REVISTA
MULTIDISPLINARY JOURNAL

Auditoria de Sistemas Automatizados.

Automated Systems Audit.

Betsy Mabel Moran Olvera [1*], Lic. Yelena Tamara Chávez Cujilán [2]

1.*, Universidad de Guayaquil, Guayaquil, Ecuador. **Email:** betsy.olveram@ug.edu.ec
ORCID: https://orcid.org/0000-0003-4644-8209

2. Magister en Sistemas Integrados de Gestión, Universidad de Guayaquil, Guayaquil, Ecuador.
Email: yelena.chavezc@ug.edu.ec **ORCID:** https://orcid.org/0000-0002-3989-9936

Destinatario: betsy.olveram@ug.edu.ec

Recibido: 25/Abril/2021 **Aceptado:** 28/Mayo/2021 **Publicado**: 30/Junio/2021

Como citar: Moran Olvera, B. M.., & Chávez Cujilán, Y. T. (2021). Auditoria de Sistemas Automatizados. E-IDEA 4.0 Revista Multidisciplinar, 3 (7), pp 49-64. https://doi.org/10.53734/mj.vol3.id168.

Resumen: En los actuales momentos, existe una realidad para las organizaciones de la cual no pueden escapar y es la rapidez de los avances tecnológicos, el crecimiento de la economía y el volumen de datos producidos, por lo cual deben ser capaces de adaptarse a fin de garantizar su subsistencia en el tiempo y para ello depende de la optimización que hagan la información a través de auditorías de sus sistemas automatizados, que son los garantes del almacenamiento y uso de la misma. La presente investigación tiene como propósito analizar las posiciones de los diferentes autores, sobre la implementación de las auditorias informáticas en las organizaciones, para ello se utilizó una metodología de tipo documental, basada en el diseño bibliográfico. Esta revisión bibliográfica permitió concluir que a pesar de los costosos que pudieran resultar el proceso de las auditorias informáticas, no es nada comparado con la toma de una mala decisión por no contar con una información fidedigna y confiable, conllevando a veces inclusive al quiebre o cierre de las empresas.

Palabras Claves: Auditoria de sistemas, auditor informático, tecnologías, información.

Abstract: At present, there is a reality for organizations from which they cannot escape and that is the speed of technological advances, the growth of the economy and the volume of data produced, for which they must be able to adapt in order to guarantee their subsistence over time and for this it depends on the optimization made by the information through audits of its automated systems, which are the guarantors of its storage and use. The purpose of this research is to analyze the positions of the different authors, on the implementation of computer audits in organizations, for which a documentary-type methodology was used, based on bibliographic design. This bibliographic review allowed us to conclude that despite the cost that the process of computer audits could result in, it is nothing compared to making a bad decision for not having trustyand reliable information, sometimes even leading to bankruptcy or closure of the companies.

Keywords: Systems audit, computer auditor, technologies, information.

INTRODUCCIÓN

En los actuales momentos, debido a la globalización y al crecimiento acelerado de las tecnologías, se han generado grandes volúmenes de datos, los cuales deben ser convertidos en información útil para las organizaciones y la sociedad, pero muchas veces esa información no recibe el tratamiento adecuado o no es válida, a fin de garantizar las decisiones que se puedan tomar con base a ella.

Las tecnologías de la información están mejorando constantemente, que se podría considerar casi imposible realizar alguna actividad en cualquier ámbito sin ellas, pero estos avances pueden generar errores, o problemas en la gestión de actividades y de la información, la dependencia que se tiene con estas tecnologías de información y comunicación en la actualidad es tan grande que si dejará de funcionar afectaría en su totalidad o de manera parcial la operación de una organización Salgado et al. (2017)

En esa misma línea se manifiesta Arcentales y Caycedo (2017) al afirma que el desarrollo vertiginoso en las redes informáticas trajo consigo un aumento considerable en la velocidad de procesamiento y en la transmisión de información del negocio, pero con riesgos cada vez mayores en lo referente a seguridad de los datos transportados por estos medios.

De igual manera expresa Zhañay, Erazo y Nárvaez (2019), en la era digital que actualmente vivimos los procesos se realizan más fácilmente y con mejor comunicación, sin embargo, esto ha causado un incremento en los delitos informáticos y fraudes.

Por las afirmaciones de los autores anteriores, es que se debe poner en consideración la importancia que tiene para la subsistencia de las organizaciones el buen uso y mantenimiento de la información, por eso considera Barba y Gutiérrez (2021) que, la información como el activo más importante de una organización requiere especial atención en su cuidado y/o protección, es la que da las pautas para encauzarla por la senda del éxito Barba y Gutiérrez (2021).

