

Estrategias de auditoría informática en la era de la transformación digital

IT audit strategies in the era of digital transformation

Leidy Angamarca^[0009-0005-8419-6745]

Universidad de Buenos Aires, Buenos Aires, Argentina
l.angamarca@gmx.com

CITA EN APA:

Angamarca, L. (2022). Estrategias de auditoría informática en la era de la transformación digital. Technology Rain Journal, 1(1), e1. <https://doi.org/10.55204/trj.v1i1.1>

Recibido: 01 de Agosto 2021

Aceptado: 1 de septiembre 2021

Publicado: 01 de enero 2022

Technology Rain Journal
ISSN: 2953-464X



Los contenidos de este artículo están bajo una licencia de Creative Commons Attribution 4.0 International (CC BY 4.0). Los autores conservan los derechos morales y patrimoniales de sus obras.

Resumen. El presente artículo tiene como objetivo proponer estrategias de auditoría informática en la era de la transformación digital. Basándose en una revisión bibliográfica exhaustiva, se identificaron normas recomendadas como ISO/IEC 27000, ITIL, COBIT y PCI DSS como fundamentales para garantizar la seguridad y protección de la información. Las estrategias propuestas incluyen la adaptación a la transformación digital, la evaluación oportuna de riesgos, la realización de auditorías periódicas, el cumplimiento normativo y la búsqueda de la mejora continua. Estas estrategias permiten a las organizaciones enfrentar los desafíos y aprovechar las oportunidades que brinda la tecnología actual en un entorno en constante evolución.

Palabras Clave: auditoría informática, transformación digital, estrategias de la auditoría informática.

Abstract. The objective of this article is to propose computer audit strategies in the era of digital transformation. Based on an exhaustive bibliographic review, recommended standards such as ISO/IEC 27000, ITIL, COBIT and PCI DSS were identified as fundamental to guarantee the security and protection of information. The proposed strategies include adaptation to digital transformation, timely risk assessment, regular audits, regulatory compliance and the search for continuous improvement. These strategies allow organizations to meet the challenges and take advantage of the opportunities offered by today's technology in a constantly evolving environment.

Keywords: IT audit, digital transformation, IT audit strategies.

1. INTRODUCCIÓN

La evolución de las tecnologías de la información y la comunicación ha dado lugar a un entorno empresarial en constante transformación conocido como entorno digital. Este entorno está generando cambios significativos en la forma en que las empresas abordan y desarrollan sus actividades, convirtiéndose en un factor determinante para su crecimiento y rentabilidad (ICJCE; Comisión de Innovación y Tecnología; Bip, 2019).

En este contexto, la digitalización también está teniendo un impacto directo en la práctica de la auditoría informática, que es un minucioso examen de la información con el fin de garantizar su exactitud. Además, el propósito principal es mejorar la utilidad de la información para los usuarios, al mismo tiempo que verifica la autenticidad, integridad y calidad de la información generada por el sistema (Jiménez & Namuche, 2019). En consecuencia, de esta evolución, el papel

del auditor ha experimentado cambios significativos. En el presente, el auditor requiere habilidades comunicativas sólidas y un pensamiento crítico y analítico, así como competencias técnicas en seguridad y conocimiento de estándares de auditoría interna para potenciar la eficiencia y calidad de las auditorías (Universidad Europea, 2021).

Las normas ISO/IEC 27000, ITIL, COBIT y PCI DSS son ampliamente utilizadas en la auditoría informática. La familia de normas ISO/IEC 27000 aborda aspectos clave de la seguridad de la información y del Sistema de Gestión de Seguridad de la Información. ITIL proporciona un marco de referencia para la gestión de servicios de tecnología de la información, mientras que COBIT es un marco integral para gobernar y gestionar las infraestructuras de TI. Por último, PCI DSS se enfoca en la seguridad de datos en la industria de tarjetas de pago. Estas normas y marcos de referencia son fundamentales para asegurar la confidencialidad, integridad y disponibilidad de la información, optimizar la gestión de servicios de TI, gobernar las infraestructuras de TI y cumplir con los estándares de seguridad de la industria (Coloma-Baños, Cañizares-Galarza, Romero-Fernández, & Quintana-Cifuentes, 2021).

