Entre riesgos y vulnerabilidades: El rol del auditor en el mundo cibernético.

Sandra Milena Zarza Ramírez
Yuceris Teresa Molina Pérez

Resumen

La creciente digitalización de las organizaciones ha transformado la forma en que operan, generando una mayor eficiencia, pero también un incremento en los riesgos cibernéticos. Los ciberataques son cada vez más sofisticados y frecuentes, y las organizaciones deben adaptarse rápidamente para proteger su información y sus activos digitales. En este contexto, el rol del auditor ha cobrado una relevancia central en la gestión de riesgos cibernéticos. Este artículo analiza cómo los auditores enfrentan los desafíos emergentes en un entorno digital, identificando las competencias, herramientas y marcos necesarios para llevar a cabo auditorías efectivas en ciberseguridad. A través de una revisión de las amenazas cibernéticas actuales y los marcos regulatorios vigentes, se presenta el papel crucial que desempeñan los auditores en la prevención, detección y mitigación de incidentes de ciberseguridad. Finalmente, se reflexiona sobre las perspectivas futuras de la auditoría de ciberseguridad y los desafíos que los auditores deben abordar para mantenerse al día con las amenazas en constante evolución.

Palabras clave

Auditoría de ciberseguridad, riesgos cibernéticos, vulnerabilidades, auditoría digital, amenazas emergentes, competencias auditoras, ciberseguridad, transformación digital.

Abstract

The increasing digitalization of organizations has transformed the way they operate, generating greater efficiency but also an increase in cyber risks. Cyberattacks are becoming more sophisticated and frequent, and organizations must adapt quickly to protect their information and digital assets. In this context, the role of the auditor has become crucial in managing cyber risks. This paper analyzes how auditors face emerging challenges in a digital environment, identifying the competencies, tools, and frameworks needed to conduct effective cybersecurity audits. Through a review of current cyber threats and regulatory frameworks, the paper presents the critical role auditors play in the prevention, detection, and mitigation of cybersecurity incidents. Finally, the paper reflects on the future of cybersecurity auditing, and the challenges auditors must address to stay up-to-date with constantly evolving threats.

Keywords

Cybersecurity auditing, cyber risks, vulnerabilities, digital auditing, emerging threats, auditing competencies, cybersecurity, digital transformation.

Introducción

La digitalización está transformando las organizaciones, mejorando la eficiencia y abriendo nuevas oportunidades, esto implica, pertenecer a un entorno global de interconexiones de sistemas; sin embargo, este avance no viene sin riesgos, por lo que representa desafíos en seguridad digital que permita proteger la información de las amenazas cibernética, promover el desarrollo de competencias digitales.

En la actualidad, el éxito de cualquier emprendimiento o empresa depende en gran medida de dos factores clave: la implementación de un sistema de control interno eficaz y el uso estratégico de herramientas tecnológicas que permitan a la organización posicionarse en el entorno digital, donde se encuentra su público objetivo (Revista Finanzas y Negocios, 2022).

Según el periódico digital INFOBAE, “nueve de cada diez organizaciones presentaron al menos una amenaza cibernética en el transcurso de 2024; además, la inteligencia artificial (IA) influyó en esta tendencia. La creciente sofisticación de los ciberataques y la vulnerabilidad de las organizaciones frente a estas amenazas han desencadenado una situación alarmante a nivel global. También, las cifras proyectadas indican que los costos relacionados con la ciberdelincuencia podrían alcanzar los 10,5 billones de dólares anuales para 2025”.

“La IA ya se está utilizando en aplicaciones del mercado para conocer los patrones de comportamiento de usuarios y diseñar campañas comerciales utilizando software de IA a disposición de todo el mundo, por lo que sería muy ingenuo pensar que los cibercriminales no lo estén utilizando también” (Ayerbe, 2020, p. 4).

Entonces, los riesgos cibernéticos, se le reconoce como un riesgo emergente, originado por la intensificación de la conectividad digital en la sociedad actual. Según el Foro Económico Mundial, los ciberataques fueron responsables de una gran parte de los riesgos globales en 2024, lo que evidencia la creciente preocupación por la ciberseguridad.