Pero, además, las organizaciones deben considerar también las tecnologías como valor agregado, ya que del uso que se haga de ellas para el tratamiento de la información marcará el éxito o no de la empresa, para León et al. (2018), el problema fundamental es que las empresas poseen un capital activo muy valioso: información y tecnología y cada vez en mayor medida, el éxito de una empresa depende de la comprensión de ambos componentes.

Ahora bien, por lo anteriormente indicado, es que resulta importante que las organizaciones sometan a sus sistemas automatizados a evaluaciones, para no comprometer sus acciones y decisiones. Indica Barba y Gutiérrez (2021), para las organizaciones el manejo de la información es algo fundamental para el correcto funcionamiento de sus actividades, pero los sistemas de información pueden estar sujetos a amenazas o vulnerabilidades que pueden causar daño en el

flujo de la información y así las actividades operativas de las organizaciones se detenga o no pueda continuar con normalidad.

En ese mismo sentido, Salgado et al. (2017), manifiesta que los avances tan marcados que se han presentado en las tecnologías de información y comunicación (TIC) y la inclusión de ellas en las actividades pueden llevar al éxito a una organización, por otro lado, también pueden aumentar la probabilidad del surgimiento de problemas, conflictos y errores al realizar alguna de las tareas en la ejecución de procesos.

A la luz de las realidades presentadas y a fin de evitar los problemas de vulnerabilidad de los sistemas automatizados, se hace indispensable la auditoria informática o la auditoria de sistemas. Para Poma (2019), al ser la información en la empresa uno de los activos más importantes y de mayor valor que posee, se deben desarrollar mecanismos de control y auditoría que le permita a la organización asegurar la integridad, efectividad, eficiencia, confidencialidad, disponibilidad, confiabilidad y cumplimiento de la información.

Si bien es cierto que los sistemas informáticos han ido en evolución para poder manejar el gran volumen de información que cada vez es mayor, también es cierto que los problemas de vulnerabilidad también han evolucionado, pero con ello se ha buscado mejorar las herramientas y técnicas de auditorías. Sustenta esta afirmación León et al. (2018) al indicar que, el desarrollo de sistemas informáticos ha sido clave en el desarrollo empresarial, los sistemas han pasado por un sinnúmero de transformaciones que cada vez han implementado beneficios, y las formas de auditar han sido modificadas en función de las necesidades que se van presentando una a continuación de otra.

Según Barba y Gutiérrez (2021), los resultados obtenidos en la auditoría informática pueden ayudar a las organizaciones en la toma de decisiones con el fin de proteger el mayor activo con el que cuentan que es la información.

Sin embargo, pese a esa razón fundamental, muchas organizaciones no hacen auditorias, afirman Infante-Moro et al. (2017), que, debido a que los sistemas de información juegan un rol cada vez más importantes en las empresas, es necesaria la realización de auditorías informáticas para medir la eficiencia de éstos y evitar posibles problemas informáticos en las empresas, aunque no todas las empresas optan por esta medida preventiva.

Pese a las negativas de algunos sectores empresariales, más son a la larga los beneficios que se presentan al auditar los sistemas automatizados, por eso en este estudio se pretende aupar a los directivos de las organizaciones a tomar medidas de prevención y no de corrección una vez haya sucedido los problemas.

METODOLOGÍA

En la investigación documental se recurre a las fuentes históricas, monografías, información estadística y a todos aquellos documentos que existen sobre el tema para efectuar el análisis del problema (Rojas, 2013). Siendo esta la metodología utilizada en la presente investigación tomando como base en el diseño bibliográfico.

Para este estudio se consideró como criterio de selección de libros, artículos de revistas, tesis, entre otros, la pertinencia de estos con el objeto de análisis, descartando aquellos que no cumplieran con dicho criterio, garantizando así la veracidad de la información en fuentes confiables.

Una vez analizadas las diferentes posiciones de los autores se pudo constatar el impacto que tiene para las organizaciones la revisión y optimización de la información y sus equipos tecnológicos, siendo esto posible a través de las auditorias de los sistemas automatizados, sostiene Barba y Gutiérrez (2021), como resultado de una auditoría, la organización conocerá el nivel de eficiencia y seguridad en sus procesos informáticos facilitando la detección de vulnerabilidades en los sistemas de información, lo cual servirá en la toma de decisiones de la alta gerencia en las organizaciones.

