Universidad Autónoma del Estado de México

Centro Universitario UAEM Valle de Chalco

Auditoría Informática para Instituciones Educativas

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

P R E S E N T A

Jesús Alberto Alva Reyes

ASESOR:
Dr. en C.E. José Luis Castillo Mendoza

Revisor:
Ing. José Antonio Villarruel Téllez

Revisor:
Mtro. Héctor Enrique Gaona Flores

VALLE DE CHALCO SOLIDARIDAD, MÉXICO FEBRERO 2023.

CENTRO UNIVERSITARIO UAEM VALLE DE CHALCO
CUVCH

AUDITORÍA INFORMÁTICA PARA INSTITUCIONES EDUCATIVAS

ÍNDICE

I. RESUMEN

Actualmente en las instituciones y negocios de cualquier tamaño sus operaciones y procedimientos dependen de los sistemas informáticos, ya que ellos pueden realizar sus operaciones de manera eficiente, para brindar mejores servicios a sus clientes y conseguir ventajas sobre sus competidores, esto da pauta a realizar un seguimiento de las organizaciones por medio de auditorías informáticas a sus sistemas informáticos.

El empleo de una auditoria informática en una institución educativa es de vital importancia, estos han derivado el establecimiento del registro adecuado de los sistemas de información, seguimiento de las políticas a seguir por los colaboradores en la evaluación de la información.

Las auditorias informáticas apoyaran al desempeño de los procesos de análisis sobre los recursos de las tecnologías de la información, para determinar si un sistema salvaguarda la integridad de los datos que se están manejando en las instituciones educativas. Se considera de importancia contar la ejecución de las auditorias informáticas en todo tipo de instituciones, esto debido a que el riesgo de fracaso que suelen tener en ocasiones es por cusa de no tener un seguimiento de la información, de los recursos, los objetivos que son llevados por los colaboradores, ya que se consideran varios aspectos que suelen ser significativos dentro de la empresa para su adecuado funcionamiento como es la eficiencia y la eficacia.

La función de la auditoria informática debe realizarse constantemente por las autoridades de las instituciones, darle el adecuado seguimiento de las salvedades que se puedan encontrar y corregirlas de acuerdo con las recomendaciones del auditor o aplicar las medidas correctivas que se hayan planeado. Las auditorias que se pueden llevar a cabo, pueden ser internas con personal con el perfil adecuado, experiencia o capacitación, puede ser también

externa por personal independiente a la institución, o mixta colaborando auditores tanto de la institución como externos.

En la investigación se procura atender los requerimientos de la revisión y el análisis que se necesitan para llevar a cabo las auditorias informáticas en instituciones educativas con las políticas necesarias, racionalidad y eficiencia que requiera cada evaluación, por mínimos que sean los rubros, áreas, lineamientos propuestos, son de suma importancia para el juicio emitido.

Con la elaboración y puesta en marcha de la auditoria informática, incorpora una oportunidad de crecimiento y confianza del servicio que se brinda la institución educativa auditada para ser mejor en cuanto a su competitividad que se requiera. Con la realización de la auditoria con los profesionales especialmente capacitados, mantiene la integridad de los datos y lleva a cabo eficazmente los fines de la institución, utilizando eficientemente el manejo de los recursos y el movimiento de la información.

Para el trabajo se emplearon técnicas de concentrado de información, entre las cual se realizó una investigación cuantitativa hacia el marco conceptual donde se buscó unificar los criterios de aplicación de la aplicación de la auditoria informática a las instituciones educativas que se requerían. La aplicación de auditorías en instituciones ayuda al fortalecimiento de la imagen pública, en optimizar las relaciones internas, el clima laboral, disminuye costos, mejora la confianza en los usuarios sobre la seguridad y control de los servicios de la tecnología de la información.

En consecuencia, de esta situación se crea la necesidad de realizar periódicamente evaluaciones a los sistemas, o también llamadas, auditorías informáticas, con las cuales se pretende identificar y evaluar los controles implantados en los sistemas y minimizar los riesgos.

II. ANTECEDENTES DE LA TEMÁTICA

Los pueblos a través de la historia muestran que conforme se expandía el comercio, pasando por el trueque en ciudades y estados, y motivados por el crecimiento en volumen y monto de sus operaciones comerciales, estos se vieron en la necesidad de establecer mecanismos de registros que les permitieran controlar sus actividades mercantiles.

A la par que esto iba evolucionando, se percataron que era necesario que alguien evaluara que sus registros, resultados, fueran correctos y veraces, entonces se vieron en la necesidad de tener alguien que verificara la veracidad y confiabilidad de las operaciones, en ese momento el acto de la auditoria hace mención Muñoz (2002).

La palabra auditoria viene del latín *auditorius* y de esta proviene auditor, que tiene la virtud de oír y revisar, examina lo ya establecido, la evaluación normal o minuciosa, lo ya hecho por otras personas, la inspección y verificación de información, para determinar una situación.

La auditoría es una disciplina expresada en conceptos, normas, técnicas procedimientos y metodologías, que tienen como objetivo examinar y evaluar determinada realidad, para emitir una opinión sobre un aspecto o la totalidad del objeto estudiado.

Andrade (1996) define la auditoría como “El examen posterior y sistemático que realiza un profesional auditor, de todas o parte de las operaciones o actividades de una entidad con el propósito de opinar sobre ellas, o de dictaminar cuando se trate de estados financieros” (p. 37).

El origen de la auditoría surge con el advenimiento de la actividad comercial y por la incapacidad de intervenir en los procesos tanto productivos como comerciales de una empresa. Por estas razones surge la necesidad de buscar personas capacitadas, de preferencia externas (imparciales), para que se desarrollen mecanismos de supervisión, vigilancia y control de los empleados que integran y desempeñan las funciones relativas a la actividad operacional de la empresa.

Así como también la información, se debe proteger ya que es el activo más preciado de cualquier organización en la actualidad, las empresas almacenan datos confidenciales sobre su negocio, documentos legales, datos de clientes, código fuente, datos de facturación, toda esta información se guarda en equipos informático y puede ser vulnerable si no se protege de forma adecuada, para evitar filtraciones o robos, se debe contar con las herramientas necesarias para protegerla correctamente (Echenique, 2009).

Una auditoría informática consiste en la revisión de un control, evaluación de los sistemas, recursos tecnológicos, instalaciones, procedimientos, hardware, software de una empresa u organización de cualquier tipo y giro, lo que hace, es asegurar la protección de la información como también lograr que los equipos funcionen de forma eficiente.

Según Aguirre (1998) la auditoría informática se refiere a la revisión, evaluación y 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 que se desarrollan y se utilizan esos recursos. La auditoría informática es el proceso de recopilar, agrupar, y evaluar evidencias para determinar si un sistema automatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

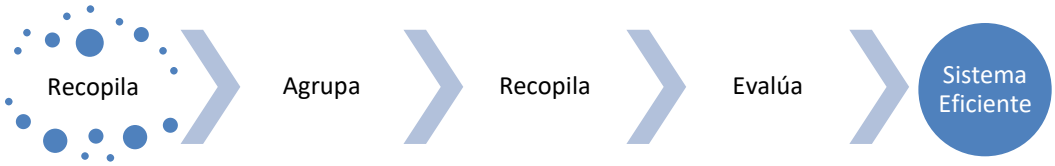

Figura 1. Proceso de auditoría. Fuente: elaboración propia.

Se hace también mención en la ISO 19011 (2018), la auditoria de sistemas es aplicable a todas las organizaciones que necesiten planear y realizar evaluaciones a los sistemas, hacer revisiones en instituciones educativa, en la que el éxito de su gestión depende, de la eficiente administración de la información que se maneje en los diferentes sectores que la integran y la tecnología de información, en la que los sistemas de gestión y contable han alcanzado un desarrollo tan notable, la participación inexcusable de la tecnología como herramienta.

La tecnología permitiéndole evolucionar al ritmo de las transformaciones incorporadas a la estructura del registro y del control interno y muy especialmente, para evaluar mediante auditorías a las tecnologías de información, los procedimientos de control específicos, dentro del ámbito de su soporte tecnológico, que, garantice una información objetiva sobre el grado de cumplimiento de las políticas y normativas establecidas por las instituciones para lograr sus objetivos (Álvarez, 2005).

Se han venido haciendo durante varios periodos, investigaciones sobre la seguridad informática, su revisión y evaluación por medio de la auditoría informática para empresas, universidades e instituciones educativas donde se localizan políticas de seguridad y diferentes métodos de detección de ataques a

sistemas de información (Chaparro, 2020; Velásquez-Rueda, 2019; Rosales-Romero, *et al.,* 2014; Montilla & Herrera, 2006).

Ahora se pasará a lo que son las instituciones educativas, se tratarán algunas consideraciones sobre la nación de institución escolar, es importante de inicio que la escuela como toda institución constituida, representa una realidad compleja, ya que en ella se concentran expectativas e intencionalidades.

Lases (2014) dice que el origen de la universidad durante la Edad Media en Europa se atribuye al afán de saber cada día más, según Aristóteles “el hombre es curioso por naturaleza” además su misma curiosidad lo lleva a descubrir lo desconocido, evolucionar y trascender, la historia de la enseñanza es la mejor de las pedagogías, ya que transmite al ser humano un proceso de constante cambio, saberes transcurridos al paso del tiempo con un sin fin de estructuras de pensamiento y argumentos que el propio hombre construye desde su realidad.

En la época de las cruzadas hubo una gran movilidad, peregrinaje y guerra nacional popular de la cristiandad unida contra los incrédulos, el imperio y el papado que solían disputarse la supremacía, Asimismo con las cruzadas, la civilización musulmana, el imperio bizantino, el desarrollo tecnológico y la producción agrícola se genera la explosión del conocimiento y por consiguiente el desarrollo de Europa en el siglo XI.

En el siglo XII con la Monarquía de los Capeto Francia se convierte en la capital y desde entonces tiene un centro que es la Escuela de París (Escuela de Notre Dame), era el claustro, la escuela maestra por excelencia; se estimula la actividad intelectual que dan origen a novedades pedagógicas y en consecuencia a la organización universitaria (Lases, 2014).

Las instituciones surgen cuando la misma evolución de las sociedades hizo notar que ya no eran suficiente la transmisión oral de las tradiciones, ni la imitación de los adultos para complementar la educación de los niños que deseaban aprender, sin embargo, un hecho fundamental en el proceso de conformación de las instituciones es el momento en que el Estado asume formalmente la dirección y el control de la educación (Escalera, 2016).

Se puede considerar la institución escolar como el espacio donde se concreta la practica educativa, no obstante, el termino espacio no solo se refiere al aspecto físico de la escuela, sino también al conjunto de elementos que determinan el acontecer de la función educativa escolarizada y no escolarizada en la educación.

Se consideran también las instituciones como un ente con influencia, ya socializa al individuo, reproduce relaciones sociales y de algún modo legítima los órdenes políticos y culturales vigentes, a la vez prepara a los estudiantes para adaptarse y funcionar de manera acorde a las necesidades de los tiempos.

Menciona Robles (1977) en la Colonia la medicina indígena era transcendental, el español colonizador se sorprendía por las habilidades de aprendizaje del indígena mexicano que con maestría refinada cuestionaba en perfecto latín. El colegio de Santa Cruz Tlatelolco, fundado en 1536 con el apoyo del virrey Antonio de Mendoza se manifestaba como el esfuerzo de los religiosos españoles por formar futuros educadores.

La primera cédula de creación de la Real y Pontificia Universidad de México fue firmada en 1547 conforme a las constituciones de la Universidad de Salamanca, gracias al esfuerzo constante del virrey Antonio de Mendoza, la población criolla disfruto de una institución de enseñanza que, en pocos años,

alcanza la fama en Europa como vanguardia de la educación superior en América desde 1553.

Durante casi 200 años el prestigio de la Real y Pontifica Universidad se afianzo sólidamente como un centro del saber de intelectuales distinguidos, en el siglo XVII la Nueva España contaba con una generación de teólogos, filósofos, poetas, literarios, educados en su propia tierra (Robles, 1977).

Al igual que la historia general del país, el desarrollo del sistema educativo se ha venido conformando bajo la influencia evolutiva de las faces determinantes de la estructura social y económica, desde la época de la Colonia hasta nuestros días, se observa que la enseñanza superior, especialmente, refleja las características del modo de producción imperante, en cada periodo histórico se distingue una corriente del pensamiento social y filosófico acorde a la distribución del poder y la riqueza.

