ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

Tema:

AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES

Proyecto de investigación previo a la obtención del título de Licenciado en Contabilidad y Auditoría

Línea de investigación:

ADMINISTRACIÓN EFICIENTE Y EFICAZ DE LAS ORGANIZACIONES PARA LA COMPETITIVIDAD SOSTENIBLE GLOBAL Y LOCAL

Autor:

Ricardo Jesús Ramírez Freire

Directora:

PhD. Verónica Leonor Peñaloza López

Ambato – Ecuador

Octubre 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **RICARDO JESÚS RAMÍREZ FREIRE,** con cédula de ciudadanía **1805324496**, autor del trabajo de graduación titulado: "AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES", previo a la obtención del título profesional de **LICENCIADO EN CONTABILIDAD Y AUDITORÍA**, en la escuela de **ADMINISTRACIÓN DE EMPRESAS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, octubre 2024

Ricardo Jesús Ramírez Freire

CC. 1805324496

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES

Línea de investigación:

ADMINISTRACIÓN EFICIENTE Y EFICAZ DE LAS ORGANIZACIONES PARA LA COMPETITIVIDAD SOSTENIBLE GLOBAL Y LOCAL

Autor:

Ricardo Jesús Ramírez Freire

Verónica Leonor Peñaloza López, Ing. PhD. f._____
CC. 1803585718
CALIFICADOR

Hernán Paúl Ortiz Coloma, Dr. Mg. f._____
CALIFICADOR

Mario Roberto Altamirano Hidalgo, Dr. Mg. f._____
CALIFICADOR

Fredy Leonardo Ibarra Sandoval, Ing. Mg. f._____
DIRECTOR ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

Pontificia Universidad Católica del Ecuador
DIRECCIÓN
ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

Diego Gonzalo Coca Chanalata, Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Octubre 2024

DEDICATORIA

Dedico esta tesis a mi padre Kleber Ramírez y a mi madre Rosa Freire, con todo mi amor y gratitud. Gracias por su amor incondicional, por sus sacrificios y por enseñarme el valor del esfuerzo y la perseverancia. Gracias por apoyarme para seguir estudiando y poder obtener mi título de tercer nivel. Su apoyo constante y sus palabras de aliento me han guiado en cada paso de este camino. Este logro es tanto mío como suyo, y no habría sido posible sin su confianza y dedicación. Los amo profundamente.

Gracias por ser un apoyo para mi cuando más lo he necesitado, sin su ayuda este logro no habría sido posible. Espero que esta tesis sea una pequeña muestra de mi gratitud hacia ustedes por su esfuerzo para que yo ingrese a esta prestigiosa universidad. Finalmente, gracias por dejarme creer en mis sueños y alentarme a que si quiero cumplir alguno de ellos tengo que trabajar duro y esforzarme, porque solo así podré cumplir todo lo que me proponga.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios que me ha dado la fuerza, la sabiduría y la perseverancia para poder culminar mi carrera universitaria. Gracias a su guía y bendiciones que han sido fundamentales en cada paso de este largo, pero hermoso proceso académico, sin su presencia en mi vida este logro no habría sido posible. También quiero agradecer a mis padres, quienes han sido un motor muy importante para mí y mi mayor fuente de inspiración. Gracias por su amor incondicional, su apoyo constante y sus sacrificios invaluables que permitieron que yo ingrese a esta prestigiosa universidad, la pontificia universidad católica del ecuador sede Ambato. La confianza que han depositado en mi me ha motivado a esforzarme siempre por alcanzar mis metas. Este logro también es de ustedes

De la misma forma quisiera agradecer a mi familia, por su cariño, comprensión y apoyo incondicional a lo largo de estos años. Cada palabra de aliento, cada gesto de amor y cada sonrisa compartida ha sido un impulso invaluable en mi camino. Gracias por creer en mí y estar siempre presentes. Por último, pero no menos importante quisiera agradecer a todos mis amigos, que han estado para mí en las buenas y en las malas. Gracias por su cariño, por esas palabras de aliento, por esos momentos compartidos, por todas las risas que hemos tenido, créanme que siempre estarán presente en mi memoria, además agradecerles por su paciencia y por entenderme en los momentos que he querido estar ausente. Su amistad ha sido muy importante para mí en este camino y siempre los llevaré en mi corazón.

RESUMEN

La Auditoría es una actividad importante para las empresas porque así se puede llevar un mejor control de todo lo que sucede dentro de la misma en todas sus áreas, la auditoría en el área de los sistemas es de igual importancia, así se salvaguarda toda la información ya sea contable o información confidencial. De ahí la necesidad de esta investigación para analizar si el sistema que maneja la empresa es seguro para salvaguardar los datos contables y si el sistema presenta las medidas adecuadas ante posibles ciberataques. Esta investigación es importante para la empresa, así se podrá analizar si el sistema que maneja la misma es de ayuda para la realización de las actividades, además de verificar el nivel de seguridad y protección de los datos contables internos.

El objetivo general de la investigación es proponer una Auditoría informática a los sistemas contables en la Empresa Eléctrica Ambato regional centro norte S.A. Dirigido al departamento financiero en el área contable y la confiabilidad de este para la correcta protección de los datos contables. La metodología planteada será con un alcance descriptivo analítico con un enfoque mixto, esperando que los datos encontrados sirvan para el análisis de la seguridad del sistema y con eso analizar las ventajas o falencias que el sistema presente.

Palabras clave: sistemas de información, seguridad, vulnerabilidad, protección.

ABSTRACT

Auditing is an important activity for companies because it allows them to have a better control of everything that happens within the company in all areas, auditing in the area of systems is equally important because it safeguards all information, whether accounting or confidential information. Hence the need for this research to analyze whether the system that manages the company is safe to safeguard accounting data and if the system presents adequate measures against possible cyber-attacks. This research is important for the company because it will be possible to analyze whether the system that the company manages is helpful for the performance of its activities, in addition to verifying the level of security and protection of internal accounting data.

The general objective of the research is to propose a computer audit to the accounting systems in Empresa Eléctrica Ambato regional centro norte S.A. Directed to the financial department in the accounting area and the reliability of this for the correct protection of accounting data. The methodology proposed will be with a descriptive analytical scope with a mixed approach, hoping that the data found will serve for the analysis of the security of the system and thereby analyze the advantages or weaknesses that the system presents.

***Keywords**: information systems, security, vulnerability, protection.*

ÍNDICE GENERAL DE CONTENIDOS

INTRODUCCIÓN

En la actualidad, la tecnología está presente en todas las organizaciones, ya sea en la parte automotriz con la creación de nuevos vehículos mucho más modernos, con las redes sociales que permiten a las personas acercarse a pesar de estar a kilómetros de distancia o con la creación de teléfonos cada vez más sofisticados y con mayores funciones que hacen la vida de las personas mucho más fácil. Es un hecho innegable que hoy en día millones de computadoras están enlazadas a la red debido a que se usan en escuelas, empresas, hospitales, universidades, bancos, fabricas, micro locales, etc.

La dependencia en gran medida de estas máquinas es porque facilitan la vida y además ayudan a optimizar el tiempo en ciertas actividades. En este sentido se engloban actividades como, por ejemplo: realizar informes, redactar oficios, poder diseñar nuevos edificios, elaborar libros, elaborar artículos, para realizar estados financieros y así poder llevar un mejor control de los ingresos contables, etc. En si son muy importantes hoy por hoy, si no existiesen sería muy difícil para los seres humanos realizar todas las actividades que se han mencionado con anterioridad.

La tecnología ha permitido el desarrollo humano, pero como toda creación tiene sus ventajas y sus riesgos. En relación con este tema Steve Jobs mencionó que "La tecnología es solo una herramienta. En términos de cómo la usas, hay gente buena y gente mala." Es decir que como la tecnología está al alcance de cualquier persona, hay gente que puede darle un buen uso, pero al mismo tiempo hay gente que emplea la tecnología de manera inadecuada o ciertas personas que la ven como un medio para poder estafar a los demás. En este contexto, del mal uso de la tecnología nace la necesidad de evaluar y verificar el buen manejo de la misma. Es asi como aparece la Auditoría que, según Flérida María Alcívar Cedeño, María Paulina Brito Ochoa y Martha Jaroslava Guerrero Carrasco (2016) mencionan que el término "auditoría" abarca tres conceptos interconectados: la labor del auditor, el estudio de la economía empresarial y la locación donde se llevan a cabo estas actividades.

Dentro de este orden de ideas, igualmente María Alcívar Cedeño, María Paulina Brito Ochoa y Martha Jaroslava Guerrero Carrasco (2016) indican que auditar implica examinar los procesos y la actividad económica de una organización para asegurar su conformidad con las leyes y estándares éticos. Principalmente, se refiere a la auditoría contable, que consiste en analizar las cuentas de una entidad. Hay que mencionar que la Auditoría no solo puede ser a las cuentas de una entidad, al contrario, existen varias clases de auditorías como lo son: Auditoría externa o legal, Auditoría interna, Auditoría operativa, Auditoría publica o gubernamental y Auditoría de sistemas.

Por tal motivo, María Alcívar Cedeño, María Paulina Brito Ochoa y Martha Jaroslava Guerrero Carrasco (2016) mencionan que la auditoría es un tipo de evaluación sistemática que suele realizarse siguiendo una metodología específica y generalmente involucra a un auditor externo. El cuál es el encargado de esta evaluación, analiza minuciosamente las acciones y documentos de la empresa para determinar la idoneidad de las medidas tomadas y su impacto en la compañía. La auditoría no se limita a la verificación de los activos financieros, sino que también proporciona directrices para mejorar las actividades empresariales, al evaluar y recomendar acciones específicas, así como al revisar el desempeño individual dentro de la organización. Es esencial para una empresa medir su desempeño organizacional para evaluar el logro de los objetivos establecidos, la auditoría constituye la herramienta principal para esta tarea.

La tecnología es una herramienta útil para el ser humano, pero con ella se presenta el riesgo de diversas formas de robo o filtración de información. Las auditorías informáticas permiten evaluar y medir si el sistema de seguridad que se maneja en la empresa realiza sus funciones adecuadamente, esto permite evidenciar si hay alguna falla que afecte al funcionamiento de la entidad y que además perjudique la imagen y la reputación de la misma. Hay que tomar en cuenta que dentro de una empresa se encuentra información importante, como, por ejemplo: balances contables, una base de datos de los clientes de la empresa, datos financieros como lo son información de tarjetas de crédito o de débito, códigos fuente y algoritmos, descripciones de procesos patentados y metodologías operativas, credenciales de

redes como son nombres de usuario y contraseñas, registros de talento humano y datos de los trabajadores, documentos privados almacenados en las computadoras, entre otros.

En la actualidad varias empresas han sufrido ataques en los sistemas de información que manejan, por ejemplo, el caso del Banco Pichincha que debido a fallas en su código ha sido víctima de robo de datos. Otro caso importante es el de Citibank que fue hackeado en Estados Unidos, Citigroup afirmó haber sido víctima de un hackeo, y que los atacantes accedieron a datos de tarjetas de crédito de unos 200.000 clientes en Estados Unidos, según se reportó esto también les ha ocurrido a grandes empresas, incluyendo a RSA Security y Lockheed Martin. El problema de que los sistemas de seguridad tengan una alta vulnerabilidad no solo conlleva a un robo de base de datos, también se pone en duda la confiabilidad de la empresa, además de ganar una mala reputación con sus clientes que no saben si sus datos están seguros.

También, un sistema inseguro provoca robo de información confidencial como lo son las credenciales de acceso a los diferentes programas internos de la empresa. Finalmente, la falta de autenticación para ingresar al sistema también es una vulnerabilidad, esto quiere decir falta de verificación de la persona que está ingresando al sistema interno, ocasionando suplantación de identidad recayendo nuevamente en el robo de información, además que se puede realizar acciones ilegitimas en nombre de la víctima. En tal sentido se plantea como problema de investigación: La vulnerabilidad de los sistemas de información contable.

Como se puede evidenciar la Auditoría tiene importancia no solo para lo que respecta al área contable sino también a la parte informática y aún más si se trabaja con sistemas contables que hoy en día son muy útiles para los contadores porque simplifican varios procesos haciéndolos más agiles y eficientes. De allí surge la idea a defender de que la Auditoría a los sistemas de información minimiza la vulnerabilidad de los sistemas contables. Dado que con un buen control periódico de los sistemas y valga la redundancia una auditoría a los mismos, se puede llevar un mejor registro de la funcionabilidad de los sistemas de la empresa, para asi evitar

los ya mencionados ataques cibernéticos. Es asi que en base a lo ya explicado en este concepto el objetivo general es proponer una Auditoría informática a los sistemas contables para la Empresa Eléctrica Ambato regional centro norte S.A. Para poder analizar el funcionamiento del sistema contable que se maneja.

Para lo cual se han planteado como objetivos específicos, en primer lugar, fundamentar teóricamente la auditoría de los sistemas informáticos y el control de datos contables, con la explicación de los conceptos básicos y necesarios respecto a la auditoría informática. Adicionalmente diagnosticar el cumplimiento de los elementos del control interno para los sistemas informáticos contables. Y, por último, identificar los componentes y las fases de la Auditoría informática a los sistemas contables de la Empresa Eléctrica Ambato regional centro norte S.A.

Para este proyecto la metodología planteada tiene un alcance descriptivo y analítico con un enfoque mixto cualitativo y cuantitativo que a través de instrumentos como cuestionarios y entrevistas se recopilara la información requerida para el diagnóstico de la empresa sujeto a la investigación. Es así como este proyecto es importante debido a que cualquier empresa está expuesta a un ataque cibernético y por ende al robo de su información tanto contable como administrativa. Además de sustracción de datos también significaría un daño a la imagen de la empresa y a su reputación con sus clientes como ya se mencionó con anterioridad. Para concluir la importancia en si del proyecto es que las auditorías informáticas son igualmente necesarias en una empresa al igual que lo son las auditorías financieras, porque ayudan a la protección de los datos contables como medio de control interno.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Antecedentes teóricos de la auditoría informática

En lo que respecta al ámbito de la Auditoría, aún no existe consenso sobre cómo nombrar la aplicación de esta práctica a los sistemas computarizados o informáticos. Ese problema conlleva a confusiones para varios lectores e investigadores que desean analizar más a fondo sobre este tema. Por ejemplo, en la auditoría de gestión financiera que son realizadas por los mismos auditores internos a los sistemas de inventarios de las compañías, los cuales son computarizados, ¿Con qué nombre se les debería referir? Hay personas que tienen el criterio de que podría ser considerada como una “Auditoría Informática”, otros en cambio opinan que ese término netamente se lo debe catalogar a la función informática exclusivamente.

