumplimiento del proyecto.

410-07 Desarrollo y adquisición de software aplicativo: esta norma establece que entre las funciones que tiene la unidad de tecnología de información indica que se deberá regular los procesos de desarrollo y adquisición de software considerando los siguientes lineamientos:

- Las adquisiciones de software o soluciones tecnológicas se realizan considerando el portafolio de proyectos.
- Adopción, mantenimiento y aplicación de políticas publica
- Identificación de requerimientos funcionales y técnicos.
- Criterios de aceptación de los requerimientos.
- En el mantenimiento de software se debe considerar estándares de desarrollo, documentación y calidad.
- Mecanismo que aseguren el cumplimiento satisfactorio de los requerimientos para el proceso de compra y contratos específicos.
- Se debe considerar mecanismos que garanticen los derechos de autor.
- Elaboración de manuales técnicos para la instalación y configuración, este manual debe ser difundido, publicado y actualizado de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica: la norma indica que la unidad de tecnología implementara la infraestructura tecnológica considerando los siguientes aspectos:

- Las adquisiciones tecnológicas estarán alineadas con los objetivos de la organización.
- Planificará el incremento de capacidades, evaluará los riesgos tecnológicos y el costo de la infraestructura.
- Para adquirir el hardware, los contratos deberán detallar las características técnicas de los componentes del hardware.
- Los contratos de servicio con proveedores deberán especificar los acuerdos, nivel del servicio y otras puntualizaciones necesarias.

410-09 Mantenimiento y control de la infraestructura tecnológica: esta norma establece que la unidad de tecnología de información deberá informar y garantizar el mantenimiento y uso correcto de la infraestructura,

considerando los siguientes puntos:

- Definición de procedimientos para para el mantenimiento de software, debido a cambios en la base legal o normativa.
- Los cambios de software que se realicen deberán ser registrados, evaluados y autorizados.
- Se beberá controlar las variaciones del software.
- Actualización de los manuales técnicos por cada cambio o mantenimiento que se realice.
- Se establecerán desarrollo de pruebas, se implementarán medidas y mecanismos lógicos y físico para resguardar los recursos informáticos.
- Se elaborará un plan de mantenimiento preventivo.
- Se mantendrá un control de inventarios informáticos mediante la actualización de estos.

410-10 Seguridad de tecnología de información: esta norma de seguridad establece que la unidad de tecnología de información establecerá guías para salvaguardar los sistemas informáticos con el objetivo de evitar pérdidas y fugas de los medios físicos, para ello se establecerán las siguientes medidas:

- Ubicación y control de acceso físico a la unidad de tecnología
- En los casos de actualización y soporte se migrará la información a otros medios físico.
- La seguridad a nivel de software y hardware se realizarán con monitoreo de pruebas periódicas y acciones correctivas.
- Instalaciones físicas adecuadas que incluyan mecanismos para controlar la temperatura y humedad de las instalaciones.
- Definición de procedimientos para el personal de seguridad que ejerce turnos en la noche.

410-11 Plan de contingencias: en esta norma se indica que esta deberá contener un plan para identificar las acciones que se deben tomar en el caso de existir una emergencia, el plan deberá contener los siguientes aspectos:

- Definición, aprobación e implementación de un plan de contingencias.
- Para asegurar que el plan se mantenga actualizado, se deberá definir y

ejecutar los procedimientos de control.

- Plan de continuidad de operaciones.
- Plan de recuperación de desastres.
- Designar roles específicos a los trabajadores con el fin de ejecutar funciones en caso de emergencia.
- El plan de contingencia será un documento confidencial.
- El plan de contingencia solo será socializado con el personal responsable de la ejecución.

410-1 Administración de soporte de tecnología de información: en esta norma se establece que para una adecuada administración del soporte tecnológico y para garantizar la seguridad, de los recursos es necesario definir, aprobar y difundir procedimientos de operación. Los aspectos para considerar son:

- Revisiones periódicas de los niveles de servicio acordados entre los usuarios.
- Seguridad de los sistemas, identificando a los usuarios interno, externos y temporales que interactúan con el sistema.
- Estandarización de documentación de los usuarios
- Medidas de prevención, detección y correcciones que protejan a los sistemas de información.
- Definición y manejo de los niveles de servicios para los usuarios.
- Administración de los incidentes reportados, requerimientos de servicios y solicitudes de información.

410-13 Monitoreo y evaluación de los procesos y servicios: en esta norma se indica que, para evaluar las operaciones, la unidad de tecnología informática deberá establecer un marco de trabajo para monitorear la contribución y el impacto de tecnología de la información en la entidad, esto le permitirá mejorar el nivel de satisfacción de los clientes.

410-14 Sitio web, servicios de internet e intranet: otra de las funciones que cumple la unidad de tecnología e información es que deberá establecer los procedimientos y normas para la instalación, configuración y utilización de los sitios web, internet y correos electrónicos.

410-15 Capacitación informática: pare esta norma se indica que se deberá establecer planes de capacitación a fin de poder cubrir las necesidades de utilización de los servicios de información, este plan se orienta los puestos de trabajo y necesidades de conocimiento específicas.

410-16 Comité informático: con esta norma se conformará dependiendo de las características de la entidad, así como también de los objetivos que persigue, las políticas y la calidad de servicios informáticos que tenga a disposición la entidad.

410-17 Firmas electrónicas: finalmente con esta norma se indica que las entidades del sector público podrán utilizar las firmas electrónicas para cumplir con sus funciones regidas al cargo que desempeñan, Las firmas electrónicas deberán disponer de mecanismos y reportes que faciliten una auditora de mensajes de datos electrónicamente firmados.

4.2. Delitos Informáticos en el Código Orgánico Integral Penal

De acuerdo con el art. 190. – Apropiación Fraudulenta por medios electrónicos, está dirigido para las personas que utilizan de manera indebida un sistema informático o redes electrónicas y de telecomunicaciones, con el propósito de facilitar la apropiación de un bien ajeno.

En el art. 186.- **Estafa.** – este artículo menciona que una estafa mediante el uso de dispositivos electrónicos puede alterar, modificar o duplicar los dispositivos bancarios como el cajero automático, con el fin de almacenar copias de información de las tarjetas de crédito, débito, etc., con el objetivo obtener dinero ajeno.

En el art. 232.- **Ataque a la integridad de sistemas informáticos**. – se establece que la persona que destruya dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento a los datos informáticos o componentes lógicos será sancionado con tres a cinco años de prisión. De igual forma, a aquellas personas que diseñen, desarrollen, programen y ejecuten dispositivos o programas informáticos maliciosos o programas destinados a causar daños en los sistemas informáticos.

En el art. 311.- **Ocultamiento de información**. – este artículo hace referencia a las personas que en calidad de representantes legal de una entidad dedicada a la captación de dinero; oculte a sus socios o acreedores los fondos de dinero existentes en la entidad, serán sancionados de tres a cinco años con pena privativa de libertad.

En el art. 312.- **Falsedad de información.** – menciona que se privará de libertad de tres a cinco años a las personas que calidad de representante legal brinden información falsa sobre operaciones que han estado a su cargo.

CAPÍTULO 5

5. Antecedentes de la Auditoría Informática

La auditoría informática mantiene sus orígenes a medida que aparecieron las computadoras y sistemas de información aplicables dentro del capo Institucional, médico, financiero, y entre otros que sea de vital importancia el uso de equipos automatizados para el registro continuo y pronto de las actividades diarias, o simplemente para cumplir con la funcionalidad de almacenar hechos importantes que sirvan de sustento para las posibles revisiones legales a las cuales están sujetas cada una de estas Instituciones.

En este contexto prácticamente desde el comienzo del uso comercial de las computadoras, se comenzaron a crear esos sistemas, a proponer esos métodos. En cierto sentido fue el desarrollo natural de los métodos y sistemas de auditoría, que el ser humano ha venido perfeccionando desde el surgimiento de la humanidad, extendidos y adaptados a un entorno de control mucho más riesgoso y complejo". (Blanco, 2008, p.9)

5.1. Introducción a la Auditoría Informática

La auditoría informática en la actualidad es una parte objetiva de estudio y discrepancias debido a que en algunos casos se considera que los auditores de profesión deben estar capacitados en el sentido de poder realizar un examen a los diferentes Sistemas Informáticos y niveles de seguridad informática que se encuentra dentro de una Institución, sin embargo se ha mencionado en algunos caso que el personal encargo de realizar este examen debe ser un Ingeniero en Sistemas o una persona que tenga conocimientos amplios sobre la rama de la informática, este dilema se ha presentado desde hace varios años atrás y un ejemplo de ello es, la introducción de un experto en informática dentro del equipo de auditoría, se menciona que este especialista analizaba el funcionamiento de los Sistemas Informáticos y sus niveles de seguridad, al final emitía un informe al respecto de la situación de la Institución con respecto a su manejo y seguridad de la información a través del uso de dispositivos tecnológicos, este informe se convertía en una guía para el auditor el cual analizaba los resultados de sus evaluaciones a la información financiera y gestión de las funciones administrativas, emitiendo a si una recomendación y conclusión con respecto a todo la entidad.

Por otra parte, existen diferentes puntos de vista de autores (Blanco, 2008), que manifiesta que este aspecto "pero poco a poco esa situación ha ido cambiando":

"Las generaciones más actuales de auditores han dejado de ser "tradicionales". Conocen los elementos fundamentales de la informática, dominan paquetes especializados de auditoría y tienen la cultura básica necesaria sobre la seguridad y protección de los recursos informativos". (p.21)

Por otra parte, de acuerdo con (Chicano, 2015), la auditoría informática aparece con el desarrollo de los sistemas de información que se mantiene dentro de cada Institución, y su objetivo es, evaluar dichos sistemas para encontrar debilidades en su funcionamiento y que puedan generar costos innecesarios para la entidad.

En base a estos dos puntos de vista mencionados anteriormente se puede afirmar de acuerdo con (Hernandez, 1993), la auditoría informática ha sufrido una evolución bastante grande de acuerdo con el avance Tecnológico que muchas empresas e instituciones a nivel mundial han ido implementando, al inicio se había centrado en la revisión de las sistematización de las áreas administrativas, pero con el paso del tiempo todas las áreas fueron implementado nuevas tecnologías por lo cual la auditoría tuvo que irse perfeccionando y acoplando al avance tecnológico actual.

Podemos mencionar en forma general que el avance de la tecnología y la implementación de la misma en las actividades Institucionales en el mundo de hoy ha dado origen a la Auditoría Informática, debido a que ahora no se solicita evaluar solo la parte económica o administrativa de una entidad, por el contrario se hace una evaluación integral y por ende el tener un conocimiento de la infraestructura tecnológica que usa le entidad a ser examinada es de vital importancia, de acuerdo con (Alfonso, Blanco, & Loy, 2012):

"Con el auge de la revolución tecnológica dentro del mundo Institución nace nuevas tecnologías informáticas en la economía, desarrollándose sistemas informáticos para el procesamiento electrónico de la información, esto implica grandes transformaciones cualitativas en la contabilidad y el control sobre el concepto tradicional del Control Interno y la estructura de los registros contables, condicionando la existencia y el desarrollo de un nuevo concepto; Auditoría con Informática". (p.3)

5.2. Definición de Auditoría Informática

Para iniciar con la contextualización de lo referente a la Auditoría Informática, es necesario conocer los términos que conforman su definición, a continuación, se muestran algunas definiciones relacionadas:

La informática de acuerdo con (Academia Francesa, 1967 citado en Aguirre, 2005) es la "Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas de la información".

Por la forma en que se reúnen esfuerzos dentro de la Institución, se define como "tratamiento sistemático de la información a través de diferentes recursos tecnológicos" (Aguirre, 2005, p.6).

Existen varias definiciones que se encuentran vinculadas a lis términos de auditoría y de informática, estas han ido evolucionando o adaptándose a las situaciones actuales, como se muestra a continuación:

"Es un proceso formal ejecutado por especialistas del Área de Auditoría y de Informática, que se orienta a la verificación y aseguramiento de que las Políticas y procedimientos establecidos para el manejo y uso adecuado de la Tecnología de Informática en la Organización se lleven a cabo de una manera oportuna y eficiente" (Hernández, 1993, p.11).

Por otra parte (Aguirre, 2005), menciona que la auditoría informática es un examen que está orientado al manejo de los recursos informáticos, con la finalidad de elaborar un informe detallando la situación actual de estos.

"La Auditoría en Informática se refiere a la revisión práctica que se realiza sobre los Recursos Informáticos con que cuenta una entidad, con el fin de emitir un informe y/o dictamen profesional sobre la situación en que se desarrollan y se utilizan, esos recursos" (p.6).

También se define a la auditoría informática de la siguiente manera:

"La auditoría informática es una prueba que se desarrolla con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión

informática y si estas han brindado el soporte adecuado a los objetivos y metas de una organización" (Villareal, 2016, p.13).

Se puede observar que ambos autores coinciden, al mencionar que la auditoría informática está orientada a la evaluación de los recursos informáticos y de información de la entidad, además hacen énfasis en detectar si están siendo usados de manera acorde a lo establecido en las políticas internas y si estos cumplen con los criterios de eficiencia y eficacia.

5.3. Marco esquemático de la auditoría de sistemas computacionales

Hablando del Marco esquemático se puede mencionar que se refiere hacer una revisión especializada, desde un punto de vista profesional y autónomo, del aspecto contable, financiero y operacional de las áreas de una empresa. En la auditoría de sistemas computacionales en cambio se debe realiza una evaluación los equipos informáticos en lo referente al:

Hardware

La evaluación de Hardware su objetivo es comprobar que existan los contratos de seguro necesarios para el **hardware** y software de la empresa (elementos requeridos para el funcionamiento continuo de las aplicaciones básicas). ... Registro del **hardware** instalado, dado de baja, proceso de adquisición, etc. Plataforma de hardware es así que modelos mencionar los diferentes elementos como:

- ✓ El mainboard o Tarjeta madre
- ✓ El o los Procesadores
- ✓ Periféricos de entrada y salida
- ✓ La arquitectura del sistema
- ✓ Instalaciones eléctricas, de datos y de telecomunicaciones
- ✓ Innovaciones tecnológicas de hardware y periféricos

Software

La evaluación de un **software** o paquete preprogramado requiere tomar en cuenta algunos factores que son fundamentales en un proceso formal de

selección, entre ellos: la funcionalidad del **software**; es decir, la forma como soporta los procesos y actividades con el uso de las TI para ello se debe considerar la siguiente evaluación:

- ✓ Plataforma software que se está utilizando
- ✓ El Sistema operativo instalado
- ✓ El o los Lenguajes y programas utilizados para el desarrollo
- ✓ Los Programas, paqueterías de aplicación y bases de datos
- ✓ La Utilerías, bibliotecas y aplicaciones
- ✓ El Software de telecomunicación
- ✓ Los Juegos y otros tipos de software

Gestión informática

El objetivo de medir la gestión Informática contribuye una ayuda para entender si la empresa o el equipo están en la dirección cierta a sus objetivos estratégicos o en una meta específica para ellos se debe considerar los siguientes aspectos:

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

Información

Se trata entonces de información que ha sido sometida a un proceso de revisión y evaluación previa a su publicación. ... Si se trata de fuentes web, procedentes de páginas de Internet: en ese caso la información obtenida no ha pasado por ningún tipo de filtro, control o revisión en este sentido es conveniente realizar una revisión de:

- ✓ La Administración, seguridad y control de la información.
- ✓ La Salvaguarda, protección y custodia de la información.
- ✓ El Cumplimiento de las características de la información.

Diseño de sistemas

El diseño de sistemas es el proceso de definición de cómo se encuentra la arquitectura, módulos, interfaces y datos de un sistema con el objeto de poder satisfacer unos requisitos previamente especificados. El diseño de sistemas podría verse como la aplicación de teoría de sistemas al desarrollo de un nuevo producto para lo cual se debe tomar en cuenta los siguientes detalles.

- ✓ La Metodologías de desarrollo de sistemas.
- ✓ Los Estándares de programación y desarrollo.
- ✓ La Documentación de sistemas.

Bases de datos

En la evaluación de la base de datos se tienen en cuenta los aspectos relacionados con su contenido, el de los registros y la indización de los documentos. En cuanto al software de recuperación, se estudian sus capacidades y prestaciones, y en la interfaz de usuario su amigabilidad y consistencia. Con estos aspectos evaluados es importantes hablar de:

- ✓ La Administración de bases de datos.
- ✓ El Diseño de bases de datos.
- ✓ La Metodologías para el diseño y programación de bases de datos.
- ✓ La Seguridad, salvaguarda y protección de las bases de datos.

Seguridad

La evaluación de la seguridad informática de una empresa debe desarrollarse desde el área de gestión del riesgo, cuyos profesionales deben ser capaces de determinar, analizar, valorar y clasificar este nivel de amenaza para mantener la seguridad de los sistemas, con estos aspectos a considerar de se debe analizar:

- ✓ La Seguridad del área de sistemas.
- ✓ La Seguridad física.
- ✓ La Seguridad lógica.
- ✓ La Seguridad de las instalaciones eléctricas, de datos y de las telecomunicaciones.