Es importante destacar que llevar a cabo una auditoría informática en una empresa u organización es fundamental. Este procedimiento permite evaluar de manera apropiada el desempeño de los Sistemas de Gestión de Seguridad de la Información, asegurando la aplicación de controles necesarios y adecuados para salvaguardar la confiabilidad y seguridad de los sistemas de la empresa (Zambrano, Vilela, Calle, & Matute, 2021).

Según Hernández, menciona que la importancia de este tipo de auditoría en la era de la transformación digital reside en su capacidad para identificar tanto las fortalezas como las debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la configuración adecuada de la plataforma informática, la calidad de los servicios proporcionados por la unidad responsable y el estado de los contratos con proveedores de productos y servicios, entre otros aspectos relacionados con el uso y aplicación de las TIC's en la organización. El propósito es brindar recomendaciones y propuestas de mejora destinadas a garantizar que estas tecnologías apoyen de manera óptima los procesos de negocio y, en última instancia, contribuyan al logro de los objetivos establecidos (Hernández, 2010).

Sin embargo, a pesar de la importancia de la auditoría informática en la era de la transformación digital, existen desafíos específicos que deben abordarse. Algunos de estos desafíos incluyen la rápida evolución de las tecnologías, la aparición de nuevas amenazas y vulnerabilidades cibernéticas, y la complejidad de los sistemas de información. Por ello, el objetivo de este trabajo es proponer estrategias efectivas de auditoría informática que aborden estos desafíos y permitan a las empresas adaptarse y prosperar en el panorama actual.

El artículo consta en primer lugar de un breve resumen que proporciona una visión general de los contenidos. A continuación, se presenta la introducción, donde se establece el contexto y se plantea la importancia del tema. Luego, se describe la metodología utilizada en el estudio, detallando las técnicas empleadas. Posteriormente, se realiza una contextualización de las definiciones clave relevantes para el tema abordado. A continuación, se presentan los resultados obtenidos y se lleva a cabo una discusión en torno a dichos resultados. Por último, se exponen las conclusiones obtenidas a partir del estudio realizado.

2. METODOLOGÍA

La metodología utilizada en este estudio se basa en un enfoque descriptivo, cuyo objetivo es proporcionar una descripción detallada de las estrategias de auditoría informática en el contexto de la transformación digital. Para llevar a cabo esta investigación, se realizó una revisión exhaustiva de la literatura existente sobre auditoría informática y transformación digital. Se recopilaron y analizaron diversos estudios, artículos científicos y documentos relevantes relacionados con el tema de estudio.

El proceso de revisión se llevó a cabo mediante la búsqueda sistemática de fuentes de información en bases de datos especializadas, así como en bibliotecas virtuales y repositorios académicos. Se utilizaron palabras clave como "auditoría informática", "ciclo de vida de la auditoría informática", "perfil del auditor moderno", "transformación digital" y "tecnologías emergentes en la auditoría".

3. CONTEXTUALIZACIÓN

Definición de Auditoría Informática

La auditoría informática se define como la orientación evaluada en los sistemas administrativos, es decir, la estructura organizativa, los procesos de gestión, las operaciones y el entorno de control establecido. Su objetivo es identificar pérdidas y discrepancias, proponer mejoras en los métodos y controles, mejorar la eficiencia operativa y optimizar la utilización de los recursos físicos y humanos disponibles (Zambrano, Vilela, Calle, & Matute, 2021).

La auditoría informática implica una serie de procesos llevados a cabo por profesionales capacitados y responsables. Estos profesionales recopilan, examinan y evalúan evidencias relevantes sin depender únicamente de un sistema de información específico. El objetivo es verificar la integridad de los datos de la organización y garantizar un uso adecuado de los recursos, cumpliendo con las leyes y regulaciones aplicables (Imbaquingo, y otros, 2020).

Asimismo, (Cuasapaz & Landázuri, 2021) indican que la auditoría es un procedimiento de evaluación de actividades llevadas a cabo en una organización, donde se analizan diversos criterios

de acuerdo a regulaciones generales o internas, con el objetivo de salvaguardar el bienestar de la empresa u organización. Como resultado de esta evaluación, se analiza el nivel de riesgo asociado a las diferentes actividades, lo que permite identificar los errores presentes en la organización y tomar medidas para mitigar o reducir dicho riesgo.

Por otra parte, la auditoría informática implica el análisis, evaluación y examen del entorno informático, que incluye hardware, software, bases de datos, redes y otras instalaciones. Se realiza siguiendo estándares reconocidos internacionalmente y utilizando modelos de referencia que se centran en las mejores prácticas de gestión de dicho entorno (Hernández, 2010).