Dentro de este marco, Blanco Encinosa, L. J. (2008) menciona que, el desafío no se limita únicamente a cuestiones terminológicas. La dificultad se intensifica al traducir los diversos términos de un idioma a otro. Muchos auditores aún mantienen la perspectiva de que la auditoría de sistemas informáticos no debería ser parte de su ámbito profesional, sino que debería ser realizada por personal especializado en informática. Estos profesionales se autodenominan "auditores" y ven a los auditores tradicionales como una categoría más general, a la que llaman "auditores informáticos".

Es debido a esta situación por la que varios autores tienen su punto de vista respecto a la denominación que debería darse o a la aplicación que debería tener la auditoría informática. Inicialmente en el libro “Conceptos de la Auditoría de sistemas” Naranjo, A. (2009) menciona que la Auditoría de Sistemas implica verificar los controles en el procesamiento de la información, el desarrollo de sistemas y su instalación, con el propósito de evaluar su eficacia y proporcionar recomendaciones. Esta actividad consiste en examinar y evaluar los procesos del Área de Procesamiento Automático de Datos (PAD) y el uso de los recursos involucrados, con el fin de determinar el nivel de eficiencia, efectividad y economía

de los sistemas informáticos, y ofrecer conclusiones y recomendaciones para corregir deficiencias y mejorar el rendimiento.

Además, hay que señalar que Naranjo, A. (2009) dice también que se trata de un examen objetivo e independiente, crítico y sistemático, selectivo según muestras, de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados. El objetivo final es emitir una opinión profesional e imparcial sobre la eficiencia en el uso de los recursos informáticos, la validez de la información y la efectividad de los controles establecidos.

Por otro lado, Chicano Tejada, E. (2023) manifiesta que la auditoría implica un examen detallado de los sistemas informáticos con el propósito de descubrir, identificar y describir las diversas vulnerabilidades que puedan surgir. Cuando se llevan a cabo funciones de auditoría en un sistema de información, los auditores deben adherirse a normas éticas y un código deontológico para cumplir con sus objetivos de manera profesional y rigurosa.

Este código deontológico consiste en una serie de principios que establecen los derechos exigibles a ciertos profesionales durante la realización de sus actividades, con el fin de alinear los comportamientos profesionales con principios éticos y morales adecuados. En este mismo sentido, Chicano Tejada, E. (2023) argumenta que, en el ámbito de la auditoría informática, existe una organización internacional, conocida como Information Systems Audit and Control Association (ISACA), que desarrolla estándares de auditoría y control de sistemas de información aceptados por la comunidad de auditoría en general. Además, ISACA otorga el certificado CISA (Certified Information Systems Auditor) a aquellos que cumplan con los requisitos establecidos en términos de normativas, código ético, procedimientos de control, entre otros aspectos.

Otra aportación importante es la del Comité Internacional de Prácticas de Auditoría, institución responsabilizada con las normas y estándares de esta actividad, en el documento 110, “Glosario de Términos”, expresa:

> Auditoría: El objetivo de una auditoría de estados financieros es hacer posible al auditor el expresar una opinión sobre si los estados financieros están preparados, respecto de todo lo sustancial, de acuerdo a un marco de referencia para reportes financieros identificado o a otros criterios. Las frases usadas para expresar la opinión del auditor son ‘dar un punto de vista verdadero y justo’ o ‘presentar en forma apropiada, en todos los aspectos sustanciales’, que son términos equivalentes.

Una aportación interesante es la que expresa W. B. Meigs (1983), en su obra Principios de auditoría. Su autor define:

> Una auditoría es un examen de los estados financieros de una compañía, realizada por una firma de contadores públicos independientes. La auditoría consiste en una investigación minuciosa de los registros contables y otras pruebas que apoyan esos estados financieros.

De modo que, al analizar los diferentes criterios mencionados por cada uno de los autores, se puede decir que concuerdan en que la auditoría informática es de gran utilidad para poder verificar y analizar las posibles vulnerabilidades que se presente en la empresa, esto para poder evaluar su eficacia y funcionamiento. Además, en base a las opiniones de los autores se destacan aspectos como que la auditoría es un procedimiento sistemático para recopilar pruebas sobre transacciones económicas que se reflejan en informes y estados financieros. Asimismo, se trata de un conjunto esencial de métodos y procedimientos lógicos y organizados que el auditor debe seguir meticulosamente para obtener la información necesaria.

Con el fin de poder analizar la vulnerabilidad de los sistemas, para asi percibir y analizar las deficiencias que los mismos presenten, y asi optar por darles el adecuado tratamiento y obtener un mejor control de la información que la compañía posea. Además, hay que recalcar que los autores también coinciden con que la comprobación de los hechos, la medición y la comparación con lo reflejado en los informes, debe estar acorde a principios metodológicos, que garanticen la estandarización de procedimientos y métodos. Lo normal es que el auditor se base

en los “Principios de contabilidad generalmente aceptados”, pero también debe hacerlo en leyes, reglamentos, resoluciones, convenios contractuales, manuales de normas y procedimientos, etc. Sin olvidarse además de tener presente el código deontológico explicado con anterioridad.

Desde una perspectiva más general y en relación con este proyecto se puede decir que a lo largo de la historia, la auditoría ha tenido como uno de sus principales objetivos la protección de los activos y datos de las entidades en las que se lleva a cabo, siendo este propósito más evidente en el caso de las auditorías internas, aunque también se aplica en las externas. Para lograr este fin, se ha adaptado a las tecnologías predominantes en el tratamiento de la información. En la actualidad, estas tecnologías son las informáticas, y la auditoría realiza su labor haciendo uso de las mismas, un enfoque que algunos autores denominan "auditoría con la informática". Además, se lleva a cabo en entornos organizacionales completamente informatizados, como se menciona en la Norma Internacional de Auditoría 15 sobre "auditoría en un ambiente de información por computadoras".

Es así como el auditor contemporáneo se desenvuelve en un entorno informatizado y es impensable que esté desconectado de este aspecto. Por lo tanto, llevar a cabo su labor en este contexto se ha vuelto normal y habitual. Como se puede evidenciar, y como ya se mencionó en un inicio la tecnología ha crecido con el paso de los años y asi también la forma en la que se desarrollan los procesos contables. De igual manera la forma en desarrollar auditorías ha cambiado debido a que antes solo se tenía en cuenta una auditoría en general, pero con el pasar del tiempo se ha descubierto otras ramas o tipos de auditorías como, por ejemplo: Auditoría externa o legal, interna, operativa, pública o gubernamental, Financiera y de sistemas o Auditoría Informática.

Dado que este proyecto se trata de una auditoría de sistemas de información como elemento de control de los programas contables, es importante mencionar la contextualización de la auditoría informática. En este sentido, Altp, V. T. L. E. (2018) menciona que la auditoría informática es un procedimiento realizado por expertos especialmente entrenados, que implica recopilar, clasificar y valorar pruebas para

verificar si un sistema de información protege los activos de la empresa, preserva la integridad de los datos, cumple eficazmente con los objetivos organizacionales, utiliza los recursos de manera eficiente y cumple con las leyes y regulaciones aplicables. Este concepto como se puede analizar es muy parecido aI de la auditoría en general, pero con ciertos detalles que la hacen diferente al resto.

Los objetivos de esta auditoría son: 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 y la revisión de la eficaz gestión de los recursos informáticos. La importancia de adoptar esta auditoría para una empresa es que sirve para mejorar algunas características dentro de la misma, como, por ejemplo: el desempeño, la fiabilidad, eficacia, rentabilidad, seguridad y privacidad. La exigencia de disponer de directrices y recursos uniformes para llevar a cabo la auditoría informática ha impulsado la aparición y evolución de prácticas mejoradas como COSO entre otros, que se explicará de una forma más detallada en el epígrafe 1.2.

Por consiguiente, Altp, V. T. L. E. (2018) menciona que, existen varios tipos de auditorías informáticas, entre los cuales destacan: Auditoría legal del Reglamento de Protección de Datos, que se encarga del cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos; Auditoría de los datos, que es la encargada de la clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas; Auditoría de las bases de datos que maneja los controles de acceso, de actualización, de integridad y calidad de los datos; Auditoría de la seguridad física, se refiere 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, circuito cerrado de televisión (CCTV), vigilantes, etc.) y protecciones del entorno; Auditoría de la seguridad en producción, que se encarga de analizar los errores, accidentes y fraudes.

Hay que tomar en cuenta además que dentro de una auditoría informática existen pruebas y herramientas para efectuarla de manera adecuada. Es por ello que, Altp,

V. T. L. E. (2018) explica que al momento de realizar la auditoría el auditor puede realizar dos tipos de pruebas, las cuales son: Pruebas sustantivas y Pruebas de cumplimiento. Las pruebas sustantivas Verifican el grado de confiabilidad del sistema informático 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. Por otro lado, de igual manera Altp, V. T. L. E. (2018) dice que las pruebas de cumplimiento en cambio 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.

1.2. Análisis del control interno como medio de protección a los sistemas contables

En el ambiente empresarial, se puede decir que toda corporación necesita de un control, este control es impuesto o dictaminado por la administración de la corporación con el fin de procurar la eficiencia, eficacia y economía de la misma. Es de gran importancia que para el cumplimiento de los controles empresariales se tiene que presentar una evidencia, es decir que todas las acciones que se realicen en la empresa deben quedar registradas para asi poder comprobarlas, demostrarlas y en el caso que lo amerite auditarlas.

Es por eso que, Mantilla Blanco, S. A. (2011) indica que el concepto de control interno se define de diversas maneras y, como resultado, se implementa de maneras diversas, lo que puede representar su principal desafío. En un esfuerzo por abordar esta complejidad, se ha intentado elaborar una definición que englobe los elementos comunes y logre consenso al respecto. Entre estos esfuerzos, el enfoque más exitoso y reconocido internacionalmente es el presentado por COSO, aunque existen otras opciones notables como Turnbull (en el Reino Unido) y CoCo (en Canadá).

Por consiguiente, Mantilla Blanco, S. A. (2011) añade que, según COSO, el control interno se entiende como un proceso llevado a cabo por la junta directiva, la alta

dirección y otros miembros del personal, con el fin de proporcionar una seguridad razonable en relación con el logro de los objetivos organizacionales. Estos objetivos abarcan la eficacia y eficiencia de las operaciones, la confiabilidad de la información financiera, el cumplimiento de normativas y obligaciones, así como la protección de activos. Se menciona también que el control interno se divide en cinco componentes según el proceso: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y monitoreo.

No obstante COSO no es el único que se puede implementar en las empresas, por otro lado, Mantilla Blanco, S. A. (2011) también hace referencia a Turnbull y CoCo, en donde explica que estos dos comparten similitudes, aunque enfatizan aspectos diferentes. Turnbull se concentra principalmente en el gobierno corporativo y en las estructuras duales de toma de decisiones típicas del Reino Unido y algunos otros países de la Unión Europea. Por otro lado, CoCo aborda el control de manera más amplia, centrándose en las personas y dando importancia al autocontrol y la autoevaluación. Ambos coinciden en la importancia de asegurar, de manera razonable, el cumplimiento de los objetivos organizacionales, y en que la responsabilidad principal del control interno recae en los directivos principales.

En otras palabras, estos sistemas ayudan a que la empresa logre cumplir los objetivos planificados por los ejecutivos o gerencia de la empresa. Y asi analizar las áreas o secciones en donde existen dificultades o son las menos productivas de la empresa para planificar un plan de acción y mejorar estas zonas. Dentro de este contexto, Estupiñán Gaitán, R. (2016) agrega que inicialmente puede existir dos tipos de control interno dentro de una organización, el control interno administrativo y el control interno contable. Ambos con ciertas diferencias muy notarias, pero con ciertas características que servirán como apoyo para el cumplimiento de los objetivos empresariales.

Así pues, Estupiñán Gaitán, R. (2016) menciona que el control interno administrativo hace referencia a que cada empresa adopta un plan de organización que incluye sus propios procedimientos y métodos operativos y contables, diseñados para facilitar el logro de sus objetivos administrativos mediante el

establecimiento de un entorno adecuado. Esto permitirá a la empresa tener un mejor análisis de los procedimientos realizados por los colaboradores y asi mejorar cada día más.

Por otro lado, Estupiñán Gaitán, R. (2016) añade que el control interno contable en cambio dice que como resultado del control administrativo sobre el sistema de información, se desarrolla el control interno contable como un instrumento con los siguientes objetivos: garantizar que todas las operaciones se registren de manera oportuna, por el monto correcto, en las cuentas adecuadas y durante el período contable correspondiente, con el fin de facilitar la preparación de estados financieros y mantener un control contable de los activos; asegurar que todo lo registrado en contabilidad exista físicamente y que todo lo existente esté registrado contablemente, investigando cualquier discrepancia para tomar las medidas correctivas apropiadas; y verificar que las operaciones se lleven a cabo conforme a las autorizaciones tanto generales como específicas otorgadas por la administración.

Se debe tener en cuenta que el control interno trae implícito un costo, este representa el costo de su evidencia. En base a este contexto Pereira Palomo, C. A. (2019) opina que, a modo de ejemplo de la creación de formatos para el control interno, podemos mencionar los registros utilizados para documentar las entradas y salidas de almacén. Estos registros, como parte del control interno, suelen diseñarse con un número consecutivo y deben incluir los nombres y firmas de quienes elaboran, autorizan y reciben los productos. Este tipo de procedimiento no está presente en una pequeña empresa informal sin un sistema de control establecido, donde los movimientos de inventario pueden registrarse en una libreta o, en muchos casos, simplemente se realizan verbalmente en empresas familiares, sin que esto tenga consecuencias negativas, el propietario evalúa los resultados globalmente en base a las diferencias entre las entradas y salidas de efectivo.