Por otra parte, Colombia fue el país latinoamericano más afectado por ciberataques en 2023, representando el 17 % del total regional, por segundo año consecutivo, el país fue señalado como el más afectado por amenazas digitales, evidenciando una tendencia preocupante en seguridad informática (Forbes, 2024); en otras palabras, los cibercriminales están al acecho aprovechando e identificando a los más vulnerables para atacar.

De acuerdo con el ministro de las TIC durante el año 2024 se presentaron más de 20.000 millones de ataques cibernéticos de diferentes modalidades, malware, phishing y ransomware. Este aumento ha creado un panorama cada vez más desafiante, en el cual, las organizaciones deben adaptarse rápidamente para proteger su información y sus activos digitales viendo la necesidad de desarrollar estrategias que les permitan fortalecer la ciberseguridad.

Luego entonces, el sin número de ataques cibernéticos, han creado el cibercrimen, dejando en evidencia la necesidad urgente de auditores especializados en ciberseguridad. Existen investigaciones importantes sobre auditoría de TI (tecnología de la información) y el aseguramiento de la información, y como profesionales, se ven en la obligación de especializarse en temas de ciberseguridad, sin embargo, existe un vacío al abordar el papel específico del auditor frente a las amenazas cibernéticas.

Los auditores, tradicionalmente enfocados en evaluar el cumplimiento y la eficiencia operativa, deben adaptarse a este nuevo panorama digital. El papel del auditor de ciberseguridad es crucial no sólo para detectar vulnerabilidades, sino para prevenir, mitigar y ofrecer recomendaciones que ayuden a las organizaciones a mantenerse protegidas en este entorno digital en constante cambio.

Diferentes investigaciones, destacan la importancia en los estudios de las amenazas y cómo buscar mecanismos que ayuden a minimizar riesgos, con una gestión cíclica y constante.

Metodología

Este artículo se desarrolló con un enfoque cualitativo, mediante la revisión de literatura con carácter sistemático, seleccionando artículos académicos publicados entre 2019 y 2024 en revistas indexadas, utilizando plataformas digitales, motores de búsqueda académica y bases de datos especializadas, además, se incorporaron noticias y reportes publicados en medios digitales confiables, con el propósito de contextualizar los hallazgos recientes y aportar una visión actual.

El análisis crítico de conceptos, enfoques teóricos y hallazgos previos permite construir una base sólida para comprender los desafíos, tendencias emergentes y el papel estratégico del auditor frente a los riesgos y vulnerabilidades en el contexto cibernético.

Este artículo busca analizar el papel crucial del auditor en el mundo cibernético, enfocado en los desafíos que enfrenta al abordar la vulnerabilidad de las organizaciones frente a las amenazas cibernéticas, especialmente en un entorno tan dinámico y cada vez más complejo.