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

Redes de cómputo

El rendimiento de red se refiere a las medidas de calidad de servicio de un producto de telecomunicaciones desde el punto de vista del cliente. El número de llamadas rechazadas es una medida de lo bien que la red está funcionando bajo cargas de tráfico pesado. Entre las diversas evaluaciones al desempeño de una red de cómputo esta:

- ✓ Las Plataformas y configuración de las redes.
- ✓ Los Protocolos de comunicaciones.
- ✓ Los Sistemas operativos y software.
- ✓ La Administración de las redes de cómputo.
- ✓ La Administración de la seguridad de las redes.
- ✓ La Administración de las bases de datos de las redes.

Especializadas

Cuando se identifica a la auditoría como una auditoría especializada, lo que se indica es que la misma es una forma de obtener evidencias para ser aportadas en una demanda judicial o sustentar hechos en una auditoria preventiva. Dentro de la evaluación de la auditoria Especializada se enmarcan las siguiente:

- ✓ De Outsourcing.
- ✓ De Helpdesk.
- ✓ La Ergonomía en sistemas computacionales.
- ✓ ISO-9000.
- ✓ Internet/intranet.
- ✓ Los Sistemas multimedia.

5.4. Enfoques de la Auditoría Informática

Al ser una rama de la auditoría que abarca varios objetivos en su desarrollo, se tiene algunos enfoques específicos como son:

Auditoría de sistemas preventivas

Las Auditorias preventivas según varios autores es importante porque va ayudar al dueño y alta gerencia a contar con información segura y confiable para la toma de decisión ayudando también permitiéndole prevenir algún tipo de fraude, pérdida monetaria y pérdida de confianza con el personal interno.

Este tipo de auditoría buscar prevenir eventos de alto riegos como: un ataque de DoS, Sqlinyection etc., a la base de datos de la Institución y de igual forma proponer correcciones en aquellos procesos en donde se maneje información manual.

Auditoría a los sistemas computarizados

Este tipo de auditoría centra su atención en la parte de la seguridad que ofrecen los sistemas de información dentro de la Institución, se puede observar que en ciertas ocasiones existen falencias en los controles que se desarrollan o suplente no existen, además se pretende verificar el grado de eficacia, eficiencia de los procesos de la entidad:

En los actuales momentos frente el incesante aumento de los ataques de ciberseguridad, phishing, Troyanos, Hacker, etc., las Instituciones deben determinar su nivel de seguridad actual y establecer el nivel que ha de conseguir para proteger los sistemas y la información corporativos. Por este motivo es necesario realizar auditorías Informáticas orientadas a las seguridades que permitan la evaluación y analizar la seguridad de los sistemas Informáticos. Dichas auditorias se realizarán normalmente por personal externo especializado, y ayudarán a mejorar la seguridad, eficacia y eficiencia de los procesos.

Auditoría al almacenamiento y procesamiento de datos

Un claro ejemplo de este enfoque radica en las auditorías informáticas al sector financiero especialmente realizadas con la finalidad de proteger la información personal de los clientes, además se busca comprobar que se estén ejecutando de forma correcta las actividades operacionales de la entidad, otro aspecto importante es el generar un informe de los hechos encontrados, los cuales estarán dirigidos a los usuarios internos como a los externos debido al giro del negocio, por último y no menos importante se encuentra el objetivo de encontrar procesos innecesario u obsoletos que se encuentren generando costos

extras para la Institución y que pueden ser eliminados lo más pronto posible a través de medidas correctivas.

También existen otros enfoques de acuerdo con los objetivos que se persiguen, según varios autores que hablan de estos temas:

Auditoría a los sistemas informáticos

Esta auditoría a los sistemas informáticos está orientada a la revisión de las funciones administrativas y operativas que son ejecutadas por la dirección y el personal del área de sistemas o de informática, se encargan de evalúa principalmente las actividades de administración, organización, dirección y control, así como también se revisa la seguridad que tiene el sistema operativo dentro de la entidad y si este es usado de una manera adecuada, también se verifica el estado de sus equipos en lo referente al Hardware y las instalaciones realizadas

Auditoría a los sistemas de redes

Esta auditoría de redes se especializa en orientar la evaluación de los diferentes tipos de redes informáticas que han sido instaladas dentro de la entidad, se analiza su estructura, topología, protocolos de seguridad y funcionamiento, además se revisa la parte no tangible del sistema operativo y se busca identificar si reflejan una seguridad en el almacenamiento y manejo de su base de datos.

Este tipo de auditorías de redes permitirá evaluar las siguientes especificaciones:

- Los objetivos para implementar una red informática de cómputo.
- Que características debe tener la red de cómputo.
- Los componentes físicos necesarios para una red informática de cómputo.
- La forma de conectividad y comunicaciones de una red informática de cómputo.
- Los servicios que va a ofrecer o proporcionar esta red informática de cómputo.
- Que sistemas operativos, lenguajes, programas, paqueterías, utilerías y bibliotecas se utilizaran en la red informática de cómputo".

- Las configuraciones, topologías, tipos y cobertura que va tener las redes informáticas de cómputo.

Auditoría integral a los centros de sistemas e informática

Esta auditoría Integral está orientada a realizar una evaluación de forma íntegra o total del área o departamento de sistemas de la Institución, se analizan las funciones ejecutadas por el personal, la infraestructura de sus equipos, la estructura y funcionamiento del sistema operativo así como también el grado de seguridad que ofrece el tener dicho sistema implantado, en este tipo de auditoría se conforma un equipo de trabajo especializado y multidisciplinario, debido a que es necesario tener conocimientos claros de todo lo que se pretende revisar y auditar.

Auditoría Outsourcing

Esta auditoría de Outsourcing está orientada a la evaluación de los servicios de informática y sistemas que ha contratado la entidad examinada a otra, se verifica la eficiencia y eficacia que se han presentado en todos los servicios contratado, así como el grado de cumplimento de la Institución prestadora del servicio, dentro de este contrato se encuentra lo relacionado con la arquitectura informática, su funcionamiento y seguridad.

Auditoría ergonómica de sistemas informáticos

Esta auditoría ergonómica está orientada a la evaluación de las posibles afectaciones físicas que pueden presentarse con el personal del área o departamento de informática, debido a la inadecuada infraestructura de los equipos e instalaciones que se encuentra en uso, además se analiza si las adquisiciones de bienes para el buen funcionamiento del departamento, tomando en cuenta todas las indicaciones realizadas para de esta manera logran cumplir los criterios de eficiencia y eficacia en los resultados esperados.

Continuando con los diferentes enfoques de la auditoría informática se menciona a algunas auditorias que también se pueden desarrollar en esta área como es:

Auditoría del desarrollo de software

Esta auditoría está orientada a la revisión durante el análisis, diseño y desarrollo del software que se pretende desarrollar para la Institución, verificando si se cumple con normas internacionales de desarrollo para una adecuada funcionalidad evitando costos innecesarios por un mal control, además se debe constatar que su uso no va a sufrir ataques de vulnerabilidades.

Dentro de las etapas del proceso de desarrollo e implementación del software se debe examinar los siguientes aspectos:

- **Examen de las metodologías utilizadas**: en esta etapa el auditor debe examinar si el software va a contar con futuras ampliaciones y si se van a poder realizar mantenimientos.

- **Revisión Interna de las Aplicaciones:** en esta etapa se evalúa el funcionamiento y estructura del software, todo lo relacionado a la parte técnica.

- **Satisfacción de usuarios:** en esta etapa se evalúa el grado de aprobación que tienen los usuarios antes el nuevo software, cabe recalcar que esto es de vital importancia para posteriormente no tener que realizar modificaciones de programación.

- **Control de Procesos y Ejecuciones Críticas**: en esta etapa se evalúa lis módulos que pertenecen a la programación requerida por la entidad, se debe constatar que únicamente debe estar programado lo requerido por el cliente.

Auditoría de riegos y amenazas

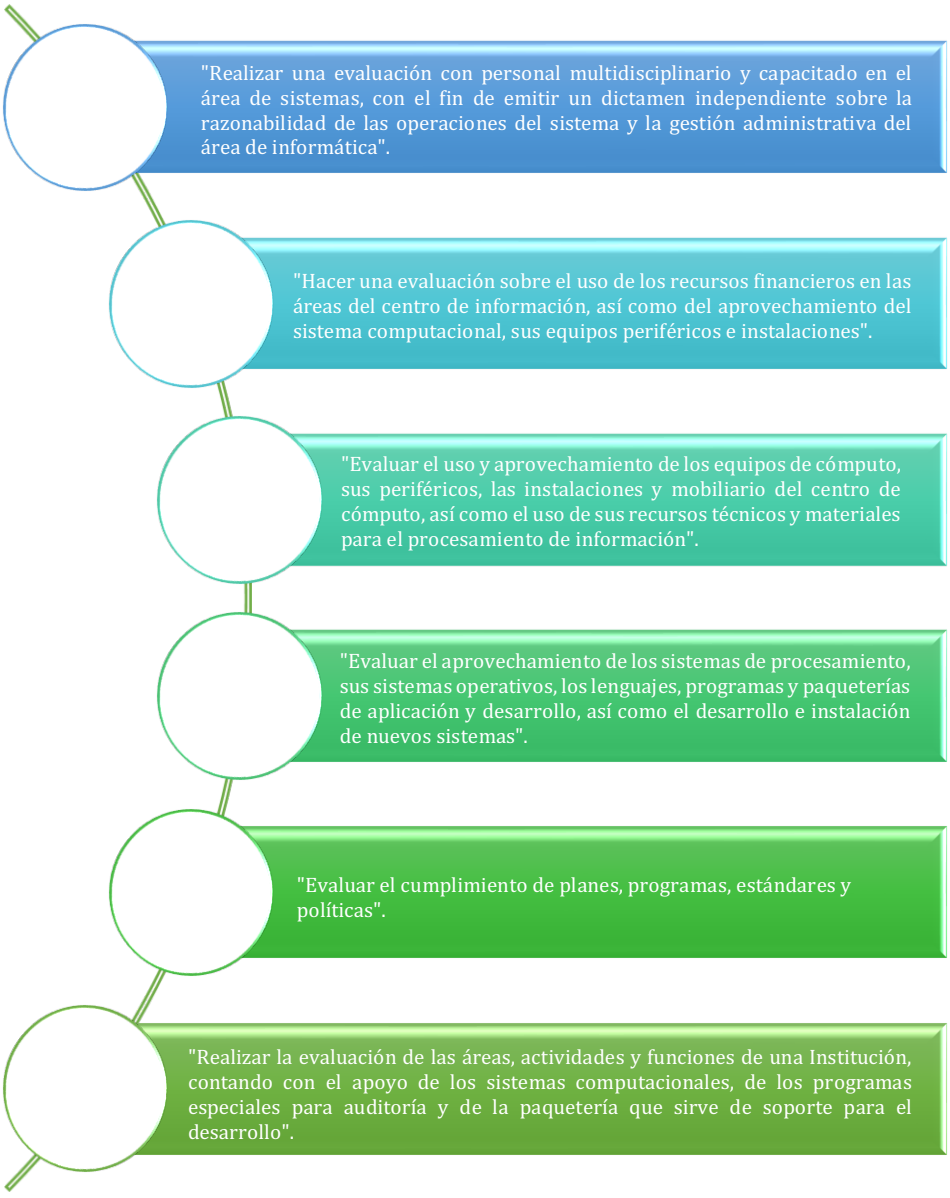
Esta auditoría enfocada a los riesgos y amenazas está orientada a la evaluación de los diferentes daños físicos o de información que puede sufrir la entidad, un ejemplo de esto, es el robo de equipo o daño de los mismos, se pretende verificar estas fallas en el entorno del área de sistemas y de la Institución, con el propósito de mitigar el riesgo.

5.5. *Objetivos de la Auditoría Informática*

Conocer los objetivos por los que se emplea la auditoría informática en las distintas organizaciones es importante, debido a que esto otorga claridad sobre el tema, permite comprender la razón por la que es necesario aplicar este tipo de auditoría en todas las Instituciones públicas sobre todo y en las Instituciones que utilizan frecuentemente la tecnología y sistemas computacionales en el desempeño de sus actividades diarias, más cuando estas se dedican al desarrollo de software o a su vez a la venta de aparatos tecnológicos o manejan gran cantidad de datos de otras instituciones. Por otro lado, es importante aclarar que estos objetivos pueden ser adaptables a cada uno de los tipos de auditoría informática existentes.

A continuación, se presenta la figura 6 la misma que muestra los objetivos que son considerados como principales dentro de lo referente a la auditoría informática:

Figura 6. *Objetivos generales de la Auditoría Informática*



Fuente: *MUÑOZ, C. (2002). Objetivos generales aplicados en la Auditoría de sistemas o informática.*

5.6. Características de la Auditoría Informática

El entorno que forma el área informática dentro de una Institución y a su vez pretende ser evaluada, está confirmado por lo siguiente elementos: Equipos, sistemas operativos y paquetes, aplicaciones y el proceso de su desarrollo, organización y funciones, las comunicaciones, la propia gestión de los recursos informáticos, la calidad de procesos y productos las políticas, estándares y procedimientos en vigor.

Además, se verifica el cumplimiento de reglamentos, políticas, estándares y demás normas de carácter interno, como: estándares y procedimientos, los objetivos fijados, los planes, los presupuestos, los contratos y las normas legales aplicables. Y para completar la evaluación al área informática se verifica lo relacionado con: el grado de satisfacción de usuarios y directivos, los controles existentes, un análisis de los posibles riesgos relacionados con la Informática.

5.7. Diferencia entre auditoría informática, financiera y de gestión

Al analizar cada una de estas auditorias se pueden establecer que existen algunas diferencias con los otros tipos de auditoría:

Tabla 1. *Diferencias de la Auditoría Informática con otras Auditorías.*

Tipo de Auditoría	**Objetivo**	**Descripción**
Financiera	Evaluar las cuentas anuales de los Estadas Financieros de una entidad a través de la aplicación de técnicas y herramientas de auditoría para determinar la razonabilidad de estas.	Elaborar un informe final y un dictamen de auditoría que muestre los hallazgos encontrados en el registro de la información de carácter contable y económico de la entidad.

De gestión	Evaluar los procesos administrativos y de gestión que se realizan en los diferentes departamentos de la Institución mediante la aplicación de herramientas y técnicas de control internos para determinar el nivel de eficiencia y eficacia de estos.	Elaborar un informe final donde se muestren las debilidades halladas en las funciones administrativas que se desarrollan dentro la Institución.
Informática	Evaluar el uso que ha realizado a los diferentes recursos informáticos que posee la entidad a través de la aplicación de herramientas y técnicas de auditoría para la obtención de información confiable que permita establecer medidas correctivas	Verificar el grado de eficiencia y eficacia de los procesos realizados dentro de la entidad de acuerdo con las normas establecidas.

Nota: *Objetivos y diferencias de la Auditoría Informática con otras auditorías.*
Fuente*: Elaboración propia con base en datos de Chicano (2015).*

5.8. Métodos, técnicas, herramientas y procedimientos de la auditoría Informática

El conjunto de métodos, técnicas, herramientas y procedimientos de auditoría informática constituyen una parte esencial en el desarrollo del examen, debido a que brindan el sustento necesario a los auditores para poder ejercer sus funciones y posteriormente obtener evidencia que sea necesaria para la elaboración del informe y recomendaciones respectivas.

5.8.1. Pruebas de cumplimiento y sustantivas

Las pruebas que se desarrollen en esta clase de auditoría están orientadas al desarrollo normal de la revisión planeada, para ellos vamos a describir algunas pruebas:

Pruebas sustantivas

Se pretende identificar si la información tiene un grado de seguridad alto y si su manejo es propicio para evitar cualquier clase de ataque o alteración, se encuentran errores relacionados a la protección de información.

Pruebas de cumplimientos

Al desarrollar estas pruebas se pretende conocer el nivel de cumplimiento de las políticas, reglamentos y demás normas de control interno establecidas para el desarrollo normal de las funciones de cada empleado.

5.8.2. Herramientas informáticas para la auditoría

Estas herramientas son usadas para la evaluación de programas y sistemas informáticos, es así que podemos definir las siguientes:

Una de las técnicas de auditoría que se utiliza es la asistida por computadoras (TAAC) constituyen una de las herramientas básicas del auditor. Estas se pueden dividir en TAAC estándar y TAAC avanzadas, el estándar consiste en la utilización de determinados softwares que actúan sobre los datos y las avanzadas consisten más bien en realizar procesos sobre los sistemas.

5.8.3. Entrevista

El auditor realiza la entrevista de una forma delicada y objetiva, con la finalidad de conocer la información necesaria para el desarrollo de su trabajo.

De acuerdo a varios Autores una entrevista es: una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

5.8.4. Muestreo

Al aplicar un tipo de muestreo en específico se está orientado a tener sustentos que formen parte de las observaciones en el informe final, así como una constatación del funcionamiento de las diversas funciones que se llevan a

cabo dentro de este departamento.

Otra finalidad que ofrece el realizar muestreos, es el tener una evidencia real sustentada en la elaboración de recomendaciones y conclusiones o en la parte de comunicación de resultados.

Existen dos clases de muestreo que son aplicadas en el desarrollo normal de una auditoría y estos son:

Muestreo estadístico
Se aplican técnicas de carácter matemático para definir ciertos aspectos a evaluar del tamaño considerado muestra, un ejemplo de esto es, el grado de riesgo que se admitirá.