Hay que recalcar que, si una empresa no posee un sistema de control interno, en primer lugar, no tiene un correcto manejo de lo que sucede en la misma ni tampoco una organización adecuada para poder lograr los objetivos planificados, por

consiguiente, tampoco va a crecer empresarialmente, debido a que se vería limitada por la competencia. No hay que olvidarse que las grandes empresas mundiales, un día fueron pequeños locales, pero para crecer tuvieron que organizarse administrativamente, implementar procesos y adaptarse a las nuevas tendencias de la época. Si una empresa no avanza conforme el tiempo y no se adapta a las nuevas modalidades, el resultado será el estancamiento de la compañía.

En la actualidad, se puede evidenciar que, si una empresa no cuenta con los recursos tecnológicos necesarios o no se moderniza en los procesos, la empresa empieza a bajar en ventas y esto conlleva al quiebre de la misma. En base a este contexto, un caso evidente de que si una empresa no se adapta a las nuevas tendencias tecnológicas las consecuencias pueden ser graves, es el de kodak. Esta empresa fue fundada por George Eastman que tenía un futuro prometedor como banquero, pero decidió renunciar a su trabajo para dedicarse hacer que la fotografía sea accesible a las personas. La empresa se basaba principalmente en la venta de rollos y suministros para imprimir las fotografías. Vendían las cámaras a bajos costos y ganaban dinero cuando la gente tomaba e imprimía las fotos.

A comienzos de los años noventa, Kodak disfrutaba de un período de esplendor, con una plantilla de más de 140,000 empleados a nivel mundial y considerables beneficios. La compañía se destacaba por su innovación y éxito, y era difícil concebir su declive. Sin embargo, el punto de inflexión que marcó el inicio de su declive surgió desde sus propios laboratorios, con el desarrollo de la primera cámara digital. Uno de los investigadores de Kodak desarrolló el primer prototipo en 1975, cuando la tecnología digital era costosa y de calidad inferior. Con el paso del tiempo, la fotografía digital se volvió cada vez más importante, y Kodak, consciente de esta tendencia, también destinó parte de sus recursos al desarrollo de cámaras digitales. Sin embargo, otros fabricantes lograron producir cámaras digitales de mayor calidad.

Este caso evidencia que, si no se piensa a futuro, si se descuida a la competencia o si simplemente no se adopta procesos más digitalizados, no se podrá crecer como

empresa. De allí, que para que una empresa hoy en día sea más productiva, facilite sus procesos, mejore sus ventas, lleve un mejor control de inventarios, entre otros. Es necesario que cuente con sistemas informáticos contables. De este modo, Bitrix, E. (2024) menciona que un programa informático de contabilidad específicamente creado para empresas de pequeña escala puede ser la solución ideal para reducir errores humanos, automatizar ciertas tareas y, al mismo tiempo, mejorar la gestión de los ingresos y gastos mensuales.

Con tan solo unos clics, es posible mantener toda la contabilidad de manera organizada y concentrada en un solo lugar. Sucede pues, que, con la implementación de un sistema informático contable la empresa obtiene varios beneficios. En función de lo explicado Bitrix, E. (2024) menciona que los principales beneficios de usar sistemas informáticos contables son: Procesamiento y administración simplificados de las transacciones, mejor almacenamiento y manejo eficaz de datos, posibilidad de facturación electrónica, personalización de documentos, generación de reportes históricos, mayor control, menores costos, automatización, nivel de seguridad alto, entre otros.

No obstante, como se mencionó en un inicio la tecnología tiene sus ventajas y desventajas, es asi que Bitrix, E. (2024) menciona que dentro de las desventajas de un software contable pueden encontrarse: Necesidad de conocimientos tecnológicos previos o entrenamiento, requerimiento de actualizaciones para su buen funcionamiento, algunos ocasionan un gasto extra para la organización, problemas para adaptar un programa genérico a las necesidades puntuales de la empresa.

Es debido a esta situación que se genera la necesidad de la protección de datos en las empresas, ningún sistema o ninguna empresa está libre de cualquier hacker que intente robar la base de datos o la información de las compañías. Asi pues, Technologies, V. (2024) menciona que la seguridad de los datos empresariales abarca el proceso de suministro, gestión y supervisión de la seguridad en todos los activos y repositorios de datos de una empresa. Es un concepto amplio que engloba diversas herramientas, políticas, técnicas y marcos diseñados para asegurar la

protección de los datos, sin importar su ubicación dentro de la organización.

Esto quiere decir que no importa la ubicación del archivo o documento, lo importante es que este seguro y libre de cualquier filtración. Además, Technologies, V. (2024) añade que este enfoque implica principalmente la implementación y administración de prácticas y estándares de seguridad de datos en la empresa. Estos estándares y procedimientos pueden variar dependiendo del uso y la importancia de los datos. Por ejemplo, se pueden proteger datos altamente confidenciales mediante la aplicación de autenticación multifactorial, restricciones de acceso y técnicas de cifrado. Esta última siendo la más utilizada hoy en día en los sistemas de mensajería, con el fin de garantizar que las conversaciones se mantengan seguras.

Por último, Technologies, V. (2024) menciona que la seguridad de los datos empresariales tiene como objetivo proteger a la organización contra la pérdida de datos y garantizar la seguridad en todos los dispositivos que utilizan datos. Esto se logra mediante la aplicación de tecnologías convencionales de seguridad informática, como antivirus y firewalls, junto con políticas y estándares de seguridad de datos que rigen y supervisan todo el proceso. Dentro de este orden de ideas y con la información previamente explicada es por lo que se necesita una correcta protección de datos a los sistemas contables de las empresas, esto con la ayuda de auditorías informáticas.

1.3. Importancia de la ciberseguridad en las empresas de servicios

En el ámbito de la tecnología existe la ciberseguridad, Cisco (2022) la define como la actividad encargada de proteger redes, sistemas y programas de ciberataques. No obstante, también hay que mencionar que la ciberseguridad implica proteger activamente diversos elementos como computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques maliciosos. También denominada seguridad de la tecnología de la información o de la información electrónica, su alcance abarca desde entornos empresariales hasta la informática móvil. Dicho de otro modo, Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021)

mencionan que, en la actualidad, la ciberseguridad ha adquirido una relevancia significativa debido al progreso tecnológico que exige la entrega de datos personales a diversas entidades y empresas, tanto públicas como privadas.

Estas entidades pueden incluir instituciones financieras, organizaciones encargadas del manejo de datos e información personal, así como entidades jurídicas y de control, con el fin de acceder a una amplia gama de bienes y servicios. Esta situación plantea un desafío en términos de control sobre la información, lo que facilita el acceso a la misma por parte de cualquier organización, institución o individuo.

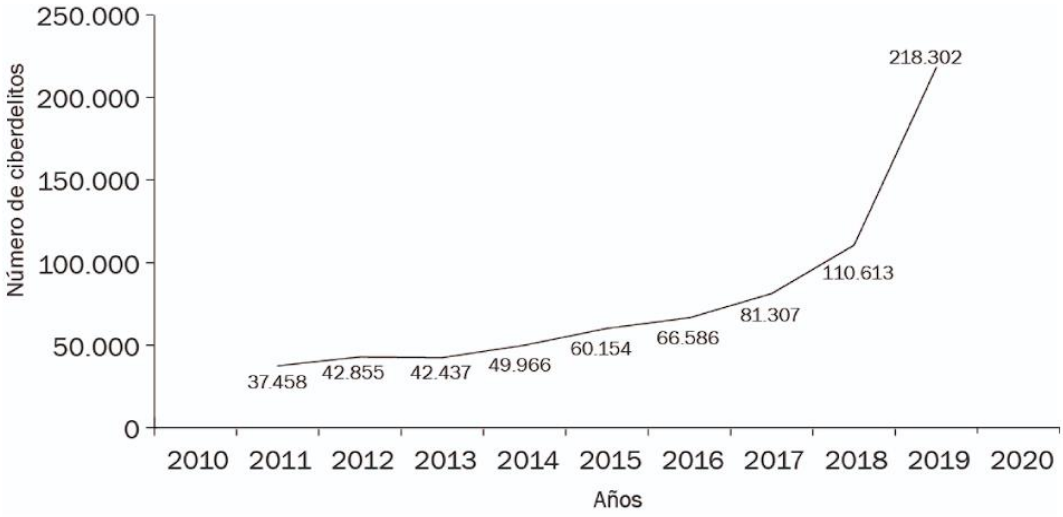
En este contexto, se puede decir que en la actualidad todas las empresas ya sean públicas o privadas están expuestas a ataques o dicho de una manera más técnica, ciberataques. Pero ¿Qué es un ciberataque?, Cisco (2022) lo define como un ataque organizado por personas maliciosas en contra de un sistema informático que apuntan a acceder de manera ilegal a un sistema, modificar o robar los datos confidenciales de personas o empresas. En relación con este tema, Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) destacan el Convenio de Budapest (CETS nº185) sobre ciberdelincuencia (o convenio sobre cibercrimen), que es el primer tratado internacional que pretende hacer frente a los ciberdelitos. Tal convenio es, de hecho, el único acuerdo internacional vinculante sobre este tema.

Del mismo modo Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) añaden también que hay más de 50 países que se han adherido al convenio. España lo firmó el 23 de noviembre de 2001 y lo ratificó el 1 de octubre de 2010. Tal ratificación ha tenido como consecuencia que, en la reforma del Código Penal español, de 2015, se introdujeran artículos para tipificar diferentes tipos de cibercrímenes, como el acceso no autorizado a sistemas informáticos.

Como se ha mencionado en anteriores párrafos, la tecnología avanza cada día y eso conlleva a que de igual manera las formas de ciberdelincuencia crezcan. Para comprender la relevancia de este tipo de crímenes, es crucial resaltar la cantidad

de incidentes que han ocurrido en los últimos años y cómo han ido en aumento con el tiempo.

Figura 1. Evolución del número de ciberdelitos entre 2011 y 2019.



Fuente: Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020). Ciberseguridad: (1 ed.). Madrid, Los libros de la Catarata. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/233122?page=7.

En relación con lo antes expuesto, Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) explican que, solo en 2019 se cometieron 218.302 delitos, lo que representa el 10% de todos los delitos cometidos y supone un crecimiento del 35,81% respecto al año 2018. De todos ellos, 192.375 estuvieron relacionados con el fraude informático, 12.782 fueron amenazas y coacciones, se llevaron a cabo 4.275 falsificaciones informáticas y 4.004 accesos e interceptaciones ilícitas, 1.422 fueron delitos contra el honor, 1.774 delitos sexuales, 1.473 se relacionaron con la interferencia en los datos y en los sistemas, y 197 lo fueron contra la propiedad industrial/intelectual. Las tres comunidades autónomas con mayor índice de ciberdelitos fueron: Cataluña con 41.577, Madrid con 37.016 y Andalucía con 28.655.

Debe señalarse que un ciberataque puede ser de cualquier tipo, por ejemplo, un virus informático. Avast (2022) lo define como un programa malicioso que

contamina los dispositivos sin previo aviso o permiso, estos se caracterizan por propagarse rápidamente por todo el sistema. No obstante, existen otros tipos de amenazas. En esta perspectiva, Olmedo, J. I., & Gavilánez, F. L (2018) mencionan que hay cuatro tipos principales de amenazas, que son phishing, ransomware, malware e ingeniería social.

El phishing, también conocido como suplantación de identidad, implica el envío de correos electrónicos engañosos que se asemejan a los originales con el objetivo de robar o manipular información. Es uno de los ataques cibernéticos más frecuentes, siendo un ejemplo típico el robo de datos de tarjetas de crédito para provocar problemas financieros a la víctima. El ransomware, o secuestro de datos, encripta la información de la víctima para luego exigir un rescate, a menudo en forma de dinero. El malware, por otro lado, obtiene acceso no autorizado a un equipo y puede causar daños irreparables. Finalmente, la ingeniería social es una combinación de las amenazas anteriores, que tiene como objetivo hacer que la víctima haga clic en un enlace para perjudicarla mediante el malware, solicitar un rescate y hacerla creer que proviene de una fuente confiable.

Hay que recalcar además que existen dos clasificaciones de ataques, los externos y los internos. Escalante Quimis, O. A (2021) explica que los ataques externos se distinguen por ser más desafiantes de llevar a cabo, dado que requieren explorar la red para entender cómo realizar el ataque. Por otro lado, los ataques internos suelen ser más graves y complejos, son perpetrados por individuos familiarizados con la red y su funcionamiento. Esto conlleva a potenciales repercusiones más severas y daños irreparables para la empresa.

Una vez analizados los posibles tipos de amenazas que existen, ahora es el momento de enfocarse en las soluciones y las prácticas recomendadas para prevenir los problemas relacionados con la ciberseguridad. Sin embargo, antes de abordar estas soluciones y buenas prácticas, es importante introducir el concepto de software libre o software privativo y explicar cómo este tipo de desarrollo contribuye a establecer y mantener altos niveles de seguridad. Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) explica que el software libre

se refiere a cualquier software cuyo código fuente se encuentra disponible para que sea examinado, modificado, utilizado sin restricciones y distribuido, ya sea con modificaciones o sin ellas. Esta definición está vinculada al surgimiento del movimiento de software libre, liderado por Richard Stallman y la creación de la Free Software Foundation en 1985.

Asimismo, Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) describe el software privativo como un software en el que el código fuente no se encuentra accesible, lo que impide a los usuarios examinarlo o alterarlo. Dado su carácter comercial, una gran cantidad de las aplicaciones que empleamos cotidianamente son privativas, abarcando desde sistemas operativos hasta programas de oficina, reproductores de música y navegadores web. En lo que respecta a las soluciones de ciberseguridad se puede mencionar que existen dos tipos los requisitos básicos y los requisitos específicos. Los requisitos básicos a tener en cuenta son: madurez y estabilidad, políticas de privacidad claras y facilidad de uso.