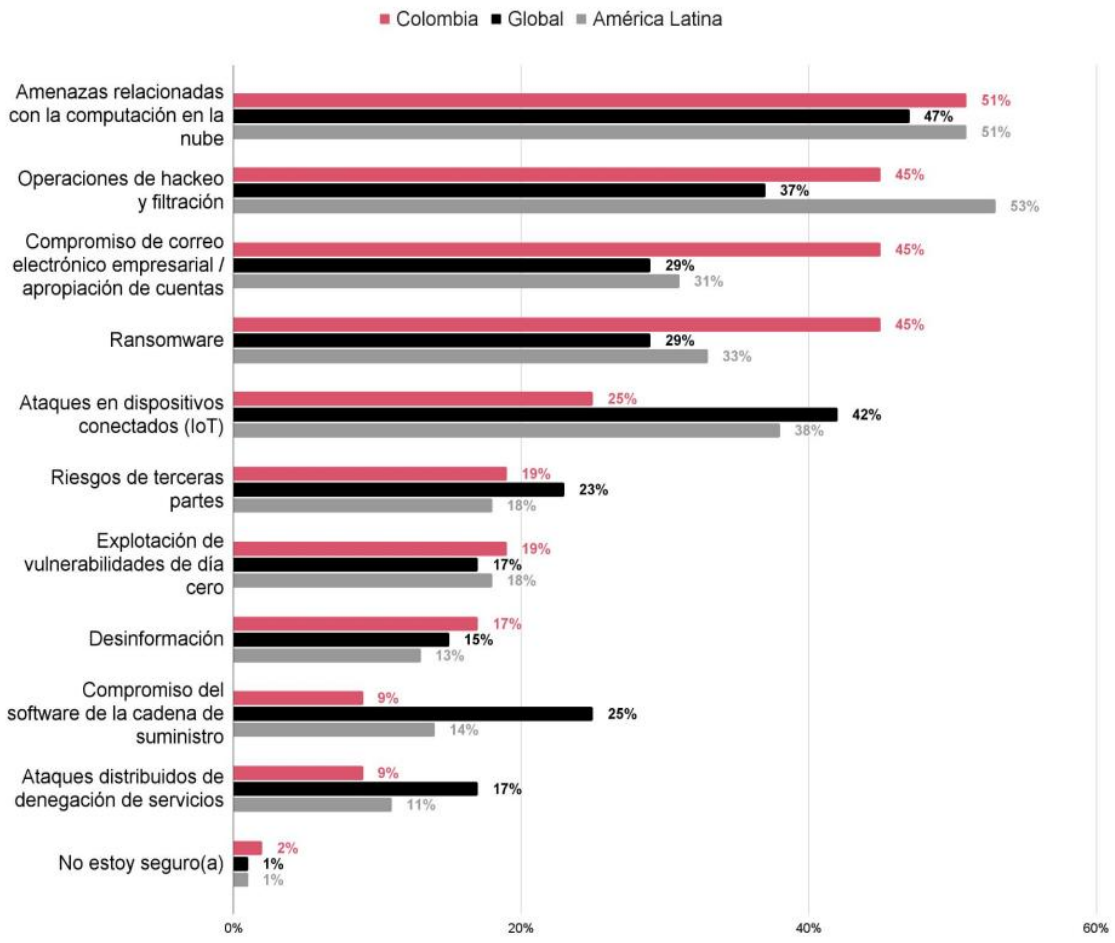
Desarrollo y discusión

La era digital ha planteado importantes desafíos a las organizaciones, ofreciendo no sólo oportunidades en optimizar la eficiencia, y eficacia en sus procesos a nivel general, a su vez implica riesgos cibernéticos, exponiéndose a amenazas y ataques constantes, como pérdida de datos confidenciales, reducción de la productividad, pérdidas económicas, daño a la reputación, pérdida de confianza de los grupos de interés (clientes, empleados, socios y usuarios).

Por su parte, el Informe de Riesgos Globales 2024 realizado por el Foro Económico Mundial; indica que la crisis climática, la desinformación generada por la IA y el incremento de los riesgos cibernéticos son la principal preocupación de las personas para los próximos años.

Al mismo tiempo, y a modo ilustrativo, según datos presentados por PwC Colombia (2024, p. 9), el ranking de riesgos en ciberseguridad identifica las principales amenazas cibernéticas que enfrentan las organizaciones en la actualidad (ver Gráfica 1).

Gráfica 1



En este escenario, el auditor asume un rol estratégico en la salvaguarda de la información y la ciberseguridad organizacional. Su labor trasciende el análisis estructural de la entidad, pues implica también el fortalecimiento de competencias

que le permitan innovar, adaptarse y aprovechar oportunidades en un entorno empresarial dinámico y en constante transformación.

Contexto de la Ciberseguridad en la Era Digital

La ciberseguridad se ha convertido en una prioridad global para las organizaciones debido a la creciente interconexión de los sistemas tecnológicos y la digitalización de los procesos comerciales. Las amenazas cibernéticas pueden originarse de diversas formas: malware, ransomware, phishing, hacking, y ataques DDoS, entre otros. Cada una de estas amenazas presenta riesgos específicos para la integridad de los datos, la privacidad de los usuarios y la continuidad operativa de las empresas.