El común detonador que se pude observar del sistema educativo en México es la demanda de las clases por ser instruidas, una sociedad cuya lucha fundamental fue lograr la separación de la Iglesia del Estado, movilizando los recursos en la libertad de enseñar.

Lases (2014) y Mendieta (1980) en cuanto a la Universidad Nacional Autónoma de México, mencionan que la Real y Pontificia Universidad de México no surgió espontáneamente, sino que fue reasentada, desde 1536 que fue solicitada por Fray Juan de Zumárraga, y fue hasta 1595 que obtuvo la Bula del Papa Clemente VIII para su fundación; el mayor contingente juvenil de la clase media eran clérigos españoles, criollos y mestizos, la concentración indígena quedó marginada.

Se puede intuir actualmente que, si México desea una superación en todos los aspectos, debe constituirse como una nación independiente y moderna, así

se debe considerar que no tiene otra vía a seguir, que la educación en todos sus niveles para poder trascender.

La importancia de la auditoría en el campo educativo permitirá verificar que se cumpla con el objetivo para el cual han sido creadas las instituciones. En esta investigación solo se enfoca a la auditoría informática.

III. IMPORTANCIA DEL PROBLEMA

Las instituciones deben hacer auditorias informáticas porque está en un proceso de revisión de los sistemas de información que maneja, ya que ayuda a las instituciones a identificar mal versaciones, hallazgos o riesgos que puedan afectar la base de datos que manejan.

La auditoría informática representa el mecanismo que tiene cualquier especialista en la Gestión de Tecnologías de Información para (GTI) verificar y dar seguimiento al buen desempeño de la función de la Administración de TI, mediante la generación de auditorías enfocadas tanto a la gestión y seguridad de la información, desempeño de la infraestructura de, así como el control de la planeación estratégica informática UAEMéx (2018).

Con la llegada de las computadoras y sistemas automatizados en el contexto laboral en las instituciones, va surgiendo la necesidad de darle seguimiento al manejo de los datos que se generan en las bases, controles y procesos para su correcto funcionamiento por medio de una revisión o examen de auditoría.

Según Piattini (2001) las tecnologías de la información (TI) están adquiriendo cada vez más relevancia y su aplicación puede llevarse a cabo en diversos entes económicos, la auditoría informática planea métodos y procedimientos de control de sistemas de información que son válidos para cualquier tamaño y tipo de empresa.

La información que manejan las instituciones educativas es de suma importancia, con ella se lleva parte importante de los datos de los alumnos, su historial, registros anteriores y presentes, los informes que se manejan en

determinados momentos pueden quedar vulnerables o manejadas inadecuadamente, es por eso por lo que hay que examinarlas en determinados periodos.

La evaluación por medio de la auditoría informática es un aspecto importante si se investigan los dispositivos del software y hardware de alguna institución, pudiendo ofreces herramientas para estar seguros de los sistemas de un modo que determinen, si en algún momento se está haciendo algo mal, brindando a las instituciones educativas llevar mejor control de sus procesos y servicios.

La aplicación de una auditoría informática servirá para que todas las personas que laboran en las instituciones desarrollando sus actividades en los diferentes procesos, áreas o departamentos, conozcan, si se están llevando adecuadamente las actividades, las reglas, las políticas, los procesos, procedimientos establecidos, para un adecuado manejo de las cuentas y rubros de operación.

Se hace hincapié que actualmente la auditoria de los sistemas de información se define como cualquier otra auditoria que debe hacerse por igual a empresas e instituciones, que abarque la revisión y evaluación de todo lo que involucre aspectos automáticos, informáticos de procesamiento de datos y las interfaces correspondientes.

IV. PLANTEAMIENTO DEL PROBLEMA

La información en estos días se encuentra sujeta a daños y negligencias imprevistas, en ocasiones suelen suceder por no darle seguimiento a lo ya establecido en los sistemas, en errores de operación, daños en infraestructuras servicios, por lo que se deben programar exámenes o revisiones en estos rubros, por mencionar algunos (Paredes, 2013).

La auditoría de sistemas se ha ido convirtiendo en una herramienta que va evolucionando a través del tiempo, está en busca de mejorar cada día o periodo la seguridad, ya que esta es fundamental, así como la eficiencia y economía de los procedimientos los sistemas de información (SI).

En ocasiones se piensa que la auditoría es parte o se subdivide de la contabilidad, esto no es así, es independiente porque cuenta con personal técnico y especializado en el área de sistemas, para su tener un su grado de valides en la aplicación de la revisión de los sistemas.

Se pretende que, en la aplicación de la auditoría de sistemas, se toma conciencia de la vulnerabilidad, de minimizar riesgos de los centros de procesos de datos de las instituciones al analizar, examinar y dar el punto de vista de los rubros de las tecnologías de la información (TI) que se examinen.

El hecho de que la información se guarde en discos magnéticos, memorias, en las nubes, y que esta información contenga los datos principales de las cuentas de los integrantes de las instituciones, hace posible que alguien con los suficientes conocimientos y experiencia, en el manejo, de los sistemas pueda modificar la información ya sea a favor suyo o de terceros, o errores

pequeños no intencionales, produzcan efectos desastrosos que afecten la base de datos que tengan registrados.

Ante esta situación, se entiende y se establece que la función de la auditoría debe prestar especial atención a lo que pase en el desarrollo y la explotación de sistemas computarizados, aplicando en algunos casos técnicas básicas como separación de funciones y responsabilidades, así como la implementación de controles que permitan detectar lo más rápidamente que se pueda un fraude o un error y tomar las respectivas medidas necesarias para corregirlo, cuando se detecte alguna salvedad o una desviación (Haro & Sánchez, 2006).

La auditoría en los SI es de importancia en las instituciones de todo tipo, que cuente con la infraestructura computacional, que manejen su base de datos en las áreas que integran una institución, para salvaguardar los controles de sistemas, sus equipos de cómputo, su eficiencia, la seguridad, los procedimientos de informática, servicios y operaciones de TI, entre otros, para llevar un adecuado manejo, validación y funcionamiento de los sistemas de información.

De ahí que surjan las siguientes preguntas de investigación:

- ¿Qué aspectos se deben considerar en una auditoría informática para instituciones educativas?

- ¿Por qué es importante que las instituciones educativas lleven a cabo auditorias informáticas en las tecnologías de información?

- ¿De qué manera beneficiará a las instituciones el contar con un dictamen de una auditoria informática?

Para dar respuesta a las preguntas se planteó como objetivo general:

Diseñar una propuesta para elaborar auditorias informáticas de información en las instituciones educativas para conocer el comportamiento y uso de los equipos de cómputo, de los procedimientos y evaluación de los sistemas en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Y como objetivos específicos:

- Determinar los elementos que deben considerarse para el desempeño de los sistemas de información para que sean confiables y seguros.

- Especificar los aspectos de seguridad operativa que deben incluir los programas informáticos de la institución educativa.

- Elaborar los instrumentos que permitan identificar el manejo adecuado de los equipos de cómputo de la institución.

- Diseñar los materiales que deben tener sobre los procedimientos de los sistemas.

Se puede deducir que las auditorias informáticas en las instituciones educativas son instrumentos importantes en estas, ya que persiguen la mayor eficiencia y eficacia en la ejecución de los datos evaluándolos donde deben estar cada uno de los datos e información.

La hipótesis de la investigación planteada: Si se desarrollan las auditorias informáticas de los sistemas de información, entonces se tendrán las normas y procedimientos estandarizados, para que se lleve un adecuado y correcto funcionamiento de una institución educativas

V. MARCO CONCEPTUAL Y TEÓRICO

Por medio de los procesos de la globalización, el avance y desarrollo de las instituciones educativas, se han visto afectadas y se ven en la necesidad de diseñar, desarrollar, actualizar e implementar programas de revisiones sobre los métodos y procedimientos a la ejecución operativa mediante auditorias informáticas.

Se presenta a continuación, el sustento que se llevó acabó para el desarrollo de la investigación, se documenta los conceptos y definiciones llevadas para la elaboración de auditorías informáticas en instituciones educativas.

El hecho de hacer auditorias informáticas sobre la actuación individual o colectiva dentro de las instituciones se hace cada día indispensable, ya que permite establecer parámetros de acción operativa de los colaboradores en áreas específicas que agilizan la puesta en marcha de cómo se está trabajando y si se alcanzan los objetivos planeados en los ejercicios.

5.1 Auditoria

Como es de conocimiento en lo general, el Instituto Mexicano de Contadores Públicos IMCP (2017). Asociación Civil (AC) por medio de su comisión de Normas de Auditoría realiza un trabajo continuo y aporte al seguimiento y actualización de la auditoria.

Se entiende por auditoría la revisión o evaluación de los estados financieros o de algo ya hecho, para efectos de emitir un reporte o dictamen de lo que se está examinando, pueden ser áreas y rubros en específico para cualquier tipo de organización, es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso (Martínez et al., 2012).

También la auditoría es un proceso sistemático independiente y documentado para obtener evidencias de lo revisado y evaluar de manera objetiva, con el fin de determinar la extensión en que se cumple con los criterios examinados.

La auditoría en general es un examen sistemático de los estados financieros, registros y operaciones con la finalidad de determinar si están de acuerdo con las normas de información financiera, con las políticas establecidas por la dirección y con cualquier otro tipo de exigencias legales o voluntariamente adoptadas, la auditoría tiene por objeto también averiguar la exactitud integridad y autenticidad de los expedientes y demás documentos administrativos contables presentado por la dirección, así como sugerir las mejoras administrativas contables, financieras y sistemáticas que procedan (Madariaga, 2004).

Uno más de los objetivos de la auditoría es revisar la forma en la cual las transacciones y situaciones que afectan a la empresa han sido medidas y comunicadas, asimismo es tarea de la auditoría determinar la adecuación y fiabilidad que los sistemas de información, de las políticas y procedimientos operativos existentes en las divisiones o departamentos de la empresa.

El campo de la auditoría cubre todas las funciones de revisión, en la mayoría de los casos utiliza la contabilidad como el vehículo más idóneo para realizar las revisiones de una organización, sin embargo, la visión de auditoría no es exclusiva de los estados financieros, sino que debe dar la visión de la empresa en su conjunto.

La auditoría está orientada a presentar un juicio completo de la empresa u organización, lo que abarcaría además del aspecto contable financiero, la forma de dirigir la empresa, la capacidad para crear y lanzar nuevos productos, así como la implantación actual y futura en los mercados y como la implantación de las tecnologías de la información donde sea requerido de acuerdo con los avances que vayan dando en el contexto (Solís, 2002).

5.2 Enfoques de la auditoria

Según el objetivo nos menciona Madariaga (2004) el tipo de empresa u organización que se persiga, o en función de la importancia que se dé a ciertos aspectos, las auditorías pueden ser o dirigidas a diferentes enfoques como lo pueden ser, las financieras, verificativas, operativas o especiales, entre otras.

5.2.1 Auditoria Financiera: La auditoría financiera es una revisión de los estados financieros similar a la auditoría externa, su objetivo este expresar una opinión sobre si las cifras del balance y la cuenta de resultados presentan razonablemente la situación de la auditoría, de acuerdo con las normas de información financiera.

5.2.2 Auditoria verificativa o de procedimientos: El objetivo de la auditoría verificativa es la revisión y puesta en práctica de los sistemas políticas y procedimientos establecidos por la dirección.

5.2.3 Auditoria operativa: No es una auditoría distinta caracterizada por programas y técnicas especiales, sino más bien una actitud mental del auditor, se trata del control sobre las actividades desarrolladas por una sociedad, es un enfoque de la auditoría encaminado a examinar los datos como medio para mejorar las actividades de la empresa.

5.2.4 Auditoria especial: La dirección general u órgano competente fija en concreto el objetivo y el alcance del trabajo de auditoría.

5.2.5 Auditoria de gestión: Tiene por misión conocer sí las principales decisiones de gestión en la empresa han sido tomadas de una forma consistente, entre otros aspectos estudia si las informaciones existentes son suficientes y óptimas para apoyar la decisión y si los procesos de estudio son razonables.

5.2.6 Auditoria organizativa: En el campo de la aplicación de la auditoría organizativa entraría el análisis de la educación de los procedimientos establecidos y de las funciones distribuidas físicamente según las necesidades y problemas de la empresa, cuando diferentes tareas técnicas son ejecutadas por partes diferentes, parece obvio la necesidad de establecer una delimitación para cada tarea y ejercer un control , seguimiento, riguroso de su acabado, igualmente importante es poder definir bien las responsabilidades dadas las consecuencias que cualquier dificultad parcial puede ejercer sobre el normal desarrollo de un proyecto (Martínez *et al.,* 2012).