La madurez y estabilidad se refieren a cómo una herramienta maneja los desafíos de seguridad y privacidad, y cómo evoluciona para satisfacer las necesidades cambiantes de los usuarios en este aspecto. Por otro lado, los requisitos específicos dependen del tipo de herramienta usada ya sea aplicaciones de mensajería instantánea, de navegación anónima y de antiseguimiento. En cualquiera de los casos es recomendable contar con una protección de credenciales, para evitar riesgos derivados de una mala gestión de las contraseñas. Además, se debe contar con copias de seguridad, estas herramientas de respaldo o backup aseguran que la información esté disponible en caso de fallos físicos del dispositivo o del sistema, la pérdida del dispositivo en sí o la eventualidad de que la información sea comprometida por un ciberataque.

Por consiguiente, Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) mencionan que los instrumentos destinados a recopilar pruebas digitales y a auditar sistemas son fundamentales en el ámbito de la ciberseguridad. Estos instrumentos posibilitan la reconstrucción de los eventos ocurridos durante un

incidente de seguridad, lo que, tras su examen y la identificación de fallos y vulnerabilidades, permite tomar medidas preventivas para evitar la repetición de tales incidentes.

En tal sentido, Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020) explican que la ciberseguridad surge como una forma de gestionar el riesgo cibernético. De manera más específica, se puede definir como el conjunto de métodos, procedimientos y protocolos diseñados para salvaguardar la información relacionada con los usuarios de las tecnologías digitales. Esta protección implica no solo resguardar la información en sí misma, sino también todos los componentes necesarios para su adecuada administración. En resumen, la ciberseguridad busca proteger cualquier tipo de activo o recurso valioso para individuos, empresas u organizaciones.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Definición de tipo y enfoque de la investigación

Inicialmente para la definición del tipo de investigación se debe conocer que es una investigación, una investigación se define como un proceso sistemático y objetivo para obtener nuevos conocimientos o utilizarlos para resolver problemas particulares, lo cual puede ser verificado mediante métodos específicos. Por otro lado, Hernández, Fernández y Baptista (2014) menciona que la investigación consiste en la aplicación de una serie de métodos sistemáticos, críticos y basados en la experiencia para examinar un fenómeno o una problemática específica. Con base en las argumentaciones expuestas de lo que es una investigación se ha determinado que el tipo de investigación para este proyecto será descriptivo.

Visto de esta forma, en primer lugar, la investigación descriptiva abarca la planificación del estudio, la formulación de preguntas y el análisis de datos relacionados con el tema en cuestión. Por esta razón, es que este proyecto tiene dicho tipo de investigación debido a que en el mismo se procederá a la formulación de preguntas con la elaboración de cuestionarios acordes al tema dirigidos a las personas que trabajen en las áreas o departamentos que sean importantes para este proyecto, además que se realizará un análisis de los datos hallados. No obstante, cabe mencionar que además de los cuestionarios, se realizará entrevistas a las personas que mejor conozcan del tema y el área determinada. Es decir, las entrevistas serán específicamente al Auditor, Departamento de Sistemas y Departamento Financiero.

Por esta razón, es que el enfoque de este proyecto es mixto, es decir cualitativo y cuantitativo. Visto de esta forma el enfoque cualitativo se vale de la recopilación y examen de datos para mejorar las preguntas de investigación o descubrir nuevas incógnitas durante el proceso de interpretación. En el contexto de este proyecto se refiere a las entrevistas dirigidas a las personas ya mencionados anteriormente. Ahora bien, el enfoque cuantitativo en cambio emplea la recopilación de datos para verificar hipótesis mediante mediciones numéricas y análisis estadístico. Su

objetivo es establecer patrones de comportamiento y validar teorías. Por consiguiente, en este proyecto se refiere a los cuestionarios, que servirán para recopilar datos necesarios para la investigación y que servirán de ayuda para el análisis del funcionamiento del sistema a tratar en la investigación.

Ahora bien, para este proyecto se tiene previsto el uso de la siguiente población.

Tabla 1. Población de la Empresa Eléctrica Ambato regional centro norte (EEASA)

N.-	CARGO	NUMERO
1	Coordinador del Departamento de Sistemas del área contable	1
2	Directora del Departamento Financiero	1
3	Auditora (EEASA)	1
4	Área financiera	17
5	Área de sistemas	5
6	Área de planificación y coordinación	8
	TOTAL	33

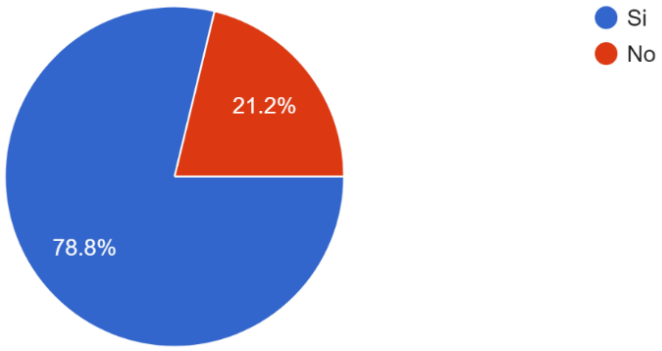
Fuente: elaboración propia

Dado que la población para la investigación no supera las 100 personas, no se requiere muestra por lo cual se trabajará con toda la población para obtener los datos y la información pertinente y necesaria para el proyecto.

2.2. Análisis de las encuestas y entrevistas realizadas al personal encargado de cada área de la Empresa Eléctrica Ambato regional centro norte

Con base en las encuestas realizadas a la población de 33 personas de las áreas detalladas de la Empresa Eléctrica Ambato regional centro norte (EEASA) se obtuvo los siguientes resultados.

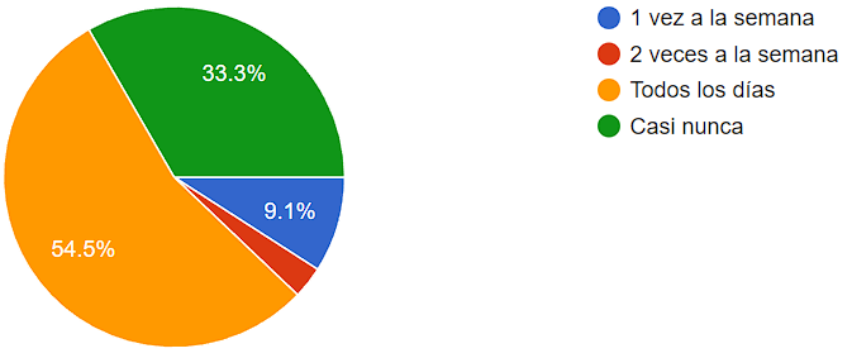
Gráfico 1. ¿Considera usted que el sistema contable es seguro?



Fuente: Encuesta

Del total de 33 encuestas, el 78.8% opina que el sistema si es seguro debido a que consideran que presenta todas las seguridades para el manejo de la información, a comparación del 21.2% que opina lo contrario debido a que ellos por otro lado notan ciertas faltantes en lo que respecta la vulnerabilidad del mismo.

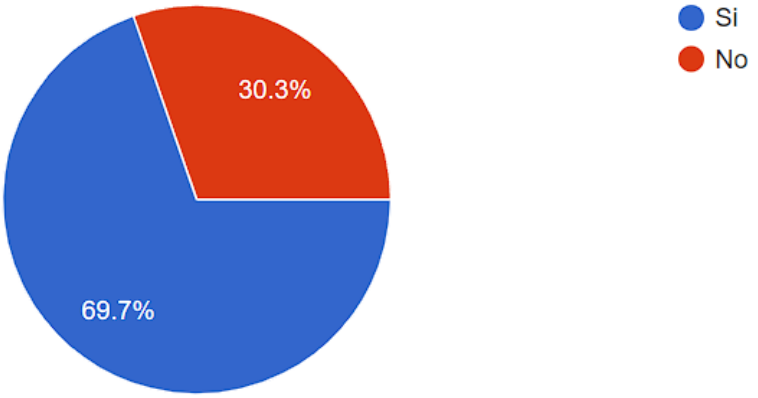
Gráfico 2. ¿Con que frecuencia utiliza el sistema contable de la empresa para enviar datos o archivos contables?



Fuente: Encuesta

De toda la población que usa el sistema contable se puede notar que más de la mitad, es decir el 54,5% utiliza el sistema todos los días. Dependiendo el área hay personas que no lo usan con frecuencia o casi nunca con un 33.3%. No obstante, existe un 9,1% que solamente lo utiliza 1 vez a la semana.

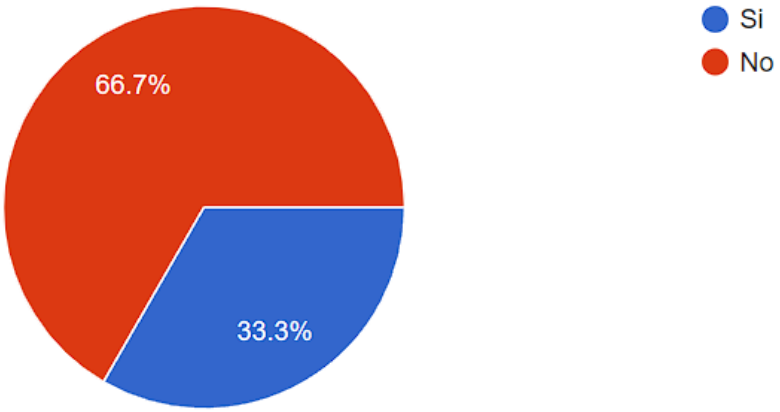
Gráfico 3. ¿Cuenta con una clave personal de acceso para el ingreso al sistema?



Fuente: Encuesta

Se puede observar que la mayoría cuenta con una clave personal para ingresar al sistema, es decir el 69.7% de los encuestados. Sin embargo, el 30,3% no cuenta con este factor de seguridad

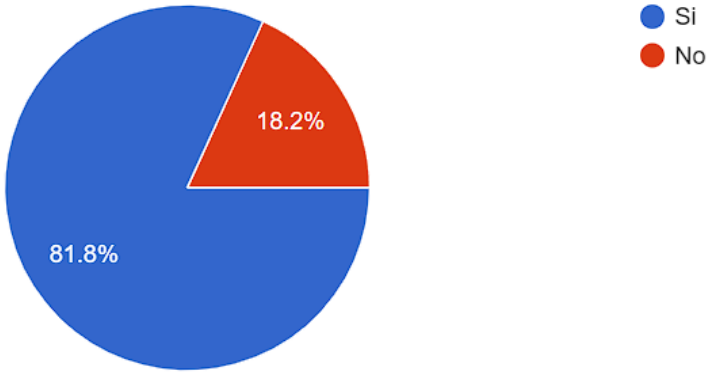
Gráfico 4. ¿Al momento de ingresar al sistema existe algún factor de confirmación de identidad?



Fuente: Encuesta

De una población de 33 personas el 66.7% de los encuestados afirma que no existe un factor de confirmación de identidad, este punto es muy grave debido a que es una vulnerabilidad muy alta para el hurto de credenciales y así acceder al sistema fingiendo ser alguien más, esto conllevaría al robo de archivos o datos importantes. Por otra parte, el 33,3% considera el usuario y contraseña como factor de confirmación de identidad, que es válido, pero no del todo seguro.

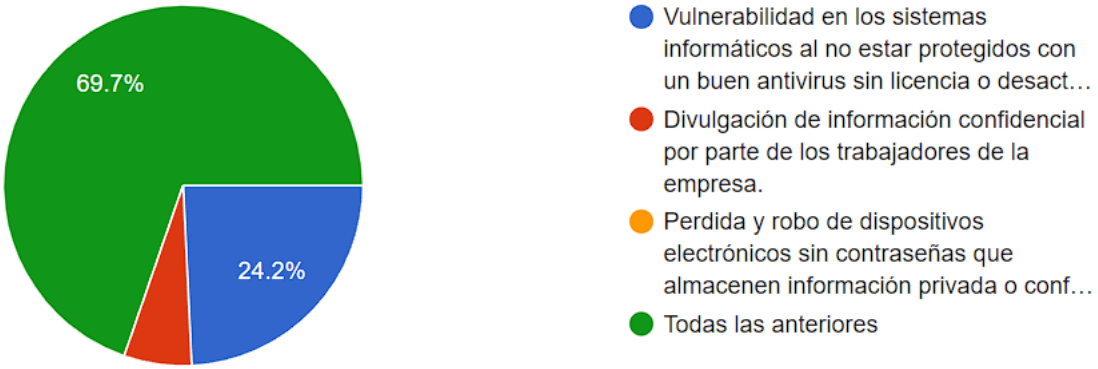
Gráfico 5. ¿Conoce lo que es un ciberataque?



Fuente: Encuesta

Del total de la población la mayoría con 81.8% si conoce lo que es un ciberataque. Lo cual es muy bueno, saben de este término y lo que podría ocasionar si se suscita alguno, a comparación del 18,2% que desconoce este término.