Muestreo no estadístico
Esta clase de muestro es considerado subjetivo, debido a que no se hace la aplicación de ninguna técnica matemática y al contrario de esto se selecciona la muestra por la experiencia del auditor encargado.

5.9. Fases de la Auditoría Informática

5.9.1. Planificación

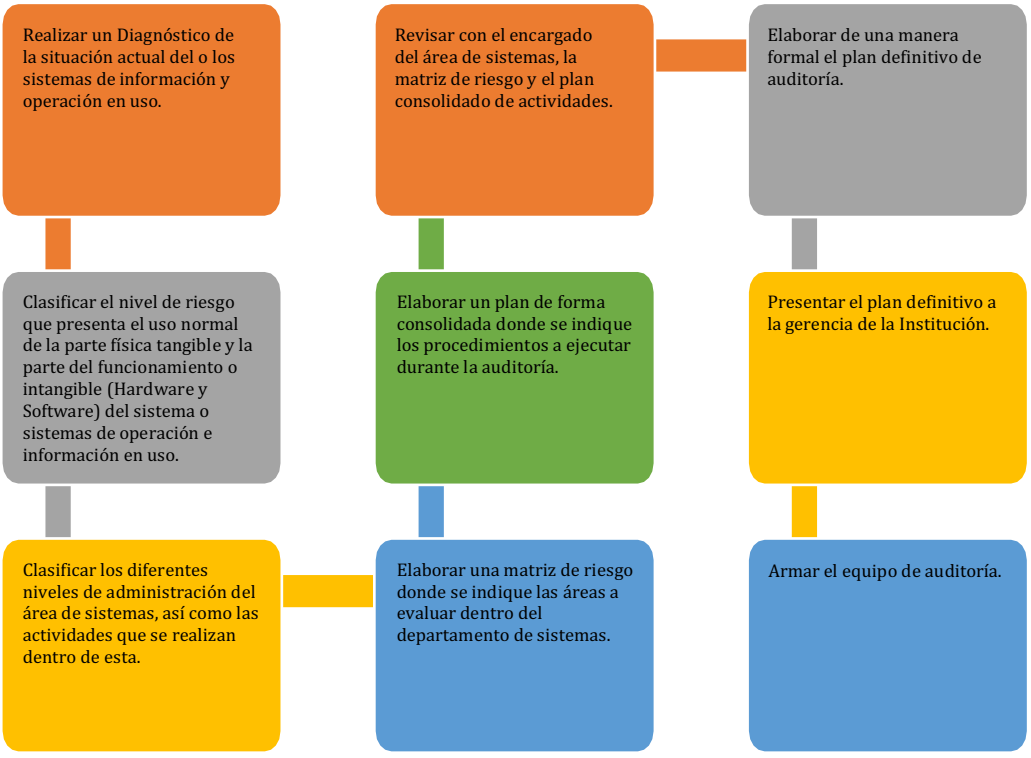
Es la primera etapa dentro de una auditoría, la cual se centra en la elaboración de procedimientos a cargo parte del auditor, estas actividades van a estar orientadas a evaluar el grado de cumplimientos y seguridad que se está realizando a los recursos informáticos dentro de la Institución.

Es así que a la planificación se la denomina como una de las actividades desarrolladas por el Auditor en Informática que tienen como objetivo principal elaborar y presentar un conjunto de Proyectos inherentes a la Función de Auditoría de Informática a la Alta Dirección, y que estarán orientados primordial mente al aseguramiento de la Calidad, Seguridad y Control de los diferentes elementos que se encuentran relacionados directa o indirectamente con los Recursos de Informática.

Esta fase permite al auditor tener un conocimiento de aquellas áreas importantes que se deben auditar y tener en consideración ante la presencia de problemas potenciales para de esa manera poder evaluar el riesgo y obtener

evidencia suficiente, competente y completa. De esa manera en la fase planificación de auditoria una de las actividades más importantes es la indagación de la información ya que partir de la investigación se puede obtener evidencias que validan la opinión del auditor. Es importante porque también permite determinar la extensión y el alcance de la auditoria para conocer los días de trabajo que se realizarán los papeles de trabajo, así como también las respectivas averiguaciones.

Figura 7. *Actividades a realizar en la planificación de la Auditoría Informática.*



Fuente: *Elaboración propia con base en datos de Hernández (1993).*

Proceso de planificación

De acuerdo lo expuesto por Hernández (1993) las siguientes actividades estarán incluidas dentro del plan de Auditoría Informática.

1. ***Realizar un Diagnóstico de la situación actual del o los sistemas de información y operación en uso.***

> ***Sistemas de operación:*** *"Aquí se manejan los datos de las áreas financieras, productivas y administrativas para la toma de decisiones" (Hernández, 1993, p.24).*

Dentro de este diagnóstico se debe considerar algunos factores importantes como son:

- Obtener una lista de los sistemas que usa la Institución y los usuarios que normalmente trabajan con ellos.
- Determinar el total de actividades que realiza cada uno de los usuarios mediante el sistema en uso.
- Detectar las fallas, sean estas mecánicas o físicas del sistemas o sistemas que mantenga en uso la Institución.
- Elaborar un informe de desempeño de todos los empleados que se encuentran a cargo del área de sistema o informática.

2. ***Clasificar el nivel de riesgo que presenta el uso normal de la parte física tangible y la parte del funcionamiento o intangible (Hardware y Software) del sistema o sistemas de operación e información en uso.***

De igual forma se debe realizar una evaluación del número de equipos físicos existentes, (discos, terminales), también lo referente a los tipos de redes, micros, minis, entre otros, para esto se puede hacer uso de la documentación donde se detalle la distribución de los mismos dentro de la Institución.

3. ***Clasificar los diferentes niveles de administración del área de sistemas, así como las actividades que se realizan dentro de esta.***

Se debe tener en consideración las asesorías realizadas por personal especializado y externo a la entidad, así como el tratamiento que se da al intercambio de datos.

4. ***Elaborar una matriz de riesgo que donde se indique las áreas a evaluar dentro del departamento de sistemas.***

En esta matriz se podrá clasificar de forma ordenada las áreas que representan un mayor nivel de riesgo y por consecuencia las primeras en

ser analizadas por el auditor.

5. ***Elaborar un plan de forma consolidada donde se indique los procedimientos a ejecutar durante la auditoría.***

   Aquí se deben especificar algunos elementos principales que al igual que en las otras auditorías se detallan dentro de la planificación preliminar:

   - Fecha de inicio y terminación del trabajo de auditoría.
   - Etapas de la auditoría.
   - Tareas que se van a desarrollar en cada etapa de la auditoría.
   - Detalles del equipo de trabajo que va a intervenir, especificando sus nombres y cargo.
   - Recursos necesarios para utilizar, tanto materiales como monetarios.

6. ***Revisar con el encargado del área de sistemas, la matriz de riesgo y el plan consolidado de actividades.***

   Al presentar esta planificación al encargado, se verifica que las tareas expuestas, se encuentren correctas y de ser necesario se realizan modificaciones.

7. ***Elaborar de una manera formal el plan definitivo de auditoría.***

   Se realiza la elaboración formal, teniendo en cuenta los siguientes aspectos:

   - Nombre del área a realizar la auditoría
   - Responsables del trabajo
   - Fechas de revisión
   - Fechas de iniciación y terminación del trabajo.

8. ***Presentar el plan definitivo a la gerencia de la Institución.***

   Se realiza esta revisión antes de poner en marcha las actividades propuestas y además para garantizar que todas las áreas que deban ser analizadas consten dentro del plan.

9. ***Realizar todos los procedimientos expuestos en el plan de*** **auditoría.**

Llevar a cabo cada uno de los procedimientos de forma acorde a los requerimientos y normas de carácter interno.

10. ***Armar el equipo de auditoría***

Debe estar integrado por personal acorde a la revisión que se va a realizar y también teniendo en cuenta los requerimientos del Jefe de Sistemas y del jefe del equipo auditor.

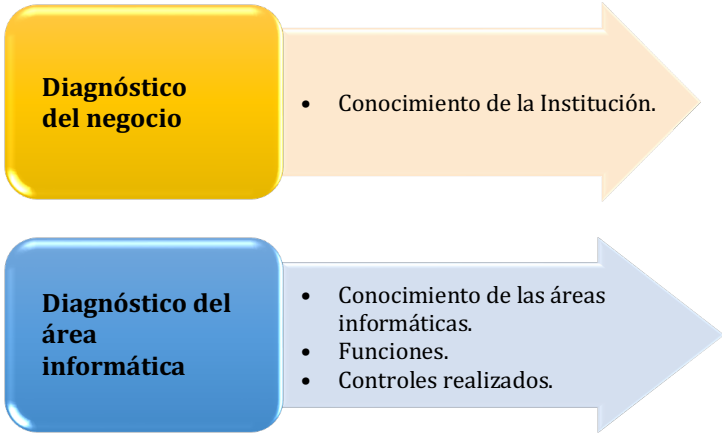
11. ***Obtener la confirmación por parte de la gerencia sobre el informe final de la planificación realizada***

Con esto finaliza la etapa referente a la planificación del trabajo.

Planificación preliminar

Es la primera etapa relacionada con la ejecución del trabajo de Auditoría y está compuesta por:

Figura 8. *Actividades que conforman la planificación preliminar.*



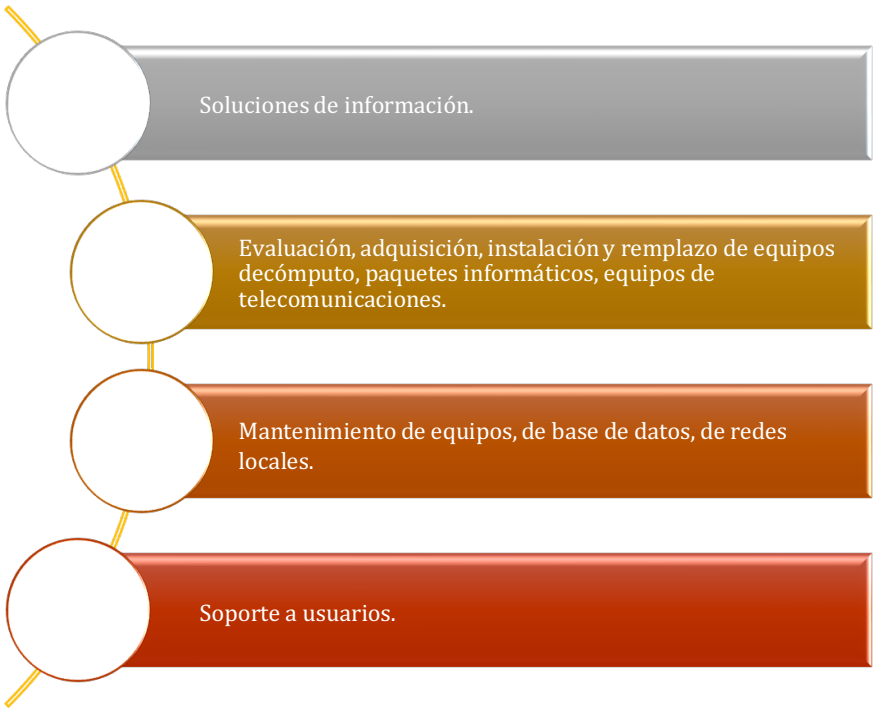
Fuente: *Elaboración propia con base en datos de Hernández (1993).*

El diagnóstico de la Institución: se obtiene un conocimiento de la Institución y de sus altos mandos, también se analiza la satisfacción de los diferentes procesos que se realizan, se analizan debilidades y fortalezas.

El diagnóstico del área de sistemas e informática: se pretende conocer todo lo relacionado con el área de sistemas.

Con respecto a las funciones que se realizan en el área de informática se tiene:

Figura 9. *Funciones que se realizan dentro del área de sistemas e informática.*



Fuente: *Elaboración propia con base en datos de Hernández (1993).*

Referente al conocimiento del auditor con respecto a los aspectos de control del área de informática se tienen los siguientes:

Figura 10. *Aspectos de Control del área de sistemas.*

Fuente: *Elaboración propia con base en datos de Hernández (1993).*

5.9.2. Ejecución

Es la segunda esta del trabajo de auditoría, aquí se ejecutan las actividades anteriormente planificadas y se busca detectar los posibles hechos que se encuentren amenazando el correcto funcionamiento de los sistemas, así como se identifica el mal uso que se pueden estar dando a los recursos informáticos.

Dentro de la ejecución existen algunos procedimientos que se realizan esta etapa y son los siguientes:

- Realizar las acciones planificadas para la auditoría.
- Aplicar los instrumentos y herramientas para la auditoría.
- Identificar y elaborar los documentos de debilidades encontradas.

- Elaborar el dictamen preliminar y presentarlo a discusión.
- Realizar una integración de todos los papeles de trabajo de la auditoría.

El objetivo principal de esta etapa es la obtención de evidencia que posteriormente servirán de sustento en la elaboración de conclusiones y recomendaciones respectivas. Para la obtención de evidencia se hace uso de las diferentes herramientas y técnicas de auditoría, como: las pruebas de auditoría, técnicas de muestreo, entre otros.

5.9.3. Comunicación de Resultados

Es la tercera etapa del trabajo de auditoría donde se detalla por escrito los diferentes hechos o irregularidades halladas en el examen de auditoría, antes de realizar el informe final que será entregado a la gerencia o mandos responsables de la Institución, se deben elaborar informes borradores, esto se da con el objetivo de poder realizar algunas medicaciones de ser el caso.

Un dictamen según varios autores indica que es el informe que se realiza una vez que se tiene el resultado de la información, investigación y el análisis efectuado por el auditor, en donde presenta de una manera formal su opinión sobre el área, proceso o actividad auditado, con respecto a los objetivos establecidos, señalando así, las debilidades encontradas, si existen, las recomendaciones que ayuden a eliminar las causas de estas falencias y promover las acciones correctivas necesarias.

Estructura del informe de Auditoría Informática

Existen varias propuestas sobre la estructura y parámetros que debe contener el informe final de auditoría:

- Escribir la fecha de redacción del informe.
- Ingresar los nombres de los integrantes del equipo de trabajo.
- Los nombres de todas las personas entrevistadas, especificando su cargo y puesto de trabajo.
- Redactar los objetivos y alcance de la auditoría.
- Enumeración de los temas que van a ser expuestos en el informe
- Exposición detallada de cada tema, se debe especificar la situación actual y pasada.

- De existir la forma de predecir tendencias, estas constaran en el informe.
- Detalle de las debilidades y amenazas encontradas.
- Redactar las recomendaciones y elaboración de planes de acción, esto se realiza con la finalidad de establecer correcciones de forma inmediata, así como medidas preventivas.
- Finalmente, redacción de la carta posterior de presentación.

5.10. Valoración del Riesgo

Para realizar la evaluación de los diferentes procesos que se desarrollan en la Institución y área de sistemas o informática, se hace uso de las herramientas de auditoría, una de ellas es la Matriz de Evaluación de Riesgos, es considera de gran utilidad debido a que se puede medir el cumplimiento de una función ejecutado por el personal, la operatividad del sistema que tiene la Institución en uso, el avance en el desarrollo de proyectos, entre otros factores.

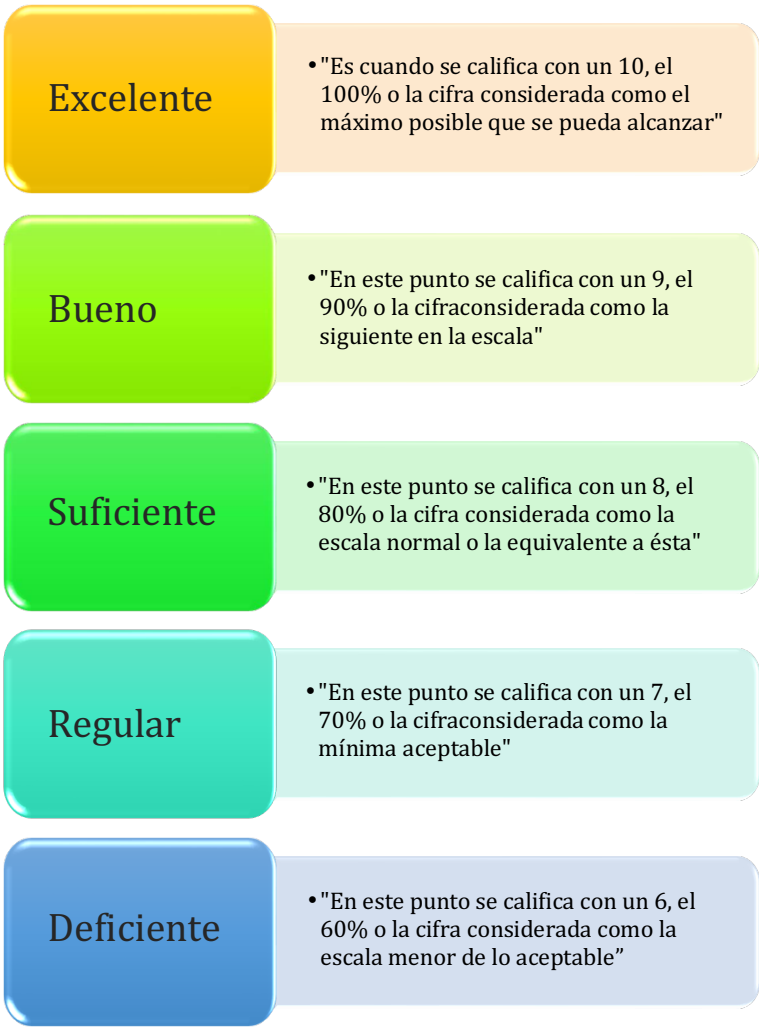
Una propuesta de uso para esta herramienta es la elaboración de una matriz de seis columnas, de las cuales la primera corresponde a la descripción del aspecto que será evaluado y las otras cinco a un criterio de calificación descendente (o ascendente), en las que se anotan los criterios de evaluación para acceder a esa calificación.