La ciberseguridad dentro de las organizaciones puede desempeñar un papel clave en la prevención y detección de actividades sospechosas o fraudulentas. Al integrarse de manera sistémica con la auditoría y la gestión del conocimiento, contribuye a respaldar la toma de decisiones del capital intelectual y a garantizar la integridad de las operaciones.

En el contexto colombiano, los ataques cibernéticos no sólo afectan a grandes corporaciones, sino también a pequeñas y medianas empresas (PYMES), que muchas veces no cuentan con las infraestructuras necesarias para protegerse.

Los avances tecnológicos, como la inteligencia artificial, el big data y la computación en la nube, han añadido una nueva capa de complejidad a la auditoría de ciberseguridad. Por ejemplo, el uso de IA en los ataques cibernéticos permite a los atacantes lanzar ataques más rápidos, inteligentes y difíciles de detectar, lo que requiere que los auditores se adapten constantemente a los nuevos métodos de ataque.

Ciberseguridad y transformación digital

Saeed, Altamimi, Alkayyal, Alshehri y Alabbad (2023) abordaron la relación entre transformación digital y resiliencia organizacional frente a amenazas cibernéticas.

Su revisión sistemática evidencia la necesidad de implementar medidas de protección cibernética y fortalecer la conciencia del personal sobre ciberseguridad.

Asimismo, destacan el papel de tecnologías emergentes como la inteligencia artificial y el big data en la mitigación de riesgos.

Este artículo destaca la importancia de la ciberseguridad en la transformación digital que evoluciona constantemente, particularmente en un escenario postpandemia donde las organizaciones migraron a tecnologías emergentes, revolucionando a nivel mundial, viéndose en la necesidad de llevar su computación en la nube, big data, analíticas, cobertura en redes, entre otros, generando al mismo tiempo mayor vulnerabilidad y abriendo brechas para ataques en materia de seguridad.

Este estudio también indica que la implementación de estas tecnologías debe ir acompañadas de estrategias que incluyan factores técnicos y humanos.

En ese contexto, el auditor es una figura clave para las estrategias que deben realizar las organizaciones para que sus procesos en materia de seguridad se encuentren protegidos; en un ambiente de la protección de datos, la integridad y seguridad de la información priman, el rol del auditor debe ser preventivo frente a las amenazas que se ven expuestas las empresas.

De igual forma, el artículo resalta la importancia del factor humano en la gestión de la ciberseguridad con la capacitación constante, lo cual refuerza una vez más que los auditores deben evaluar el sistema de control interno, el ambiente de control y a través del monitoreo con procesos de formación continua; esto sitúa al auditor en evolución constante que no se limita solo a controles correctivos sino desde la prevención y detección, aliándose a los objetivos estratégicos de las compañías.

Inteligencia artificial para la detección de ciberataques

El estudio de Álvarez Carreño y Carrillo Naizaque (2024) se centra en la aplicación de inteligencia artificial generativa para la detección de ciberataques en el sector financiero colombiano. Los resultados muestran que estas tecnologías permiten una detección proactiva de amenazas y refuerzan la seguridad digital.

Se destaca la importancia de integrar la IA en los planes de seguridad de las entidades financieras.

De acuerdo a este artículo se resalta el papel fundamental que juega la inteligencia artificial (IA) para combatir la ingeniería social de los ciberdelincuentes en un sector crucial como lo es, el financiero.

Las entidades financieras diseñan estrategias frente a la prevención de fraudes y amenazas latentes en su entorno digital, buscando siempre generar un nivel de confianza para sus usuarios, donde les permita, que el uso de canales, portales, plataformas frente a posibles incidentes no lleguen a ser tan perjudicial.