5.2.7 Auditoria física: Abarca el activo informático registrado en el inventario de la entidad auditada, se proporciona evidencia del nivel de la seguridad física en el ámbito en el que se va a desarrollar la actividad, no limitándose a comprobar

que existen los medios físicos, sino también su funcionalidad, racionalidad y seguridad, la seguridad física garantiza la integridad de los activos humanos, lógicos y materiales en un centro de procesamiento de información.

5.2.7 Auditoria ofimática: Son los programas o aplicaciones que en conjunto sirven de herramienta para generar, procesar, almacenar, recuperar, comunicar y presentar la información en un lugar de trabajo, así como de forma doméstica, el software de ofimática comprende una serie de aplicaciones que se distribuyen de forma conjunta para así mismo ser empleadas simultáneamente en diversos sistemas, de estos se pueden mencionar los siguientes como, por ejemplo; hojas de cálculo, procesadores de texto, presentadores de ideas, gráficos, etc. (Castro, 2012).

Existen características que se pueden analizar de los entornos ofimáticos, como la distribución de las aplicaciones por los diferentes departamentos de la organización en lugar de centralizarse en una única ubicación, y el traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios finales no dedicados profesionalmente a la informática, quienes pueden no comprender de un modo adecuado la importancia de éstos y la forma de realizarlos.

5.3 Elementos de la auditoria

La auditoría como todo proceso de trabajo, también se divide en varios elementos para su adecuada aplicación, detallando cada uno de sus elementos para poder controlar e ir trabajando en orden y así entregar una evaluación de los elementos que se van a examinar.

5.3.1 Programa de auditoria

Es el conjunto de una o más auditorías planificadas para un período de tiempo determinado y dirigido hacia un propósito específico

5.3.2 Planificación

Indica Cervantes (2002) la planificación puede ser la parte más importante a la hora de realizar la auditoría, ya que si se falla a la hora de establecer la planificación seguramente está condenada al fracaso, la planificación debe incluir diversos elementos, como pueden ser:

- Tener preparados todos los procedimientos necesarios y el programa de auditoría.

- Preparar un esquema claro y la agenda de la auditoría, para conocer las fechas en las que se darán todos los acontecimientos.

- Definición de las tareas y las responsabilidades de todo el proceso de auditoría.

- Recopilar y resumir la información ofrecida por el auditor como centro de control del negocio, los esquemas de cómo está organizada la empresa para conocer la situación de cada zona y otras informaciones necesarias.

5.3.3 Criterios de auditoria

Conjunto de normas, políticas, procedimientos o requisitos utilizados como referencia, frente a la cual se podrá comparar la evidencia de la auditoría o evidencia objetiva, esta tiene que ser verificable para poder analizarla y hacer la observación correspondiente (Oviedo, 2018).

La auditoría tiene entre otras cosas sus objetivos, uno de ellos es determinar el grado de conformidad del sistema de gestión que se va a auditar con los criterios de auditoría, así que, previamente, se deben determinar cuáles son dichos criterios, mencionar, cuál va a ser la referencia frente a la que determinar e identificar posibles áreas de deficiencias que pueden representar un riesgo para el desempeño del sistema ISO 19011, define, criterios de auditoría como el conjunto de requisitos usados como referencia frente a la cual se compara la evidencia objetiva, los criterios de auditoría determinan, entre otros factores, la competencia del auditor, los métodos de auditoría seleccionados para llevarla a cabo y la extensión de la auditoría.

5.3.4 Hallazgos de auditoria

Seles conoce como los resultados de la evaluación de las evidencias de la auditoría recopiladas frente a los criterios evaluados, es el ejercicio de la función de control, cuyo objeto es la vigilancia de la gestión para determinar el grado de eficacia, eficiencia, economía, equidad y sostenibilidad en el recaudo y aplicación de los recursos, se lleva a cabo mediante la aplicación concurrente de distintos sistemas de control, a través de auditorías de regularidad o cumplimiento y auditorías de desempeño (Restrepo-Medina, 2018).

Se dice también que son aquellas situaciones que revisten importancia relativa, para la actividad u operación objeto de examen del auditor, que requiere

ser documentada y debidamente comprobada, que va a ser de utilidad para exponer o emitir criterio, en el respectivo documento o informe de auditoría.

5.3.5 Conclusiones de auditoria

Menciona Pallerola (2014) una vez realizada y cerrada la revisión de un área en concreto, el auditor deberá redactar sus conclusiones con las debilidades que pudieran haberse encontrado, por si pudieran tener una mención expresa en su informe de auditoría, toda información debe ser siempre su supervisada por otra persona, con ello se contribuirá a la seguridad y la consistencia de las conclusiones, las cuales pueden o no confirmarse en dicha segunda revisión.

Siempre debe existir una redacción de las conclusiones y las pruebas tanto documentales que la soportan cómo en la revisión de los resultados debe estar comprendida la supervisión de todo el programa de trabajo y la exactitud de los papeles de trabajo que son la base fundamental de las conclusiones alcanzadas.

5.4 Auditoria Informática

La auditoría informática es un proceso que es llevado a cabo por profesionales especialmente capacitados para el efecto, y consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas (Cervantes, 2002).

Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades,

duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes (Alfonso *et al.,* 2012).

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de estos, los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia (Solís, 2002).

También es considerado un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia y la rentabilidad del servicio, o del sistema, que resultan auditados.

El examen que realiza una auditoría informática según Cervantes (2002) abarca una serie de controles, verificaciones, juicios, entre otros, para concluir en un conjunto de recomendaciones y un plan de acción. Es la elaboración de este plan de acción lo que diferencia la auditoría informática de lo que por lo visto hasta ahora podría ser una auditoría de gestión.

La auditoría tradicional concluye emitiendo un juicio del estado de todo aquello que sea verificado, la auditoría informática avanza un paso más y se atreve a elaborar un plan de actuación, cómo lo podemos observar en el siguiente cuadro comparativo (tabla 1) entre auditoría de control y control de gestión.

Tabla 1. Cuadro comparativo entre auditoría de control y de gestión.

	Auditoria de control	Control de gestión
¿Qué hace?	Examina, enjuicia y recomienda	Establece dispositivos de seguridad
¿Cuándo se hace?	Dando un corte en el calendario	Permanente mente
¿Cómo se hace?	Desmonta los mecanismos	Vigila y lleva acabó acciones correctivas

Fuente: Rivas, 2000.

5.4.1 Objetivo de la auditoria informática

Madariaga (2004) menciona en su contenido que se pueden aludir algunos de los objetivos de la auditoria Informática para las instituciones, empresas u organizaciones, los cuales pueden ser los siguientes y poderlos tomar en cuenta:

- El control de la función informática.
- El análisis de la eficiencia de los Sistemas Informáticos.
- La verificación del cumplimiento de la Normativa en este ámbito.
- La revisión de la eficaz gestión de los recursos informáticos.

La auditoría informática es un proceso de relevante importancia y sirve para mejorar ciertas características en las organizaciones como las siguientes que se mencionan:

- Desempeño.
- Fiabilidad.
- Eficacia.

- Rentabilidad.
- Seguridad.
- Privacidad.

La auditoría informática como proceso de evaluación y revisión de lo ya establecido, se puede desarrollar en alguna o combinación de las siguientes áreas:

- Gobierno corporativo.
- Administración del Ciclo de vida de los sistemas.
- Servicio de Entrega y Soporte.
- Protección y Seguridad.
- Planes de continuidad y Recuperación de desastres.

Resulta importante conocer los objetivos a los que se debe concentrar el auditor informático, para no desviarse a lo ya planeado y programado en los exámenes de auditoría.

5.4.2 Tipos de auditoría informática

Como es sabido dice Madariaga (2004) también los procesos o la auditoría informática se pueden clasificar en diversos tipos, de los culés se mencionan brevemente para su conocimiento a continuación:

- **Auditoria de la gestión**: La contratación de bienes y servicios, documentación de los programas, etc.

- **Auditoria legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

- **Auditoria de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

- **Auditoria de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos, la difusión de los Sistemas Administradores de Bases de Datos (DBMS – Data base Management Systems) y la identificación de los datos como uno de los recursos fundamentales de las empresas, ha hecho que la auditoría y control interno de esta área cobre mayor interés.

Algunos de los objetivos y técnicas de control están basados en el ciclo de vida de una BD son los siguientes:

- Estudio previo y plan de trabajo. Se debe verificar que: se ha realizado un estudio tecnológico de viabilidad en el cual se contemplen varias alternativas para alcanzar los objetivos.

- Diseño y carga. Los diseños lógicos y físicos se realicen correctamente donde se contemple restricciones oportunas, especificaciones de almacenamiento y cuestiones relativas a la seguridad.

- Explotación y mantenimiento. Donde se establecen procedimientos de explotación y mantenimiento que aseguran que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas se modifica sólo con la autorización adecuada.

- Revisión post-implantación. Donde los resultados esperados satisfacen las necesidades del usuario tanto los costos y beneficios coinciden con los previstos.

Conocer estos objetivos y técnicas, son de relevancia para las revisiones en las auditorías informáticas para expresar una adecuada opinión de este apartado.

- **Auditoria de la seguridad**: Es el área principal para auditar, hasta el punto
  de que en algunas entidades se creó inicialmente la función de auditoría informática para revisar la seguridad, la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnología de información y comunicaciones, por lo que el impacto de las fallas, los accesos no autorizados, la revelación de la información, entre otros problemas, tienen un impacto mayor.

- **Auditoria de la seguridad física:** Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

- **Auditoria de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.

- **Auditoria de las comunicaciones**: Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.

- **Auditoria de la seguridad en producción**: Frente a errores, accidentes y fraudes.

- **Auditoria de Redes:** Se encarga de una serie de mecanismos mediante los cuales se, pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización eficiente y segura de la información, en primera instancia se inicia una gestión responsable de la seguridad es identificar la estructura física (hardware, topología) y lógica (software, aplicaciones) del sistema (sea un equipo, red, intranet, extranet), y hacerle un análisis de la vulnerabilidad, para saber en qué grado de exposición se encuentran la entidades.

Es importante conocer el tipo de auditorías informáticas para saber en qué apartados se va a hacer el examen y enfocarnos a esos rubros con las herramientas y planes necesarios que se deben formular.

5.4.3 Pruebas para efectuar una auditoría informática

Hace mención Cervantes (2002) que cuando se tenga presente o se solicite una auditoría informática interna, externa o mixta podrá ayudarse de las siguientes pruebas para asegurarse de lo que se examinó y poder emitir una buena evidencia de auditoría:

- **Pruebas sustantivas**: Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

- **Pruebas de cumplimiento**: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

5.4.4 Herramientas para efectuar una auditoría informática

Menciona Martínez *et al.* (2012) para poder realizar la evaluación correspondiente de la auditoría informática, se podrá auxiliar de algunas de las principales herramientas que a continuación se mencionan:

- Observación.
- Realización de cuestionarios.
- Entrevistas a auditados y no auditados.
- Muestreo estadístico (Trazas y/o huellas).
- Flujogramas.
- Listas de chequeo (checklist).
- Mapas conceptuales.
- Inventario.

Martínez *et al.* (2012) mencionan en su artículo que existe una amplia variedad de paquetes de programas orientados hacia la práctica de auditorías, para poder apoyar al auditor en la realización de pruebas sustanciales y la verificación de las operaciones que son objeto del examen.

5.4.5 Fases para efectuar una auditoría informática

También como los demás tipos de auditoría, dice Delgado (1998) la auditoria informática cuenta con diferentes fases para llevarla a cabo los exámenes correspondientes y emitir una adecuada opinión, las cuales se mencionarán a continuación:

- Fase I: Conocimientos del Sistema.
    - Aspectos Legales y Políticas Internas.
    - Características del Sistema Operativo.
    - Características de la aplicación de computadora.
- Fase II: Análisis de transacciones y recursos.
    - Definición de transacciones
    - Análisis de las transacciones
    - Análisis de los recursos
    - Relación entre transacciones y recursos
- Fase III: Análisis de riesgos y amenazas
    - Identificación de riesgos
    - Identificación de amenazas
    - Relación entre recursos/amenazas/riesgos
- Fase IV: Análisis de controles
    - Codificación de controles
    - Relación entre controles
    - Análisis de cobertura de los controles requeridos
- Fase V: Evaluación de controles
    - Objetivos de la evaluación
    - Plan de pruebas de los controles
    - Pruebas de controles
    - Análisis de resultados de las pruebas
    -

- Fase VI: El informe de auditoria

    - Informe detallado de recomendaciones
    - Evaluación de las respuestas
    - Informe resumen para la alta gerencia

- Fase VII: Seguimiento de las Recomendaciones

    - Informes de seguimiento
    - Evaluación de los controles implantados

Las fases de una auditoría informática o como también se les pueden llamar etapas, son la serie de pasos importantes y relevantes para la evaluación de la institución ya que estas proporcionan información valiosa para la dirección, para la adecuada toma de decisiones y la mejora continua, basado en Delgado (1998).