El objetivo de utilizar esta matriz, según varios autores es detectar las áreas de mayor riesgo e impacto que existen en relación con Informática y que requieren una revisión de manera formal y oportuna.

Parámetros de evaluación

Esta matriz determina una calificación porcentual en rangos de 10%, se recomienda que, para evaluar determinado factor, este sea detallado de forma clara para así evitar errores en la calificación.

Figura 11. *Parámetros de evaluación de la matriz de riesgo.*



Fuente: *Elaboración propia con base en datos de Villareal (2016).*

5.11. Componentes del Riesgo

Conociendo el concepto de un riesgo Informático, el riesgo se caracteriza por una combinación de dos factores. La probabilidad de que ocurra el incidente no deseado y su impacto.

5.12. Riesgos en la Auditoría Informática

En la actualidad hoy en día, las Instituciones desarrollan sus actividades partiendo de procesamiento datos que posteriormente son utilizados para la toma de decisiones, la información que las organizaciones manejan son de vital importancia para el funcionamiento de la misma, por tal motivo, en el caso de que se pierda información o existan personas que quieran dañar los sistemas informáticos, estas situaciones se transformarían en actos de mayor riesgo, por lo tanto, se deben tomar medidas necesarias que permitan proteger los recursos.

La administración de riesgo es un término aplicado a métodos tanto lógicos como sistemático que permitirán identificar, analizar, evaluar, dar seguimiento y comunicar los riesgos agrupados con las operaciones de una manera que permita a la organización minimizar las debilidades y optimizar las oportunidades.

En ese sentido es necesario tener en cuenta todas las debilidades consideradas como riesgos que pueden afectar en la Institución, es así como para mitigar los riesgos informáticos es necesario considerar un marco metodológico que permita identificar la mayor cantidad de riesgos.

Al momento de referirse al riesgo es necesario tener en cuenta los tipos de riesgo que se pueden presentar durante el desarrollo de auditoria:

Riesgo de control: sucede en el momento en que existe falta de control en las actividades que normalmente desarrolla la Institución, generando una falta de eficiencia en el sistema de control interno.

Riesgo de detección: le corresponde asumir a los auditores como consecuencia de no detectar las debilidades, problemas o errores que existan en el sistema de control interno.

Riesgo Inherente: es considerado como un riesgo especifico ya que es específico de una actividad que puede provenir del ambiente externo o interno. Por lo tanto, este riesgo es inherente o ajeno al sistema de control interno.

Riesgo informático: es un proceso que comprende la identificación de activos informáticos, sus distintas vulnerabilidades y amenazas a los que se encuentran expuestos dichos activos esto con el fin de determinar los controles más adecuados para mitigar, disminuir, transcurrir o evitar la ocurrencia del riesgo este es a lo mejor quizás el que tiene mayor alcance y complejidad de todos los que integran el riesgo operativo, esto se debe a dos causas principales: las tecnologías de información se extienden por todos los procesos y niveles de decisión de la Institución, y que las tecnologías de información siguen siendo un tema muy complejo y técnico, las cuales deben ser manejadas por especialistas, quienes son presionados por las empresas cada vez más en la entrega de servicios oportunos, eficiente y de calidad.

Existen algunas categorías de riesgo que se deben considerar en tecnología de la información al hablar de los riesgos, entre las que tenemos:

Riesgo de generación de valor: este debe considerar qué tan bien alineadas se encuentran las capacidades de las TI con los objetivos, estrategias de la Institución para aprovechar las operaciones tecnológicas con el fin de mejorar la eficiencia o efectividad de los procesos de la Institución.

Riesgo de entrega de programas: aquí debe existir un nivel de seguridad optimo que permita la adecuada gestión de programas informáticos y de esa manera evitar deficiencias en los equipos tecnológicos.

Riesgo en la entrega de servicios y operaciones de TI: en este riesgo se encuentra comprometida la efectividad de los servicios de soporte de tecnología, así como la infraestructura, esto puede influir directamente en el valor que genera la Institución.

Para poder evaluar una apropiada gestión del riesgo es necesario tener en consideración las políticas, procesos y procedimiento que le permitan mitigar el riesgo, algunas de esas consideraciones son las que se detallan a continuación:

- La administración de la tecnología debe preparar los requerimientos de operaciones actuales y futuras a través de planes de contingencia que le permiten a la organización prever futuros desastres en los sistemas informáticos.

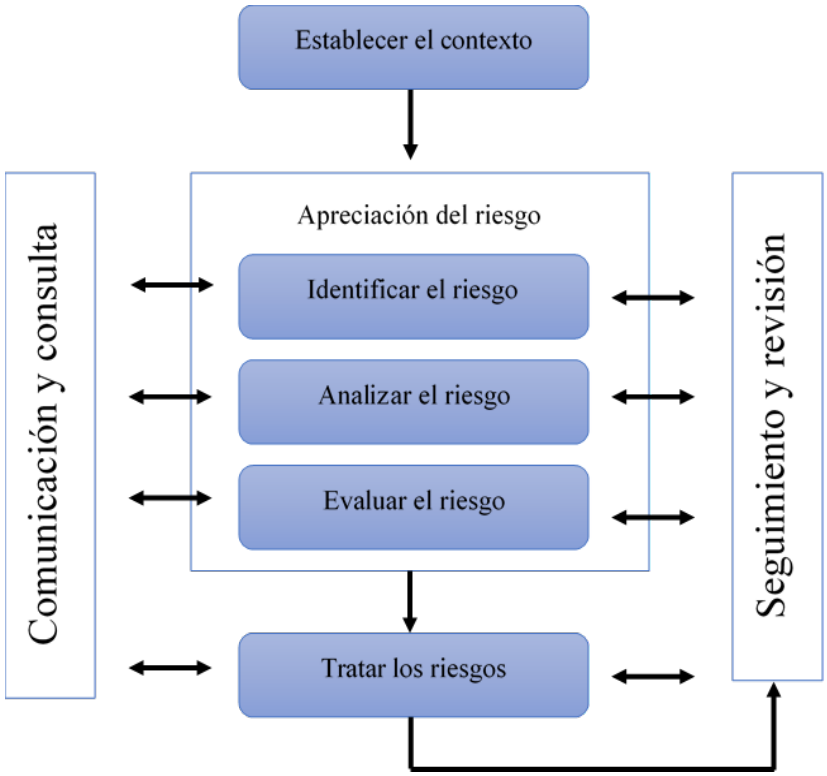
- Las operaciones de tecnología se establecen con el fin de satisfacer todas las necesidades que requiere la Institución.
- Los recursos informáticos adquiridos a terceros deben monitorearse constantemente para asegurar la efectividad y eficiencia de los equipos o servicios.
- La infraestructura de tecnología debe tener la capacidad de soportar todas las operaciones establecidas como necesidades de la Institución.

Otro punto importante que se debe considerar al hablar de los riesgos informáticos es tratar el riesgo y la gestión de la seguridad informática en donde se deben considerar los siguientes aspectos:

- Los sistemas de seguridad informática deben salvaguardar la información contra actos como, daños, perdidas, robos, inestabilidad de las redes, etc.
- Continuidad de las operaciones frente a situaciones como imprevistos que afecten los sistemas de información, complicando las operaciones de la Institución.
- Los planes contingentes deben garantizar la forma continua de las operaciones, así como minimizar las perdidas, el seguimiento a las operaciones, etc.

Analizado todos estos aspectos podemos mencionar que la gestión de riesgo es el conjunto de procesos que se debe desarrollar por parte de la organización para cumplir con ciertos objetivos como, disminuir la probabilidad y ocurrencia de debilidades; por otra parte, deben aumentar la probabilidad y ocurrencia de aprovechar las oportunidades para mejorar los procesos informáticos. Es decir que, se trata de una metodología diseñada para encargarse de disminuir la incertidumbre de las debilidades que se presentan.

Figura 12. *Fases de la Gestión de Riesgo.*



Fuente: *IMBAQUINGO, D., PÚSDA, M., & JÁCOME, J., (2016). Figura de los procesos de gestión de riesgo. [Figura]. Recuperado de: https://issuu.com/utnuniversity/docs/ebook-fundamentos- auditoria-informa (p. 74).*

5.13. El Control Interno

Es el conjunto de actividades que están orientadas a la prevención, identificación y corrección de irregularidades o falencias que estén inmersos en los procesos que realiza la entidad de manera normal y que a su vez afecten o impidan el cumplimiento de los objetivos institucionales.

La buena y correcta aplicación de las normas, los procedimientos, las prácticas y las estructuras organizativas que hayan diseñado para proporcionar una seguridad razonable permitirán a la Institución alcanzar sus objetivos y que

los eventos no deseados se prevean, se detecten y se corrijan.

5.13.1. Objetivos del Control Interno Informático

De acuerdo a varios autores existen algunos objetivos relacionados con el control interno Informático, entre los cuales podemos mencionar los siguientes:

- Controlar que todas las actividades que se va a realizar cumplan con los procedimientos y normas fijados para el mismo y de esta forma poder evaluar su bondad y asegurarse del cumplimiento de las normas legales
- Asesorar sobre el conocimiento y la aplicación efectiva de las normas".
- Apoyar y colaborar con el trabajo realizado en la Auditoria Informática interna, así como las auditorías externas que se pretendan realizar.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informática.

Se puede observar que el control interno informático que se desarrolla dentro de una Institución se realiza con la función de evaluar si todos los procedimientos se están realizando de una manera acorde a la normativa y a las metas establecidas, además de establecer medidas correctivas que contribuyan a la generación de resultados positivos.

5.13.2. Tipos de control interno informático

Se puede clasificar al control interno informático en tres clases, que son los siguientes:

Controles Preventivos: los controles preventivos son aquellos que están aplicados con anterioridad a la ocurrencia del hecho, esto con la finalidad de prevenirlo, un ejemplo de esto sería: contar con un programa que bloquee el acceso de terceros a la información contenida en el sistema Informático de la Institución.

Controles detectivos: los controles detectivos son aquellos controles que se aplican después de que el riesgo se ha detectado y en donde ya se ha presentado una violación a los controles preventivos, este control detectivo se ejecuta con la finalidad de conocer en el menor tiempo posible el hecho que está originando problemas, un ejemplo de esto es, verificar el número de errores que o veces fallidas que ha presentado un usuario al

intentar ingresar a su cuenta.

Controles correctivos: los controles correctivos son aquellos controles aplicados con el objetivo de disminuir los daños creados por los diversos problemas encontrados, un ejemplo de esto es, el realizar un análisis del sistema o disco dura de una computadora para poder recuperar un archivo eliminado.

5.13.3. Controles internos aplicados por áreas funcionales

Al realizar un examen de auditoría informática se debe tener en consideración las diferentes actividades que se desarrollan dentro de la Institución y de la propia área de sistemas, a continuación, se podrían mencionar alguno de los controles a implementar en un sistema de control interno:

Controles generales organizativos

- Evaluación de la aplicación de políticas y reglamentos internos.
- Evaluación de planes estratégicos de información, planes del área de sistemas, plan general de seguridad del área de informática, plan de contingencias o emergencias.
- Evaluación de estándares relacionados con la adquisición, mantenimiento, diseño y desarrollo de sistemas.
- Evaluación a la organización existente en el departamento de informática.
- Evaluación de la segregación de funciones dentro del departamento de informática.
- Evaluación de las políticas de selección de personal.
- Evaluación de políticas referentes al acceso y manejo de la información.

Controles de desarrollo, adquisición y mantenimiento de sistemas de información

- Verificación de la existencia de una normativa donde se detalle el ciclo de vida de desarrollo de un sistema.
- Verificación de exigencia de controles en el manejo de información referente al sistema.

Controles de explotación de sistemas de información

- Evaluación de controles existen para el buen uso de recursos informáticos.
- Verificación de procedimientos aplicados en lo referente a: selección, instalación, mantenimiento y seguridad de sistemas.
- Evaluación de políticas de seguridad existe, tanto físicas y de información.
- Evaluación de normar que regulas el acceso y uso de recursos informáticos.
- Existencia de un plan de contingencias ante posibles imprevistos que interrumpan las actividades normales de los empleados.

Controles en aplicaciones

- Evaluación de controles que garanticen la seguridad de los datos, todo lo relacionado con la actualización, mantenimiento y validez de la información contenida en dichos programas.

5.14. Metodología COBIT

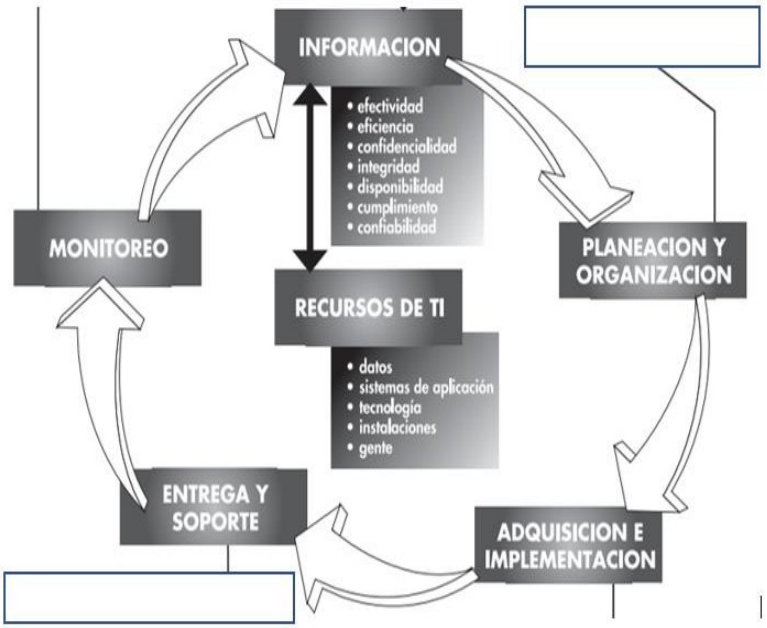
COBIT es una metodología que fue publicado en el año 1996, teniendo un total de cinco ediciones hasta diciembre del 2005. Sin embargo, para el año 2007 estaría disponible la versión 4.1, como resultado de su versión COBIT conforma un conjunto de lineamientos y estándares de manera internacional que contiene 34 objetivos, existen las definiciones del marco de referencia que determina una clasificación de procesos divididos en cuatro dominios que hacen referencia a las unidades de tecnología de información, estos dominios se basan en la planificación y organización, adquisición e implementación , entrega o servicios, supervisión o monitoreo y evaluación.

A medida que la tecnología va avanzando, los procesos de gestión y control requieren de herramientas orientadas a prever información suficiente y necesaria de todas las Instituciones. Este modelo de control interno tiene la función de establecer sus bases en los recursos de la tecnología de información o TI.

El modelo COBIT fue creado para auditar la gestión y el control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores de las tecnologías de información (TI), usuarios y, por supuesto, a los auditores involucrados en el proceso.

En ese sentido se puede decir que, una de las responsabilidades de la administración de todas las Instituciones, realizar todas las acciones necesarias para el modelo COBIT permita proporcionar enfoque integral y sistemático de los componentes de la tecnología de información. Por tal motivo, el COBIT permite entender los Sistemas de Información y tomar decisiones acerca del nivel de seguridad y control que permita proteger los activos de la Institución mediante el desarrollo de este modelo de administración de TI.

Figura 13. *Dominios de relación COBIT.*



Fuente: *Governance Institute COBIT, (2017). Figura de la relación de los diferentes dominios COBIT. [Figura]. Recuperado de: https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf (p. 19).*

El modelo COBIT sirve para identificar objetivos de Control Interno para mejorar las tecnologías e información que se encuentra construido por un conjunto de prácticas establecidas para el desarrollo de la información, así como, distribución, almacenamiento y administración que permiten asegurar los resultados del procesamiento de la información.