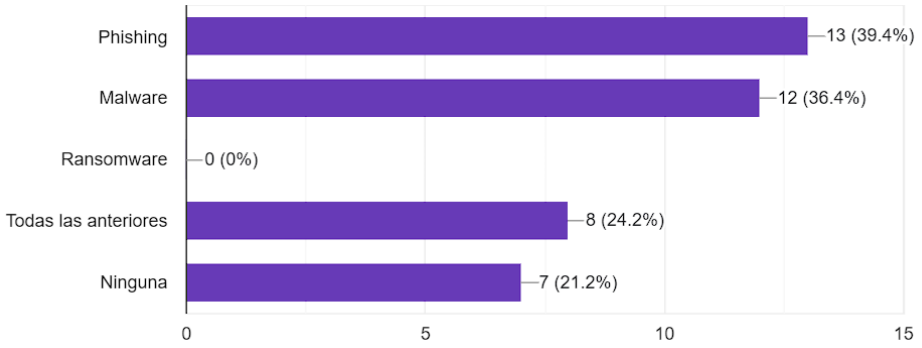
Gráfico 6. Indique cuales considera que son las principales causas de un ciberataque



Fuente: Encuesta

De una población de 33 personas la mayoría, con un 69,7% conoce todas las principales causas de un ciberataque, esto es bueno porque se mantienen informados y saben de los riesgos que estos podrían causar a la empresa. No obstante, un pequeño grupo de 24,2% solo considera como causa de un ciberataque la vulnerabilidad en los sistemas informáticos al no estar protegidos con un buen antivirus sin licencia o desactualizado

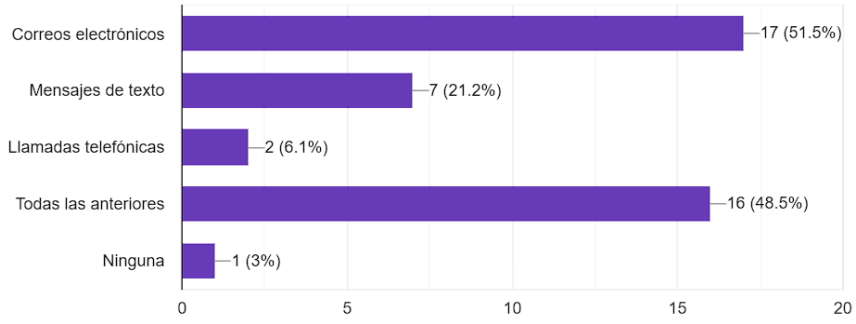
Gráfico 7. De los siguientes tipos de ataques cibernéticos seleccione los que usted conoce



Fuente: Encuesta

Con una población de 33 personas, se observa que el 39,4% conoce lo que es phishing, el 36,4% malware, 0% ransomware, 24,2% conocen todas y el 21,2% ninguna. Este 21,2% es un numero preocupante porque no saben que tipos de ataques existen y cuales podrían ser las consecuencias ante los mismos.

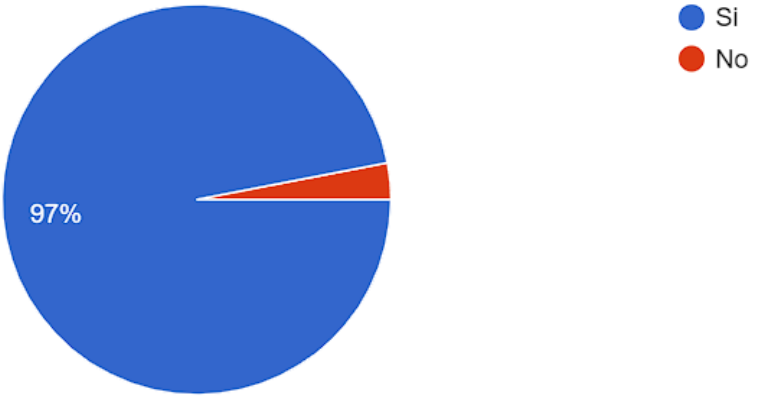
Gráfico 8. De los medios utilizados por los ciberdelincuentes para engañar y robar información personal y corporativa seleccione los que usted conoce



Fuente: Encuesta

De un total de 33 personas encuestadas el 51,5% conoce que los ciberdelincuentes usan solo los correos electrónicos como medio para engañar y robar información, aunque también el 48,5% considera que son todas (correos, mensajes, llamadas) los medios de robo de información. Sin embargo, existe solo el 3% de la población que no conoce ninguna.

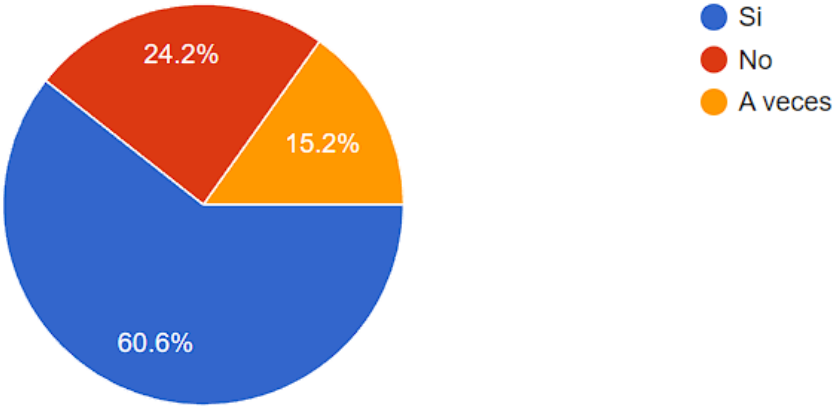
Gráfico 9. ¿Sabe lo que es un correo spam?



Fuente: Encuesta

Del total de personas encuestadas la mayoría es decir el 97% conoce lo que es un correo spam.

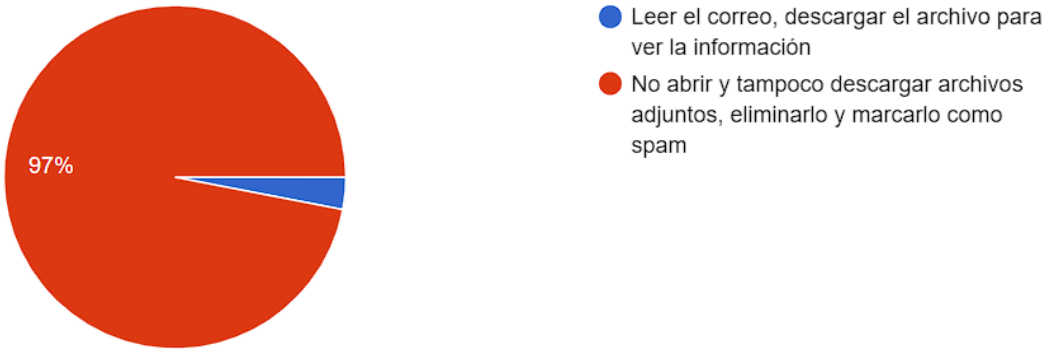
Gráfico 10. Al momento de recibir un correo electrónico en el computador de la empresa, ¿usted verifica que el remitente sea real?



Fuente: Encuesta

De un total de 33 encuestas el 60,6% si verifica que los correos recibidos sean de un remitente real, un 15,2 % lo hace a veces, pero el 24,2% no verifica los correos. Al no revisar los correos recibidos en las computadoras de la empresa, el sistema corre peligro al ser vulnerable ante un posible robo o filtración de datos.

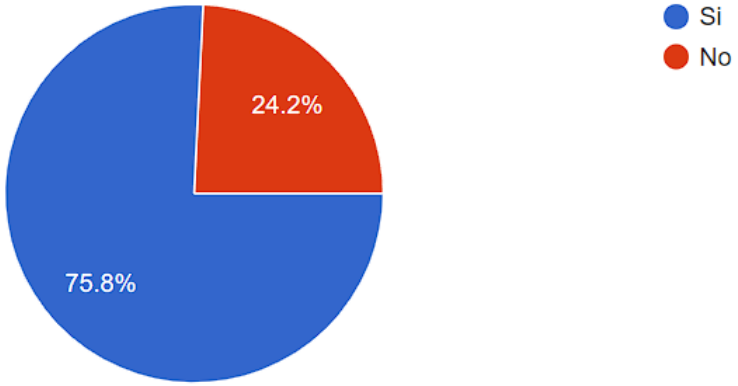
Gráfico 11. ¿Qué considera usted que se debe hacer al momento de recibir correos electrónicos de remitentes desconocidos, que solicitan descargar archivos adjuntos?



Fuente: Encuesta

Del total de la población el 97% conoce lo que hay que hacer al momento de recibir correos de remitentes desconocidos, esto permite que la información que se almacena en el computador se mantenga segura.

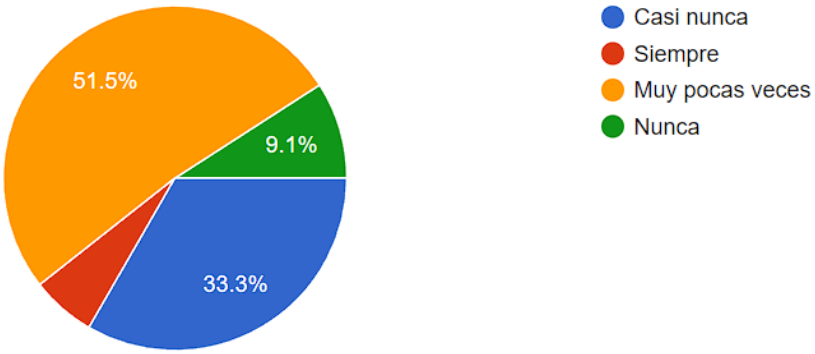
Gráfico 12. Considera que el sistema que maneja la empresa es fluido y no presenta trabas al momento de usarlo.



Fuente: Encuesta

En esta parte se observa que el 75,8% considera que el sistema contable que se usa en el área financiera no presenta trabas y es fluido al momento de su uso, lo cual es bueno, se puede trabajar con fluides en los archivos contables. Por otra parte, el 24,2% no opina lo mismo, debido a que ellos opinan que el sistema si presenta trabas y no es fluido al momento de ocuparlo, aunque el porcentaje de oposición es bajo, hay que tomarlo en cuenta.

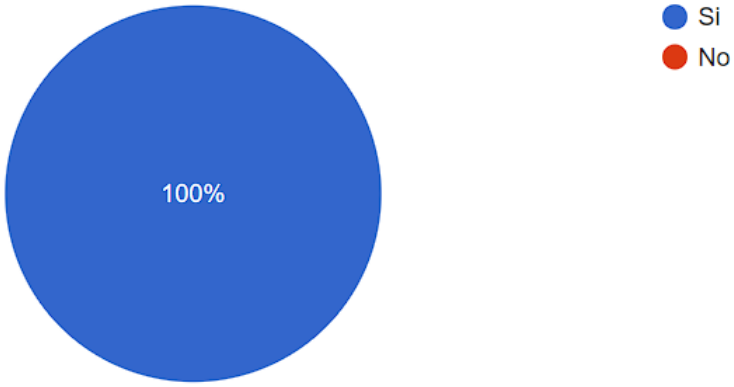
Gráfico 13. Con que frecuencia ha tenido que reiniciar el sistema o el computador debido a fallas presentadas en el mismo.



Fuente: Encuesta

Basado en las 33 encuestas el 51,5% ha reiniciado muy pocas veces el sistema debido a trabas, no obstante, el 33,3% casi nunca reinicia el sistema por lo que se puede decir que, si el sistema es un poco inestable, pero se debe a las circunstancias de cada sección. Por ejemplo, según la entrevista realizada al coordinador de sistemas del área financiera supo manifestar que estas trabas se presentan al final de mes, debido a cierre contable, presentación de estados, realización de roles de pago y como todo esto se realiza al final de mes por la mayoría del departamento es evidente que se colapse por la gran demanda de usuarios.

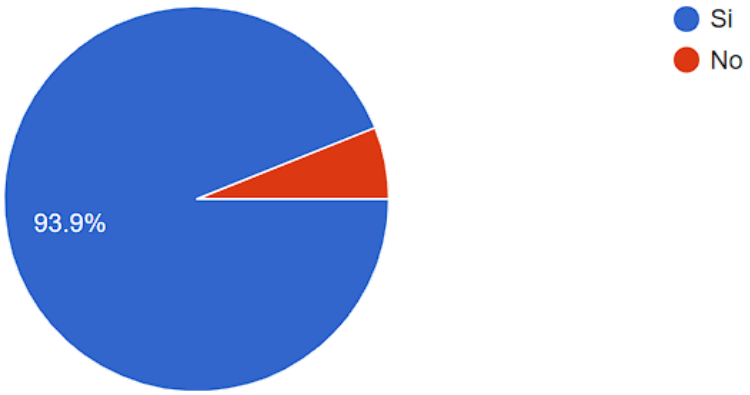
Gráfico 14. Considera que se debería realizar auditorías periódicas a los sistemas informáticos contables para evitar robo de datos y ataques cibernéticos.



Fuente: Encuesta

Esta pregunta es clave para el desarrollo del proyecto, del total de personas encuestadas todas están de acuerdo con que se debería realizar auditorías periódicas a los sistemas contables de la empresa, esto con el fin de que los mismos estén actualizados y puedan brindar un mayor desempeño. Además, que estén protegidos ante cualquier vulnerabilidad al código de fuente y esto conlleve al robo de archivos o información.

Gráfico 15. Cree usted necesario que se realice una revisión mensual a los sistemas de información contables para analizar si los mismos están actualizados y son seguros para la protección de la información confidencial de la empresa.



Fuente: Encuesta

Del total de la población el 93,9% está de acuerdo en que si se tuviera que realizar revisiones mensuales para analizar el desempeño y la seguridad de los sistemas que se manejan en la empresa específicamente en el área financiera. Esto con el objetivo de revisar si los sistemas están funcionando bien y si además de eso los mismos son seguros para el manejo de la información contable que se realiza en esta área.

En cuanto a las entrevistas realizadas al Coordinador del Departamento de Sistemas del área contable, a la directora del departamento financiero y a la auditora, se obtuvo la siguiente información.