5.4.6 Normas técnicas y procedimientos de auditoría informática

Al realizar una auditoría informática, se requieren de la aplicación y ayuda de varias herramientas, así como de técnicas y procedimientos para llevar a cabo esta en la institución que requiera de una auditoría informática, es de importancia mencionar que para el auditor en informática conocer los productos de software que han sido creados para apoyar su función aparte de los componentes de la propia computadora resulta esencial, esto por razones económicas y para facilitar el manejo de la información (IMCP, 2017).

El auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad, de su experiencia, su capacitación y perfil en el que le sea requerido para su desempeño.

El auditor adquiere responsabilidades, no solamente con la persona que directamente contratan sus servicios, sino con un número de personas desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones.

La auditoría informática no es una actividad meramente mecánica, que implique la aplicación de ciertos procedimientos cuyos resultados e informes que entregara a la institución, una vez llevados a cabo son de carácter indudable, la auditoria requiere el ejercicio de un juicio profesional, sólido, maduro, para juzgar los procedimientos que deben seguirse y estimar los resultados obtenidos (Blanco, 2015).

Las normas de auditoria informática, según se describe en IMCP (2017) son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña ya la información que rinde como resultado de este trabajo.

Las normas de auditoria se clasifican en:

- Normas personales: son cualidades que el auditor debe tener para ejercer sin dolo una auditoria, basados en sus conocimientos profesionales, así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.

- Normas de ejecución del trabajo: son la planificación de los métodos y procedimientos, tanto como papeles de trabajo a aplicar dentro de la auditoria.

- Normas de información: son el resultado que el auditor debe entregar a los interesados para que se den cuenta de su trabajo, también es conocido como informe o dictamen.

Las técnicas de auditoría se dice que son, como los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias.

Menciona Solís (2002) al aplicar su conocimiento adquirido a lo largo del tiempo y experiencia que tenga el auditor, podrá conocer los datos e información de la empresa u organización a ser auditada, que pudieran necesitar una mayor atención para su evaluación de ciertas áreas o rubros.

Las técnicas de auditoria se clasifican en:

- Estudio General.
- Análisis.
- Inspección.
- Confirmación.
- Investigación.
- Declaración.
- Certificación.
- Observación.
- Cálculo.

Las técnicas y procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas, así como los procedimientos de auditoría tienen suma importancia para el auditor basado en Blanco (2015).

A los procedimientos**,** se les conoce como el conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que nos sirven para fundamentar la opinión del auditor dentro de una auditoría, se les dan el nombre de procedimientos de auditoría en informática.

La combinación de dos o más procedimientos, derivan en programas de auditoría, y al conjunto de programas de auditoría se le denomina plan de auditoría, el cual servirá al auditor para llevar una estrategia y organización de la propia auditoría.

El auditor no puede obtener el conocimiento que necesita de forma inmediata para sustentar su opinión en una sola prueba, debe hacer uso de su experiencia, así como es necesario examinar los hechos, mediante varias técnicas de aplicación simultánea.

En General los procedimientos de auditoría permiten:

- Obtener conocimientos del control interno.
- Analizar las características del control interno.
- Verificar los resultados de control interno.
- Fundamentar conclusiones de la auditoría.

5.4.7 Normas técnicas y procedimientos de auditoría informática

Dentro del trabajo de la auditoría informática se desarrollan diversos tipos de técnicas y procedimientos de auditoría, de los cuales destacan el análisis de datos, ya que para las organizaciones el conjunto de datos o información son de tal importancia que es necesario verificarlos y comprobarlos, así también tiene la

misma importancia para el auditar ya que debe de utilizar diversas técnicas para el análisis de datos, basados en Solís (2002) las cuales se describen a continuación:

- **Comparación de programas**, esta técnica se emplea para efectuar una comparación de código (fuente, objeto o comandos de proceso) entre la versión de un programa en ejecución y la versión de un programa piloto que ha sido modificado en forma indebida, para encontrar diferencias.

- **Mapeo y rastreo de programas**, esta técnica emplea un software especializado que permite analizar los programas en ejecución, indicando el número de veces que cada línea de código es procesada y las de las variables de memoria que estuvieron presentes.

- **Análisis de código de programas**, se emplea para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual, en cuyo caso sólo se podría analizar el código ejecutable.

- **Datos de prueba**, se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

- **Datos de prueba integrados**, técnica muy similar a la anterior, con la diferencia de que en ésta se debe crear una entidad, falsa dentro de los sistemas de información.

- **Análisis de bitácoras**, existen varios tipos de bitácoras que pueden ser analizadas por el auditor, ya sea en forma manual o por medio de

programas especializados, tales como bitácoras de fallas del equipo, bitácoras de accesos no autorizados, bitácoras de uso de recursos, bitácoras de procesos ejecutados.

- **Simulación paralela**, técnica muy utilizada que consiste en desarrollar programas o módulos que simulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos de forma paralela e identificar diferencias entre los resultados de ambos.

5.4.8 Análisis de Datos

Menciona Solís (2002) que se desarrollan diversos tipos de técnicas y procedimientos de auditoría, de los cuales destacan el análisis de datos, para las organizaciones, el conjunto de datos o información son de tal importancia que es necesario verificarlos y comprobarlos, así también tiene la misma importancia para el auditor ya que debe de utilizar diversas técnicas para el análisis de datos, las cuales se describen a continuación:

- Comparación de programas: Esta técnica se emplea para efectuar una comparación de código, fuente, objeto o comandos de proceso, entre la versión de un programa en ejecución y la versión de un programa piloto que ha sido modificado en forma indebida, para encontrar diferencias.

- Mapeo y rastreo de programas: Esta técnica emplea un software especializado que permite analizar los programas en ejecución, indicando el número de veces que cada línea de código es procesada y las de las variables de memoria que estuvieron presentes.

- Análisis de código de programas: Se emplea para analizar los programas de una aplicación. El análisis puede efectuarse en forma manual, en cuyo caso sólo se podría analizar el código ejecutable.

- Datos de prueba: Se emplea para verificar que los procedimientos de control incluidos los programas de una aplicación funcionen correctamente. Los datos de prueba consisten en la preparación de una serie de transacciones que contienen tanto datos correctos como datos erróneos predeterminados.

- Datos de prueba integrados: Técnica muy similar a la anterior, con la diferencia de que en ésta se debe crear una entidad, falsa dentro de los sistemas de información.

- Análisis de bitácoras: Existen varios tipos de bitácoras que pueden ser analizadas por el auditor, ya sea en forma manual o por medio de programas especializados, tales como bitácoras de fallas del equipo, bitácoras de accesos no autorizados, bitácoras de uso de recursos, bitácoras de procesos ejecutados.

- Simulación paralela: Técnica muy utilizada que consiste en desarrollar programas o módulos que simulen a los programas de un sistema en producción. El objetivo es procesar los dos programas o módulos de forma paralela e identificar diferencias entre los resultados de ambos.

El análisis de datos permite al auditor informático, analizar lo que pueda pasar más adelante en el mercado y poder responder de forma rápida a esto, con ello se puede ofrecer aun ventaja competitiva de la empresa en el mercado, analizando tendencias para la eficiente toma de decisiones.

5.4.9 Monitoreo

El IMCP (2017) menciona que dentro de las organizaciones donde se llevan a cabo las auditorias informáticas deben monitorearse los procesos, estos necesitan ser evaluados a través del tiempo para verificar su calidad en cuanto a

las necesidades de control, integridad y confidencialidad, este es precisamente el ámbito de esta técnica, a continuación, se muestran algunos procesos:

- Monitoreo del proceso. Puede asegurar el logro de los objetivos para los procesos de TI, lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño y la implementación de sistemas de soporte, así como la atención regular a los reportes emitidos, para eso la gerencia podrá definir indicadores claves de desempeño y factores críticos de éxito y compararlos con los niveles propuestos para evaluar el desempeño de los procesos de la organización.

- Evaluar lo adecuado del control Interno. Asegura el logro de los objetivos de control interno establecidos para los procesos de TI, para ello se debe monitorear la efectividad de los controles internos a través de actividades administrativas, de supervisión, comparaciones, acciones rutinarias, evaluar su efectividad y emitir reportes en forma regular.

- Obtención de aseguramiento independiente. Incrementa los niveles de confianza entre la organización, clientes y proveedores, este proceso se lleva a cabo a intervalos regulares de tiempo, para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, así como para trabajar con nuevos proveedores de servicios de tecnología de información, luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información, de los proveedores de estos servicios así como también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de dichos servicios.

- Proveer auditoría independiente. Incrementa los niveles de confianza de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo, para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoría, el auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado para mayor validación de la revisión y en lo posible deberá ser independiente de la propia empresa, esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría informática (Zavaro & Martínez, 1999).

Así se puede observar que la función de la auditoría informática deberá proporcionar un reporte que muestre los objetivos, período de cobertura, naturaleza y trabajo de auditoría realizado, así como también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría informática llevado a cabo por todos los involucrados en la auditoría informática.

La utilización de equipos de computación en las organizaciones, ha tenido una repercusión importante en el trabajo del auditor, no sólo en lo que se refiere a los sistemas de información, sino también al uso de las computadoras en la auditoría, al llevar a cabo auditorías donde existen sistemas computarizados, el auditor se enfrenta a muchos problemas de muy diversa condición, uno de ellos, es la revisión de los procedimientos administrativos de control interno establecidos en la empresa que es auditada.

Según Zavaro & Martínez (1999) la utilización de paquetes de programas generalizados de auditoría ayuda en gran medida a la realización de pruebas de auditoría, a la elaboración de evidencias plasmadas en los papeles de trabajo, las técnicas de auditoría Asistidas por Computadora son la utilización de determinados paquetes de programas que actúan sobre los datos, llevando a cabo con más frecuencia los trabajos que se describen a continuación.

5.5 Auditorías en TI

Actualmente en todos los niveles y tipos de instituciones, la introducción de nuevas tecnologías mediante el uso de equipos como sistemas informáticos es una herramienta fundamental para el desarrollo de las actividades diarias, para ello se utilizan tecnologías de información para gestionar sus funciones de forma rápida y eficiente, con el fin de obtener beneficios económicos y de costos, su correcta utilización facilita al usuario y directivos la realización de sus tareas en el menor tiempo posible, aumentando así la productividad (Castro, 2012).

En toda actividad hay riesgos, que deben ser minimizados o bien ser previstos, de ahí se llevan a la práctica las auditorías a las TI, las cuales es importante que existan y se realicen periódicamente, dado que la información es uno de los activos más importantes de las empresas e instituciones, es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología, frente a esta realidad se hace posible llevar a cabo auditorias en informática.

La Auditoria en TI es un conjunto de procedimientos y técnicas para agrupar, recoger, evaluar y controlar total o parcialmente la información de un sistema informático, telecomunicaciones, redes o equipamiento, con el fin de

proteger actividades y recursos, verificar si las actividades se desarrollan eficientemente y de acuerdo con la normatividad informática y general en cada empresa o institución, para conseguir la eficacia exigida por la organización.

Es importante recalcar que la función de la auditoria en TI es prevenir desvíos, modificaciones o manipulaciones a la información, analiza el de la función informática, el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normatividad general, la revisión de la gestión de los recursos materiales, humanos e informáticos, los niveles de seguridad, etc.

5.5.1 Técnicas y herramientas para la obtención de información

Castro (2012) menciona que para la recolección de información y detectar errores en equipo tecnológico se debe recurrir a la investigación de los datos, ya sea observada o documentada donde se analicen las situaciones de debilidad o fortalezas de los diferentes entornos, es por eso que se deben utilizar algunas técnicas para recabar información relevante como se muestra a continuación:

Cuestionario. Es un instrumento de investigación que se basa a través de listas escritas de preguntas que se distribuyen entre los usuarios que nos permiten obtener información útil y eficaz en un tiempo breve, también se le considera como una herramienta de punto de partida que permiten obtener información y documentación de todo el proceso de una organización, que piensa ser auditado.