Según otros autores definen a la auditoría informática como un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso (Yeiniel, Blanco, & Loy, 2012).

Estas definiciones resaltan la importancia de la auditoría informática como un medio crucial para detectar y abordar estos riesgos, garantizando la protección de la información y la integridad de los sistemas en un entorno altamente desafiante. Adicionalmente, este tipo de auditorías puede ser tanto interna como externa, y debe ser una actividad independiente de las influencias propias de la entidad.

Ciclo de vida de la auditoría informática

El proceso de auditoría consta de varias etapas en las que el auditor debe mantener el cumplimiento de las normas de auditoría con el fin de emitir una opinión profesional sobre el objeto de la auditoría. El modelo del proceso para realizar las auditorías sigue un ciclo continuo de actividades (Cuasapaz & Landázuri, 2021), a continuación, se describe cada fase:

- Inicio: Esta etapa se inicia mediante la realización de una entrevista inicial con los encargados de la institución. Durante esta entrevista, se solicita un inventario detallado de los recursos que serán objeto de auditoría, con el fin de comprender la magnitud del trabajo y poder estimar adecuadamente los recursos necesarios para llevar a cabo la auditoría.
- Fase de planificación: En esta etapa se establecen las actividades requeridas para llevar a cabo la auditoría, lo cual implica identificar las razones que motivan su realización y determinar su objetivo específico. Además, se diseñan los métodos, técnicas y procedimientos necesarios para llevar a cabo la auditoría, y se elaboran planes, programas y presupuestos documentales para su ejecución.

- Fase de ejecución: se llevan a cabo las actividades planificadas previamente, teniendo en cuenta las características específicas, puntos y requisitos establecidos durante la fase de planificación.
- Fase de revisión: El equipo encargado de la auditoría debe asegurarse de que haya concordancia entre los riesgos documentales identificados y el plan de acción propuesto. Para realizar esta verificación, se pueden emplear técnicas de muestreo, aunque en esta fase no se tiene como objetivo analizar exhaustivamente los registros, sino más bien confirmar su existencia.
- Fin: integración precisa de los papeles de trabajo, ya que estos serán utilizados en caso de futuras aclaraciones y para dar seguimiento a las soluciones de las desviaciones identificadas. Es importante que los papeles de trabajo estén organizados de manera coherente y detallada, facilitando así su uso efectivo en el proceso de auditoría.

Definición de transformación digital

La Transformación digital es un proceso en el cual las organizaciones adoptan y se adaptan a los avances tecnológicos y digitales que impactan en diversos aspectos de su funcionamiento. Surge como resultado de la convergencia de diversas innovaciones digitales, como el uso de datos, la inteligencia artificial, el Internet de las cosas y la computación en la nube, entre otros. Estas innovaciones generan cambios significativos en los actores involucrados, las estructuras organizativas, las prácticas empresariales, los valores y las creencias en el entorno empresarial (Hinings, Gegenhuber, & Greenwood, 2018).

La transformación digital es un proceso de reconversión y adaptación de tecnologías digitales, las mismas que están inmersas en la rutina diaria de las personas, lo que motiva a las instituciones u empresas a incorporar procedimientos innovadores para cubrir la demanda de sus clientes con productos o servicios novedosos que satisfagan sus necesidades y deseos (Medina-Chicaiza, Chango-Guanoluisa, Corella-Cobos, & Guizado-Toscano, 2021).

En resumen, la transformación digital busca aprovechar las tecnologías y herramientas digitales para mejorar la competitividad, la agilidad y la capacidad de adaptación de las organizaciones en un entorno empresarial en constante cambio.

4. RESULTADOS

Normas recomendadas para las auditorías informáticas

ISO/IEC27000: esta norma proporciona una visión general y un vocabulario común para los estándares relacionados con la seguridad de la información y el Sistema de Gestión de Seguridad

de la Información (SGSI). A continuación, en la tabla 1 se presentan las diferentes versiones de la norma ISO/IEC27000 y una breve descripción de cada una (Coloma-Baños, Cañizares-Galarza, Romero-Fernández, & Quintana-Cifuentes, 2021):