El avance de la tecnología ha transformado la manera en que las personas interactúan con los servicios financieros, privilegiando cada vez más lo digital por su practicidad y rapidez. No obstante, este mismo entorno expone a las entidades a riesgos significativos como la suplantación de identidad, el robo de datos personales o la indisponibilidad de plataformas, poniendo en juego la confianza y seguridad del usuario final. En este escenario, la inteligencia artificial se convierte en una herramienta estratégica, capaz de anticipar, detectar y mitigar estos riesgos mediante el análisis predictivo, la identificación de patrones anómalos y la automatización de respuestas frente a incidentes de seguridad.

Teniendo en cuenta lo anterior, la implementación de la inteligencia artificial en soluciones orientadas a prevenir fraudes en el sistema financiero debe estar liderada por profesionales altamente capacitados.

En este contexto, el auditor especializado adquiere un papel fundamental, no solo al evaluar la eficacia de los controles y mecanismos de prevención existentes, sino también al incorporar una visión estratégica que permita aprovechar el potencial de la IA como aliada en la detección temprana de amenazas y en la gestión proactiva de riesgos.

Este enfoque no se limita al ámbito técnico, sino que debe complementarse con la promoción de una cultura organizacional de seguridad, dado que, a pesar de los avances tecnológicos y la acelerada digitalización, persisten vulnerabilidades humanas. La ingeniería social continúa siendo un terreno poco comprendido por muchos usuarios, lo que abre oportunidades para los ciberdelincuentes. Por ello, la integración de la IA con procesos de auditoría y capacitación continua resulta clave para fortalecer la resiliencia del sistema financiero frente a los desafíos del entorno digital.

Arquitectura de Malla de Ciberseguridad (CSMA)

Orozco y Flórez Montoya (2024) propusieron estrategias para implementar la Arquitectura de Malla de Ciberseguridad en empresas colombianas, especialmente en PYMES. Identificaron barreras tecnológicas y económicas, pero también señalaron ventajas significativas en cuanto a protección descentralizada y dinámica ante ataques cibernéticos.

La seguridad cibernética se convierte en una prioridad crítica. Proteger datos y sistemas en un mundo digital complejo es esencial.

Para las pequeñas y medianas empresas, lograr un equilibrio entre la adopción tecnológica y la protección de sus activos digitales resulta un desafío estratégico y determinante para su sostenibilidad. No basta con recurrir únicamente a herramientas tradicionales como firewalls o antivirus; es necesario complementar estas defensas con medidas proactivas, tales como sistemas de monitoreo

inteligente, planes de respuesta ante incidentes y, especialmente, programas de formación y sensibilización para los empleados.

La verdadera fortaleza en ciberseguridad radica en combinar el uso de tecnologías avanzadas con una cultura organizacional orientada a la prevención y resiliencia.

De esta manera, las pymes pueden enfrentar con mayor solidez el aumento de las amenazas cibernéticas, proteger la integridad de sus operaciones y asegurar un crecimiento sostenible en un entorno digital cada vez más dinámico y competitivo (TicTac, 2023).

De acuerdo con Gartner la arquitectura de malla de ciberseguridad (Ciber-Security Mesh Architecture), es un ecosistema colaborativo de herramientas y controles diseñado para asegurar una empresa moderna y distribuida. Se basa en la estrategia de integrar herramientas de seguridad componibles y distribuidas al centralizar el plano de datos y control para lograr una colaboración más efectiva entre las herramientas.

Los resultados incluyen capacidades mejoradas de detección, respuestas más eficientes, políticas consistentes, gestión de posturas y procedimientos, y un control de acceso más adaptable y detallado; todo ello con el fin de lograr una mayor seguridad (Gartner, s.f.a).

En el mundo digital actual, donde constantemente las amenazas cibernéticas se aceleran y cada vez más se vuelven complejas, la ciberseguridad se convierte en la práctica para garantizar disponibilidad, integridad, confidencialidad y autenticidad de la información y los sistemas, tanto para usuarios individuales como para las organizaciones, especialmente en las pequeñas y medianas empresas.