Tabla 2. Entrevista dirigida al Coordinador del Departamento de Sistemas del área contable de la (EEASA)

Preguntas	Respuesta e Interpretación
1.- ¿Cuáles son las medidas de seguridad implementadas actualmente en los sistemas informáticos?	La empresa tiene implementado un login que permite autenticar con usuario y clave a la persona, este método se maneja a nivel institucional a través de una intranet, donde es ahí cuando se crea un único usuario y clave personal que le permite a la persona portadora de estas credenciales acceder a los sistemas no solamente al financiero, si no a la intranet institucional, por ejemplo, al sistema de recursos humanos, al sistema de viáticos, de subsistencias, que utiliza una persona o un empleado a nivel empresarial. Hablando específicamente del sistema financiero las personas encargadas de sistemas obtienen las credenciales y permiten al usuario el acceso al sistema. Además, el coordinador añade que se maneja un sistema Client servidor, que es el core financiero, es el sistema donde se contabiliza todas las transacciones de la empresa eléctrica y también se maneja un sistema Web que de igual manera se han ido trabajando para autenticarse con la intranet MIS, con el usuario clave institucional que se mencionó.
2.- ¿Qué procesos de análisis de riesgos y evaluación de vulnerabilidades se llevan a cabo en los sistemas?	Actualmente se tiene un índice de auditorías en donde se van registrando las transacciones que se van haciendo, entonces por ejemplo para los pagos, se tiene un esquema en donde cuando se ingresa una transacción se nutre el mismo. El sistema principal que es Client servidor al ser un sistema cliente servidor no se tiene más que un acceso login y como es un sistema solo login no se tiene muchas seguridades al tratar de verificar vulnerabilidades al sistema. Debido a la tecnología obsoleta, el core del sistema es del año 2012 como son varios años de antigüedad si se convierte en cuello de botella a posibles ataques. Pero en el área informática ya se está trabajando respecto a esto con productos web en donde se pretende implementar toquens de autenticación que mitigan muchas vulnerabilidades actuales. Como es muy poco el personal en sistemas no se puede hacer todo lo previsto en corto tiempo.
3.- ¿Con que frecuencia se realiza un diagnóstico a los sistemas informáticos específicamente al área contable?	Depende de las circunstancias, por ejemplo, cuando una persona se siente mal acude al médico por un diagnóstico, lo mismo sucede en este caso, cuando se suscita un problema en el sistema acuden a la oficina del coordinador de sistemas o a través de correo electrónico, ingresan la petición de soporte necesaria, esto debido a que la metodología frecuente es a través de correo. Hay días en los que no hay soportes ni revisiones, pero hay casos por ejemplo en fin de mes específicamente en financiero que hay más soportes, debido a que cierran balances, se cierra periodo contable y por la cantidad de usuarios el sistema colapsa y en resumen más frecuente se realizan diagnósticos en fin de mes.
4.- ¿La empresa cuenta con algún sistema de monitoreo de amenazas y ataques cibernéticos en tiempo real?	Hay lideres de cada departamento, cada uno trabaja con un especialista del sistema, en este caso el coordinador del área informática se encarga del programa contable y como los mismos se automatizan. Hay mecanismos de ciberataques, por ejemplo, la empresa cuenta con un servidor de aplicaciones y sobre ese servidor existe un programa que se llama WAF, el cual es un firewall de aplicaciones el cual se maneja en el área de planificación.
5.- ¿Qué medidas de seguridad se toman para	La ciberseguridad es un mundo nuevo que ha tomado mayor importancia con el paso de los años, por lo que el sistema es

proteger los archivos contables de la empresa?	centralizado con una base de datos institucional en un sitio seguro, antes cada archivo o información generada en el computador se quedaba ahí mismo, por lo cual se corría el riesgo de pérdida o robo de datos, visto ese riesgo lo que se trabajó en el 2019 fue comprar un AS que es un servidor network attachment storage, el cual es un servidor de almacenamiento en la nube , esto permite no tener reportes solo en la maquina sino además tener un respaldo en el servidor comúnmente llamado la nube. Este está en un centro seguro en el centro de cómputo empresarial donde existe energía redundante, se hace mantenimientos y a toda información se le hace un backup como respaldo de información.
6.- ¿Se realizan pruebas de penetración o simulaciones de ataques para evaluar la resistencia del sistema contable frente a posibles amenazas?	No, debido a la limitante del personal y con los reportes de diagnóstico que se suscitan cada día es muy complicado estar al pendiente de nuevas tendencias de seguridad o de implementación de pruebas de vulnerabilidad a los sistemas, existe el pentester que es la persona encargada de pruebas de penetración con conocimientos específicos, si se han hecho, pero de modo didáctico o de aprendizaje mas no como implementación en la empresa.

Fuente: elaboración propia

Tabla 3. Entrevista dirigida a la directora del departamento de finanzas de la (EEASA)

Preguntas	Respuesta e Interpretación
1.- ¿Cuáles son las principales amenazas cibernéticas que podrían afectar la integridad y confidencialidad de la información contable?	La parte informática netamente es responsabilidad del jefe de área informática, en lo que respecta a las amenazas cibernéticas que podrían afectar a la integridad y confidencialidad de la información contable. Sin embargo, por la experiencia que tiene en la empresa, el mayor riesgo que se tiene es que colapsen los racks en donde se almacena la información. Y como ya pasó en algún momento, se tenga que reconstruir gran parte de la misma.
2.- ¿Qué tipos de archivos contables se transfieren o se envían con el uso del sistema contable de la empresa?	El sistema financiero es un sistema hecho a la medida de la empresa, el mismo ha servido para obtener todos los reportes que se utilizan en la gestión contable. Como por ejemplo el plan de cuentas mayores, libro diario, auxiliares contables, estados financieros, reportes de movimientos, roles de pago, entre otros.
3.- ¿Qué controles de acceso se han establecido para garantizar que solo personal autorizado pueda acceder y manipular la información contable?	Se realiza a través de los líderes de información que se tiene en la empresa, que son parte del comité informático, se establecen los protocolos para que se eviten los riesgos en la información.
4.- ¿Se lleva a cabo algún tipo de capacitación o concientización sobre seguridad cibernética para el personal que utiliza el sistema contable?	El jefe informático eventualmente les ha brindado tips respecto a seguridad cibernética con el fin de evitar riesgos, pero en si capacitaciones o concientización respecto a seguridad cibernética no.
5.- ¿Considera que el sistema contable que maneja la empresa es útil y seguro para la gestión de la información contable?	El sistema contable que maneja la empresa ha sido muy útil durante los últimos años, les ha brindado todas las facilidades y seguridades, sin embargo, con el cambio tecnológico y la gran cantidad de información que se maneja día a día se considera que sí se hace necesario ya un cambio.

Fuente: elaboración propia

Tabla 4. Entrevista dirigida a la auditora de la (EEASA)

Preguntas	Respuesta e Interpretación
1.- ¿Con que frecuencia se ejecutan auditorías de seguridad a los sistemas informáticos contables?	La auditoría interna trabaja en base a una planificación anual que es conocida por el directorio y aprobada por el directorio de la empresa. La última que se realizó a los sistemas informáticos fue en el año anterior, en el 2023, en una revisión sobre asuntos referentes a control interno, también la contraloría general del estado realizo una auditoría los sistemas informáticos hace unos dos o tres años y la misma emitió el respectivo informe.
2.- ¿Cómo se abordan las recomendaciones resultantes de estas auditorías?	Todo informe de un examen especial o una evaluación que se realiza a los sistemas informáticos contienen conclusiones y recomendaciones. Las recomendaciones son emitidas a los funcionarios que son responsables de su cumplimiento y estos tienen la obligación de ejecutarlas. La auditoría interna evalúa el cumplimiento de estas recomendaciones.
3.- ¿Cuál es el alcance de la auditoría que se realiza al sistema informático contable?	Al sistema informático contable específicamente no se lo ha realizado, porque esto ya lo realizó la Contraloría como se había indicado anteriormente. Entonces hay algunas recomendaciones del sistema informático financiero ya emitidas por la contraloría.
4.- ¿Cómo se verifica el cumplimiento de las políticas de seguridad implementadas en el sistema contable?	La Contraloría ya hizo un examen a todos los sistemas informáticos, encontró algunos hallazgos, algunos sistemas, pero en asuntos de seguridad de igual manera es al nivel general, es decir por las seguridades, se considera que exactamente de ese punto el encargado es el coordinador informático quien emite esas recomendaciones.
5.- ¿Se examinan los registros de actividad y los registros de auditoría para detectar posibles actividades sospechosas o no autorizadas?	Se ha realizado revisiones aleatorias a movimientos por ejemplo de colegas que tienen relación también con la contabilidad. porque estos movimientos se van a la contabilidad. Si se realizan, y se han dado algunas sugerencias para el departamento financiero sobre el sistema informático.
6.- ¿Qué medidas se toman para asegurar que las vulnerabilidades identificadas se aborden de manera oportuna y efectiva después de la auditoría?	Eso se hace con el seguimiento de cumplimiento de recomendaciones, las cuales se realizan cada seis meses, se tiene previsto realizar cada tres meses también el cumplimiento de las recomendaciones, si hay alguna que se tenga prevista, se tiene que evaluar de parte del departamento de auditoría.

Fuente: elaboración propia

2.3. Caracterización de la empresa

La Empresa Eléctrica Ambato Regional Centro Norte S.A., EEASA, es una institución distribuidora de los servicios básicos de energía eléctrica y alumbrado público que con 64 años de existencia y con una eficiente trayectoria de servicio a la sociedad, ha mantenido sus altos estándares técnicos, laborales y de servicio al cliente en su área de concesión, gracias a la efectiva gestión de sus trabajadores, directivos y autoridades.

El trabajo mancomunado ha dado lugar a que la EEASA sea catalogada como Distribuidora Clase “A”, es decir, una organización que sabe a dónde va y conoce exactamente lo que tiene que hacer. Por su eficiencia en la prestación de servicios cuenta con la certificación ISO 9001:2015 en gestión de calidad, lo que sin duda constituye un honor, pero al mismo tiempo, compromete a una constante mejora. Tiene a su cargo el área de cobertura más grande del País, que incluye las provincias de Tungurahua, Pastaza, Napo y Morona Santiago. La Empresa cuenta con aproximadamente 310,534 clientes.

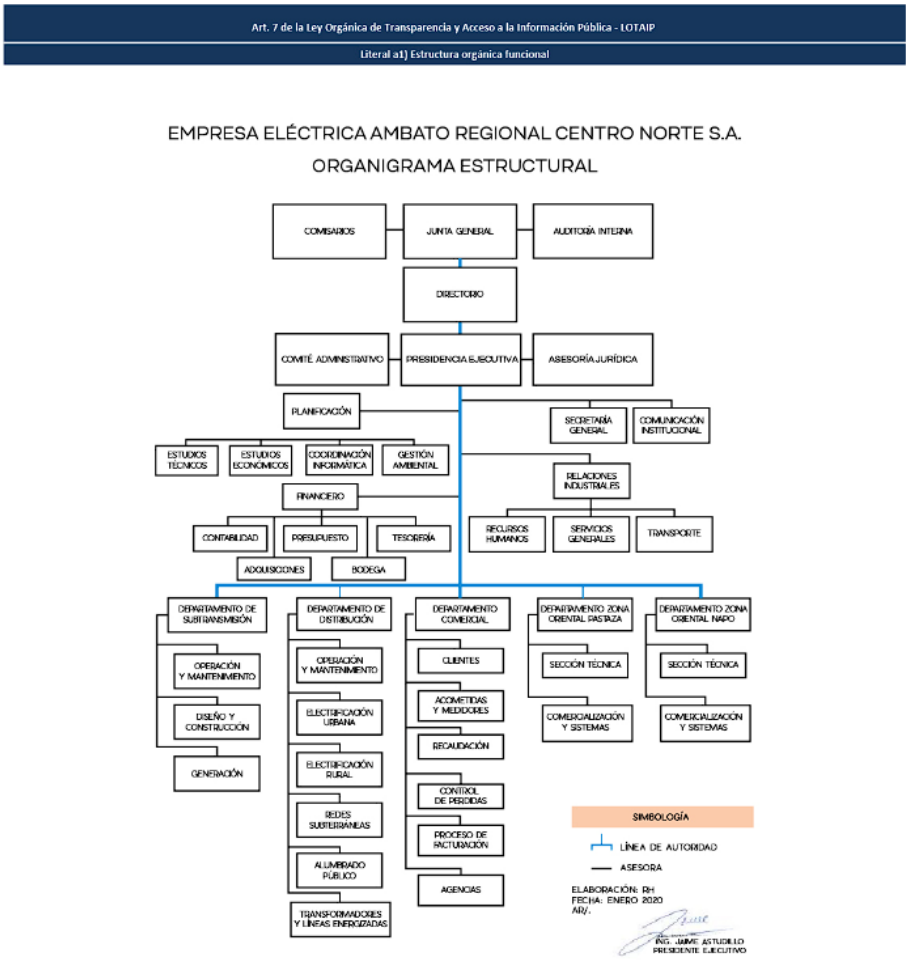
Su misión es “Suministrar energía eléctrica, con las mejores condiciones de calidad y continuidad para satisfacer las necesidades de los clientes en su área de concesión, a precios razonables y contribuir al desarrollo económico y social”.

Además, su visión es “Constituirse en una Empresa líder en el suministro de energía eléctrica en el País”

Los principios de esta prestigiosa empresa son:

- Disponer de recursos humanos capacitados, motivados y comprometidos con los objetivos constitucionales.
- Practicar una gestión gerencial moderna, dinámica, participativa y comprometida en el mejoramiento continuo.
- Disponer de un sistema eléctrico confiable, utilizando tecnología adecuada.
- Tener procesos automatizados e integrados

Organigrama de la Empresa Eléctrica Ambato regional centro norte



Fuente: https://www.eeasa.com.ec/organigrama-institucional/

Además, es necesario mencionar la historia de esta prestigiosa institución. El 2 de julio del año 1959, inicia sus operaciones la Empresa Eléctrica Ambato S.A., como entidad privada con finalidad social y pública, luego de que se suscribiera la escritura de constitución el 29 de abril del mismo año. Participaron en este acto societario inicial, el Ilustre Municipio de Ambato que en ese entonces estaba dirigido por su alcalde, el Dr. Ruperto Camacho, y la ex H. Junta de Reconstrucción de Tungurahua que estaba presidida por el señor Germánico Holguín. Su capital inicial fue de 97 millones de sucres; de ellos, 64 millones correspondían al Municipio y el resto a la Junta de Reconstrucción. Los activos iniciales se sustentaban en la

Central Hidroeléctrica Miraflores de 1200 kW que estaba en servicio desde el año 1914; los terrenos y bienes de la central Río Verde, así como la de la Central Hidroeléctrica La Península que en ese momento se encontraba en construcción la segunda etapa; y, las redes eléctricas que permitían brindar el servicio de distribución en la parte urbana en la ciudad de Ambato a aproximadamente 5.965 clientes, con 110 trabajadores.