Tabla 1: Versiones de la norma ISO/IEC27000

Norma	Descripción
ISO/IEC27001	Es una certificación para organizaciones y establece los requisitos detallados para implementar el Sistema de Gestión de Seguridad de la Información.
ISO/IEC27002	Proporciona un conjunto de buenas prácticas para la gestión de la seguridad de la información. Ofrece directrices y recomendaciones para establecer controles de seguridad que aborden los diversos aspectos de la seguridad de la información.
ISO/IEC27003	Ofrece directrices para la implementación del Sistema de Gestión de Seguridad de la Información. Proporciona orientación sobre cómo establecer, operar, mantener y mejorar continuamente un SGSI en una organización.
ISO/IEC27004	Se enfoca en las métricas utilizadas para la gestión de la seguridad de la información
ISO/IEC27005	Aborda la gestión de riesgos en seguridad de la información.

Elaborado por: El autor

ITIL: es una colección de buenas prácticas destinada a mejorar la gestión y provisión de servicios de tecnología de la información. Fue desarrollada por Central Computing and Telecommunications Agency y se basa en cinco fases: estrategia o planificación, diseño, transición, operación y mejora continua. Su objetivo principal es mejorar la calidad de los servicios de TI ofrecidos y anticipar o resolver los problemas asociados a estos servicios (Peña-Casanova & Anias-Calderón, 2020).

COBIT: es un marco de referencia que permite una gestión integral de las infraestructuras de tecnología de la información, buscando el equilibrio entre la generación de beneficios, la optimización de los niveles de riesgo y el uso eficiente de los recursos (Peña-Casanova & Anias-Calderón, 2020). Además, cuenta con varias versiones y la más actual es la versión COBIT 5.

PCI DSS: estándar de seguridad de datos para la industria de tarjetas de pago se centra en la configuración y auditoría de los sistemas de información. Su aplicación abarca tanto

transacciones con tarjetas de débito y crédito como la protección de la información en tecnologías Fintech (Guerra, 2019).

Al adoptar estas normas, las organizaciones pueden reforzar su postura de seguridad y mitigar los riesgos asociados a la gestión de la información. Es importante tener en cuenta que estas normas no funcionan de manera independiente, sino que se complementan entre sí, ofreciendo un enfoque integral y eficiente para garantizar la seguridad informática. En definitiva, estas normas desempeñan un papel crucial en la construcción de un entorno digital seguro y confiable en el que las organizaciones puedan prosperar y enfrentar los desafíos de seguridad actuales y futuros (Macias, Macias, Navarrete, & Navarrete, 2021).

Perfil de Auditor Informático Moderno

El auditor debe ser una persona que cuente con una sólida formación técnica y esté familiarizada con las prácticas empresariales actuales. Además, deben poseer las siguientes características para mantener su perfil profesional actualizado: aquellos que asuman este rol deben combinar conocimientos en auditoría financiera y en informática en general en su formación básica. (Jiménez & Namuche, 2019).

En cambio, según la (Universidad Europea, 2021) el perfil de un auditor informático requiere una combinación de habilidades y competencias específicas. En primer lugar, es fundamental contar con excelentes habilidades de comunicación que permitan al auditor transmitir de manera clara y comprensible los resultados de su trabajo a personas no especializadas en el campo. Además, se espera que el auditor tenga una mentalidad crítica y analítica, lo que le permitirá identificar de forma precisa errores, áreas de mejora, así como detectar patrones y tendencias que puedan suponer riesgos en los sistemas informáticos.

Así como también, el auditor informático debe poseer un sólido conocimiento técnico, con un enfoque especial en las habilidades de seguridad. Esto implica tener un dominio profundo de los fundamentos de seguridad y la infraestructura de TI, así como una comprensión completa de los principales riesgos de seguridad asociados con la tecnología informática. Además, se espera que el auditor esté familiarizado con herramientas de visualización y análisis de datos, así como con los estándares de auditoría interna, como MAR, COBIT, etc. Estas competencias técnicas son esenciales para llevar a cabo una auditoría informática efectiva y garantizar la integridad y seguridad de los sistemas de información (Universidad Europea, 2021).