Los cuestionarios de acuerdo con Cayssials (2012) son instrumentos de considerable importancia y su característica esencial es que la información se obtiene a través de una serie de preguntas ya preparadas y estructuradas. En general, son autodescriptivos. Se trata de una técnica de lápiz y papel, económica y rápida y, por lo general, apropiada para la aplicación colectiva.

El auditor debe realizar una tarea de campo para obtener la información necesaria, basado en evidencias o hechos demostrables. Inicia su trabajo solicitando que se cumplimenten los cuestionarios enviados a las personas correspondientes, marcadas por el auditor.

Los cuestionarios no tienen que ser los mismos en caso de organizaciones distintas, ya que deben ser específicos para cada situación, la fase de cuestionarios puede omitirse si el auditor ha podido recabar la información por otro medio.

- **Entrevista.** Se utiliza para recabar información en forma verbal, a través de preguntas que propone el interesado, quienes responden pueden ser gerentes o empleados, los cuales son usuarios actuales del sistema existente, usuarios potenciales del sistema propuesto o aquellos que proporcionarán datos o serán afectados por la aplicación propuesta.

- **Las trazas.** Se basan en el uso de software, que permiten conocer todos los pasos seguidos por la información, sin interferir el sistema, además del uso de las trazas, el auditor utilizará, los ficheros que el próximo sistema genera y que recoge todas las actividades que se realizan y la modificación de los datos, que se conoce con el nombre de log, el log almacena toda aquella información que ha ido cambiando y como ha ido cambiando, de forma cronológica (Castro, 2012).

- **Checklist.** Es una herramienta útil para definir un problema y organizar ideas, se encuentra dentro de las fases de definición, medición y análisis del ciclo de un proceso donde se identifica información específica para la descripción de un problema.

Se le considera también como un conjunto de preguntas respondidas en la mayoría de las veces oralmente, destinados principalmente a personal técnico. Por estos motivos deben ser realizadas en un orden determinado, muy sistematizadas, coherentes y clasificadas por materias, permitiendo que el auditado responda claramente. Existen dos tipos de filosofía en la generación de *checklists*:

- De rango: las preguntas han de ser puntuadas en un rango establecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y 5 la más positiva).

- Binaria: las respuestas sólo tienen dos valores (de ahí su nombre), cuya respuesta puede ser Si o No.

La primera permite una mayor precisión en la evaluación, aunque depende, claro está, del equipo auditor, los binarios, con una elaboración más compleja, deben ser más precisos. No existen *checklists* estándares, ya que cada institución y su auditoría tienen sus peculiaridades.

5.6 Instituciones educativas

“Las instituciones educativas son espacios de elaboración de cultura, caracterizada esta por su singularidad diferencial y por el desafío que supone de mejora existencial, académica i relacional para cuántas personas contribuyen a su gestión” (Gento, 1996, pág. 11).

La mejora continua de las instituciones educativas necesita de la acción conjunta de todos los participantes, en los que las ilusiones y desilusiones, las

expectativas y necesidades, los logros y desvelos son valorados en su significación y proyección global.

Las instituciones escolares son ecosistemas sociales de carácter educativo qué pretenden que los estudiantes se eduquen a lo largo de su vida adquiriendo hábitos, competencias, destrezas, valores, actitudes, entre otros, qué integrados en un proyecto vital sienten la base del pensar, actuar y ser más humanos (Medina *et al.,* 2015).

Las instituciones educativas se enfrentan a la necesidad de cambios continuos de la sociedad del conocimiento, la pluralidad cultural y la complejidad, ante tales cambios se precisa de modelos pertinentes para comprender y propiciar las transformaciones, logrando descubrir el verdadero sentido y el ritmo equilibrado entre los logros conseguidos en la diversidad de prácticas educativas.

Las instituciones sin un equilibrio, un seguimiento y sin una revisión constante durante un tiempo adecuado, las organizaciones podrían convertirse en una veleta sin rumbo, movida por el agitador cambio de direcciones del viento por lo que se requiere una constante vigilancia mediante auditorias y auditorías de sistemas (Gento, 1996).

Se puede hacer mención porque, mediante las evaluaciones continuas, con las auditorías pueden ser estrategia que aspira a predecir cambios auto sostenidos, de manera que continuamente acelere su propio crecimiento y desarrollo al operar como un ciclo de refuerzo.

Las instituciones creadas por los seres humanos y sobre todo las educativas, se destacan por avanzar el conocimiento y sentar las bases para que cada persona aprenda a aprender, a compartir e innovar y a valorar la educación pertinencia de múltiples interacciones, estas interacciones consolidan la energía

del sistema y logran un fuerte impacto en el desarrollo que las mismas (Medina *et al.,* 2015).

El sistema educativo es esencialmente dinámico y sus procesos se dan como una auténtica reingeniería del cambio de la transformación continua de los estudiantes en general, las escuelas son organizaciones de aprendizaje y de desarrollo de este mediante procesos representativos, en los que ha de colaborar toda la comunidad escolar para conseguir una plena cultura de aprendizaje e innovación.

VI. MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN EMPLEADAS

La investigación fue inicialmente documental, se partió de la revisión de literatura sobre la auditoria informática. Posteriormente, fue de tipo descriptiva, solo se observó lo que está ocurriendo con la investigación, solo se identifica como es y cómo se manifiesta la problemática encontrada con la mayor precisión posible.

El presente estudio está dirigido en base con las pregunta de investigación y los objetivos con un diseño de tipo transversal, porque es el que mejor se adapta a las necesidades del estudio (Dzul, 2013), solo se observaron y recabaron los datos obtenidos, tal y como se da en forma natural para analizarlos y comprender, el diseño transversal se usó para recolectar datos en un cierto tiempo (Mata, 2019), para poder ser utilizados de acuerdo con las necesidades.

Para la recolección de datos se tomó en cuenta toda la información pertinente acerca del el análisis y evaluación informática, se aplicarán principalmente: la revisión de documentos de las instituciones, licencias, permisos, diseño, eficiencia y eficacia informática. Para detectar el uso y manejo de la información a través recursos informáticos que puedan afectar el correcto uso y funcionamiento de las TI en las instituciones.

Y finalmente, la investigación descriptiva otorgó la información que se debe utilizar para la elaboración de la propuesta de auditoria el cual dice Vivanco (2017), que en la actualidad las instituciones a nivel mundial se mueven mediante procesos así nace la necesidad de controlar y examinar cada proceso para que este se desarrolle de una manera eficiente por lo que es importante el control

interno aplicado al adecuado funcionamiento en el caso de las TI, los que al mismo tiempo son guías operativas para los pasos que asigna a una persona o actividad dentro de una organización en una auditoria informática. Para la elaboración de las auditorias, examen de los sistemas de información, las entradas y las salidas y procesamiento de datos, por el hecho de minimizar los riesgos de la entidades o instituciones.

VII. PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS

Se presentan los resultados obtenidos durante la investigación concerniente a, las auditorías informáticas en las instituciones educativas, en las cuales se podrá ver la importancia que estas representan para estas organizaciones. Aquí se expone un proceso de desarrollo e investigación de información a través de la descripción de diversos datos, de utilización como la de la aplicación de una metodología de desarrollo describiendo desde el proceso de recolección hasta la integración de la información para su análisis y misión de reportes o dictámenes donde se puedan mostrar las recomendaciones.

Con el objetivo de beneficiar a las instituciones de cualquier tipo o nivel educativo, así como a los funcionarios, es necesario que se realicen auditorías Informáticas para recoger y evaluar posibles equivocaciones o fallas, y así proponer soluciones con el objetivo de mejorar la calidad de servicio para sus beneficiarios.

Menciona Muñoz (2002) con el fin de identificar sus principales aplicaciones en la auditoría de sistemas y para entender cómo se pueden satisfacer, con eficiencia y eficacia, las necesidades de evaluación, razonabilidad, oportunidad en la protección y seguridad de los bienes de la información y del personal del área de sistemas de una institución.

Se presentan las siguientes recomendaciones a contemplar, para tomar en cuenta, cuando se realice o se pida una auditoría informática en alguna institución educativa, contemplando la información de los manuales, controles, seguridad, salvedades, recomendaciones, instrumentos de recolección de

información como lo es el cuestionario y la matriz FODA y la norma ISO 27001, si así lo permite la infraestructura de la institución educativa.

Manuales e instructivos del usuario. Estos son los documentos que le servirán de guía al usuario, en las instituciones, ahí deberán anotar todas las instrucciones sobre el uso del sistema, incluyendo las guías de operación, los términos más comúnmente utilizados, la descripción de las operaciones básicas, pantallas y demás acciones sobre el sistema.

Manual técnico del sistema. En este documento especializado, se indican todos los aspectos técnicos que se deben considerar para el adecuado manejo del sistema, estos aspectos suelen ser sofisticados y con características especiales sobre el funcionamiento técnico de los sistemas computacionales, no sólo en cuanto al software y hardware, sino también en cuanto a sus instalaciones, equipos y manejo de información que deben contar las instituciones.

Manual e instructivo de mantenimiento del sistema. En este documento se deben anotar y llevar registro de las actualizaciones, preventivas o correctivas, que van surgiendo durante la vida activa de las instituciones, garantiza la continuidad, ya que sirve de referencia y orientación para entender el funcionamiento del sistema y para su mantenimiento, además, ayuda al auditor a realizar estadísticas sobre el comportamiento, utilidad, descomposturas y demás detalles del funcionamiento del sistema.

Controles internos para la seguridad del área de sistemas, hace referencia Muñoz (2002) dentro de los aspectos fundamentales que se deben contemplar en el diseño de cualquier centro de informática en cualquier institución, se encuentra la seguridad de sus recursos informáticos, del personal, de la información, de sus programas que se deben contemplar se puedan lograr a través de medidas preventivas o correctivas, o mediante el diseño de

programas de prevención de contingencias para la disminución de riesgos, para el mejor entendimiento de la importancia de este elemento y de su aplicación correcta, se indican sus principales aspectos a cuidar y revisar constantemente:

- Seguridad física. Aquí se debe tomar en cuenta lo relacionado con la seguridad y salvaguarda de los bienes tangibles de los sistemas computacionales de las instituciones, tales como el hardware, periféricos y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos, las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos al centro de sistematización, es todo lo relacionado con la seguridad, la prevención de riegos y protección de los recursos físicos informáticos de las organizaciones.

- Seguridad lógica. En este apartado se verifica todo lo relacionado con la seguridad de los bienes intangibles de los centros informáticos, tales como software (aplicaciones, sistemas operativos y lenguajes), así como lo relacionado con los métodos y procedimientos de operación, los niveles de acceso a los sistemas y programas institucionales, el uso de contraseñas , los privilegios y restricciones de los usuarios, la protección de los archivos e información de las instituciones, las medidas, programas para prevenir y erradicar cualquier virus informático.

Seguridad de las bases de datos. Se debe verificar continuamente la protección específica de la información que se maneja en las áreas de sistemas de la empresa, ya sea a través de las medidas de seguridad y control que limiten el acceso y uso de esa información, o mediante sus respaldos periódicos con el fin de mantener su confidencialidad y prevenir las alteraciones, descuidos, robos y otros actos delictivos que afecten su manejo.

Seguridad en la operación. Al igual se debe verificar la seguridad en la operación de los sistemas computacionales, en cuanto a su acceso y aprovechamiento por parte del personal informático y de los usuarios, al acceso a la información y bases de datos, a la forma de archivar y utilizar la información y los programas institucionales, a la forma de proteger la operación de los equipos, los archivos y programas, así como las instalaciones, mobiliario, entre otros.

Seguridad del personal de informática. Darle el seguimiento a la seguridad y protección de los operadores, analistas, programa- dores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los beneficiarios de la información.

Seguridad en las redes. Se debe checar continuamente la seguridad y control de contingencias para la protección adecuada de los sistemas de redes de cómputo, en cuanto a la salvaguarda de información y datos de las redes, la seguridad en el acceso a los sistemas computacionales, a la información y a los programas del sistema, la protección de accesos físicos, del mobiliario, del equipo y de los usuarios de los sistemas, el respaldo de información y los privilegios de accesos a sistemas, información y programas.

Prevención de contingencias y riesgos. Revisar todas las acciones tendientes para prevenir y controlar los riesgos y posibles contingencias que se presenten en las áreas de sistematización, las cuales van desde prevenir accidentes en los equipos, en la información y en los programas, hasta la instalación de extintores, rutas de evacuación, resguardos y medidas preventivas de riesgos internos y externos, así como la elaboración de programas preventivos y simulaciones para prevenir contingencias y riesgos informáticos.