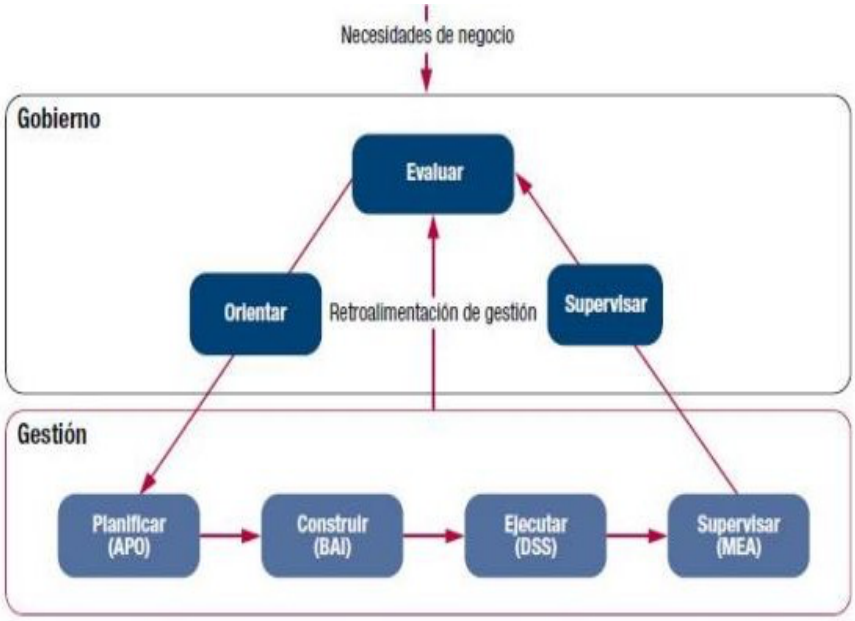
Cobit se aplica a los sistemas de información de las diferentes Instituciones públicas o privadas, donde se incluyen los pc o computadoras personales y las redes, está basado en la filosofía que los recursos de tecnología de información necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Este modelo de control es considerado como preciso para realizar auditorías a la gestión y control de los sistemas de información y tecnología, generalmente este tipo de control utilizan las Instituciones que poseen un capital activo significativo y se menciona que el éxito de una Institución se basa en la comprensión de los componentes de información y tecnología. Cabe mencionar que este tipo de Instituciones tiene mayor riesgo o vulnerabilidad ya que debido a las operaciones que realizan y la enorme cantidad de información que procesan tiene un porcentaje alto de probabilidad de caer en algún ataque informático, De esa manera los requerimientos regulatorios deben tratar de mitigar los riegos que se presenten y de esa manera permitir que la Institución se mantenga en un nivel se seguridad estable.

Dominios COBIT Ver. 5

Los dominios de COBIT son grupos de procesos que corresponden a una actividad específica. Existen dos dominios principales que son el gobierno y la gestión. El dominio de gobierno cuenta con cinco procesos de gobierno, y dentro de cada uno de ellos se establecen prácticas de evaluación, orientación y supervisión (EDM). Mientras que, el dominio de la gestión contiene cuatro dominios e igualmente dentro de cada uno de ellos se establecen prácticas de planificación, implementación, soporte y evaluación de las TI.

Figura 14. *Dominios COBIT.*



Fuente: *GUALSAQUÍ, J., (2013). Figura de los dos dominios principales de COBIT. [Figura]. Recuperado de: http://repositorio.puce.edu.ec/bitstream/handle/22000/6078/T-PUCE6320.pdf?sequence=1 (p. 18).*

Planeación y organización: contribuye a la mejora de los objetivos, la consecución de estrategias, en ese sentido se puede decir que, este objetivo cubre las estrategias que se refieren a la identificación de la forma en que se utiliza la tecnología de la información. Los procesos que se deben seguir para alcanzar este objetivo son:

- PO1: Definir un Plan Estratégico de TI
- PO2: Definir la Arquitectura de la Información
- PO3: Determinar la dirección tecnológica
- PO4: Definir la Organización y Relaciones de TI
- PO5: Manejar la Inversión en TI
- PO6: Comunicar las directrices y aspiraciones gerenciales

- PO7: Administrar Recursos Humanos
- PO8: Asegurar el cumplir Requerimientos Externos
- PO9: Evaluar Riesgos
- PO10: Administrar proyectos
- PO11: Administrar Calidad

Adquisición e Implementación: Para llevar a cabo las estrategias de TI, se debe identificar soluciones a ser implementadas en los procesos de control interno. Este objetivo tiene que ver con el mantenimiento que se realiza a los sistemas de la Institución.

- AI1: Identificar Soluciones
- AI2: Adquirir y Mantener Software de Aplicación
- AI3: Adquirir y Mantener Arquitectura de TI
- AI4: Desarrollar y Mantener Procedimientos relacionados con TI
- AI5: Instalar y Acreditar Sistemas
- AI6: Administrar Cambios

Servicio y soporte: hace referencia a la entrega y recepción de información, que abarca las operaciones, el entrenamiento y la continuidad de los procesos de información, este objetivo tiene el fin de proveer servicios debe existir procesos de soporte.

- DS1: Definir niveles de servicio
- DS2: Administrar Servicios de Terceros
- DS3: Administrar Desempeño y Calidad
- DS4: Asegurar Servicio Continuo
- DS5: Garantizar la Seguridad de Sistemas
- DS6: Identificar y Asignar Costos
- DS7: Capacitar Usuarios
- DS8: Asistir a los Clientes de TI
- DS9: Administrar la Configuración
- DS10: Administrar Problemas e Incidentes
- DS11: Administrar Datos
- DS12: Administrar Instalaciones
- DS13: Administrar Operaciones

Monitoreo: existe este objetivo porque los procesos necesitan ser evaluados con el fin de garantizar la viabilidad de los procesos además de verificar la calidad y suficiencia del control establecido.

- M1: Monitorear los procesos
- M2: Evaluar lo adecuado del control interno
- M3: Obtener aseguramiento independiente
- M4: Proveer auditoría independiente

Principios y Habilitadores de COBIT

Este modelo de control conta de 5 principios y 7 habilitadores que se utilizan en las prácticas de control interno:

- **Satisfacer las necesidades del accionista**: se refiere a establecer un criterio para vincular los objetivos de la organización con los objetivos que tiene la tecnología de información.

- **Considerar la Institución de punta a punto**: la Institución debe ser considera de manera general e integral con el fin de considerar todas las áreas de la Institución y convertir al TI en un activo y no en un gasto.

- **Aplicar un único modelo de referencia integrado:** establecer un estándar que permita seguir un marco integrado que permita optimizar los activos de la organización.

- **Posibilitar un enfoque holístico:** es decir que los componentes de la Institución deben analizarse de manera conjunta, completa e integral para mejorar las políticas, procesos, cultura e información.

- **Separar gobierno de la gestión:** el gobierno debe ser independiente de la gestión ya que deben evaluarse las necesidades de manera separada con el fin de priorizarlas y tomar decisiones que contribuyan al progreso de los resultados.

Por otra parte, los habilitadores de COBIT son elementos que hacen posible los proceso y políticas que se reflejarán en el rendimiento y alcance de

los objetivos de la organización.

Principios, políticas y marcos de trabajo: son documentos que sirven de guía para conducir al buen comportamiento deseado que los miembros de la organización deben alcanzar.

Procesos: describen las operaciones que realiza la organización para alcanzar los objetivos y cumplir con las necesidades.

Estructura organizacional: se refiere a los miembros que toman decisiones específicas que contribuyen a la mejorar de las actividades de la organización.

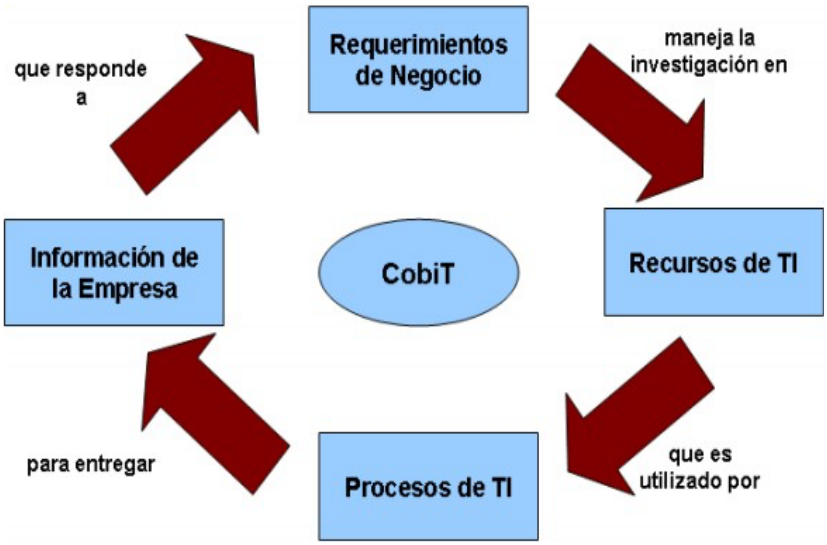
Cultura, ética y comportamiento: son las características de los miembros de la organización que deben considerarse para el desarrollo de las funciones.

Información: se refiere a los datos y documentos que utiliza la organización con el fin de convertirlos en información de utilidad.

Servicios, Infraestructuras y Aplicaciones: se refiere a todos los elementos relacionados con la tecnología, equipos, aplicaciones que tiene la Institución para realizar sus funciones.

Personas, Habilidades y competencias: se refiere a las personas que se laboran en la Institución y que son necesarias para desarrollar las actividades y tomar decisiones en beneficio de la entidad.

Figura 15. *Proceso de los principios de COBIT.*



Fuente: *Governance Institute COBIT, (2017). Figura de la relación de los diferentes dominios COBIT. [Figura]. Recuperado de: https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf (p. 17).*

Criterios COBIT

Los criterios de control que debe seguirse alcanzar los objetivos son:

Efectividad: hace referencia a la información importante y pertinente que facilitan información de manera oportuna, correcta y consistente.

Integridad: se relaciona con la información precisa y validez de esta.

Disponibilidad: la información debe estar disponible en cualquier momento, sin motivo de espera por cualquier situación.

Cumplimiento: se refiere a cumplir con las disposiciones, reglamentos, leyes y demás reglamentos que disponga la entidad.

Confiabilidad: hace referencia a que la información debe ser apropiada para que la gerencia pueda tomar decisiones pertinentes.

Gestión de tecnología de información

La gestión de TI comprende el proceso de planificación y alineación estratégica de TI, la organización y estructuración del área de TI, las políticas, normas y programas de capacitación continua, la arquitectura y gestión de la información, los servicios de atención y soporte a usuarios y la infraestructura tecnológica. En ese sentido se puede decir que para garantizar una gestión eficiente los recursos informáticos deben interactuar con los demás recursos de la Institución de esa manera se logra una sinergia entre todas las áreas de la Institución.

Por lo tanto, para lograr una adecuada gestión las Instituciones deben mantener una estructura organizacional bien definida con personas capacitadas constantemente con un enfoque de liderazgo en el ambiente de trabajo, con ello se pretende, satisfacer las necesidades de la Institución a través de indicadores, la administración debe medir el rendimiento del área de tecnología e información ya que el rendimiento permitirá conocer si esta área está cumpliendo con las metas, objetivos, estrategias y demás consideración que permitan conocer el grado de eficiencia y eficacia en las operaciones en el área de tecnología e información. En el caso de obtener indicadores deficientes, se debe plantear controles que permitan una correcta gestión.

5.15. COSO

El COSO por sus siglas en inglés que significan Committee of Sponsoring Organizations of the Treadway es una Comisión voluntaria constituida por representantes de cinco organizaciones del sector privado en EEUU, para proporcionar liderazgo intelectual frente a tres temas interrelacionados: la gestión del riesgo Institucionrial (ERM), el control interno, y la disuasión del fraude. Estas cinco organizaciones son:

- La Asociación Americana de Contabilidad (AAA)
- El Instituto Americano de Contadores Públicos Certificados (AICPA)
- Ejecutivos de Finanzas Internacional (FEI), el Instituto de Auditores Internos (IIA)

- La Asociación Nacional de Contadores (ahora el Instituto de Contadores Administrativos [AMI]).

Desde su fundación en 1985 en EEUU, promovida por las malas prácticas Institucionales y los años de crisis anteriores, COSO estudia los factores que pueden dar lugar a información financiera fraudulenta y elabora textos y recomendaciones para todo tipo de organizaciones y entidades reguladoras como el SEC (Agencia Federal de Supervisión de Mercados Financieros) y otros.

El COSO es un escrito en el que se encuentran las principales directrices para la implementación, gestión y control de un sistema de control, este informe se ha convertido en un estándar para la implementación de los sistemas de control interno en las Instituciones. Este informe posee ciertas ventajas las cuales se mencionan a continuación:

- Permite a la dirección de la Institución 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.

La misión del COSO en auditoria es:

Proporcionar liderazgo intelectual a través del desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones.

Figura 16. *Ventajas del COSO y sus componentes.*

Fuente: *La Fuente (2016). Ventajas del COSO y sus componentes [Figura]. Recuperado de: https://fraudeinterno.wordpress.com/2016/02/19/coso-gestion-de-riesgos/*

Beneficios de usar el COSO

Algunos de los beneficios de utilizar el estándar COSO en las organizaciones son:

- Promueve la gestión de riesgos en todos los niveles de la organización y establece directrices para la toma de decisiones de los directivos para el control de los riesgos y la asignación de responsabilidades.
- Ayuda a la integración de los sistemas de gestión de riesgos con otros sistemas que la organización tenga implantados
- Ayuda a la optimización de recursos en términos de rentabilidad
- Mejora la comunicación en la organización
- Mejora el control interno de la organización.

5.15.1. Control Interno

El control interno es considerado como un proceso que se llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objetivo de proporcionar un grado de seguridad razonables en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento.

El control es la tarea de examinar los resultados de una gestión que accede a obtener disposiciones para hacer progresos inmediatos y adquirir medidas provisorias. Además, tiene como ambición primordial, conservar la acción de cualquier Institución y ayudar a su progreso; su finalidad es aportar al desarrollo de los resultados deseados. Se puede afirmar que: El control interno es el conjunto de planes, sistemas y recursos amparados por una compañía u organización, con el fin de certificar que los activos estén correctamente protegidos, que los registros contables sean fehacientes y que la actividad de la entidad se desenvuelva efectivamente de acuerdo con las políticas asignadas por la Gerencia, en cumplimiento de los objetivos previstos.

El control interno como base fundamental debe facilitar a la alta gerencia la medición de los resultados obtenidos en su desempeño, con la finalidad de mejorar, implementar o eliminar procesos que dificulten llegar a la eficiencia y la eficacia de las operaciones.

Objetivos

El control interno, establece categorías de objetivos:

- **Objetivos operativos**: tienen que ver con la eficiencia de las operaciones que desarrolla una Institución incluyendo los objetivos de parte financiera como los rendimientos financieros y operacionales.

- **Objetivos de información:** se refiere a la información financiera y no financiera que proviene de los ambientes internos y externos pueden comprender la confiabilidad, oportunidad, transparencia y otros conceptos mencionados por los reguladores.

- **Objetivos de cumplimiento**: comprende todas las normas, leyes y regulaciones que la entidad establece para la mejora de las actividades de los procedimientos.

Responsabilidades del Control Interno

Los comités u oficinas de control interno están responsabilizadas por todas acciones de las Instituciones que poseen oportunidades financieras para crearlas, caso contrario el compromiso por las acciones, recaerá en la gerencia, la responsabilidad del control interno debe adaptarse a los requerimientos de cada Institución.

Es importante establecer un Sistema de control interno que les permita tener una confianza moderada de que sus acciones administrativas se adapten en todo a las normas aplicables a la Institución, misma que va a variar en relación a la actuación o naturaleza de cada Institución u organización.

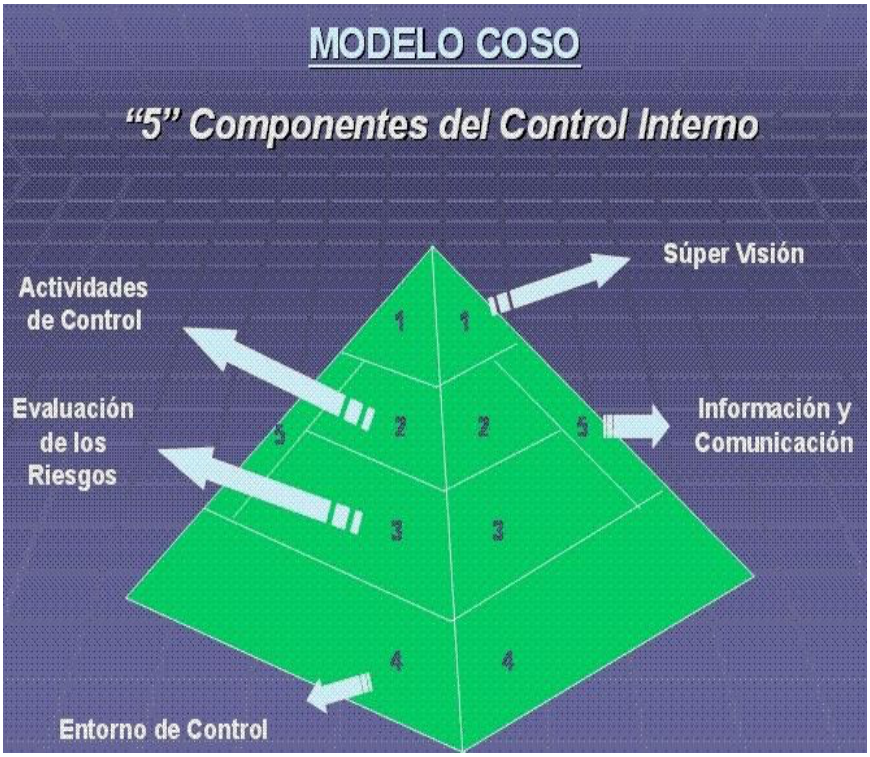
El sistema de control interno tiene que ser un conjunto sistemático, compuesto por el sistema de planeación, reglas, técnicas y tácticas utilizados para el desenvolvimiento de las actividades de la organización y los elementos y dispositivos de búsqueda y calificación que se establezcan para realimentar su periodo de operaciones.