Tecnologías emergentes en la auditoría

Seguidamente, se exponen algunas tecnologías actuales que están siendo utilizadas en el ámbito de las auditorías (Plastino, Marchiano, Michelini, Taglialegne, & Vieira, 2021):

- **Procesamiento y análisis de datos:** La velocidad de procesamiento contribuye a uno de los principios rectores de la auditoría. La mayoría de las empresas implementan sistemas ERP, que son conjuntos de programas informáticos utilizados por las organizaciones para gestionar sus actividades diarias. El término "Big Data" se refiere a conjuntos de datos de gran tamaño y complejidad que requieren tecnologías y herramientas especializadas para su captura, gestión, procesamiento y análisis. Para realizar el análisis de datos se puede usar la herramienta ACL acrónimo de Lenguaje de Comandos de Auditoría es un software para análisis y extracción de datos. Así como también IDEA, es un software de auditoría que proporciona funciones avanzadas de análisis para la realización de auditorías internas y externas, así como para el control de procesos.
- **Robótica:** La automatización robótica de procesos es una tecnología que se utiliza para automatizar tareas repetitivas y predecibles que solían ser realizadas por humanos. Esta tecnología permite recopilar, analizar y procesar datos a una velocidad y escala mucho mayores que las capacidades humanas.
- **Realidad virtual y aumentada:** estas son tecnologías fundamentales en el proceso de transición hacia la era digital. La realidad aumentada se utiliza en el diseño y control de instalaciones industriales, proporcionando información en tiempo real sobre los procesos productivos. Además, se está explorando su aplicación en la formación de auditores, permitiéndoles simular situaciones y generar informes personalizados.
- **Inteligencia artificial:** La inteligencia artificial en la actualidad agiliza y simplifica tareas que antes requerían mucho tiempo para los auditores. Mediante su uso, es posible detectar actividades ilegales en correos electrónicos, generar resúmenes imparciales de desempeño empresarial a partir de libros contables, conciliar cuentas bancarias y verificar discrepancias en facturas de venta, entre otras funciones. Estas tareas, que solían tomar horas para los auditores humanos, ahora se realizan en segundos gracias a la inteligencia artificial.
- **Blockchain:** También conocido como cadena de bloques, es una base de datos segura y distribuida en la cual múltiples usuarios se encargan de verificar y validar las transacciones. Los auditores deben adquirir conocimientos especializados en esta tecnología para comprender su funcionamiento y realizar auditorías efectivas.

Estrategias de auditoría informática en la era de la transformación digital

En base de la revisión bibliográfica realizada, a continuación, se presentan algunas estrategias que pueden ser adoptadas para una auditoría informática efectiva en esta era de transformación:

- **Adaptación a la transformación digital:** Los auditores informáticos deben estar actualizados con las nuevas tecnologías como inteligencia artificial, análisis de datos, ciberseguridad, realidad virtual y aumentada, entre otras áreas para comprender cómo impactan en los procesos de negocio de las organizaciones.
- **Evaluación de riesgos a tiempo:** se presentan nuevos desafíos en términos de seguridad de la información, protección de datos y continuidad empresarial. En este contexto, los auditores informáticos tienen la responsabilidad de identificar y evaluar dichos riesgos, así como de diseñar estrategias efectivas para mitigarlos al menor tiempo posible.
- **Auditorías periódicas:** Realizar auditorías informáticas de forma regular ayuda a evaluar la efectividad de los controles implementados y a detectar posibles vulnerabilidades o brechas de seguridad. Esto podría incluir revisar políticas de seguridad, acceso a sistemas, gestión de identidades, cifrado de datos y protección contra intrusos.
- **Auditoría de cumplimiento normativo:** Verificar el cumplimiento de las regulaciones y estándares relevantes en el ámbito de la seguridad de la información, como la ISO 27001, ITIL, COBIT y PCI DSS.
- **Mejora continua:** La auditoría informática debe ser un proceso continuo y adaptativo. Los auditores deben estar dispuestos a aprender y evolucionar junto con las nuevas tecnologías, actualizando constantemente sus habilidades y conocimientos.

Estas estrategias de auditoría informática en la era de la transformación digital se centran en garantizar la seguridad, el cumplimiento normativo y la mejorar continua del papel del auditor en un entorno tecnológico en constante cambio.