Parte de la metodología del desarrollo en la auditoria informática, se inicia con la obtención e investigación de los datos que se van a utilizar, para su análisis y conocimiento para posteriormente clasificarlos en los rubros que les pertenezcan para su evaluación y recomendación. Sin embargo, el principal objetivo que constituyen a la auditoría informática es el control de la función tecnológica, juntamente con la revisión de la gestión de los recursos materiales y humanos informáticos, permitiendo de esta forma la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información, se lleven a cabo de manera oportuna y eficiente., además, que operen en un ambiente de seguridad y control para generar confiabilidad, integridad y exactitud en los datos que dispone la unidad educativa (Muñoz, 2002).

Salvedades

Durante la investigación basada en el marco conceptual, mencionan algunos autores e investigadores, situaciones en las salvedades que se pueden encontrar al examinar la organización y su posible solución, de acuerdo con cada institución educativa y su infraestructura que esta tenga (González, 2017).

Las cuestiones que se indican a continuación Castro (2012), son los hallazgos encontrados en lo general y se podría mencionar que también en lo particular, en las auditorias informáticas que se les realizan a las organizaciones educativas:

A. Las instituciones cuentan con personal para realizar el mantenimiento preventivo y/o correctivo en los equipos de las organizaciones, pero la programación que se realiza no se cumple

según lo planeado por diversos factores como la falta de tiempo, la falta de personal capacitado o la del perfil deseado.

B. Los procedimientos realizados en el mantenimiento correctivo y preventivo no son normalizados los procedimientos técnicos, provocando que la solución no sea la más efectiva o la más eficaz para el correcto funcionamiento de las instituciones.

C. En el manejo de hardware no existe un adecuado control ni restricciones para el manejo y uso de estos dispositivos, como el del almacenamiento de datos o copia de estos, los llamados, tipo USB, provocando la infección fácilmente en los sistemas. En cuanto a los recursos auditados en este apartado se pudieron observar las siguientes situaciones:

   - No existe un plan de resguardo de los datos.
   - No se cuanta con un servicio de soporte permanente.
   - No se cuenta con un plan o programa de actualización de software establecido.

D. Si se presenta una falla irrecuperable por diversas causas, ya sean accidentales o no de hardware en un equipo de cómputo de uso fundamental, no se cuenta con planes de contingencias que permitan hacer un proceso de recuperación que se pueda comprometer.

E. En las investigaciones se percibe que no todas las instituciones se tienen implementado un resguardo de los datos que permitan recuperar la continuidad de la organización ante una contingencia, dado que no se realizan copias de seguridad periódicamente.

F. Igualmente, algunas instituciones educativas, cuenta con un servicio ocasional de respaldo o de soporte contratado con un tercero, para atender las eventualidades que se presenten ya que se sabe estas suelen ocurrir continuamente.

G. También se puede percatar que no se cuenta con procedimientos desarrollados o definidos, ni registro de aplicación de actualizaciones de software o parches de seguridad en los sistemas fundamentales en algunas de las instituciones.

H. Se debe llevar un monitoreo al sistema que permita identificar amenazas internas o externas ya que en ocasiones no se lleva, ya que sin esto no permite prevenir situaciones críticas que puedan suceder o identificar si se está siendo vulnerado el sistema.

I. En las instituciones la red Wifi presenta alta vulnerabilidad, dado que los estudiantes y parte de la comunidad alrededor de la institución se conectan constantemente, debido a la falta de datos y al alto número de personas que quieren ingresar a la red.

J. Algunas organizaciones en sus instalaciones físicas se pueden conocer que el estado del cableado estructurado encontrado en la sede principal son de tipo UTP categoría 6 de los cuales no cumplen con las normas mínimas de instalación, como son el caso de los armarios de cableados, patch-panel y patch cord donde se encuentran desorganizados y en malas condiciones, como también se encontró que cualquier persona tiene acceso a dichos recursos provocando así inseguridad.

K. En las instituciones las condiciones ambientales y de seguridad que presentan son en algunas organizaciones las siguientes, no cuenta

con un sistema inteligente de prevención contra incendios, no siempre se encuentran los sistemas de aires acondicionados encendidos, no existe restricción al acceso a estos lugares y todo esto afecta a las instalaciones.

L. Se deben definir políticas de seguridad para la red de la institución educativa y diseñar un paquete que de soluciones para establecer y mantener la seguridad de la información de modo que se pueda garantizar la continuidad del servicio ante algún evento. En cuanto a los recursos auditados en este apartado se pudieron observar las siguientes situaciones:

- No se realiza un monitoreo al sistema que permitan identificar las amenazas internas o externas. Ya que la navegabilidad es lenta, a pesar de contar con un ancho de banda suficiente para los procesos que se realizan en la red.
- Falta de restricción a la red wifi.
- Ingeniería social.

M. Se recomienda segmentar la red al nivel de oficinas, así como realizar la configuración del firewall, aislando la red externa con la red interna para los terminales, así como configurar parámetros de seguridad de routers, realizando una encriptación segura.

N. En instituciones se pudo observar qué hace falta la capacitación del personal a cargo del departamento de tecnologías de la información, así como darles seguimiento a los colaboradores de estos departamentos, también se debe restringir el servicio en horarios no laborables.

O. Se deben establecer estrategias de resguardo para los datos ya sea a través de un proceso de soporte interno o externo e implementar un servicio del soporte de prevención que permita identificar posibles vulnerabilidades que se puedan presentar en las instalaciones.

P. En las instalaciones, se determinó que el cableado estructurado y las canaletas que soportan este cableado se encuentran en malas condiciones y los armarios, no cumplen con los requisitos mínimos de instalación.

Q. Instalaciones físicas. En cuanto a los recursos auditados en este apartado se pudieron observar las siguientes Las condiciones ambientales y de seguridad que presenta la institución en la sede principal son las siguientes: no cuenta con un sistema inteligente de prevención contra incendios, no siempre se encuentran los sistemas de aires acondicionados encendidos, no existe restricción al acceso a estos lugares.

R. Seguridad informática, en cuanto a los recursos auditados en este apartado se pudieron observar las siguientes situaciones:

- Suplantación de identidad.
- Pérdida y robo de información.
- Alteración de la información.
- Posible pérdida de la continuidad del servicio.

S. Se debe hacer una revisión constante al hardware, para poder detectar si existe alguna falla y poder actuar con un mantenimiento preventivo que se realicen los equipos ya que varios equipos se encuentran se encuentran en malas condiciones. En cuanto a los

recursos auditados en este apartado se pudieron observar las siguientes situaciones:

- El cronograma de mantenimiento no se cumple satisfactoriamente.
- Los procedimientos de mantenimiento preventivo y correctivo no son realizados correctamente.
- No existen restricciones en la utilización de dispositivos de almacenamientos tipos USB.
- No se cuenta con planes de contingencias que permitan hacer un proceso de recuperación de la información los cuales puedan comprometer a la institución.

Las salvedades identificadas en la investigación y su posible solución son la base fundamental para la emisión de la opinión o el dictamen del auditor según lo examinado.

Recomendaciones o posibles soluciones para las instituciones según su infraestructura

Estas son las llamadas acciones correctivas o preventivas que se pueden integrar en los informes de las auditorías realizadas, resultantes del proceso de valuación de las áreas, departamentos o rubros. Estas recomendaciones que a continuación se mencionan son solo algunas de las muchas que se pueden expresar y que se deben adecuar a las necesidades de cada institución:

- Crear concientización del valor de los activos tecnológicos a las partes administrativas de las instituciones, para así poder cumplir con el plan de mantenimiento.

- Dar apoyo al equipo de mantenimiento en la consecución de herramientas para cumplir con sus objetivos programados.

- Utilizar políticas y mecanismos de restricción o medidas adecuadas como capacitaciones para el uso seguro de los dispositivos de almacenamiento USB en los equipos de cómputo de la institución e implementar planes de contingencia que permita la recuperación de la información a los activos informáticos de la institución.

- Implementar un resguardo de datos, los cuales le permita realizar copias de seguridad periódicamente y así recuperarlos y darle continuidad al servicio ante una contingencia.

- Establecer un servicio de soporte permanente contratado por un tercero para atender las eventualidades que se presenten.

- Se debe verificar que se cumplan con el plan de actualizaciones en las fechas establecidas, así como implementar un sistema de monitoreo que permita identificar las amenazas, internas o externas, permitiéndole prevenir situaciones críticas.

- Implementar un sistema de control de restricciones a la red, que permita dar permisos a los usuarios, así como dar capacitaciones a los usuarios en seguridad informática, según lo establecido en los cronogramas.

- En cuanto a las instalaciones físicas, implementar un proyecto de mantenimiento de redes que le permitan mejorar el servicio a la institución.

- Efectuar políticas que establezcan condiciones ambientales y de seguridad en la prevención de incendios, la restricción al acceso a estos lugares, entre otros.

- En cuanto a la seguridad informática se requiere la capacitación en los modelos de seguridad existentes y contar con copias de seguridad y controles de acceso a la información e implementar un sistema de validación de usuarios.

- Realizar auditorías Informática periódicamente en los rubros que se tengan identificados, como de dudoso funcionamiento con el fin de proponer soluciones viables, si así lo requiriera y que permitan un mejor desenvolvimiento de las instituciones en lo general.

- Se recomienda a los funcionarios proteger sus contraseñas de manera segura, así como cambiarlas periódicamente, para evitar que cualquier tipo de persona interna y externa puedan accedan a la información que des de importancia para las organizaciones.

- Crear e implementar un plan de contingencias, para que las instituciones se encuentren preparada ante cualquier tipo de imprevisto que se pueda presentar, ya sea por cuestiones naturales u ocurridos por el factor humano que por lo regular suceden.

- Revisar constantemente los equipos para identificar y eliminar aplicaciones innecesarias, que no se ocupan o están obsoletas de las computadoras para prevenir saturación de memoria y beneficiar el cumplimiento de las labores diarias.

- Hacer mención a las instituciones que en el menos tiempo y en lo posible adquieran software que se requieren y se hacen necesarios para el manejo y cuidado de la información como un antivirus con licencia para que los problemas provocados por virus no sea frecuente.

- Se hace la sugerencia ampliamente a las instituciones de todos los niveles y tipos que el departamento de TI se realicen chequeos periódicos de los

equipos de cómputo para un mejor desempeño de las actividades diarias y evitar fallos en estos equipos.

En las auditorias se presentan informes del trabajo donde se describe y se detallan los hallazgos encontrados en estas y así mismo se hacen de su conocimiento unas situaciones y posibles soluciones, presentando las recomendaciones técnicas que pueden realizar.

Como se establece, la auditoría informática permite la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que está inmersa en el procesamiento de la información con el fin de lograr una utilización eficiente y segura, que servirá para una adecuada toma de decisiones, considerada fundamental en las organizaciones, tanto los sistemas como la estructura física deben estar sometidos a controles de calidad ya que los ordenadores como procesamiento de datos son blanco fácil para la delincuencia, terrorismo o espionaje (Castro, 2012).

Instrumentos de recolección de información

Castro (2012) menciona que para la recolección de información y detectar errores en equipo tecnológico se debe recurrir a la investigación de los datos, por medio de instrumentos adecuados para la obtención de estos, qué servirán para la emisión de opiniones y recomendaciones al informe de la auditoria informática de las instituciones educativas.

El Cuestionario. Es el instrumento de investigación que se basa a través de listas escritas de preguntas que se distribuyen entre los usuarios que nos

permiten obtener información útil y eficaz en un tiempo breve, en seguida se muestran algunos ejemplos de las preguntas que pueden hacerse en la recolección de información, de acuerdo con el tipo de institución que se audite y a sus características particulares.

Este banco de preguntas que se presentan a continuación, están elaborador de manera general para cualquier tipo de institución y tamaño, de acuerdo con sus necesidades y características de cada institución, estas deben adecuarse:

1) ¿El área o departamento informática cuenta con manual de usuario?
2) ¿Existe un procedimiento para el manejo de la información del cuarto frío?
3) ¿La infraestructura asignada a los servidores de datos cuentan con aire acondicionado?
4) ¿La infraestructura asignada a los servidores de datos tiene protección contra fuego?
5) ¿Qué información mínima contiene el inventario de los servidores de datos?
6) ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?
7) ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?
8) ¿La institución posee planes de contingencia ante cualquier eventualidad?

9) ¿Existe control de acceso a los computadores para usuarios no autorizados?