Partiendo la Empresa del ámbito municipal, empezó a funcionar en un local ubicado en la calle Bolívar y Lalama, facilitado por el señor Víctor Hugo Oviedo, presidente del Directorio; poco tiempo después, se trasladó al local que entregó el I. Municipio de Ambato, en la Av. 12 de noviembre, entre Espejo y Mariano Eguez, aquí funcionó hasta el mes de febrero de 1982. Posterior al análisis de las encuestas realizadas a la población de la (EEASA) y seguidamente analizar las entrevistas a cada encargado de área, se puede notar la necesidad de este proyecto de investigación.

A causa de que en la pregunta número 14 de la encuesta realizada a la población de la empresa, el 100% de la población considera que, si es necesario realizar auditorías periódicas a los sistemas informáticos contables, de igual manera en la pregunta numero 15 el 93,9% considera que es necesario que se realice una revisión mensual a los sistemas de información contables para analizar si los mismos están actualizados y son seguros, además de las respuestas analizadas por los encargados de áreas, que en ciertas preguntas se evidencia que los sistemas no están actualizados o en ciertas ocasiones presentan trabas además de que no cuentan con un sistema de monitoreo en tiempo real que prevea las amenazas o trate de mitigarlas.

Vista esta problemática y tomando en cuenta de que la última auditoria a los sistemas informáticos contables fue realizada por la contraloría en el 2023, cabe recalcar que no fue hecha por la empresa, se considera necesario a la fecha actual una auditoria más actualizada y con un mayor alcance, para así mejorar la seguridad y precautelar la vulnerabilidad de los sistemas informáticos contables, para evitar posibles ataques que conlleven a robo de información confidencial de la empresa y esto a su vez ocasione una mala imagen de la empresa ante el público

general. De la presente investigación se desprende la propuesta de una auditoría a los sistemas de información contable como elemento de control interno para verificar la vulnerabilidad de los mismos.

CAPÍTULO III. Propuesta de una Auditoría informática a los sistemas contables de la Empresa Eléctrica Ambato Regional Centro Norte S.A.

3.1. Fases generales de una auditoría

En este punto se explicará cuáles son las fases de una auditoría en forma general, debido a que consta de ciertos puntos muy importantes que la (EEASA) puede tomar en consideración al momento de realizar una auditoría a su sistema informático contable.

3.2. Planificación inicial, objetivos y alcance

En primer lugar, como se trata de una auditoría interna, se debe organizar una reunión entre el gerente de la empresa y el departamento de auditoría de la misma para definir aspectos clave como el alcance de la auditoría, objetivos, recursos, entre otros. La planificación inicial de una auditoría informática es crucial para asegurar que el proceso de auditoría sea efectivo y eficiente. Durante esta fase, se llevan a cabo diversas actividades para establecer una base sólida para el trabajo posterior. A continuación, se detallan actividades que se realizan en esta primera fase:

Tabla 5: Planificación inicial

Actividad	Procedimiento
Definición del Alcance y Objetivos:	Determinar qué áreas y sistemas serán auditados. Además de establecer los objetivos específicos de la auditoría, como evaluar la seguridad, la integridad de los datos, el cumplimiento normativo, etc.
Identificación de Recursos:	Identificar los recursos necesarios, tanto humanos como técnicos. Y posterior a eso asignar roles y responsabilidades al equipo de auditoría.
Evaluación del Entorno de TI:	Realizar una revisión preliminar del entorno de TI para entender la infraestructura, los sistemas y las aplicaciones, para asi identificar las principales áreas de riesgo.
Revisión de Documentación:	Recopilar y revisar documentación relevante, como políticas de seguridad, procedimientos operativos, diagramas de red y manuales de usuario.

Fuente: elaboración propia

En esta fase también se define la duración de la auditoría, que depende del tipo de auditoría y los equipos a auditar.

3.3. Recopilación de datos

Esta fase es un proceso crítico que implica la obtención de información detallada y precisa sobre los sistemas y procedimientos de TI de la organización auditada, en este caso la (EEASA). Este proceso se lleva a cabo para evaluar la seguridad, eficiencia y conformidad de los sistemas informáticos con las políticas internas y las regulaciones externas. A continuación, se describen las principales actividades involucradas en la recopilación de datos durante una auditoría informática:

Tabla 6: Actividades para la recopilación de datos

Actividad	Procedimiento
Identificación de Activos	Enumerar y documentar todos los activos de TI, incluyendo hardware, software, redes y datos críticos. Esto incluye la creación de un inventario detallado de los equipos y sistemas que serán auditados.
Revisión de Documentación	Examinar la documentación existente como políticas de seguridad, procedimientos operativos, manuales de usuario, diagramas de red, y registros de configuración. Esta revisión ayuda a entender cómo deberían operar los sistemas y qué controles están implementados.
Entrevistas y Encuestas	Realizar entrevistas y encuestas a empleados clave, administradores de sistemas y personal de TI para obtener información sobre prácticas operativas, conocimiento de los procedimientos de seguridad, y posibles vulnerabilidades.
Inspección Física	Verificar físicamente los sistemas y recursos de TI para asegurar que se encuentran en las ubicaciones correctas y que están protegidos adecuadamente contra accesos no autorizados.
Revisión de Configuraciones y Registros	Analizar configuraciones de sistemas y una inspección a los archivos que registran eventos específicos dentro de un sistema (logs) de eventos para identificar configuraciones incorrectas, accesos no autorizados y posibles incidentes de seguridad.
Pruebas de Penetración y Vulnerabilidades	Realizar pruebas técnicas para identificar vulnerabilidades en los sistemas y redes. Esto puede incluir pruebas de penetración (pentesting), escaneos de vulnerabilidades y análisis de configuraciones de seguridad.
Monitoreo y Análisis de Tráfico	Observar y analizar el tráfico de red para detectar comportamientos anómalos, posibles intrusiones y verificar la efectividad de los controles de seguridad de la red.
Revisión de Políticas y Procedimientos	Evaluar las políticas y procedimientos de seguridad para determinar si son adecuados y si se siguen correctamente dentro de la organización.
Análisis de Cumplimiento	Verificar que los sistemas y procedimientos cumplen con las normativas y estándares aplicables, como las leyes de protección de datos, regulaciones del sector y estándares de seguridad como ISO 27001.

Fuente: elaboración propia

Análisis de riesgos y amenazas

Se lleva a cabo un análisis minucioso de los riesgos relacionados con la seguridad y eficiencia de los sistemas. Se identifican y evalúan las vulnerabilidades, comprobando la implementación de claves de acceso a información sensible. Por lo tanto, en esta etapa, se lleva a cabo un análisis de los riesgos y amenazas a los que la empresa está expuesta, por consiguiente, se identifica las vulnerabilidades y el nivel de amenaza, y se evalúa las posibles consecuencias si dicha amenaza se llegara a materializar.

Los aspectos a analizar serán:

- Evaluar la seguridad del hardware, sistemas operativos, aplicaciones y redes.
- Verificar el cumplimiento de las políticas y procedimientos.
- Asegurarse que se respetan las normativas vigentes en protección de datos y ciberseguridad.
- Analizar la formación del personal involucrado en la seguridad informática, dado que a menudo es el eslabón más débil debido a la falta de capacitación adecuada para el puesto.
- Revisar el correcto funcionamiento de los protocolos de actuación ante incidentes. Por ejemplo, si un servidor falla, se debe verificar que el plan de recuperación es efectivo y funciona correctamente. Esto incluye comprobar si se puede recuperar la información en caso de acceso no autorizado y cifrado de datos, y si se cuenta con un procedimiento de copias de seguridad y su restablecimiento.

Por otro lado, toda vulnerabilidad es debido a alguna causa o falla en el sistema es por eso que, seguidamente se indican las causas de las vulnerabilidades de los sistemas informáticos.

- Debilidad en el diseño de los protocolos utilizados en las redes.
- Errores de programación.

- Configuración inadecuada de los sistemas informáticos.
- Políticas de seguridad deficientes o inexistentes.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes

Como se puede observar son varias las causas que conllevan a una vulnerabilidad en un sistema informático y más aún si es un sistema informático contable que almacena información financiera confidencial de la empresa. Por esta razón, existen dos tipos de vulnerabilidades, las que afectan a los equipos y las que afectan a programas y aplicaciones informáticas.

Tabla 7: Vulnerabilidades que afectan a los equipos

Vulnerabilidad	Consecuencia
Routers y cable-modems	Las vulnerabilidades encontradas en estos dispositivos permiten el acceso a los equipos y redes conectados a través de los routers y módems comprometidos, o facilitan la ejecución de ataques de Denegación de Servicio (DoS) que pueden resultar en el bloqueo total o parcial de las redes de ordenadores conectadas mediante estos dispositivos.
Cámaras web y servidores de video:	Los fallos encontrados en este tipo de dispositivos podrían ocasionar el control remoto de la cámara por parte de un usuario malicioso y en este caso se podría hacer capturas de las imágenes y afectar en gran medida a la persona.
Vulnerabilidades en otros equipos conectados a una red, como son impresoras, escáneres, faxes, entre otros:	Las vulnerabilidades en este tipo de dispositivos podrían ocasionar el robo de información reservada, además de provocar el cambio de configuración para provocar un funcionamiento incorrecto.
Celulares:	Aquí se da un fenómeno conocido como snarfing o bluesnarfing, que básicamente consiste en el acceso y control remoto de los teléfonos celulares y por ende en sus contactos y todas las aplicaciones que este contenga.

Fuente: Gómez Vieites, Á. (2015). Auditoría de seguridad informática: (ed.). Madrid, Spain: RA-MA Editorial. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/62464?page=23.

Tabla 8: Vulnerabilidades que afectan a programas y aplicaciones informáticas

Vulnerabilidad	Consecuencia
Sistemas operativos, servidores y bases de datos:	En los últimos años se ha descubierto que la mayoría de los sistemas operativos como son: Windows de Microsoft, las familias de Linux, MacOS entre otros, presentan una gran cantidad de fallas y vulnerabilidades. Estas fallas provocan que un virus se propague con mayor velocidad.
Navegadores:	De igual manera que en los sistemas operativos la mayoría de los navegadores que se usan con mayor frecuencia han sido detectados con problemas y fallas en la seguridad, esto podría ocasionar ejecución de código arbitrario, sustracción de algunos ficheros del ordenador o incluso mostrar direcciones de páginas webs falsas en la barra de direcciones.
Aplicaciones ofimáticas como Word o Excel:	Estas aplicaciones han sido afectadas por agujeros de seguridad que permitirían acceder a información en el equipo de la víctima y por ende al robo o manipulación de la misma.

Fuente: Gómez Vieites, Á. (2015). Auditoría de seguridad informática: (ed.). Madrid, Spain: RA-MA Editorial. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/62464?page=23.

Informe y recomendaciones

Dentro de una auditoría informática, el informe y recomendaciones es una fase muy importante, consolidan los hallazgos y además brindan una guía para poder mejorar los sistemas y aspectos evaluados en el transcurso de la auditoría. Inicialmente el informe de auditoría informática proporciona una visión general de los objetivos de la auditoría, los hallazgos más significativos y las recomendaciones clave. Es un resumen conciso dirigido a la alta dirección y a las partes interesadas clave. Respecto a los objetivos y alcance, se detalla los objetivos específicos de la auditoría y el alcance del trabajo realizado. Incluye qué sistemas, procesos y controles fueron evaluados y cuáles no fueron considerados. Posteriormente se explica la metodología, la cual describe los métodos y técnicas utilizados durante la auditoría, incluyendo las herramientas de software empleadas, los tipos de pruebas realizadas (pruebas de penetración, análisis de vulnerabilidades, revisión de políticas, etc.) y los enfoques adoptados (muestreo, entrevistas, revisión documental).

Asimismo, se presentan los hallazgos, que son los resultados de la auditoría, enumerando los problemas y deficiencias encontradas en los sistemas y procesos. Los hallazgos suelen clasificarse según su gravedad (alta, media, baja) para ayudar a priorizar la atención y las acciones correctivas. Finalmente se detalla el impacto, es decir se explica las posibles consecuencias de los hallazgos identificados,

incluyendo riesgos potenciales para la organización, como violaciones de seguridad, incumplimiento normativo, interrupciones operativas o pérdidas financieras, perdida de información confidencial, manipulación de archivos, entre otros.

En segundo lugar, respecto a las recomendaciones, se presentan las acciones correctivas, las cuales proporcionan sugerencias detalladas para abordar los problemas y deficiencias identificadas. Las recomendaciones deben ser claras, específicas y viables, indicando qué cambios se deben hacer, cómo implementarlos y quién debería ser responsable de llevarlos a cabo. Hay que mencionar que se debe indicar las prioridades y plazos, es decir establecer la prioridad de cada recomendación en función de la gravedad del hallazgo asociado y su impacto potencial. También puede sugerir plazos para la implementación de las acciones correctivas, ayudando a planificar y gestionar el proceso de mejora. De este modo las mejores de control sugieren avances en los controles existentes para fortalecer la seguridad y la eficiencia de los sistemas y procesos auditados. Esto puede incluir la implementación de nuevas políticas, procedimientos, tecnologías o prácticas de gestión.

Seguimiento y revisión

Son procesos esenciales que garantizan la implementación efectiva y sostenibilidad de las recomendaciones propuestas en el informe de auditoría. En primer lugar, el seguimiento se refiere al proceso continuo de monitorear y verificar la implementación de las recomendaciones y acciones correctivas sugeridas en el informe de auditoría.

Tabla 9: Objetivos de la fase de Seguimiento y revisión

Objetivo	Explicación
Asegurar Implementación:	Se confirma que las recomendaciones se están llevando a cabo según lo planificado.
Evaluar Eficacia	Verificar que las acciones correctivas son efectivas para resolver los problemas identificados.
Detectar Desviaciones:	Identificar cualquier desviación o retraso en la implementación de las recomendaciones.
Proporcionar Apoyo:	Ofrecer asistencia y orientación adicional si se encuentran dificultades durante la implementación.