De acuerdo con el estudio, la arquitectura de malla de ciberseguridad permite que diferentes herramientas de protección trabajen de manera integrada, generando una defensa más sólida y efectiva del sistema. Cuando esta arquitectura se complementa con las prácticas establecidas en la norma ISO 27001, que ofrece

directrices claras sobre cómo gestionar de forma eficiente la seguridad de la información, se logra un marco mucho más robusto.

En este escenario, el auditor juega un papel esencial: debe contar con capacidades técnicas, visión estratégica y conocimiento normativo que le permitan no solo verificar la existencia de controles o la aplicación de políticas, sino también evaluar y fortalecer la arquitectura de seguridad. Su rol trasciende la simple revisión documental, convirtiéndose en garante de que los datos estén protegidos, de que exista capacidad de respuesta ante incidentes y de que la organización pueda adaptarse a un entorno digital dinámico y en constante evolución.

Desafíos de la Auditoría de Ciberseguridad

Los auditores enfrentan varios desafíos al abordar los riesgos cibernéticos.

Entre los más destacados se encuentran la falta de herramientas adecuadas para detectar amenazas emergentes y la necesidad de un conocimiento actualizado sobre las tecnologías más recientes.

Las metodologías tradicionales de auditoría, como las basadas en los marcos COBIT o ISO 27001, a menudo no son suficientes para evaluar los riesgos cibernéticos que surgen a partir de tecnologías emergentes como el Internet de las Cosas (IoT) y la inteligencia artificial.

Además, los auditores deben lidiar con la velocidad y la sofisticación de los ataques. Los cibercriminales están cada vez mejor equipados para explotar las vulnerabilidades de los sistemas.

Los informes de la organización ISACA sugieren que muchas auditorías de TI (tecnología de la información) aún no incluyen una evaluación adecuada de los riesgos relacionados con los dispositivos conectados y la nube, áreas que son cada vez más críticas para las organizaciones modernas.

Otro desafío significativo es la falta de capacitación y especialización de los auditores en ciberseguridad. Si bien la mayoría de los auditores tienen un conocimiento básico sobre la seguridad de TI, muchos no están preparados para enfrentarse a las amenazas complejas que enfrentan las organizaciones hoy en día.

Modelos de auditoría en ciberseguridad

Sabillón y Cano (2019) propusieron un modelo de auditoría en ciberseguridad (CSAM Cybersecurity Audit Maturity Model) aplicable a organizaciones de cualquier naturaleza.

A partir de un estudio experimental, demostraron que el modelo fortalece los controles de seguridad y promueve la conciencia sobre los riesgos cibernéticos. Este enfoque resulta relevante en un entorno donde la digitalización ha incrementado la vulnerabilidad de las entidades frente a amenazas tecnológicas.

En el entorno digital actual, donde las organizaciones están constantemente expuestas a riesgos cibernéticos, el rol del auditor adquiere una importancia crucial. Su labor no solo se orienta a la protección de los activos de información, sino también al fortalecimiento y la mejora continua de los controles de ciberseguridad, garantizando así la resiliencia y confianza en los sistemas organizacionales.

Sabillón y Cano, en su artículo, mencionan como la aplicación de modelos pueden ayudar a las empresas de cualquier sector y tamaño en la seguridad cibernética, del mismo modo, la concientización sobre la ingeniería social, dado que no es solo lo que representa en términos monetarios un ataque cibernético, sino que muchas organizaciones no se encuentran preparado para ello y su respuesta, recuperación tienden a demorarse.

La implementación de modelos como el CSAM representa una herramienta estratégica en la ejecución de auditorías en ciberseguridad, con sus dominios abarcan todas las áreas funcionales de una organización asegurando la

evaluación efectiva en ciberseguridad, su madurez y respuesta a las amenazas cibernéticas.

Con este modelo el auditor no solo estará verificando controles, sino que evaluará el nivel de madurez cibernética de la empresa y como este se encuentra alineado en los objetivos estratégicos.