10) ¿Las claves de acceso al computador son visibles a otros usuarios?

11) ¿Con que frecuencia se renueva las claves de seguridad en el sistema informático de la institución?

12) ¿Cuándo se produce alguna falla en la parte tecnología, solucionó el problema por sí solos?

13) ¿Se realizan respaldos habitualmente de la información de la institución?

14) ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?

15) ¿Se realizan auditorías periódicas a los medios de almacenamiento?

16) ¿Qué medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

17) ¿En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?

18) ¿El Departamento de tecnología cuenta con el personal suficiente para cubrir las necesidades de la institución?

19) ¿Existen controles de seguridad y claves para acceso a los ordenadores y sistemas informáticos?

20) ¿Se capacita al personal entorno al ámbito tecnológico?

21) ¿Tiene conocimiento de todo el software instalado en su computador?

22) ¿El software de protección de virus es eficaz para detectar los mismos?

23) ¿Se efectúan actualizaciones de software periódicamente?

24) ¿Los programas que utiliza habitualmente poseen las respectivas licencias?

25) ¿Se requiere claves de acceso del sistema operativo Windows en todas las computadoras?

26) ¿Cómo calificaría, al sistema informático que utiliza en el ejercicio de sus funciones dentro de la institución?

27) ¿Se recibe capacitación por parte de la institución para el buen manejo del sistema informático?

28) ¿La institución cuenta con conexión de internet segura?

29) ¿El personal informático de la institución verifica la banda y el ancho de la red?

30) ¿Qué calidad de navegación de internet dispone la institución?

31) ¿Considera que las redes, servidores, ordenadores y sistemas informáticos satisface las necesidades de los estudiantes?

32) ¿La Institución educativa, cuenta con página web?

33) ¿La institución educativa cuenta con registro de entrada y salidas de los docentes en los laboratorios informáticos?

34) ¿El centro de cómputo da hacia el exterior?

35) ¿Se cuenta con una salida de emergencia?

36) ¿Existen señalamientos que hagan visibles las salidas de emergencia?

37) ¿Existe lugar suficiente para los equipos?

38) ¿Se dispone de aire acondicionado?

39) ¿Existe algún otro medio de ventilación aparte del aire acondicionado?

40) ¿Cuenta con algún lugar para almacenar otros equipos de cómputo, muebles, suministros, aparte del centro de cómputo?

41) ¿La institución educativa cuentan con equipos de cómputo suficiente en sus laboratorios informáticos para los estudiantes?

42) ¿Es suficiente la iluminación del centro de cómputo?

43) ¿Considera que los equipos informáticos de la institución educativa cuentan con los implementos necesarios para su uso?

44) ¿Se realiza chequeos habituales de mantenimiento del equipo de cómputo en la institución?

45) ¿Al realizar las actividades diarias, los equipos de cómputo responden con agilidad en el proceso?

46) ¿La institución cuenta con un registro de inventario de los laboratorios informáticos?

47) ¿Cómo califica el estado de los equipos informáticos de la institución?

48) ¿El equipo informático que utiliza permite realizar sus funciones de manera eficiente?

49) ¿Se efectúan controles o revisiones del buen estado de los equipos de cómputo?

50) ¿Los equipos cuentan con un regulador?

51) ¿Se cuenta con los planos de instalación eléctrica?

52) ¿La instalación eléctrica del equipo de cómputo es independiente de otras instalaciones?

El objetivo de los cuestionarios es recolectar información de importancia y suficiente sobre ciertos aspectos de las TI de las instituciones para poder emitir un informe de auditoría dictamen, que permita alinear al departamento de informática con sus necesidades en las áreas o rubros objeto de estudio.

El propio auditor puede elaborar estas preguntas para poder validar las respuestas en el momento que las recibe, y las puede elaborar en grupo o de manera individual; pero es él quien debe anotar las respuestas de los encuestados, es recomendable elaborar las preguntas previamente y efectuar pruebas piloto antes de aplicarlas, además pueden aplicarse de manera grupal o individual (Castro, 2012).

Matriz FODA. Es un método moderno de análisis y diagnóstico administrativo de utilidad para la evaluación de un centro de cómputo, debido a que no sólo permite recopilar información, sino que admite evaluar el desempeño de los sistemas computacionales.

Por medio de este documento se puede tener una apreciación preliminar sobre las fortalezas y debilidades del propio centro de información de las instituciones, y se pueden analizar sus posibles amenazas y áreas de

oportunidad, con dicho análisis, el auditor evalúa el cumplimiento de la misión y objetivo general del área de sistemas computacionales de la empresa.

La matriz DOFA es un acrónimo de Debilidades, Oportunidades, Fortalezas y Amenazas de las organizaciones, las cuales se estudian cada una por separado en cuanto a su presencia interna y a la influencia que la empresa recibe del exterior.

El fundamento para la aplicación de la matriz de Debilidades, Oportunidades, Fortalezas y Amenazas en una auditoría de sistemas computacionales es que mediante dicha matriz se pueden estudiar las influencias que afectan el comportamiento del área de las instituciones educativas, tanto las que recibe de su ambiente interior, como las de su ambiente exterior, ya sean de la propia organización o de sus proveedores, desarrolladores o del entorno donde se encuentra establecida (Muñoz, 2002).

Los factores que se podrían evaluar para la auditoria de sistemas computacionales en las instituciones educativas, de acuerdo con la investigación y el marco conceptual serán:

Los factores de carácter interno en el área de sistemas:

- Factores humanos que influyen en el área de sistemas.
- Misión, visión y objetivo del área de sistemas
- Cultura informática del área de sistemas y de la empresa.
- Sistemas computacionales, muebles, equipos y bienes informáticos.
- Servicios de cómputo que proporciona el área de sistemas.
- Estrategias de servicio computacional.
- Estructura de organización del área de sistemas.

- Idiosincrasia, valores y costumbres del área de sistemas.
- Filosofía de calidad del servicio de cómputo.

Los factores de carácter externo en el área de sistemas.

- Usuarios de los sistemas computacionales.
- Canales de distribución de los servicios de cómputo.
- Proveedores y distribuidores.
- Competencia Inter computacional.
- Desarrollo de la tecnología informática.
- Influencia social del ambiente informático.
- Influencia política del ambiente informático.
- Influencia económica del ambiente informático.
- Influencia cultural del ambiente informático.

El uso de la matriz les permite a las instituciones analizar planos específicos de influencia en el servicio de cómputo que se proporciona a la empresa, mismos que influyen en el comportamiento de los integrantes del área de sistemas y en los usuarios.

Norma ISO 2700. Esta norma debe ser incluida para la realización de una auditoria informática, ya que esta es un estándar de seguridad que muestra los requisitos sugeridos para crear rastrear y mejorar un SGSI (sistema de seguridad de la información), esta son las políticas que administran y protegen la información confidencial de las instituciones u organizaciones (Wilson, 2019).

La norma es empleada voluntariamente, la cual debe ser auditada por un organismo acreditado independiente para confirmar el cumplimiento de las

políticas y los estándares de la norma así se reduce el riesgo de que la información se vea comprometida.

Como se ha mencionado anteriormente el uso de la norma es de carácter voluntario para su aplicación, las instituciones que lo deseen y cuenten con infraestructura o ciertas características para su diligencia, podrán basarse en la norma si así lo consideran necesario en su auditoria informática.

El cumplimiento de la ISO 27001 es necesaria para quien la llegue aplicar, para crear una política de gobernanza de seguridad de la información que este manejando y sea de importancia para las instituciones que deseen certificarse en esta norma.

La institución requiere adquirir recursos, infraestructura y personal que implementen un SGSI de manera eficiente, esto implica tutoría y capacitación del personal sobre cómo manejar información confidencial, a los colaboradores también se les debe informar como contribuir para que la norma sea efectiva.

La institución debe documentar las acciones tomadas para asegurarse de que los procesos se lleven a cabo según lo estipulado, ya que la evaluación del desempeño asegura que el sistema de seguridad de la información se mejore constantemente.

VIII. CONCLUSIONES Y SUGERENCIAS

La finalidad de esta investigación busca solucionar a las preguntas de ¿Qué aspectos se deben considerar en una auditoría informática para instituciones educativas?, ¿Por qué es importante que las instituciones educativas lleven a cabo auditorias informáticas en las tecnologías de información?, ¿De qué manera beneficiará a las instituciones el contar con un dictamen de una auditoria informática? por lo que estas cuestiones se responden de acuerdo con lo investigado de acuerdo con Castro (2012).

De acuerdo con los informes o dictámenes arrojados por las auditorias, ya sea internas, externas o mixtas, se llega a las siguientes conclusiones para la administración de las instituciones que han pedido la revisión de las auditorias informáticas, haciendo hincapié en que no todas las organizaciones tienen las mismas observaciones o recomendaciones, ya que la mayoría de nivel universitario cumple con las normas, políticas, lineamientos establecidos, los que carecen de infraestructura, de seguimiento de sus TI son en mayor grado las de menor nivel escolar.

Una de las conclusiones es que los funcionarios de TI en su mayoría en las instituciones básicas, (antes de universidades), no todos, aclarados esto, deja a visibilidad las contraseñas de sus ordenadores bajo teclados, en hojas adhesivas en los monitores lo que hace posible que terceros puedan ingresar libremente y tomar información importante.

No existe un plan de contingencia en la institución en el ámbito informático ante cualquier eventualidad o desastre natural, que pueda suscitarse la cual puede afectar de manera significativa el desempeño de las instituciones.

Los funcionarios que administran las instituciones poseen en sus computadoras software que la mayoría de las veces no es utilizada, lo cual ocupa espacio de memoria y lentitud en sus equipos para la solución de problemas que se requieren solucionar rápidamente.

El antivirus utilizado por la institución es deficiente por lo que la proliferación de, virus en los computadores es frecuente, algunas organizaciones ni siquiera cuentan con estos.

No existe mantenimiento periódico de los equipos de cómputo de la institución lo que evitaría fallos recurrentes en las computadoras y molestias en los usuarios, por lo regular no cuentan con personal adecuado y capacitado para estas actividades.

Debido a los avances tecnológicos, el trabajo investigativo muestra lo importante que es contar con sistemas de gestión de la seguridad de la información, el cual permitirá contar con sistemas seguros. Razón por la cual las instituciones de educación cada día toman mayor interés por el área de seguridad informática, las cual brindará la posibilidad de salvaguardar la información y datos, de esta manera las organizaciones cumplirán con los principios básicos de la información, confidencialidad.

IX. REFERENCIAS DE CONSULTA

Aguirre, J. (1998). *Apuntes de Auditoría*. [Consultado 20 de junio de 2022]. Disponible en http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

Alfonso, Y., Blanco, B., & Loy, L. (2012). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería*, 6(2),1-14. [fecha de Consulta 15 de septiembre de 2022]. Disponible en: https://www.redalyc.org/articulo.oa?id=193924743004

Álvarez, L. (2005). Seguridad en informática (auditoría de sistemas) (Maestría). Universidad 9 de junio de 2022]. Disponible en http://www.bib.uia.mx/tesis/pdf/014663/014663_s.pdf

Andrade, R. (1996). *Auditoría. - Teoría Básica.* - Enfoque Moderno. Editorial Autores Varios CEL: Ecuador.

Blanco, Y. (2015). *Auditoría integral: normas y procedimientos Colección Ciencias administrativas*. Editor Eco e Ediciones: Colombia.

Castro, M (2012). Auditoria informática para optimizar el manejo de la información y equipamiento informático en el mie infa Tungurahu. Tesis de Ingeniería en Sistemas Computacionales e Informáticos. Universidad Técnica de Ambato. Disponible en https://repositorio.uta.edu.ec/bitstream/123456789/2901/1/Tesis_t765si.pdf

Cayssials, A. N. (2006). ¿Subjetividad en un cuestionario?. *Subjetividad y Procesos Cognitivos,* (8),80-87. [fecha de Consulta 20 de septiembre de 2022]. ISSN: 1666-244X. Disponible en: https://www.redalyc.org/articulo.oa?id=339630247005

Cervantes, J. (2002). *La transición a las nuevas ISO 9000:2000 y su implantación: un plan sencillo y práctico*. Ediciones Díaz de Santos

Chaparro, J. (2020). Herramienta para la realización de auditorías internas para empresas con sistemas HSEQ. *SIGNOS-Investigación en Sistemas de Gestión*, 12(2),47-57. [Consultado 2 de julio de 2022]. Disponible en https://www.redalyc.org/articulo.oa?id=560467941004

Delgado, X. (1998). *Auditoría Informática*. EUNED: Costa Rica.