4. DISCUSIÓN

En la era de la transformación digital, resulta crucial implementar estrategias de auditoría informática que desempeñen un papel vital en la eficiencia del proceso de auditoría en cualquier institución. Una de estas estrategias fundamentales es la adaptación a los cambios que trae consigo la transformación digital, y esto tiene un impacto significativo en el papel del auditor informático, el cual es la base de todas las demás estrategias mencionadas. En la ilustración 1 se observa las características principales de un auditor:

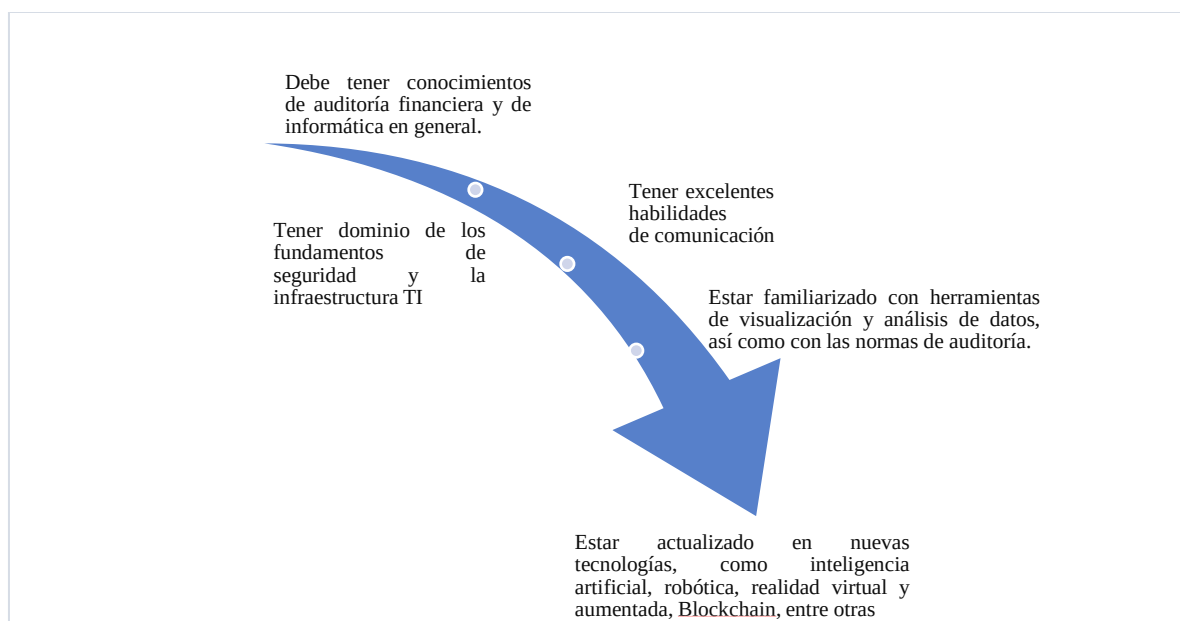


Ilustración 1: Características del auditor moderno
Elaborado por: El autor

Además, las normas recomendadas para las auditorías informáticas desempeñan un papel crucial en la seguridad y protección de la información. Las normas ISO/IEC 27000 ofrecen un marco sólido para establecer y poner en práctica un Sistema de Gestión de Seguridad de la Información. La implementación de estándares como ITIL y COBIT mejora la gestión de los servicios de TI y la gobernanza tecnológica, asegurando la eficiencia y efectividad de los procesos informáticos. Asimismo, el cumplimiento del estándar PCI DSS es esencial para salvaguardar datos de usuarios.

5. CONCLUSIONES

El trabajo realizado ha permitido proponer estrategias efectivas de auditoría informática que abordan los desafíos y riesgos emergentes asociados a la tecnología. En la era de la transformación digital, las organizaciones se encuentran frente a un panorama en constante evolución, donde la seguridad de la información, la privacidad de los datos y la continuidad del negocio son aspectos críticos a considerar. Los auditores informáticos desempeñan un papel fundamental al identificar y evaluar estos desafíos, y al desarrollar soluciones que permitan a las empresas adaptarse y progresar. Al adoptar estrategias como la adaptación a las nuevas tecnologías, la evaluación oportuna de riesgos, la realización de auditorías periódicas, el cumplimiento normativo y la búsqueda de la mejora continua, las organizaciones podrán fortalecer su postura de seguridad, garantizar la confianza de los clientes y cumplir con los requisitos regulativos. Estas estrategias ofrecen un enfoque integral y efectivo para la auditoría informática en la era de la transformación digital, permitiendo a las empresas enfrentar los desafíos y aprovechar las oportunidades que brinda la tecnología actual.