RESULTADOS

A lo largo de este proceso investigativo documental, analizando las diferentes posiciones de los autores, se pudo evidenciar que existen tres puntos muy importantes de coincidencia y son los referidos a la información, al buen manejo de la misma en los sistemas de información y la revisión de esos sistemas a través de auditorías a fin de evitar problemas de malas praxis o tomas de decisiones erradas.

Siendo que, en las empresas el uso de sistemas de información computarizados se ha vuelto una práctica común, y por ende los riesgos en los mismos se han multiplicado se vuelve necesaria la auditoría de los sistemas tecnológicos Proaño et al. (2017)

Con base a lo anterior, se presentan a continuación los aspectos más resaltantes que permita discernir con base a esos puntos.

Auditoria de sistemas

La Auditoria es muy antigua y diversa, naciendo principalmente para sistemas contables y financieros, encargándose de la verificación de la información financiera con base en cumplimiento de las normas contables Zhañay et al. (2019).

Posteriormente, ésta terminología fue acuñada para revisión de los sistemas automatizados, procedimiento que se ha hecho necesario debido al avance de las tecnologías y la producción de grandes volúmenes de datos, a fin de evitar problemas como por ejemplo fraudes, robos de identidades, toma de malas decisiones que pudieran colapsar o cerrar una empresa, entre otros.

La auditoría de los sistemas automatizados, toma también el objetivo principal de las auditorias que es verificar la información, pero en este caso de los sistemas informáticos. Ese proceso de revisión según Biler ((2017), debe ser realizado por un experto profesional suficientemente cualificado, determinado procedimiento, actividad, informe, proceso, entre otros, con intención de obtener un alto grado de garantía de la correcta elaboración o desarrollo de los mismos.

Por otra parte, la importancia de las auditorías informáticas radica en que permiten determinar las fortalezas y debilidades del sistema de información de las organizaciones Arcentales y Caycedo (2017)

En consideración se toman las siguientes definiciones de las auditorias de sistemas:

Tapia, et al. (2019), definen a la auditoría informática como la revisión y evaluación de los controles, sistemas y procedimientos de informática de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización, los cuales participan en el procesamiento de la información, a fin de que por medio de los cursos alternativos se logre una utilización eficiente y segura de la información que da soporte a la toma de decisiones.

Las auditorías informáticas son protocolos preventivos que buscan la eficiencia de los recursos tecnológicos disponibles, establecen una política de mantenimiento de los sistemas de información preventiva para el aprovechamiento de los equipos, establecen una política de uso de los mismos para sus empleados, analizan la eficiencia de las redes informáticas, establecen una política de seguridad online y crean un manual de actuación en caso de problemas informáticos Infante-Moro et al. (2017)

La auditoría informática es la revisión, evaluación, verificación y confirmación de la existencia de políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos informáticos por parte del personal de una organización con el fin de lograr el uso eficiente, eficaz, efectivo y seguro de la información que sirva para una adecuada toma de decisiones (Solarte, 2017)

La auditoría de sistemas de información es un procedimiento que recoge, agrupa y evalúa evidencias de un sistema, y parte de la necesidad de verificar que los sistemas informáticos funcionen correctamente Zhañay et al. (2019)

Con base a las afirmaciones de los diferentes autores podemos discernir la coincidencia de que la auditoria involucra procesos como de revisión, verificación, evaluación y análisis de los sistemas, pero estos procesos deben realizarse siempre de manera preventiva para garantizar la eficiente y efectiva información para la toma de decisiones y que debido a la importancia que traen consigo la auditoria esta debe ser realizada por personas o equipos de profesionales en el aérea.

Es importante resaltar que cuando se habla de los sistemas automatizado no es solo la información, sino además otros componentes, indica Proaño et al. (2017) en los sistemas automatizados, se considera al hardware, software, datos, entre otros, con lo cual el horizonte de cobertura de la auditoría informática se amplía sustancialmente.

Otro factor importante que se logra con las auditorias de sistemas es que permite a las organizaciones, alcanzar los estándares internacionales en el uso adecuado de las tecnologías de información, con miras a una certificación de calidad Arcentales y Caycedo (2017)

La seguridad de la información

"La Auditoría Informática ha sido tomada como un sinónimo de detección de errores y fallas" Salgado et al. (2017)

Pero esa detección de errores o fallas a destiempo, puede generar graves problemas para las organizaciones como pérdidas económicas, confiabilidad, hasta cierre de las mismas, por eso es importante que la auditoria de sistemas automatizados, o de informática o de seguridad informática, se realice en el tiempo de prevención o que permita tomar medidas a fin de no caer en graves situaciones.