Fuente: elaboración propia

Por otro lado, la revisión se refiere a la evaluación periódica de los sistemas, procesos y controles después de la implementación de las recomendaciones para asegurar su efectividad y sostenibilidad a largo plazo. Esta revisión a las recomendaciones ayuda a validar mejoras, detectar cualquier problema que pueda surgir en el transcurso del proceso, asegurar un cumplimiento continuo de las recomendaciones presentadas y sobre todo a una mejora continua de la empresa con la identificación de oportunidades adicionales para mejorar los sistemas y procesos.

La importancia del seguimiento y la revisión es que genera eficacia de las acciones correctivas debido a que garantizan que las acciones correctivas no solo se implementen, sino que también sean efectivas para resolver los problemas identificados. Además, brindan sostenibilidad, aseguran que las mejoras implementadas sean sostenibles a largo plazo y que los controles continúen siendo efectivos. Para concluir se puede decir que el seguimiento y la revisión son componentes críticos de una auditoría informática, aseguran la implementación efectiva de las recomendaciones y la mejora continua de los sistemas y procesos dentro de la empresa.

CONCLUSIONES

- Se explicaron los antecedentes teóricos de la auditoría, concluyendo que existen diversas opiniones sobre el concepto y la aplicación de la auditoría informática. Esto se debe al constante cambio tecnológico y a los nuevos riesgos que surgen, lo cual destaca la importancia actual de las auditorías informáticas para las empresas. Estas auditorías ayudan a mantener un mejor control de los sistemas informáticos contables. Respecto al control interno, se identificó su gran importancia para el correcto funcionamiento de la organización. En particular, el sistema de control interno más importante y utilizado a nivel internacional es COSO, aunque existen otros sistemas disponibles. En conclusión, el control interno contribuye al cumplimiento de objetivos y asegura un orden y funcionamiento adecuado de la empresa.

- Por otro lado, en relación con la ciberseguridad se concluye que ayuda a proteger redes, sistemas y programas de ciberataques. Debido al avanzado crecimiento de la tecnología en los últimos años y por ende el mismo avance de formas de robo, la ciberseguridad ha tomado un papel más importante en las empresas. Como conclusión se puede decir que la ciberseguridad en las empresas es de gran importancia para el cuidado, protección y prevención de los ataques a los sistemas informáticos contables.

- De acuerdo con los resultados obtenidos por medio de las encuestas a los trabajadores de la (EEASA) se concluye que el sistema informático contable que se maneja en el área financiera de la (EEASA) en ocasiones presenta ciertas vulnerabilidades. Además, los mismos trabajadores consideran necesario la realización de auditorías informáticas periódicas para corregir las vulnerabilidades que presenta el sistema hasta el momento de la realización de la encuesta. De la misma forma en base a las entrevistas realizadas a los encargados de cada departamento se puede concluir que el sistema informático contable ha sido de gran ayuda para el departamento financiero, además de que en el área de sistemas se trata de trabajar en la actualización del mismo e implementación de nuevos procesos para hacerlo

más ágil y seguro. A pesar de no contar con el personal requerido para este departamento. Finalmente, Auditoría menciona que por parte de la empresa no se ha realizado una auditoría a los sistemas informáticos contables, pero que sería de gran ayuda para la revisión del funcionamiento de el mismo. Por último, después de la explicación teórica de las fases de la auditoría informática y contemplar los riesgos que existen en la actualidad se considera necesaria la importancia de la auditoría informática en la empresa, considerando las vulnerabilidades que podrían afectar tanto a la información contable como a la imagen de la misma empresa.

RECOMENDACIONES

- Se recomienda hacer un análisis al control interno de los departamentos que fueron objeto de investigación para poder revisar si los procedimientos que se están realizando son los óptimos y adecuados.

- Además, se sugiere al departamento de sistemas darle mayor importancia a la ciberseguridad en los sistemas de la empresa, esto con el fin de evitar posibles ciberataques a los sistemas.

- Debido al poco personal que se encarga del departamento de sistemas se recomienda incrementar el personal de este departamento para asi poder realizar pruebas de penetraciones y simulaciones de ataques, además que se podrá llevar de mejor manera el control del funcionamiento del sistema informático contable del departamento financiero.

- Después de revisar la importancia de la ciberseguridad en las empresas, las consecuencias de posibles ciberataques y de la importancia de las auditorías informáticas, se recomienda a la (EEASA) la realización de una auditoría informática a los sistemas de información contables como elemento de control para asi precautelar la información contable de la empresa y cuidar la imagen y reputación de la misma.

BIBLIOGRAFÍA

Arroyo Guardeño, D. Gayoso Martínez, V. y Hernández Encinas, L. (2020). Ciberseguridad: (1 ed.). Madrid, Los libros de la Catarata. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/233122

Avast. ¿Qué es un virus informático? | Definición de virus en un PC. (2021, November 25). Avast 2022, Recuperado 08/09/2022, del sitio web https://www.avast.com/es-es/c-computer-virus

Bitrix, E. (2024). 10 mejores programas de contabilidad para pequeñas empresas. Recuperado de https://bitrix24.es/articles/10-mejores-programas-de-contabilidad-para-peque-as-empresas.php

Blanco Encinosa, L. J. (2008). Auditoría y sistemas informáticos: (ed.). La Habana, Cuba: Editorial Félix Varela. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/71229?page=13.

Cando Segovia, MR y Chicaiza, R. (2021). Prevención de ciberseguridad: enfatizada en los procesos de infraestructura tec. TIC: cuadernos de desarrollo aplicados a las TIC, 17-41.

Chicano Tejada, E. (2023). Auditoría de seguridad informática. IFCT0109: (2 ed.). Antequera, IC Editorial. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/232692?page=1.

Cisco. ¿Qué es la ciberseguridad? Cisco (2022). Recuperado 07/09/2022 del sitio web: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Comité Internacional de Prácticas de Auditoría. Codificación de Normas Internacionales de Auditoría (NIAs) y Declaraciones Internacionales de Auditoría, pp. 18-19. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/71229?page=13.

De Altp, V. T. L. E. (2018, 11 febrero). BII11. Auditoría Informática. Objetivos, alcance y metodología. Técnicas y herramientas. Normas y estándares. Recuperado de https://gsitic.wordpress.com/2018/01/25/bii11-auditoria-informatica-objetivos-alcance-y-metodologia-tecnicas-y-herramientas-normas-y-estandares/

Escalante Quimis, O. A. (2021). Prototipo de sistema de seguridad de BD en organizaciones públicas para mitigar ataques de ciberseguridad en Latam (Bachelor's thesis).

Flérida María Alcívar Cedeño, María Paulina Brito Ochoa y Martha Jaroslava Guerrero Carrasco (2016): “Auditoría en las empresas”, Revista Contribuciones a la Economía (julio-septiembre 2016). En línea: http://eumed.net/ce/2016/3/auditoria.html

Gómez Vieites, Á. (2015). Auditoría de seguridad informática: (ed.). Madrid, Spain: RA-MA Editorial. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/62464?page=18.

Hernández, R., Fernández, C. & Baptista, M. (2014). Metodología de la Investigación. México D.F., México: McGraw-Hill Interamericana

Mantilla Blanco, S. A. (2011). Auditoría del control interno: (2 ed.). Bogotá, Ecoe Ediciones. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/228510?page=19.

Menéndez Arantes, S. C. (2022). Auditoría de seguridad informática: curso práctico: (1 ed.). Madrid, RA-MA Editorial. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/222672?page=24.

Naranjo, A. (2009). Conceptos de la auditoria de sistemas: (ed.). Santa Fe, Argentina, Argentina: El Cid Editor | apuntes. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/29096?page=5.

Olmedo, J y Gavilánez F (2018). Análisis de los ciberataques en Latam. INNOVA Research Journal, 172 - 181.

Pereira Palomo, C. A. (2019). Control interno en las empresas: (ed.). Ciudad de México, Instituto Mexicano de Contadores Públicos. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/124953?page=20.

Technologies, V. (2024). Enterprise Data Protection: The Definitive Guide. Recuperado de https://www.veritas.com/es/mx/information-center/enterprise-data-protection#:~:text=%C2%BFQu%C3%A9%20es%20la%20protecci%C3%B3n%20de,de%20datos%20de%20una%20organizaci%C3%B3n.

W.B. Meigs (1983): Principios de auditoría, p. 24. Recuperado de https://elibro.puce.elogim.com/es/ereader/puce/71229?page=14.

ANEXOS

Anexo 1.

ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA DEL PROYECTO DE INVESTIGACIÓN: AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES

Reciba un cordial saludo, se dirige a usted, Ricardo Jesús Ramírez Freire, estudiante de la Escuela de Administración de Empresas, carrera de Contabilidad y Auditoría, el objetivo de esta encuesta es recolectar información sobre la vulnerabilidad del sistema informático contable que usa la empresa.

La información que nos facilite mediante sus respuestas será confidenciales y útiles para el desarrollo de este proyecto de investigación.

1. ¿Considera usted que el sistema contable es seguro?
    - Si
    - No
2. ¿Con que frecuencia utiliza el sistema contable de la empresa para enviar datos o archivos contables?
    - 1 vez a la semana
    - 2 veces a la semana
    - todos los días
    - Casi nunca
3. ¿Cuenta con una clave personal de acceso para el ingreso al sistema?
    - Si
    - No
4. ¿Al momento de ingresar al sistema existe algún factor de confirmación de identidad?
    - Si

- No

5. ¿Conoce lo que es un ciberataque?
    - Si
    - No
6. Indique cuales considera que son las principales causas de un ciberataque
    - Vulnerabilidad en los sistemas informáticos al no estar protegidos con un buen antivirus sin licencia o desactualizado.
    - Divulgación de información confidencial por parte de los trabajadores de la empresa.
    - Perdida y robo de dispositivos electrónicos sin contraseñas que almacenen información privada o confidencial.
    - Todas las anteriores
7. De los siguientes tipos de ataques cibernéticos seleccione los que usted conoce
    - Phishing
    - Malware
    - Ransomware
    - Todas las anteriores
    - Ninguna
8. De los medios utilizados por los ciberdelincuentes para engañar y robar información personal y corporativa seleccione los que usted conoce
    - Correos electrónicos
    - Mensajes de texto
    - Llamadas telefónicas
    - Todas las anteriores
    - Ninguna
9. ¿Sabe lo que es un correo spam?
    - Si
    - No
10. Al momento de recibir un correo electrónico en el computador de la empresa, ¿usted verifica que el remitente sea real?
    - Si
    - No

- A veces

11. ¿Qué considera usted que se debe hacer al momento de recibir correos electrónicos de remitentes desconocidos, que solicitan descargar archivos adjuntos?
    - Leer el correo, descargar el archivo para ver la información
    - No abrir y tampoco descargar archivos adjuntos, eliminarlo y marcarlo como spam
12. Considera que el sistema que maneja la empresa es fluido y no presenta trabas al momento de usarlo.
    - Si
    - No
13. Con que frecuencia ha tenido que reiniciar el sistema o el computador debido a fallas presentadas en el mismo.
    - Casi nunca
    - Siempre
    - Muy pocas veces
    - Nunca
14. Considera que se debería realizar auditorías periódicas a los sistemas informáticos contables para evitar robo de datos y ataques cibernéticos.
    - Si
    - No
15. Cree usted necesario que se realice una revisión mensual a los sistemas de información contables para analizar si los mismos están actualizados y son seguros para la protección de la información confidencial de la empresa.
    - Si
    - No

Anexo 2.

ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA DEL PROYECTO DE INVESTIGACIÓN: AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES

ENTREVISTA DIRIGIDA A LA DIRECTORA DEL DEPARTAMENTO DE FINANZAS DE LA EMPRESA ELECTRICA AMBATO REGIONAL CENTRO NORTE

1. ¿Cuáles son las principales amenazas cibernéticas que podrían afectar la integridad y confidencialidad de la información contable?
2. ¿Qué tipos de archivos contables se transfieren o se envían con el uso del sistema contable de la empresa?
3. ¿Qué controles de acceso se han establecido para garantizar que solo personal autorizado pueda acceder y manipular la información contable?
4. ¿Se lleva a cabo algún tipo de capacitación o concientización sobre seguridad cibernética para el personal que utiliza el sistema contable?
5. ¿Considera que el sistema contable que maneja la empresa es útil y seguro para la gestión de la información contable?

Anexo 3.

ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA DEL PROYECTO DE INVESTIGACIÓN: AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES

ENTREVISTA DIRIGIDA A LA AUDITORA DE LA EMPRESA ELECTRICA AMBATO REGIONAL CENTRO NORTE

1. ¿Con que frecuencia se ejecutan auditorías de seguridad a los sistemas informáticos contables?
2. ¿Cómo se abordan las recomendaciones resultantes de estas auditorías?
3. ¿Cuál es el alcance de la auditoría que se realiza al sistema informático contable?
4. ¿Cómo se verifica el cumplimiento de las políticas de seguridad implementadas en el sistema contable?
5. ¿Se examinan los registros de actividad y los registros de auditoría para detectar posibles actividades sospechosas o no autorizadas?
6. ¿Qué medidas se toman para asegurar que las vulnerabilidades identificadas se aborden de manera oportuna y efectiva después de la auditoría?

Anexo 4.

ESCUELA DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA DEL PROYECTO DE INVESTIGACIÓN: AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMO ELEMENTO DE CONTROL DE LOS PROGRAMAS CONTABLES

ENTREVISTA DIRIGIDA AL COORDINADOR DE SISTEMAS DEL AREA CONTABLE DE LA EMPRESA ELECTRICA AMBATO REGIONAL CENTRO NORTE

1. ¿Cuáles son las medidas de seguridad implementadas actualmente en los sistemas informáticos?
2. ¿Qué procesos de análisis de riesgos y evaluación de vulnerabilidades se llevan a cabo en los sistemas?
3. ¿Con que frecuencia se realiza un diagnóstico a los sistemas informáticos específicamente al área contable?
4. ¿La empresa cuenta con algún sistema de monitoreo de amenazas y ataques cibernéticos en tiempo real?
5. ¿Qué medidas de seguridad se toman para proteger los archivos contables de la empresa?
6. ¿Se realizan pruebas de penetración o simulaciones de ataques para evaluar la resistencia del sistema contable frente a posibles amenazas?

Anexo 5.