COSO I

El propósito de este informe es mejorar la calidad de la información que

se maneja a través de un estudio de la conducción de la sociedad, las practicas éticas y el control interno, este proceso de control interno debe ser desempeñado por el directorio, gerencias u otros empleados de una organización, es diseñado a fin de garantizar seguridad en el cumplimiento de los objetivos Institucionales.

Figura 17. *Componentes de Control Interno.*



Fuente: *La Fuente (2016). Figura de los componentes del Control Interno [Figura]. Recuperado de: https://fraudeinterno.wordpress.com/2016/02/19/coso-gestion-de-riesgos/*

En 1992 la comisión publicó el primer informe "Internal Control - Integrated Framework" denominado COSO I con el objeto de ayudar a las entidades a evaluar y mejorar sus sistemas de control interno, facilitando un modelo en base al cual pudieran valorar sus sistemas de control interno y generando una definición común de "control interno".

Según COSO el Control Interno es un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

Eficacia y eficiencia de las operaciones. Confiabilidad de la información financiera.

Cumplimiento de las leyes, reglamentos y normas que sean aplicables. La estructura del estándar se dividía en cinco componentes:

- Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Supervisión

Figura 18. *Componentes Coso I.*

Fuente: *Elaboración propia*

COSO II

En 2004, se publicó el estándar "Enterprise Risk Management - Integrated Framework" (COSO II) Marco integrado de Gestión de Riesgos que amplía el concepto de control interno a la gestión de riesgos implicando necesariamente a todo el personal, incluidos los directores y administradores.

Para, (Cadena, 2011), COSO II (ERM) amplía la estructura de COSO I a ocho componentes:

1) Ambiente de control: son los valores y filosofía de la organización, influye en la visión de los trabajadores ante los riesgos y las actividades de control de los mismos.
2) Establecimiento de objetivos: estratégicos, operativos, de información y de cumplimientos.
3) Identificación de eventos, que pueden tener impacto en el cumplimiento de objetivos.
4) Evaluación de Riesgos: identificación y análisis de los riesgos relevantes para la consecución de los objetivos.
5) Respuesta a los riesgos: determinación de acciones frente a los riesgos.
6) Actividades de control: Políticas y procedimientos que aseguran que se llevan a cabo acciones contra los riesgos.
7) Información y comunicación: eficaz en contenido y tiempo, para permitir a los trabajadores cumplir con sus responsabilidades.
8) Supervisión: para realizar el seguimiento de las actividades.

En la revista digital conexión esa pertenece a una conocida escuela de negocios de Perú menciona lo siguiente respecto al COSO II y que es importante mencionar:

> *El COSO II es un sistema de gestión de riesgo y control interno para cualquier organización. Se basa en un marco cuyo objetivo es diagnosticar problemas, generar los cambios necesarios para gestionarlos y evaluar la efectividad de estos. El COSO II brinda una serie de beneficios, entre los cuales están:*

- Alinea la gestión de riesgos con la estrategia para analizarlos.
- Mejora las decisiones importantes de respuesta ante los riesgos o crisis.

- Reduce el número de eventos sorpresivos y, en consecuencia, de pérdidas operacionales.
- Identifica, agrupa y gestiona toda la diversidad de eventos perjudiciales para la Institución.
- Mejora la inversión y el presupuesto de una compañía, disminuyendo los impactos negativos.

Los componentes claves del COSO II se basan en los siguiente ocho elementos. El correcto manejo de estos aspectos brindará una operación efectiva de este sistema.

Ambiente interno. Hace referencia al entorno interno de una Institución y establece la base de cómo el personal percibe y trata los riesgos.

Establecimiento de objetivos. Deben estar alineados con la visión y misión de la organización, teniendo en cuenta que cada decisión conlleva un riesgo que debe ser previsto.

Identificación de acontecimientos. Deben identificarse los eventos que afectan los objetivos de la compañía, para que la Institución los pueda enfrentar y prevenir de la mejor forma posible.

Evaluación de riesgos. Estos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser administrados.

Respuesta a los riesgos. Luego de ser evaluado el riesgo, la gerencia debe identificar y evaluar posibles repuestas con relación a las necesidades de la organización.

Actividades de control. Comprenden las políticas y procedimientos que permiten asegurar que se tomen las medidas necesarias para controlar los riesgos.

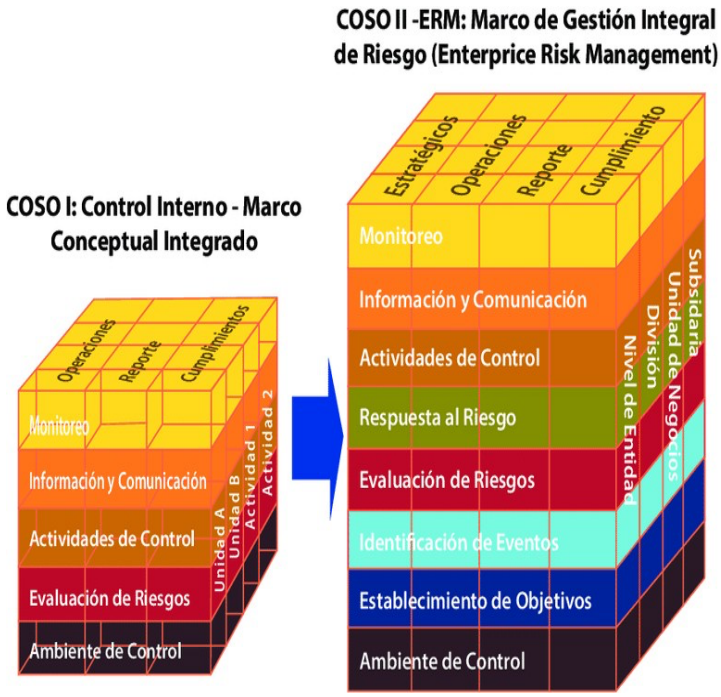
Información y comunicación. La primera es necesaria para hacer frente a los riesgos identificando, evaluando y dando respuesta ante ellos. Asimismo, debe existir una buena comunicación con los clientes, proveedores, reguladores y accionistas.

Supervisión. Se monitorea que el proceso de administración de los

riesgos sea efectivo a lo largo del tiempo y que todos los elementos del marco COSO funcionen adecuadamente.

Es importante considerar que los tipos de riesgo varían según las compañías en los que aparezcan. Es por ello que se necesita un control bajo un marco global que permita administrarlos. Solo así se asegurará el éxito de una organización en todo nivel.

Figura 19. *Cubos del COSO I y COSO II.*

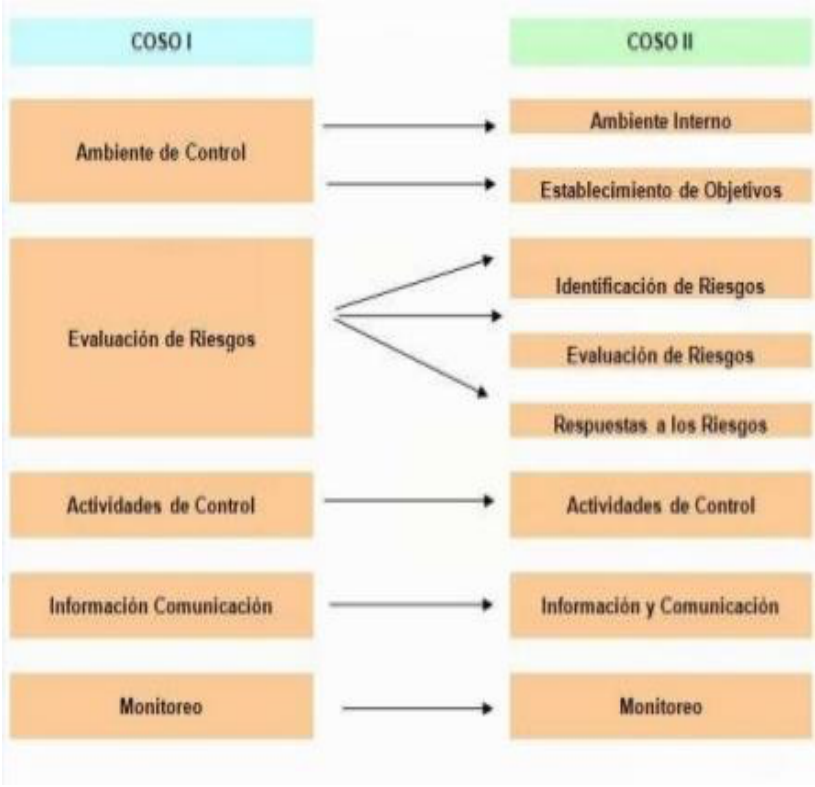


Fuente: *Vega (2017). Figura de cubos de COSO I y COSO II [Figura]. Recuperado de: https://www.researchgate.net/figure/Figura-3-Cubos-de-gestion-de-riesgo-de-COSO-I-y-COSO- II_fig1_329323970*

Además, amplía la visión del riesgo a eventos negativos o positivos, o sea, a amenazas u oportunidades; a la localización de un nivel de tolerancia al riesgo; así como al manejo de estos eventos y a la gestión de riesgos. Aspectos claves a tener en cuenta en el análisis de Coso II:

- Administración del riesgo en la determinación de la estrategia
- Eventos y riesgo
- Apetito de riesgo
- Tolerancia al riesgo
- Visión de portafolio de riesgo.

Figura 20. *Relación entre el COSO I y COSO II.*



Fuente: *Alonso y Cuarezma., (2014). Figura de relación entre el COSO I y el COSO II. [Figura]. Recuperado de: https://es.slideshare.net/scry01/coso-y-coso-erm*

COSO III

En mayo de 2013 se ha publicado la tercera versión COSO III. Las novedades que introducirá este Marco Integrado de Gestión de Riesgos son:

- Mejora de la agilidad de los sistemas de gestión de riesgos para adaptarse a los entornos
- Mayor confianza en la eliminación de riesgos y consecución de objetivos
- Mayor claridad en cuanto a la información y comunicación.

5.15.2. Ambiente Interno

Se lo conoce también como entorno de control y hace referencia al conjunto de circunstancias o conductas que define el accionar de la entidad considerando la perspectiva del control interno. Es decir que el control interno conforma las actitudes asumidas por los altos mandos de la entidad y todos los miembros que hacen parte de una entidad. En otras palabras, el entorno interno es el conjunto de medios y reglamentos que se han establecido previamente para establecer ciertas conductas del personal, de esta manera se espera que el personal tome conciencia de las normas, políticas, reglamentos y demás normas de control interno que tiene la Institución para el correcto funcionamiento de sus actividades.

Según varios Autores el ambiente de control es aquel que define parámetros para gestionar el control interno de la compañía que tiene que ver con la estructura organizacional, las políticas administrativas, ética institucional y las relaciones de jerarquía, la autoridad y responsabilidad; así como la integridad, los valores de la compañía y la filosofía administrativa.

Por otra parte, otro concepto relacionado al ambiente de control está relacionado con el entorno que existe en la entidad con respecto al control. En otras palabras, con la actitud que adoptan los gerentes, los administradores y los empleados con respecto al control.

El entorno de control incluye la integridad y los valores éticos de la organización; los parámetros que permiten al consejo llevar a cabo sus responsabilidades de supervisión del gobierno corporativo; la estructura organizacional y la asignación de autoridad y responsabilidad; el proceso de atraer, desarrollar y retener a profesionales competentes; y el rigor aplicado a las medidas de evaluación del desempeño, los es- quemas de compensación para incentivar la responsabilidad por los resultados del desempeño.

En ese sentido se puede decir que, el entorno de control es el ambiente que se puede considerar como base para posicionar a los demás elementos ya que el primer componente es el elemento que influye principalmente en los objetivos y estrategias de las entidades. Por tal motivo, es necesario priorizar el ambiente de control como se muestra en la imagen.

- **Principio 1:** Organización comprometida con la integridad y valores éticos.
- **Principio 2:** Es preciso demostrar independencias en las áreas de gerencia, vigilancia y control interno.
- **Principio 3:** Se restablece estructuras líneas de reporte y comunicación que deben set apropiadas para la autoridad competente.
- **Principio 4:** Demostrar compromiso para desarrollar un adecuado plan de reclutamiento de personas que se ajuste a las necesidades de cada Institución.
- **Principio 5:** Uno de los perfiles que debe considerar la Institución es que, el personal contratado debe ser responsable para cumplir con los requerimientos de control interno.

Figura 21. *Priorización de los componentes del ambiente de control.*

Fuente: *GUZMÁN, J., (2017). Figura de los componentes del ambiente de control. [Figura]. Recuperado de: https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf (p. 15).*

Factores del Ambiente de Control

- La integridad y los valores éticos.
- El compromiso a ser competente
- Las actividades de la Junta Directiva y el comité de Auditoría
- La mentalidad y estilo de operación de la Gerencia.
- La estructura de la organización

5.15.3. La asignación de autoridad y responsabilidades.

- Las políticas y prácticas de recursos humanos.

5.15.4. Evaluación del Riesgo

Es el segundo componente del COSO en el que se evalúa los riesgos considerados como amenazas que afectan el cumplimiento de los objetivos de control interno, entre estos objetivos están los de operación, los de información financiera y los de cumplimiento. Los riesgos son cambiantes por tal motivo, es necesario establecer procesos continuos que permitan identificarlos.

Una condición que se puede encontrar previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos.

En sentido contrario se puede mencionar que la evaluación del riesgo no es una tarea para cumplir de una vez para siempre. Debe ser un proceso continuo, una actividad básica de la organización, como la evaluación continua de la utilización de los sistemas de información o la mejora continua de los procesos.

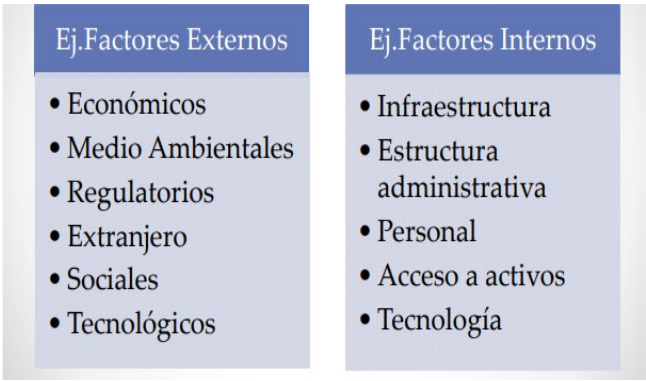
Dentro de la Auditoria se pueden presentar condiciones previas a la evaluación de riesgos como es el establecimiento de objetivos asociados a los diferentes niveles de la entidad. La dirección debe definir los objetivos operativos, de información y de cumplimiento, con suficiente claridad y detalle para permitir la identificación y evaluación de los riesgos con impacto potencial

en dichos objetivos. Asimismo, la dirección debe considerar la adecuación de los objetivos para la entidad. La evaluación de riesgos también requiere que la dirección considere el impacto que puedan tener posibles cambios en el entorno externo y dentro de su propio modelo de negocio, y que puedan provocar que el control interno no resulte efectivo.

Los principios que se debe seguir en el componente de evaluación de riesgo son:

- **Principio 6:** La Institución debe contar con objetivos que le permitan identificar y valorar el riesgo correspondiente a cada área.
- **Principio 7:** La Institución debe ser capaz de identificar y analizar el momento, espacio o actividad que genera el riesgo
- **Principio 8:** Entre una de las competencias de las Instituciones está considerar la valuación del riesgo correspondiente al fraude.
- **Principio 9:** Otra responsabilidad que recae sobre la Institución es que debe identificar los cambios en el sistema de control interno con el fin de conocer al inicio de los procesos cuales son los riesgos que se deberían considerar para mitigar.

Figura 22. *Factores Externos e Internos de la evaluación del control interno.*



Fuente: *BARRERA, Gabriel, (2015). Figura de los factores internos y externos que se deben considerar en la evaluación del control interno. [Figura]. Recuperadode: https://archivo.consejo.org.ar/comisiones/com_43/files/coso_2.pdf (p. 15).*

5.15.5. Actividades de Control

Las actividades de control son aquellas que implementó la administración para los distintos procedimientos y actividades que debe desarrollar la Institución, por tal motivo, estos procedimientos deben emplearse en todos los niveles o áreas de la organización, con el fin de cubrir de manera integral todos los procedimientos. En otras palabras, las actividades control son todas las políticas y procedimientos que permiten definir las acciones correctas que permitirán gestionar el riesgo, uno de los factores que favorecen a este componente es la toma de decisiones ya que se encuentran relacionados con directamente.

Una actividad de control se refiere a las políticas y procedimientos que trazan las acciones adecuadas para gestionar los riesgos, tomar decisiones que favorezcan la operación y el logro de los objetivos. Todas las áreas de la compañía, sin excepción, son las responsables de ejecutar las actividades de control, que lleven a una correcta toma de decisiones y cumplimiento de los objetivos".