Para Arcentales y Caycedos (2017), así como la tecnología ha ido evolucionando, los fraudes y delitos informáticos han ido a la par, a tal punto que en la actualidad un delincuente informático puede sustraer recursos económicos de una organización desde la comodidad de su hogar, sin dejar rastro alguno, o estructurar grandes delitos desde el interior de la organización.

Los autores anteriores, afirman que la gestión de la seguridad de la información es un factor importante para proteger los activos de información de una organización; el auge del comercio electrónico a través de los proveedores de servicios y directamente con los clientes, la pérdida de barreras organizacionales y exposiciones de seguridad de alto perfil tales como riegos físicos (robos, daños por siniestros, destrucción de equipamiento, entre otros.) y lógicos (virus, acceso clandestino de redes, violación de contraseñas, entre otros), han elevado el perfil de riesgo de la información, y la necesidad de administrar la seguridad de la información.

Por lo que, no solo se debe prestar atención a los ataques intencionales, sino también a posibles fallas de software o hardware que atenten contra la seguridad, tratando de minimizar los

riesgos asociados al acceso y utilización de un determinado sistema de forma no autorizada o malintencionada, para revelar, utilizar, modificar o destruir accidental o intencionalmente la información que en este se encuentre Bracho et al. (2017)

En este sentido, los sistemas informáticos de detección de malas prácticas se erigen como el medio idóneo para prevenir la corrupción de forma eficaz y a su vez implantar una cultura de la ética y la integridad (Amoedo, 2018).

Esos sistemas de detección de malas praxis tienen su fundamento en las auditorias, ya que a través del mismo se verifican la confiabilidad de los datos que se encuentran en los sistemas automatizados. Para Cassetto (2019), "la seguridad de la información es un conjunto de herramientas y buenas prácticas usadas para proteger la información digital y análoga de las organizaciones. Esta incluye su infraestructura, la seguridad de las redes, la auditoría y las pruebas."

Asimismo, Barba y Gutiérrez (2021), manifiestan que la seguridad de la información tiene como objetivo preservar y proteger la información de una organización mediante un conjunto de actividades o medidas que ayuden a mantener la confidencialidad, la disponibilidad e integridad de los datos. Esas acciones para la prevención y protección de la información buscan mantener los tres pilares de la seguridad de la información que son la confidencialidad, integridad y disponibilidad de los datos.

Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de este análisis, implantar medidas preventivas y correctivas que eliminen o reduzcan los riegos asociados hasta niveles manejables Bracho et al. (2017)

Por todo lo anterior se vuelve a poner de manifiesto el uso de herramientas de auditorías que permita conjuntamente con los sistemas de seguridad garantizar la información, el hardware y el software de las organizaciones. Salgado et al. (2017) sustenta que a la par del impulso que han provocado las tecnologías de información y comunicación (TIC), se presentan situaciones de riegos en las actividades basadas en Tic, al igual que todas las áreas deben ser evaluadas de manera efectiva a través de la adopción de controles y revisiones detalladas, es decir, con una auditoría informática.

Herramientas para la auditoria de sistemas.

Existe una gama de herramientas para auditar, la selección de ellas depende de los recursos, disponibilidad, pero sobre todo el compromiso de la organización a darle el debido tratamiento a su activo más importante, la información.

Barba y Gutiérrez (2021), plantean que las herramientas presentes en el mercado que abarcan la temática de auditoría de sistemas, son de pago o sus versiones gratuitas son muy limitadas, esto

hace que muchos auditores decidan realizar este procedimiento utilizando herramientas no destinadas para esta actividad ocasionando un incremento en el tiempo y recursos utilizados.