REFERENCIAS

- Coloma-Baños, N., Cañizares-Galarza, F., Romero-Fernández, A., & Quintana-Cifuentes, M. (2021). La seguridad informática para la toma de decisiones en el distrito de educación 12d03.Mocache-Ecuador. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología*, 8(4). doi:<https://doi.org/10.35381/cm.v8i4.898>
- Cuasapaz, N., & Landázuri, D. (marzo de 2021). *Auditoría informática usando el marco de referencia cobit 5 para el departamento de tic del gobierno autónomo descentralizado municipal de montúfar*. Obtenido de UPEC Repositorio Digital: <http://repositorio.upec.edu.ec/bitstream/123456789/1752/1/092-%20CUASAPAZ%20%20NARVAEZ%20KEVIN%20ALEXANDER-%20LANDAZURI%20NARVAEZ%20KEVIN%20DAVID.pdf>
- Guerra, J. (2019). Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones financieras de la economía popular y solidaria basada en las buenas prácticas de la PCI DSS, caso de estudio Cooperativa. *Universidad Internacional SEK, Facultad Arquitectura e Ingeniería*. Obtenido de <https://repositorio.uisek.edu.ec/bitstream/123456789/3321/1/Tesis%20Final.pdf>
- Hernández, A. (2010). Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs). *Compendium*, vol. 13(núm. 25), pp. 3-4. doi:88019355001
- Hinings, B., Gegenhuber, T., & Greenwood, R. (2018). Innovación y transformación digital: una perspectiva institucional. *Innovación y transformación digital: una perspectiva institucional*, vol 28(num 1), pp 52-61. doi:<https://doi.org/10.1016/j.infoandorg.2018.02.004>
- ICJCE; Comisión de Innovación y Tecnología; Bip. (marzo de 2019). *La transformación digital en el sector de la auditoría*. Obtenido de ICJCE: <https://www.icjce.es/adjuntos/transf-digital.pdf>
- Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jesús, J. (2020). *Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura*. Obtenido de Revista Ibérica de Sistemas e Tecnologías de Informação: <https://www.proquest.com/scholarly-journals/análisis-de-las-principales-dificultades-en-la/docview/2452331691/se-2>
- Jiménez, D., & Namuche, J. (junio de 2019). *Estado del arte de la auditoría informática y su importancia para las empresas*. Obtenido de Repositorio Institucional UNP: <https://repositorio.unp.edu.pe/bitstream/handle/UNP/1971/FCC-JIM-ORT-2019.pdf?sequence=1&isAllowed=y>
- Macias, M., Macias, R., Navarrete, M., & Navarrete, J. (2021). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. *revista científica arbitrada multidisciplinaria pentaciencias*, 5(4). doi:<https://doi.org/10.59169/pentaciencias.v5i4.700>
- Medina-Chicaiza, P., Chango-Guanoluisa, M., Corella-Cobos, M., & Guizado-Toscano, D. (2021). Transformación digital en las empresas: una revisión conceptual. *Journal of Science and Research*, vol 7, 756-769. doi:<https://doi.org/10.5281/zenodo.7726439>
- Peña-Casanova, M., & Anias-Calderón, C. (2020). Integración de marcos de referencia para gestión de Tecnologías de la Información. *Revista Ingeniería Industrial*, 41(1). Obtenido de <https://www.redalyc.org/journal/3604/360464918003/html/>
- Plastino, A., Marchiano, L., Michelini, M., Taglialegne, N., & Vieira, Y. (2021). *El impacto de las nuevas tecnologías en el perfil del auditor*. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/142170/Documento_completo.pdf?sequence=1
- Universidad Europea. (22 de marzo de 2021). *Las características de un auditor informático*. Obtenido de [https://universidadeuropea.com/blog/caracteristicas-auditor-informatico/#:~:text=El%20auditor%20inform%C3%A1tico%20debe%20dominar,SOX%2C%20COBIT%20y%20COSO\)](https://universidadeuropea.com/blog/caracteristicas-auditor-informatico/#:~:text=El%20auditor%20inform%C3%A1tico%20debe%20dominar,SOX%2C%20COBIT%20y%20COSO))
- Yeiniel, A., Blanco, B., & Loy, L. (2012). Auditoría con Informática a Sistemas Contables. *Arquitectura e Ingeniería*, vol. 6(núm. 2), pp. 1-14. doi:1990-8830
- Zambrano, L., Vilela, C., Calle, J., & Matute, J. (2021). *Auditoría informática dentro de la empresa "Promaelec"*. Obtenido de Revista Universidad y Sociedad: <https://rus.ucf.edu.cu/index.php/rus/article/view/2244/2216>