Dentro de la actividad de control algunos autores mencionan que estas actividades de control son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos. Las actividades de control se ejecutan en todos los niveles de la entidad, en las diferentes etapas de los procesos de negocio, y en el entorno tecnológico.

Los principios que debe seguir este componente son los siguientes:

- **Principio 10:** La Institución debe diseñar e implementar actividades de control con el propósito de mitigar los riesgos.
- **Principio 11:** Debe crear e implementar controles para el sistema de información, es decir debe aplicar controles automáticos y tecnológicos que permitan definir acciones para mejorar el desempeño de las actividades.
- **Principio 12:** Las políticas y procedimientos en este componente son de vital importancia.

5.15.6. Información y Comunicación

La información y comunicación menciona que, es importante identificar la clase de información que se produce y se procesa hacia el interior de las organizaciones. Una información primaria, relacionada con los datos provenientes de los usuarios y clientes y una información secundaria, como resultados de las operaciones financiera, administrativas, y jurídicas de la organización, como son los estados financieros, presupuestos, planes, correspondencia, quejas y reclamos, entre otros; lo anterior, procesado a través de sistemas de información compuesto por recursos tecnológicos y humanos produce el tipo de información que se requiere.

Así mismo se determina que la comunicación interna es el medio por el cual la información se difunde a través de toda la organización, que fluye en sentido ascendente, descendente y a todos los niveles de la entidad. Esto hace posible que el personal pueda recibir de la alta dirección un mensaje claro de que las responsabilidades de control deben ser tomadas seriamente. La comunicación externa persigue dos finalidades: comunicar, de fuera hacia el interior de la organización, información externa relevante y proporcionar información interna relevante de dentro hacia fuera, en respuesta a las necesidades y expectativas de grupos de interés externos.

Es por eso por lo que, tomar atención en el componente de información y comunicación es importante ya que a través de métodos, canales, medios y acciones se debe realizar un enfoque sistemático y regular los flujos de información a fin de proporcionar fuentes fidedignas de calidad y oportunidad para cumplir con las obligaciones de manera individual y grupal.

- **Principio 13:** La organización debe obtener, generar y utilizar la información relevante, es decir que sea de calidad para el soporte del funcionamiento del Control Interno.
- **Principio 14:** Mediante la aplicación de reuniones con los trabajadores, la Institución comunica los objetivos y responsabilidades del Control Interno.
- **Principio 15:** La Institución tiene la responsabilidad de comunicar a terceros los problemas que afectan el correcto desarrollo del Control interno.

La comunicación interna es el medio por el cual la información se difunde a través de toda la organización, que fluye en sentido ascendente, descendente y a todos los niveles de la entidad. Esto hace posible que el personal pueda recibir de la alta dirección un mensaje claro de que las responsabilidades de control deben ser tomadas seriamente. La comunicación externa persigue dos finalidades: comunicar, de fuera hacia el interior de la organización, información externa relevante y proporcionar información in- terna relevante de dentro hacia fuera, en respuesta a las necesidades y expectativas de grupos de interés externos.

5.15.7. Monitoreo

Está dirigidos a las actividades relacionadas con el control de los sistemas internos que deben ser supervisados de manera constante debido a que existe mayor riesgo, en ese sentido se puede decir que las Instituciones establecer una evaluación continua mediante la aplicación de estrategias que se consideren necesarias para disminuir errores y concretar metas. De esa manera se podrá comprobar qué tan eficiente es el control interno de la entidad, ya que al implementar un control interno adecuado la gestión de las actividades se optimiza para poder minimizar riesgos y esto se logra a través de la supervisión y monitoreo constante de todas las actividades que se desarrollan en la entidad.

El monitoreo corresponde al proceso de realizar evaluaciones concurrentes o separadas, o una combinación de ambas. Es utilizado para determinar si cada uno de los componentes del Control Interno, incluidos los controles para efectivizar los principios dentro de cada componente, está presente y funcionando. Los hallazgos son evaluados y las deficiencias son comunicadas oportunamente, las significativas son comunicadas a la alta gerencia y al directorio.

Complementado la idea anterior según las evaluaciones de monitoreo debe conducir a la identificación de los controles débiles, insuficientes o innecesarios, para promover con el apoyo decidido de la gerencia, su robustecimiento e implantación**.** Esta evaluación puede llevarse a cabo de tres formas: durante la realización de las actividades diarias en los distintos niveles de la organización; de manera separada por personal que no es el responsable directo de la ejecución de las actividades (incluidas las de control) y mediante la combinación de las dos formas anteriores.

Las evaluaciones continuas, que están integradas en los procesos de negocio en los diferentes niveles de la entidad, suministran información oportuna. Las evaluaciones independientes, que se ejecutan periódicamente, pueden variar en alcance y frecuencia dependiendo de la evaluación de riesgos, la efectividad de las evaluaciones continuas y otras consideraciones de la dirección. Los resultados se evalúan comparándolos con los criterios establecidos por los reguladores, otros organismos reconocidos o la dirección y el consejo de administración, y las deficiencias se comunican a la dirección y al consejo, según corresponda.

Otro criterio importante vertido por autores menciona a las evaluaciones continuas, que están integradas en los procesos de negocio en los diferentes niveles de la entidad, suministran información oportuna. Las evaluaciones independientes, que se ejecutan periódicamente, pueden variar en alcance y frecuencia dependiendo de la evaluación de riesgos, la efectividad de las evaluaciones continuas y otras consideraciones de la dirección. Los resultados se evalúan comparándolos con los criterios establecidos por los reguladores, otros organismos reconocidos o la dirección y el consejo de administración, y las deficiencias se comunican a la dirección y al consejo, según corresponda.

Por lo tanto, se debe considerar las siguientes actividades o para conseguir un adecuado seguimiento:

- **Principio 16:** El personal debe conocer acerca de las funcionalidades del sistema de control interno y saber si está funcionando adecuadamente.
- **Principio 17:** La información externa es recibida de fuentes confiables. Revisar después de cada auditoría, si existen recomendaciones propuestas por el auditor e implementar dichas recomendaciones.

Cuando se va a determinar el control interno se debe considerad lo siguiente:

- Se puede llevar operaciones que alcanzan un nivel de operaciones con efectividad y eficiencia cuando es poco probable que los eventos que son del ambiente externo estén agrupados con los riesgos que generen un impacto significativo.
- Se prepara informes de acuerdo con lo establecen las reglas, regulaciones y normas que deben aplicarse tomando en consideración

los objetivos específicos de la entidad.

5.16. ITIL

Tuvo sus inicios en 1980 por el gobierno británico con el objetivo de organizar, gestionar y controlar el área informática, esto en el sentido de que gran parte de las organizaciones son dependientes de la tecnología e información, y lo que se busca es establecer una guía para que las áreas del gobierno británico trabajarán con mayor eficiencia con el objetivo de reducir costos que se generaban por la tecnología de información. Con el pasar del tiempo la guía ITIL establecida por el gobierno británico demostró ser adaptable a cualquier organización, por tal motivo años más tarde las Instituciones privadas deciden implementar esta guía. ITIL resultó ser tan útil que actualmente recoge la gestión de los servicios TI como uno de sus apartados, habiéndose ampliado el conjunto de "buenas prácticas" a gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones. Estas buenas prácticas provienen de las mejores soluciones posibles que diversos expertos han puesto en marcha en sus organizaciones a la hora de entregar de servicios TI, por lo que en ocasiones el modelo puede carecer de coherencia ITIL funciona como una herramienta de gestión enfocada a la tecnología de información y las operaciones relacionadas con la TI. Establece un modelo de mejores prácticas que permite actualizar, verificar, evaluar las actividades de la organización con el objetivo de promover el cambio cultural de los departamentos encargados de la tecnología, de esa manera permite transformar un modelo tecnológico normal o tradicional en un modelo tecnológico en el que su principal objetivo es la gestión, enfocado a seguir los lineamientos establecidos por la organización para la lograr los objetivos organizacionales, las metas y estrategias.

Buscando conceptos de ITIL podemos mencionar que es la definición de las mejores prácticas para los procesos y responsabilidades que hay que establecer para gestionar de forma eficaz los servicios de ti de la organización, y cumplir así los objetivos Institucionales en cuanto a la distribución de servicios y la generación de beneficios.

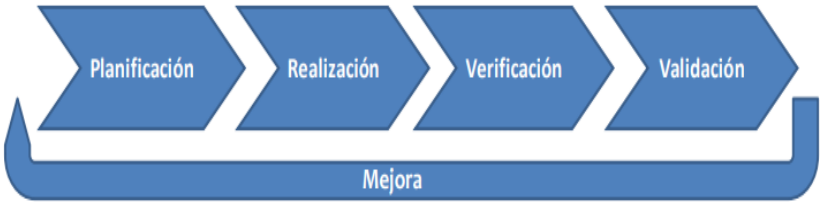
Por tal motivo, describe las mejores prácticas y las responsabilidades que deben utilizarse para gestionar de manera eficaz los servicios de TI. Dichas normas sirven para detallar de forma precisa los procedimientos de gestión que se diseñan con la finalidad de contribuir a la eficiencia y la calidad de las

operaciones de los departamentos de las Instituciones.

ITIL sigue un proceso de o ciclo de calidad para permitir a la Institución garantizar los objetivos, este modelo que se presentan como principios de calidad son similares a los que utiliza COBIT para la gestión del control interno en TI. Estos procesos se basan en las siguientes fases:

- Planificación
- Realización
- Verificación
- Validación

Figura 23. *Ciclo de la Gestión del Nivel de Servicio.*



Fuente: *ALBARRÁN, S., PÉREZ, J., & SALGADO, M., (2017). Figura del ciclo de mejora continua para los servicios de TI. [Figura]. Recuperado de: https://ideasencienciasingenieria.uaemex.mx/article/download/14591/10992/ (p. 41)*

Para desarrollar ITIL es necesario considerar cinco etapas:

Estrategias del servicio: se refiere a que se debe alinear las estrategias de TI con los objetivos, necesidades, normas y demás aspectos internos de la Institución para asegurar que las decisiones generen valor agregado.

Diseño del servicio: se refiere a que es necesario garantizar la optimización de los costos para mejorar el desempeño de las operaciones.

Transición del servicio: asegurar que los nuevos servicios de TI cumplan con las necesidades que requiere el negocio. En el caso de existir cambios por motivos de que los servicios no cumplen con las necesidades de la Institución,

deben ser gestionados y controlados de manera eficiente logrando los cambios de manera ágil.

Operación del servicio: las operaciones de TI deben ser gestionadas de forma segura generando confianza como respuesta al apoyo de las necesidades de la Institución.

Mejora continua del servicio: los procesos de TI deben seguir una secuencia centrada en mejorar la calidad, eficiencia y efectividad de los servicios TI.

Obtener una calificación ITIL permite a las organizaciones desarrollar las habilidades y destrezas de toda la organización para mejorar el desempeño en TI, ya que la tecnología de información con los lineamientos de la organización debe mantenerse en sintonía. El valor agregado que proporciona ITIL tiene beneficios como los que se menciona a continuación:

- Servicio Confiable
- Clientes satisfechos
- Todas las áreas de la organización se entienden
- Optimización de los costos por tecnología de información.
- Aumento de la productividad
- Mejora el proceso de innovación.

Figura 24. *Proceso de mejora continua.*

Fuente: *ALBARRÁN, S., PÉREZ, J., & SALGADO, M., (2017). Figura del proceso de mejora continua de los servicios bajo ITIL. [Figura]. Recuperado de: https://ideasencienciasingenieria.uaemex.mx/article/download/14591/10992/ (p. 19).*

CAPÍTULO 6

6. *Caso Práctico*

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
PLANIFICACIÓN PRELIMINAR

DATOS GENERALES
ENTE: Productos Lácteos Gonzáles CÍA. LTDA.
AREA: Contable
TIPO DE EXAMEN: Auditoría Informática

MOTIVO
La presenta auditoría se realiza luego de analizar las propuestas de firmas auditoras y se autoriza a Carlos Lema Gerente General de la Institución, con oficio No. 002, la contratación de los servicios profesionales de Auditores y Consultores.

ALCANCE
Elaborar la Auditoría Informática al departamento de tecnología e Información de la Institución Productos Lácteos Gonzáles CÍA. LTDA, para el periodo 2020.

OBJETIVOS DE LA AUDITORÍA GENERAL
Realizar una Auditoría Informática al departamento de Tecnología e Informática de la Institución Productos Lácteos Gonzáles CÍA. LTDA. mediante la aplicación de métodos, técnicas y procedimientos para determinar el grado de eficiencia de las aplicaciones

ESPECÍFICOS
Recabar información del personal de la entidad mediante la aplicación de entrevistas que permitan conocer el departamento de tecnología e información.
Evaluar el control interno para establecer el correcto funcionamiento de las aplicaciones informáticas mediante la valoración de la matriz de riesgos.

LIMITACIONES

La principal limitación es el tiempo que se demora en la entrega de información considerando que el personal debe cumplir con sus funciones primero y posteriormente ayudar en el proceso de auditoría.

DÍAS PRESUPUESTADOS

90 días laborables, distribuido en las siguientes fases

CRONOGRAMA

N °	FASE	PRIMER MES				SEGUNDO MES				TERCER MES			
1	P. preliminar												
2	P. específica												
3	Ejecución												
4	Comunicación de resultados												

ELABORADO POR: APR	FECHA: 13/02/2021
REVISADO POR: WGY	FECHA: 13/02/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
INFORMACIÓN GENERAL DE LA ENTIDAD

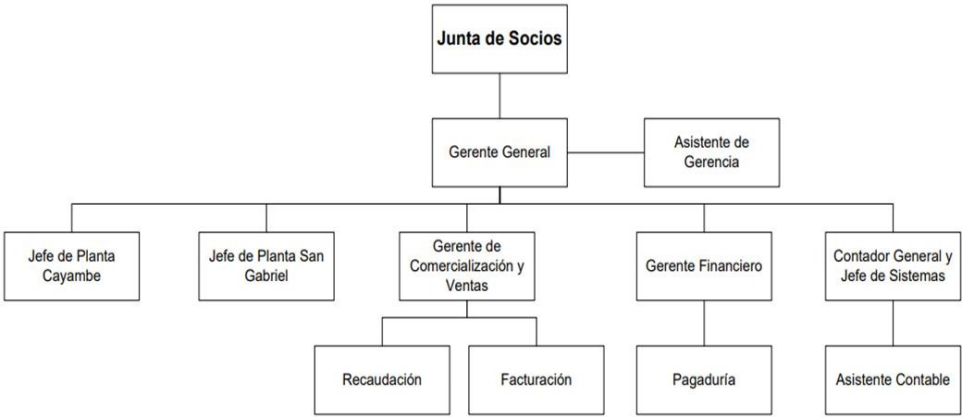
MISIÓN:

Productos Lácteos González es una industria dedicada a la elaboración y comercialización de productos lácteos artesanales especializada en quesos maduros, frescos y parmesanos, manteniendo características de origen y calidad exigidas por el mercado, asegurando una relación personal, justa y transparente con nuestros clientes, proveedores, la comunidad y el medio ambiente.

VISIÓN:

Alcanzar hasta el año 2020 el crecimiento sustentable de productos lácteos a nivel nacional e internacional, aprovechando su experiencia y armonía organizacional, que sirvan de base para la formación de un grupo Institución rial y familiar que impulse iniciativas para mejorar las condiciones nutricionales, culturales de educación y medio ambiente tanto para sus miembros como para la comunidad, sus clientes y proveedores. Alcanzar hasta el año 2020 el crecimiento sustentable de productos lácteos a nivel nacional e internacional, aprovechando su experiencia y armonía organizacional, que sirvan de base para la formación de un grupo Institución rial y familiar que impulse iniciativas para mejorar las condiciones nutricionales, culturales de educación y medio ambiente tanto para sus miembros como para la comunidad, sus clientes y proveedores.

ESTRUCTURA ORGÁNICA



ELABORADO POR: APR	FECHA: 13/02/2021
REVISADO POR: WGY	FECHA: 13/02/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
PROGRAMA DE PLANIFICACIÓN PRELIMINAR

OBJETIVO: Recabar información del personal de la entidad mediante la aplicación de entrevistas que permitan conocer el departamento contable.

No	PROCEDIMIENTO	P/T	REALIZADO POR	FECHA
1	Elabore el programa de planificación preliminar	PP	APR	15/1/2021
2	Realice la entrevista a la persona encargada del departamento de tecnología e información	E	WGY	20/1/2021

ELABORADO POR: APR	FECHA: 15/02/2021
REVISADO POR: WGY	FECHA: 15/02/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
ENTREVISTA

ENTE: Productos Lácteos Gonzáles CÍA. LTDA.
GOBIERNO AUTÓNOMO
DESCENTRALIZADO
PROVINCIAL DE PASTAZA

AREA: Contable

TIPO DE EXAMEN: Auditoría Informática

Entrevista dirigida al encargado de la unidad de tecnología e información

---

1. ¿Cree Usted que la ejecución de una Auditoría Informática en el departamento, mejorará el manejo de recursos informáticos?
Si, ya que mediante la aplicación de una auditoría se puede conocer las debilidades del departamento.