Algunas de estas herramientas se presentan a continuación:

- **La Norma ISO/IEC 27001** es un estándar internacional que tiene buenas prácticas o controles que permite la evaluación o análisis de los sistemas de información que manejan las empresas con el fin de reducir los riesgos o amenazas que se enfrentan y que cumple con los tres objetivos de los sistemas de información que son la confidencialidad, integridad y disponibilidad de los datos Barba y Gutiérrez (2021),

La ISO 27001, proporciona un conjunto formal de especificaciones para que las organizaciones manejen el riesgo de seguridad de la información y busquen la certificación para su Sistema de Gestión de la Seguridad de la Información (ISMS) Arcentales y Caycedo (2017) .El ciclo de vida de la implementación de la norma ISO 27001 está basado en Planear – Hacer – Verificar – Actuar de Demming, Zhañay et al. (2019)

- **ITIL** (Information Technology Infrastructure Library) Es una colección de libros que tratan acerca de la infraestructura de las tecnologías de la información. Es un marco de trabajo o recomendaciones, no estándar y mucho menos una norma. El enfoque ITIL se basa en la experiencia, es un enfoque pragmático de la informática Baud (2017), mencionado por Barba y Gutiérrez (2021).

Para Arcentales y Caycedo (2017), es una serie de documentos, que se utilizan para ayudar a la implementación de un marco de ciclo de vida para la gestión de servicios de tecnología de la información. Este marco personalizable define cómo se aplica la gestión de servicios dentro de una organización, y se alinea con la norma internacional, ISO 20000. También indica que el ITIL se organiza en una serie de cinco elementos: estrategia de servicio, diseño de servicio, transición de servicio, operación de servicio y mejora continua del servicio, los describen un sistema de retroalimentación de bucle cerrado, que proporciona retroalimentación en todas las etapas del ciclo de vida.

- **IT4IT** (IT for IT), comprende una arquitectura de referencia y un modelo operativo basado en la cadena de valor para gestionar el negocio de la tecnología de la información. La cadena de valor se agrupa en dos categorías principales de actividades: 1. actividades primarias, que se refieren a la producción o entrega de bienes / servicios, y 2. actividades de apoyo, que facilitan la eficiencia y la eficacia de las actividades primarias. Además, el estándar IT4IT divide la cadena de valor en cuatro flujos de valor, las cuales representa un área de valor que las TIC proporcionan el ciclo de vida integral de los servicios, estos son: estrategia para cartera, requisito

para implementar, solicitud para cumplir y detectar para corregir Arcentales y Caycedo (2017).

- **ISO 22301** Esta normativa es la primera norma internacional para la Gestión de Continuidad del Negocio, la cual incluye los requerimientos base que permitan recuperarse en el menor tiempo posible de las interrupciones que pueda tener una organización, además de establecer adecuadamente un sistema de Gestión de Continuidad de Negocio Zhañay et al. (2019)

Afirman los autores anteriores que, la norma ISO 22301 responsabiliza a la Gerencia del área auditada de asegurarse que cualquier acción correctiva se realice de manera de eliminar cualquier no conformidad detectada y sus causas.

- **COBIT** (Control Objectives for Information and related Technologies). Es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes,se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes León, et al. (2018)

La estructura del modelo COBIT, además permite un marco de acción para la evaluación de los criterios de información como la efectividad, la eficiencia, la confidencialidad, la integridad, la disponibilidad, el cumplimiento y la confiabilidad de la información. (Solarte, 2017).

Por su parte Santacruz et al. (2017) definen el COBIT como una guía o modelo para realizar auditorías de la gestión y control de los sistemas de información y tecnología, orientado a los departamentos informáticos de una organización.

- **COBIT** es la fusión entre prácticas de informática (ITIL, ISO/IEC 17799) y prácticas de control (COSO), las cuales plantean tres tipos de requerimientos de negocio para la información: requerimientos de calidad (calidad, costo y entrega de servicio), requerimientos fiduciarios (efectividad y eficiencia de operaciones, confiabilidad de la información y cumplimiento de las leyes y regulaciones), y por último, requerimientos de seguridad (confidencialidad, integridad y disponibilidad). Todo lo anterior bajo la auditoria o revisión de cuatro dominios de control, como lo son: planificación y organización, adquisición e implementación, entrega/soporte y monitoreo Arcentales y Caycedo (2017)

- **COSO** (Committee of Sponsoring Organizations of the Treadway Comission) es un Marco de Referencia desarrollado por el Comité de Organizaciones que patrocinan la comisión de Treadway, se trata de una organización privada de los Estados Unidos que ha desarrollado este marco de referencia como un modelo a seguir de Control

Interno para que las organizaciones evalúen sus sistemas de control. Zhañay et al. (2019). Los principios del COSO son 17, enmarcados en 4 ítems:

Ambiente de Control: 1. Demuestra compromiso para con la integridad y los valores éticos 2. Ejerce responsabilidad por la vigilancia. 3. Establece estructura, autoridad, y responsabilidad 4. Demuestra compromiso para con la competencia 5. Hace forzosa la accountability

Valoración del riesgo: 6. Especifica objetivos confiables 7. Identifica y analiza el riesgo 8. Valora el riesgo de fraude. 9. Identifica y analiza el cambio importante.