Dzul, M. (2013). *Diseño No-Experimental*. [Consultado 9 de junio de 2022]. Disponible en https://repository.uaeh.edu.mx/bitstream/handle/123456789/14902.

Echenique, J. (2009). *Auditoría en Informática. Una nueva era*. McGraw-Hill: México.

Escalera, I. (2016). *Las instituciones educativas y su cultura: Prácticas y creencias construidas a través del tiempo.* Narcea Ediciones: España.

Gento, S. (1996). *Instituciones educativas para la calidad total: (Configuración de un modelo organizativo) Aula abierta.* La Muralla: España.

González, J. (2017). Auditoría de seguridad informática para las instituciones educativas departamental. Título de especialista en seguridad informática.

Universidad Nacional Abierta y a Distancia. https://up-pe.libguides.com/c.php?g=1043492&p=7613287

González, P. & Berná, J. V. (2018). Cuestionario para auditoría TI. Trabajo Fin de Grado Auditoría en la Asociación APSA Universidad de Alicante. España [fecha de Consulta 21 de septiembre de 2022]. Disponible en https://rua.ua.es/dspace/bitstream/10045/76667/1/20180618-

Haro, M.O. & Sánchez, D.J. (2006). Sistema para realizar auditoría de la información del SAE (Licenciatura). Escuela Politécnica Nacional. [Consultado 4 de julio de 2022]. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/268/1/CD- 0689.pdf

Lases, M. A. (2014). Evolución y trascendencia de las instituciones de educación superior. *Logos Boletín Científico De La Escuela Preparatoria No. 2*, *1*(2). Disponible en https://repository.uaeh.edu.mx/revistas/index.php/prepa2/article/view/1101

Madariaga, J. (2004). *Manual práctico de auditoría Finanzas y contabilidad*. Editor Grupo Planeta. Ediciones Deusto: España.

Mata, L.D. (2019). *Diseños de investigaciones con enfoque cuantitativo de tipo no experimental*. [Consultado 4 mayo 2022]. Disponible en https://investigaliacr.com/investigacion/disenos-de-investigaciones-con-enfoque- cuantitativo-de-tipo-no-experimental/

Medina, A., Domínguez, M. C., Ruíz, A., Medina, M., Pérez, R., Gómez M. J. A., Gairín, J., Pérez, E., Sáez, J. M., Cacheiro, M. L., García, J. L., & López, E. (2015). *Innovación de la Educación y de la Docencia Ciencias sociales y jurídicas.* Editorial Universitaria Ramon Areces: España.

Mendieta, L. (1980). Ensayo Sociológico sobre la Universidad. México: UNAM. Editorial: Universidad Nacional Autónoma de México, Instituto de Investigaciones Sociales, Biblioteca de Ensayos Sociológicos. Disponible en http://ru.iis.sociales.unam.mx:8080/jspui/handle/IIS/5703

Montilla, O. J., & Herrera, L.G. (2006). *El deber ser de la auditoría. Estudios Gerenciales*, (98),83-110. [Consultado 15 de Julio de 2022]. Disponible en https://www.redalyc.org/articulo.oa?id=21209804

Muñoz, C. (2002). *Auditoría en sistemas computacionales.* Pearson educación: México.

Norma de auditoría para atestiguar, revisión y otros servicios relacionados. (2017). *Comisión de Normas de Auditoría y Aseguramiento*. Editor IMCP: México.

Norma ISO 19011. (2018). *Directrices para la Auditoría de Sistemas de Gestión*. [Consultado 3 julio 2022]. Disponible en https://cmdcertification.com/wp-content/uploads/2020/11/ISO-19011-2018.pdf

Oviedo, A (2018). *Auditoría Interna ISO 9001:2015: Sistema de Gestión de Calidad ISO 9001:2015; ISO 14001:2015 Sistema de Gestión ISO 9001:2015; ISO 14001:2015*. Editor Educa Digital.

Paredes, M.V. (2013). *Diseño de un modelo de auditoría de gestión para empresas productoras de aditivo para combustible caso práctico aplicado a la empresa ecología y energía Ecoenergy Cía. LTDA.* (Licenciatura). Universidad Politécnica Salesiana.

Pallerola, J. (2012). *Auditoría (MF0232_3).* Grupo Editorial RA-MA: México.

Piattini, G. (2001). *Auditoría Informática.* Un enfoque practico. Alfaomega: México.

Robles, M. (1977). *Educación y sociedad en la historia de México*. Siglo XXI: México.

Restrepo-Medina, M. A. (2018). Calidad de los hallazgos de auditoría. Análisis de caso de las contralorías territoriales de Colombia. INNOVAR. *Revista de Ciencias Administrativas y Sociales*, 28(70),115-128. [fecha de Consulta 17 de septiembre de 2022]. ISSN: 0121-5051. Disponible en: https://www.redalyc.org/articulo.oa?id=81857786009

Rosales-Romero, W., Pimentel-Rivero, A., Trujillo-Márquez, D., Bravo-García, L., Azán- Basallo, Y., & García-Romero, E.A. (2014). Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos. *Revista Cubana de Ciencias Informáticas,* 8(2),52-68. [Consultado 20 de Julio de 2022]. Disponible en https://www.redalyc.org/articulo.oa?id=378334194004

Solís, G. (2002). *Reingeniería de la Auditoría Informática*. Editorial Trillas: México.

UAEMéx. (2018). *Plan de estudios de Informática Administrativa*. Toluca, México: UAEMex.

Velásquez-Rueda, M.R. (2019). *Auditoría interna como herramienta pedagógica para las organizaciones. SIGNOS-Investigación en Sistemas de Gestión*, 11(1),145- 160. [Consultado 2 de junio de 2022]. Disponible en https://www.redalyc.org/articulo.oa?id=560465980010

Vivanco, M. E. (2017). Los manuales de procedimientos como herramientas de control interno de una organización. *Universidad y Sociedad*. 9(2), 247-252. Disponible en http://rus.ucf.edu.cu/index.php/rus

Wilson, A. (2019). *Lo esencial del hackeo: La guía para principiantes sobre hackeo ético y pruebas de penetración*. Editorial Babelcube Inc.: Estados Unidos de Norteamérica.

X. ANEXOS

Anexo 1

Contenido del perfil de puestos

Se presenta un ejemplo del contenido del perfil de puesto, que podría implementarse de acuerdo con la institución que así lo requiera para su aplicación, en su forma clásica, se deben contemplar como mínimo los siguientes puntos, los cuales se deben adecuar a las necesidades específicas del propio puesto:

Nombre genérico del puesto. _____
Objetivo del puesto. _____
Líneas de autoridad. _____
Responsabilidad sobre y funciones del puesto. _____
_____
_____
Requisitos del puesto: _____
_____
Conocimientos en sistemas en áreas similares. _____
_____
Otros conocimientos del puesto. _____
_____
Experiencia en el puesto. _____
Experiencia en el área. _____
Características de personalidad. _____
_____
Otros requerimientos. _____
Otros conocimientos. _____

Fuente: Elaboración propia. Basado en González & Berná (2018).

Anexo 2

Propuesta de una matriz DOFA para una auditoria de sistemas computacionales

El diseño de esta matriz consta de dos partes menciona Castro (2012) una es la identificación y la explicación de los aspectos que serán utilizados en el análisis, y la otra comprende las respuestas a la investigación sobre las fortalezas y debilidades internas del área de sistemas, así como a las amenazas y oportunidades externas que afectan el área.

MATRIZ DE EVALUACIÓN DE FORTALEZAS, DEBILIDADES, OPORTUNIDADES Y AMENACAS QUE IMPACTAN AL ÁREA DE SISTEMAS DE LA EMPRESA: _____

Fecha _____/_____/_____

Entrevistado: _____

Área o departamento: _____

Puesto: _____

Fuente: Elaboración propia. Basado en Castro (2012).

Con la finalidad de efectuar un estudio del funcionamiento del área de sistemas de la empresa, se solicita su valiosa respuesta para las siguientes preguntas**:**

(Guía de preguntas para realizar una entrevista)

1. ¿Conoce la misión, visión y objetivo general del área de sistemas computacionales de su empresa? Describa brevemente cada uno de ellos, y si en su opinión es necesario modificarlos o eliminarlos, coméntelo también.

2. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las fortalezas del área de sistemas y sus sugerencias para aumentarlas:

3. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las debilidades del área de sistemas y sus sugerencias para corregirlas o disminuirlas:

4. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las oportunidades del área de sistemas y sus sugerencias para aprovecharlas:

5. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las amenazas al área de sistemas y sus sugerencias para evitarlas o disminuirlas:

6. Considerando su estancia en el área y las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, señale cuál cree que sea la cultura informática del área y de la empresa:

7. ¿Cree que en la empresa existen estrategias para la prestación del servicio informático?

8. ¿Conoce el lugar que ocupa en el organigrama del área de sistemas? ¿Cree que dicha estructura es adecuada para satisfacer la prestación

del servicio informático en la empresa?

9. Considerando su estancia en el área de sistemas computacionales de la empresa, ¿cuál es, a su juicio, la idiosincrasia del área de sistemas?, ¿cuáles son los valores y las costumbres informáticas de esta área? Comente sus cambios y modificaciones:

10. ¿Conoce la filosofía de calidad del área de sistemas computacionales?, ¿qué opinión tiene de ella?

11. ¿Qué influencia ejercen en el cumplimiento de su trabajo los usuarios de los sistemas computacionales de la empresa?

Las preguntas anteriores son un ejemplo de muchas más cuestiones a investigar en las instituciones, de lo que se podría investigar sobre la matriz DOFA, todo esto de acuerdo con la infraestructura, tamaño y tipo de institución a la que se le aplique el instrumento.

Anexo 3

Glosario de Auditoria Informática

A

- **Amenaza**: Según [ISO/IEC 13335-1:2004], causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis de riesgos**: Según [ISO/IEC Guía 73:2002], uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Análisis de riesgos cualitativo**: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.
- **Análisis de riesgos cuantitativo**: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
- **Auditoría**: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.
- **Auditor**: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Autenticación**: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

B

- **Backup**: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla

acción evita numerosos, y a veces irremediables problemas si se realiza de forma habitual y periódica.

C

- **Centro de cómputo**: Es un área de trabajo cuya función es la de concentrar, almacenar y procesar los datos y funciones operativas de una empresa de manera sistematizada.

- **Checklist**: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

- **Cliente**: Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

- **COBIT**: (Control Objetives for Information and related Technology) Objetivos de Control para la información y tecnología relacionadas. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información, aceptados para ser empleados por gerentes de empresas y auditores.

- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

D

- **Datos**: Término general para la información procesada por una computadora.
- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Dominio**: Agrupación de objetivos de control de etapas lógicas en el ciclo de vida de inversión de TI.

E

- **Evaluación de riesgos**: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

G

- **Gestión de riesgos**: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

H

- **Hardware**: Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el ratón, las unidades de disco y el monitor.

I

- **Impacto**: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej,. pérdida de reputación, implicaciones legales, etc.

- **Información**: En sentido general, es todo lo que reduce la incertidumbre y sirve para realizar acciones y tomar decisiones.

- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1: 2004] propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **Infraestructura**: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

- **Internet**: Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

- **Inventario de activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **ISACA**: (*Information Systems Audit and Control Association*) Asociación de Auditoría y Control de los Sistemas de Información. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

- **ISO**: (*International Organization for Standardization*) Organización Internacional para la Normalización. Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

M

- **Mantenimiento Correctivo**: Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad, con el fin de prevenir su repetición.

- **Mantenimiento Preventivo**: Medida de tipo proactivos orientada a prevenir potenciales no-conformidades.

N

- **Norma**: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

O

- **Objetivo**: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

- **Organización**: Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones. Una organización puede ser pública o privada.

P

- **Políticas de seguridad**: Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

- **Procedimiento**: Forma especificada para llevar a cabo una actividad o un proceso.

- **Proceso**: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toman las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables, rol claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

R

- **Red**: Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: Network. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

- **Riesgo**: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo residual**: Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

S

- **Seguridad de la información**: Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.
- **Servidor**: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa *server*.
- **Software**: Componentes inmateriales del ordenador: programas, SO, etc.

T

- **TI**: Tecnologías de Información.
- **Tratamiento de riesgos**: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

U

- **Usuario**: Una persona o una entidad externa o interna que recibe los servicios empresariales de TI.

V

- **Valoración de riesgos**: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
- **Vulnerabilidad**: Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.