2. ¿Cuenta con un plan de mantenimiento para los recursos de la Unidad de TICs?
Existe un plan de mantenimiento, sin embargo, no se cumple con el mismo.

3. ¿Se ha establecido políticas de uso y acceso al software de la institución para su correcto uso?
Las políticas de uso están establecidas, sin embargo, no se cumplen.

4. ¿Cuál es la facilidad de operación que tiene el software?
Tiene una facilidad de manejo aceptable.

5. ¿Existen un manual o instructivos para el manejo de los programas?
Si existe un manual, sin embargo, no se utiliza.

6. ¿Con qué frecuencia se realiza el mantenimiento a las aplicaciones y programas?
No se realiza constantemente.

ELABORADO POR: APR	FECHA: 20/02/2021
REVISADO POR: WGY	FECHA: 20/02/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
PROGRAMA DE PLANIFICACIÓN ESPECÍFICA

OBJETIVO: Evaluar el control interno para establecer el correcto funcionamiento de las aplicaciones informáticas mediante la valoración de la matriz de riesgos.

N°	PROCEDIMIENTO	P/T	REALIZADO POR	FECHA
1	Elabore el programa de planificación específica	PE	APR	25/2/2021
2	Lista de verificación	LV	APR	28/2/2021
3	Realice el cuestionario de control interno	CCI	APR	3/3/2021
4	Elabore la hoja de hallazgos	HH	WGY	7/3/2021
5	Elabora el Informe	I	WGY	10/3/2021

ELABORADO POR: APR	FECHA: 25/02/2021
REVISADO POR: WGY	FECHA: 25/02/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
CUESTIONARIO DE CONTROL INTERNO
EVALUACIÓN AL SOFTWARE UTILIZADO

Nombre del Entrevistado: Carlos Lema
Cargo: Jefe de Sistemas
Entrevistador: APR
Hora: 9:30 a.m.
Lugar: Instalaciones de la Institución

PREGUNTAS	RESPUESTAS			DESCRIPCIÓN
	SI	NO	N/A	
1. ¿Tiene conocimiento de las operaciones a realizar en el área informática?	X			
2. ¿Las aplicaciones y programas utilizados facilitan el procesamiento de la información?		X		H1: Las aplicaciones y programas no facilitan el procesamiento de la información
3. ¿El mantenimiento del software es constante?		X		H2: No es constante el mantenimiento del software
4. ¿Existen manuales de manejo para el software?	X			
5. ¿Existe un técnico de asistencia?	X			

NIVEL DE CONFIANZA		
BAJO	**MODERADO**	**ALTO**
15% - 50%	51% - 75%	76% - 95%
NIVEL DE RIESGO		
ALTO	**MODERADO**	**BAJO**
85% - 50%	49% - 25%	24% - 5%

Cálculo:		Porcentaje:
Total, preguntas afirmativas	3	60%
Total, preguntas negativas	2	40%
Total, preguntas	5	

Análisis: En la evaluación al software informático, se obtuvo un nivel de confianza moderado con un porcentaje del 60% ¿. Por otra parte, existe un nivel de riesgo moderado del 40% considerado con ese porcentaje debido a que las aplicaciones y programas no permiten el procesamiento adecuado de la información y el mantenimiento del mismo no se realiza de manera permanente.

ELABORADO POR: APR	FECHA: 03/03/2021
REVISADO POR: WGY	FECHA: 03/03/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
HOJA DE HALLAZGOS

TÍTULO DEL HALLAZGO: FALTA DE ASISTENCIA AL SOFTWARE UTILIZADO

Condición:
No existe el mantenimiento constante para aplicaciones y programas utilizados en las operaciones de la entidad, lo que dificulta el procesamiento de información.

Criterio:
De acuerdo con las normas de control interno, en el párrafo 53 acerca del uso y mantenimiento de los sistemas informáticos, menciona que "*De acuerdo con lo establecido en los manuales e instructivos para el manejo y desarrollo de hardware y software, se utilizará de manera constante dichos documentos para evitar daños en las aplicaciones y programas que se utilizan en las operaciones de la Institución. En el caso de existir inconvenientes en cualquier dispositivo o programa se recurre al asistente de mantenimiento*"

Causa:
El encargado de sistemas no está cumpliendo con sus funciones para el uso adecuado del software por motivos de no utilizar el manual e instructivos que existe para el correcto manejo de la tecnología de la Institución.

Efecto:
Sin el cumplimiento correcto de las funciones del encargado de la asistencia al sistema informativo, no es posible utilizar de manera adecuada el software que dispone la Institución.

Conclusión:
El encargado de sistemas no considero los lineamientos establecidos en el manual e instructivo para uso de las aplicaciones y programas informáticos por tal motivo, no se consideraban mantenimientos de manera periódica y la eficiencia del software empezó a disminuir.

ELABORADO POR: WGY	FECHA: 07/03/2021
REVISADO POR: APR	FECHA: 07/03/2021

PRODUCTOS LÁCTEOS GONZÁLEZ CÍA. LTDA.
INFORME DE AUDITORÍA

Riobamba, 10 de marzo de 2021

Señor
Carlos Lema
Gerente General
Presente

Me permito dirigir a usted el Informe de Resultados de la auditoría practicada a las aplicaciones y programas del sistema informático de la Institución, correspondientes al periodo 2020.

El examen realizado fue sobre la evaluación al software utilizado por los usuarios, con el fin de determinar falencias en el uso del software.

En el presente informe encontrará con los respectivos hallazgos más significativos. Basadas en la revisión de los hallazgos, se ha redactado la recomendación con el fin de mejorar el sistema de control interno informático. Dichas sugerencias tienen el objetivo de mejorar potencialmente los problemas existentes.

H1: No existe el mantenimiento constante para aplicaciones y programas utilizados en las operaciones de la entidad, lo que dificulta el procesamiento de información.

Conclusión
El encargado de sistemas no considero los lineamientos establecidos en el manual e instructivo para uso de las aplicaciones y programas informáticos por tal motivo, no se consideraban mantenimientos de manera periódica y la eficiencia del software empezó a disminuir.

Recomendación
Se recomienda al encargado de sistemas revisar los manuales e instructivos con el fin de mejorar el uso de las aplicaciones y programas y de esa manera aumentar la eficiencia del software de la Institución.

Atentamente

Jefe de Equipo

ELABORADO POR: WGY	FECHA: 10/03/2021
REVISADO POR: APR	FECHA: 10/03/2021

CONCLUSIONES

Después de haber realizado una revisión bibliográfica respecto al tema principal de Auditoría Informática, se puede concluir que la evaluación que se realiza en esta auditoría no difiere en un cien por ciento de las auditoría clásicos como son: financieras o de gestión, debido a que sus fundamentos básicos siguen un mismo camino pero con la diferencia del hecho a evaluar debido a que este va a estar dirigido al área de sistemas o informáticas, a sus funciones, procesos, infraestructura, seguridad, entre otro aspecto que esté vinculado con el manejo de los recursos informáticos.

Se puede concluir por otra parte que en cuento al sistema de control interno que debe existir dentro de la Institución, se evalúan diferentes procesos, funciones o recursos dependiendo del trabajo que se esté realizando, cada área funcional debe tener sus propios controles vigentes y acordes a reglamento internos.

BIBLIOGRAFÍA

1) Academia de administración y sociales. (2021). *Auditoría Informática.* Universidad Auntónoma del Estado de Hidalgo.
2) AEC.(2018).*RevistaCalidad*.ObtenidodeRevistaCalidad: https://www.aec.es/web/guest/centro-conocimiento/coso
3) Aguirre, J. d. (2005). *Auditoría en Informática.* Méxici: Universidad Autonoma de México.
4) Albarrá, S., Pérez, J., & Slagado, M. (24 de Noviembre de 2017). *Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares.* Obtenidode
5) https://ideasencienciasingenieria.uaemex.mx/article/download/1459 1/10992/
6) Alfonso, Y., Blanco, B., & Loy, L. (2012). Auditoría con Informática a sistemas contables . *Revista de arquitectura e ingeniería*, 1-14.
7) Arens, Randal y Mark. (2007). *Auditoría un enfoque integral* (Decimoprimera edición ed.). México: PEARSON EDUCACIÓN,.
8) Barrera, G. (2015). *Componentes y principios del COSO.* Obtenido de https://actualicese.com/componentes-y-principios-del-informe-coso/
9) Bertani et. al, . (2014). *Uncu*. Obtenido de Uncu: https://bdigital.uncu.edu.ar/objetos_digitales/6694/bertanipolesellos ancheztroil a-tesisfce.pdf
10) Biable Management, (2016). *B-able.* Obtenido de https://docs.supersalud.gov.co/PortalWeb/planeacion/Administracion SIG/GSD E01.pdf
11) Blanco, L. (2008). *Auditoría y sisemas informáticos.* Editorial Felix Varela . Obtenido de https://elibro.net/es/ereader/espoch/71229?page=9
12) Cadena,L.(6deEnerode2011).*Auditool.*Obtenidode https://www.auditool.org/blog/control-interno/292-la-comunicacion-y-la- informacion-como-componentes-del-control-interno
13) Chacón,F.(2014).*SistemasInformaticos.*Obtenidode https://www.preparadores.eu/temamuestra/PTecnicos/PComerciales.pdf
14) Chicano, E. (2015). *Auditoría de seguridad informática.* IC Editoral. Obtenido de https://elibro.net/es/ereader/espoch/44136
15) Coronel, K. (2012). *Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro y Crédito "Fortuna" aplicando el marco de trabajo COBIT.* Loja: Universidad Técnica

Particular de Loja.
16) Correa, J., Pérez, H., & Martínez, A. (2016). Virus Informáticos. *Ciencia y tecnología*, 54-55. doi:https://www.redalyc.org/pdf/944/94403112.pdf
17) Dona,D.(2015).*Introducciónalossistemasinformáticos.*Obtenidode https://www.danieldona.com/informatica%20basica/2%20sistemas%20inform aticos.pdf
18) EAE Business School. (2020). *EAE Business School*. Obtenido de EAE Business School:https://retos-directivos.eae.es/conoces-los-principales-tipos-de- auditoria-que-existen/
19) ESAN.(25de01de2019).*conexionesan*.Obtenidodeconexionesan: https://www.esan.edu.pe/apuntes-Institucionales/2019/01/coso-ii-los- sistemas-para-el-control-interno/
20) Galaz,YamazaquiyRuiz.(2015).*Deloitte*.ObtenidodeDeloitte: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO- Sesion1.pdf
21) Governance Institute COBIT. (6 de Octubre de 2017). *Marco Referencial.* Obtenido de http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03Marco Referenci al.pdf
22) Gualsaquí, J. (2013). *Repositorio Pontificia Universidad Católica del Ecuador.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/6078/T-PUCE-6320.pdf?sequence=1
23) Guevara, M., Recalde, T., Avilés, J., & Bravo, L. (2018). Importancia de realizar audtoría de sistemas preventiva en las Organizaciones. *Espirales revista multidisciplinaria de investigación*, 25-38.
24) Guzmán,J.(Enerode2017).*Academiasespeciales.*Obtenidode https://www.piranirisk.com/es/academia/especiales/coso-una-vision-360- grados-para-gestionar-el-riesgo
25) Hernandez,E.(1993).*AuditoríadeInformática:Unenfoquemetodológico.*
26) Universidad Autónoma de León.
27) Imbaquingo, D., Pusdá, M., & Jácome, J. (2016). *Fundamentos de Auditoría Infórmatica Basada en Riesgo.* Ibarra: Editorial UTN. doi:https://issuu.com/utnuniversity/docs/ebook-fundamentos-auditoria-informa
28) Instituto Nacional de Ciberseguridad. (s.f). Auditoría de Sistemas: Polítcas de seguridad para la PYME. *incibe*.
29) Jaramillo, J. (10 de Septiembre de 2018). *Tic. Portal.* Obtenido de https://www.ticportal.es/glosario-tic/hardware

30) La Fuente. (19 de 02 de 2016). *Wordpress*. Obtenido de Wordpress: https://fraudeinterno.wordpress.com/2016/02/19/coso-gestion-de-riesgos/
31) Landsittel,D.(2013).*ControlInterno-MarcoIntegrado.*Obtenidode https://auditoresinternos.es/uploads/media_items/coso-resumen-ejecutivo.original.pdf
32) León, V. (6 de Marzo de 2017). *Componentes de control interno.* Obtenido de https://bdigital.uncu.edu.ar/objetos_digitales/6694/bertanipolesellos ancheztroil a-tesisfce.pdf
33) Millán, Obando. (2015). *Evaluación del control interno seguún modelo COSO I en el área de bodega de la compañía TECNOMILLAN S.A. en el año 2014.* Guayaquil.Obtenidode https://dspace.ups.edu.ec/bitstream/123456789/9985/1/UPS-GT001114.pdf
34) Mora, E., León, V., & Huilcapi, M. (26 de Febrero de 2011). *El modelo COBIT 5 para auditoríayelcontroldelossistemasdeinformación.*Obtenido de https://repositorio.pucesa.edu.ec/bitstream/123456789/2355/1/Modelo%20Co bit.pdf
35) Moreno, J., & Serrano, J. (2014). *Fundamentos de Hardware.* Madrid: Editorial RA- MA.Obtenidode https://elibro.net/es/ereader/espoch/62457?fs_q=hardware_____y software&pre v=fs
36) Muñoz, C. (2002). *Auditoría en sistemas computacionales.* México: Pearson Education, .
37) Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* México: Pearson Education.Obtenidodehttp://up-rid2.up.ac.pa:8080/xmlui/bitstream/handle/123456789/1352/Auditor%C3%AD a%20en%20sistemas%20computacionales.pdf?sequence=1
38) Normas de Control Interno de la Contraloría General de Estado. (16 de Diciembre de 2014).*ContraloríaGeneraldelEstado.*Obtenidode https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_4 00_cge.pdf
39) Nuñez,A.(17deSeptiembrede2018).*ValoraData.*Obtenidode https://www.valoradata.com/blog/gestiona-la-informacion-con-seguridad- logica/
40) Ochoa,M.(Enerode2013).Obtenidode http://eprints.uanl.mx/3619/1/SEGURIDAD_FISICA_PREVENCION_Y_DETE CCION.pdf

41) Peréz, D. (26 de Octubre de 2017). *Sistema Informático.* Obtenido de http://www.maestrosdelweb.com/que-son-las-bases-de-datos/
42) Piattini, M. (2001). *Auditoría Informática: Un enfoque práctico.* Méxixo, D.F: ALFAOMEGA GRUPO EDITOR, S.A de C.V.
43) Pinto,M.(2019).*Alfineees.*Obtenidode http://www.mariapinto.es/alfineees/sistemas/como.htm
44) Ramos, M. (2000). *Auditiría Infirmática.* Infirmátcos Europeos Extertos.
45) Reis, L. (2015). *Fundamentos de COBIT 5.* Obtenido de cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI5.pdf
46) Romero, M., Figueroa, G., & Vera, D. (2018). *Introducción a la seguridad informática y el ánilis de vulnerabilidad.* Mdrid: Editorial Área de Innovación y Desarrollo,S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46
47) Sánchez. (2006). *Auditoría de estados financieros.* México: Pearson Education, .
48) Villareal, V. (2016). *Folleto del Curso de Auditoría de Redes.* Panamá: UNIVERSIDAD TECNOLÓGICA DE PANAMÁ.

AUTORES

Alberto Patricio Robalino

Licenciado en Contabilidad y Auditoría; Doctor en Contabilidad y Auditoría; Magíster en Docencia Universitaria e Investigación Educativa; Magister en Contabilidad y Auditoría; Director Administrativo Financiero JNDA; Auditor Interno/Externo calificado del sector financiero y no financiero de la Superintendencia de Economía Popular y Solidaria; Profesor auxiliar ESPOCH (2010-2011); Profesor agregado ESPOCH (2011-actualmente); Docente en la Universidad Agraria del Ecuador, sede Alausí; Docente en el Instituto Superior Técnico y Tecnológico Juan de Velasco; Presidente Colegio de Contadores de Chimborazo; Vocal Director Federación Nacional de Contadores del Ecuador; Vocal Instituto de Investigaciones Contables del Ecuador; Perito Judicial Corte Suprema de Justicia de Chimborazo (2002-2003).

Willian Geovanny Yanza Chávez

Técnico Superior en Programación de Sistemas; Tecnólogo en Programación de Sistemas; Ingeniero de Ejecución en Informática; Ingeniero en Sistemas Informáticos; Magíster en Informática Educativa; Profesor Ocasional ESPOCH (2013- Actualidad); Profesor Universidad Nacional de Chimborazo; Unidad Educativa Isabel de Godín; Unidad Educativa Simón Bolívar; Docente Instituto República Federal de Alemania.

Johana Katerine Montoya Lunavictoria

Licenciada En Ciencias De La Educación Mención Educación Básica; Licenciada En Ciencias De La Educación Especialización Administración Y Docencia Intercultural Bilingüe; Ingeniero En Sistemas Informáticos; Magister En Desarrollo De La Inteligencia Y Educación; Magister En Informática Educativa; Profesor Ocasional Universidad Nacional de Chimborazo (2018-Actual); Profesor Escuela Superior Politécnica de Chimborazo.

Auditoría Informática

ISBN: 978-9942-42-606-2