Actividades de control:10. Selecciona y desarrolla las actividades de control 11. Selecciona y desarrolla los controles generales sobre la tecnología 12. Despliega mediante políticas y procedimientos. Información y Comunicación 13. Usa información relevante 14. Comunica internamente 15. Comunica externamente

Actividades de Monitoreo: 16. Dirige evaluaciones continuas y/o separadas 17. Evalúa y comunica deficiencias.

Como se mencionó anteriormente estas son solo algunas herramientas que pueden facilitar el trabajo de auditar los sistemas automatizados, sin embargo, la selección de ellos va a depender de factores inherentes a las características de la organización. Arcentales y Caycedo (2017) afirman que la elección del marco adecuado es vital para asegurar que los profesionales hagan referencia al mejor marco para una gestión eficaz de la seguridad de la información. Y Concluye el mismo autor que, existen posiciones encontradas para dicha elección, pero que la mayoría termina señalando que la combinación de los Estándares de Auditoría (ISA, SOX) y los Estatutos de la Organización de Seguridad de la Información (COSO, COBIT, ISO27001 / BS7799), sería el mejor enfoque para ayudar a los auditores en la búsqueda de la excelencia en la gestión de auditorías informáticas.

Procedimiento para las auditorias de sistemas de tecnologías de información

Independientemente de la herramienta a utilizar, otro punto en el cual hay coincidencia por parte de los autores consultados en el tema de la auditoria de sistemas automatizados, es el procedimiento que se debe ejecutar para la misma, el cual consta de tres fases: Planeación, ejecución e informes de auditoría. Para Yanza (2014) mencionado por Barba y Gutiérrez (2021) esas fases las define como sigue:

- **La planeación de auditoría** consiste en definir las actividades a realizar tales como la recolección de información, definición de objetivos, puntos a evaluarse, la selección de procedimientos y herramienta a utilizarse en la auditoría.

- **La ejecución** es la aplicación de lo anterior realizando la recolección de documentos y evidencias de auditoría para una posterior revisión e integración. Indica otros autores que esta fase se puede realizar a través de entrevistas, encuestas, formularios, entre otros.

- **Realización de un informe** con los resultados obtenidos indicando las situaciones encontradas con sus respectivos comentarios.

Cada fase viene compuesta por una serie de actividades que permiten en detalle la ejecución de la auditoria. Sostiene Solarte (2017) Para realizar el proceso de auditoría informática y de sistemas, se requiere planear una serie ordenada de acciones y procedimientos específicos, que deben ser ejecutados de forma secuencial, cronológica y ordenada, teniendo en cuenta fases, eventos y actividades que se requieran para su ejecución que serán establecidos de acuerdo con las necesidades de la organización.

Según Arcentales y Caycedo (2017), en toda auditoría que se lleve a cabo en una empresa con el fin de determinar la razonabilidad de datos, funciones, operaciones, actividades, informes y reportes, la mayor parte del trabajo consiste en la recopilación de evidencia que sirva para sustentar las conclusiones, opiniones y recomendaciones.

Sin embargo, todas las fases requieren de mucha atención y cuidado de parte del auditor, ya que ellas dependerán las decisiones que tome la organización sobre el futuro del sistema auditado o de la organización misma.

El auditor informático o de sistemas

Como se pudo observar el punto anterior, los procedimientos mencionados están bajo la responsabilidad de una persona, esa persona es llamada auditor informático o de sistema.

Los auditores de sistemas son los encargados de dar soluciones que ayuden a mejorar su nivel de seguridad de los sistemas Barba y Gutiérrez (2021); que pueden ser del propio personal o ajeno a la organización Bracho et al. (2017).

El auditor informático debe ser una persona que transmita confianza y con un record de pulcritud ética al máximo debido a que como indica Arcentales y Caycedo (2017), la auditoría es una práctica de trascendental importancia social y económica, permite entablar relaciones de diversa índole entre los agentes económicos, debido a la confianza que se deposita en el trabajo de los auditores cuando ellos extienden su garantía personal o fe pública, respecto del trabajo de investigación denominado auditoría.

Pero precisamente, uno de los problemas que tiene el auditor informático al emitir una opinión sobre un hallazgo es la subjetividad que puede deberse a muchos aspectos, entre los

principales: emocionales, capacidades o habilidades técnicas, con lo cual esta opinión puede ser acertada o errada. Este es un problema importante debido a que el informe de auditoría emitido puede tener distorsiones de la realidad de los hechos Proaño et al. (2017)

Con respecto a esta última afirmación, resulta importante que se consideren las herramientas que servirá de apoyo al auditor, así como la experiencia, muchos conocimientos, ética, confianza para el auditor y su equipo de trabajo. Para Granados (2016) nombrado por Proaño et al. (2017) otros aspectos a tomar en cuenta son:

Astucia para identificar aspectos claves para encontrar inconsistencias en los procesos que se están auditando.

- Creatividad para el cumplimiento de sus actividades.
- Inteligencia para una adecuada toma de decisiones.
- Honestidad para el desarrollo de sus actividades.
- Confidencialidad en el manejo de la información a la que tiene acceso.
- Organización para un trabajo sistemático y meticuloso

Por supuesto, el auditor a fin de lograr eficiencia y eficacia en esos procedimientos y funciones debe contar con herramientas tecnológicas, sin embargo, aún existen organizaciones que no cuenta con esas herramientas, haciendo que el trabajo del auditor lleve más tiempo y con riesgos de posibles errores.

Por ello, es importante contar con una herramienta que ayude al auditor, a optimizar el proceso además de brindar resultados precisos que ayude a la toma de decisiones por parte de las organizaciones en cuanto a medidas que asegure y proteja la información que maneja para el desempeño de sus actividades Barba y Gutiérrez (2021)

Las razones que, según los autores anteriores, señalan algunas organizaciones para la no adopción de alguna herramienta tecnológica son:

- Costo elevado del software y hardware que soporte la herramienta.
- Costo elevado de la renta anual del software para continuar haciendo uso del sistema pagado
- Costo de la capacitación del personal para el manejo del sistema adquirido

Como se puede observar, las razones circulan en base al costo, pero a pesar de los altos costo que pudieran tener esas herramientas, a la larga resultará menor, debido a que al adoptar las tecnologías garantizan la seguridad de la información, la cual es la vida de la organización y si la información está errada es posible que esa organización se pierda en el tiempo.

DISCUSIÓN Y CONCLUSIONES

Para las organizaciones es vital la información y por ello es catalogada como el activo más preciado, por eso es importante que la misma genere ganancias y no perdidas, siendo esto posible con la realización de auditorías periódicas sus sistemas automatizados, que son los encargados de su almacenamiento y procesamiento de dicha información.

En una sociedad en la que los sistemas de información y la información se consideran imprescindibles para sus empresas, es necesaria la realización de auditorías informáticas para medir su eficiencia Infante-Moro et al. (2017)

Al realizar auditoria informática en las actividades de sistemas de información para evaluar que se cumplen los procedimientos, estándares y normas fijadas por la dirección se lograr alcanzar las metas planteadas estratégicamente y aumentar la competitividad de la organización Salgado et al. (2017)

Por ello, a través de la presente investigación y considerando las razones anteriores como eje fundamental, se realizó una revisión bibliográfica, a fin de indagar y analizar las posiciones de los diferentes autores con respecto a la auditoria de los sistemas automatizados, evidenciando que todos coinciden en que las auditoria garantiza una mayor confiabilidad en la eficiencia y eficacia de los sistemas, así como la certeza de que se cuenta con una información optima que permita tomar las mejores decisiones en un momento determinado para la organización. Bajo esta premisa se desglosan los siguientes puntos finales:

- Las herramientas tecnológicas permiten agilizar y garantizar los procedimientos de la auditoria. Manifiesta Amoedo (2018), estos sistemas, en sus diferentes versiones y con funcionalidades diversas, ponen sobre la mesa soluciones prácticas, eficaces y diligentes ante un problema con imbricación en numerosos ámbitos.
- Es necesario que las organizaciones adopten como parte de sus prioridades la elección de auditorías periódicas, es decir que forme parte de su cultura organizacional, indica Salgado et al. (2017) la cultura informática adecuada en el seguimiento a los controles internos y procesos no es una actividad predominante en algunas de las organizaciones, lo cual puede provocar que no se salvaguarden los activos, no se mantenga la integridad de los datos y la información, no se les dé el uso adecuado a los recursos y que no se alcancen los objetivos. Sin embargo, el proceso de auditoría es una parte fundamental de los marcos de referencia más utilizados por las organizaciones a nivel mundial; ya que se trata de una herramienta para verificar el correcto funcionamiento de un proceso dentro de la entidad para asegurar la mejora continua Zhañay et al. (2019)
- También es importante auditar los equipos que almacenan y procesan la información, Salgado et al. (2017) afirma que, a través de una auditoría informática se podrán evaluar los controles, sistemas y procedimientos equipos de cómputo, pensando en eficiencia

y seguridad de la organización, con el fin de que se logre una utilización eficiente y segura de la información.

- El proceso de auditorías informáticas periódicas va a permitir generar y establecer políticas y procesos adaptados a una particular organización, para Salgado et al. (2017), se deben establecer controles, procesos, normas y políticas para el aseguramiento de los activos, también, se deben definir la gestión e innovación tecnológica y la generación del conocimiento dado que la información es la estrategia de competencia.

La implementación y actualización educativa como parte de la profesión del auditor informático o de sistemas, debe ser prioridad para los currículos universitarios, los gobiernos y la actividad del profesional.

REFERENCIAS BIBLIOGRÁFICAS

Amoedo, D. (2018). Los sistemas informáticos de detección de malas prácticas, herramientas esenciales para la prevención de la corrupción. Revista internacional de transparencia e integridad , 6.

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. Dominio de las Ciencias , 3 (3), 157-173.

Barba, J., & Gutiérrez, D. (2021). Desarrollo de una herramienta de auditoría de sistemas para evaluar el cumplimiento y aplicación de controles según la Norma ISO/IEC 27001. Universidad de Guayaquil, Ingenieria en Sistemas Computacionales. Trabajo especial de grado de la Universidad Nacional de San Agustín de Arequipa.

Biler, S. (2017). Auditoria. Elementos esenciales. Dominio de las Ciencias , 3 (1), 138-151.

Bracho, C., Cuzme, F., Pupiales, C., Suárez, L., Peluffo, D., & Moreira, C. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio. Maskana , 8, 307-319.

Cassetto, O. (30 de Julio de 2019). Information Security (InfoSec): The Complete Guide. Recuperado el 09 de Febrero de 2022, de https://www.exabeam.com/information-security/information-security

Infante-Moro, A., Infante-Moro, J., Martínez-López, F., García-Ordaz, M., & Gallardo-Fernández, M. (2017). La auditoría informática en las grandes empresas españolas. XIX Seminário Luso-Espanhol (SLE) de Economia Empresarial., (págs. 1-12).

La universidad en Internet. (23 de septiembre de 2021). Funciones y reponsabilidades de un auditor informático. Obtenido de UNIR: https://ecuador.unir.net/actualidad-unir/funciones-auditor-informatico/

León, J., Mora, J., Huilcapi, M., Tamayo, A., & Armijos, C. (2018). COBIT como modelo para auditorías y control de los sistemas de información. Polo del Conocimiento , 3 (4), 17-36.

Poma, L. (2019). Propuesta de un modelo de auditoría de sistemas de información para entidades públicas. Universidad Nacional de Piura, Escuela profesional de Ingeniería Informática. Piura. Perú: Trabajo especial de grado de la Universidad Nacional de Piura.

Proaño, R., Saguay, C., Jácome, S., & Sandoval, F. (2017). PSistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información. Enfoque UTE , 8, 148-159.

Rojas, R. (2013). Guía para la realización de investigaciones sociales. España: Plaza y Valdez.

Salgado, M., Osuna, N., Sevilla, M., & Morales, J. (2017). La Auditoría Informática en las organizaciones. Revista Electrónica Sobre Cuerpos Académicos y Grupos de Investigación , 4 (8).

Santacruz, J., Remigio, C., Pinos, L., & Cárdenas, O. (2017). Sistema cobit en los procesos de auditorías de los de sistemas informáticos. Ciencia e Investigación. , 2 (8), 65-68.

Solarte, F. (2017). Metodología práctica para auditoría de sistemas aplicando el estándar de mejores prácticas Cobit 4.1. Ciencia, Innovación y Tecnología, , 3, 99-103.

Tapia, C., Castillo, S., Mendoza, S., & Guevara, E. (2019). Fundamentos de la Auditoría. Aplicación práctica de las normas internacionales de Auditoría. Instituto Mexicano de Contadores Públicos. México: Instituto Mexicano de Contadores Públicos.

Zhañay, O., Erazo, J., & Nárvaez, C. (2019). Modelo de Auditoria de Sistemas de Información para las Cooperativas de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca. CIENCIAMATRIA , 5 (1), 361-393.