En este sentido el auditor ya no puede ser un espectador de la tecnología sino que tiene como reto apropiarse de esta transformación, generando valor a las empresa con visiones estratégicas, ya no desde un punto de verificación de controles con hallazgo de debilidades sino con visión crítica, implementando herramientas modernas reguladas por estándares internacionales y que se adapten a cualquier tipo de amenazas, siendo fundamental su rol desde la toma de decisiones, la mejora continua en los procesos y generando conciencia de cultura cibernética.

El Rol del Auditor en la Ciberseguridad

Su trabajo no se limita a evaluar los controles de seguridad, sino que también debe identificar, prevenir y mitigar los riesgos cibernéticos a través de un enfoque integral.

Una de las responsabilidades más importantes del auditor es realizar auditorías de seguridad periódicas para identificar posibles vulnerabilidades en los sistemas. Estas auditorías deben abarcar tanto los aspectos tecnológicos como los humanos de la seguridad, ya que muchas veces los errores humanos, como el phishing, son una de las principales vías de entrada para los atacantes.

Además de realizar auditorías, los auditores deben estar a la vanguardia en la implementación de nuevos marcos normativos y metodologías de auditoría. El modelo CSAM (Cybersecurity Audit Maturity Model), por ejemplo, se ha utilizado para mejorar la eficacia de las auditorías de ciberseguridad en diversas organizaciones. Este modelo ayuda a evaluar el nivel de madurez de una organización frente a los riesgos cibernéticos y proporciona un marco estructurado para mejorar continuamente las prácticas de seguridad.

Es evidente entonces, que el rol del auditor en ciberseguridad actúa como un garante del sistema de control interno digital, ayudando a prevenir incidentes, reducir la exposición al riesgo y asegurar el uso responsable de las tecnologías. Su rol está en constante evolución, adaptándose al ritmo acelerado de los avances tecnológicos y a la sofisticación creciente de las amenazas cibernéticas.

Después de las consideraciones anteriores, el auditor debe contar con una visión técnica sólida, con competencias analíticas y estratégicas que le permitan identificar vulnerabilidades, evaluar riesgos y generar recomendaciones concretas, esto a su vez, implica auditorías periódicas y exhaustivas para identificar posibles vectores de ataques cibernéticos.

Ahora bien, cualquier entorno empresarial, sin importar su tamaño, es vulnerable a ataques cibernéticos, de allí la importancia de implementar medidas de seguridad confiables y sólidas, y que deben ser medibles, auditables, por ejemplo, en entornos industriales, el auditor en ciberseguridad no solo debe evaluar vulnerabilidades técnicas, sino también comprender los procesos operativos y su exposición a riesgos digitales.

Su rol implica revisar protocolos, redes de control y dispositivos industriales, con el fin de detectar brechas que puedan ser aprovechadas por ciberatacantes, garantizando así la continuidad operativa y la integridad de los sistemas críticos (Teruel Carrera, 2023).

No obstante, es importante señalar que existen dos tipos generales de auditores: los internos y los externos. Aunque ambos cumplen funciones esenciales en el fortalecimiento de la ciberseguridad, se distinguen por su vinculación con la organización; los auditores internos forman parte de la estructura organizacional, mientras que los externos actúan de manera independiente.

En este contexto, Ghirardotti y Renna (2022) destacan que, actualmente, el auditor externo enfrenta el reto de integrar la ciberseguridad en su evaluación de riesgos financieros, en respuesta al aumento de las amenazas digitales. Si bien su

intervención en el análisis de controles no financieros sigue siendo limitada, se espera que examine cómo la tecnología empleada por la entidad auditada puede comprometer la integridad de los estados financieros, ajustando así sus procedimientos ante posibles incidentes cibernéticos con implicaciones materiales.

La función del auditor en la protección de datos

La Torre et al. (2021) analizaron el papel de los auditores en la protección de datos, destacando su responsabilidad en la identificación de riesgos y la garantía de integridad de la información. Mediante un enfoque cualitativo y el estudio de casos, concluyeron que los auditores deben desarrollar competencias digitales y mantenerse en constante actualización para enfrentar los retos del mundo cibernético.

Con base en lo anterior, el cumplimiento de las leyes de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa, la Ley 1581 de 2012 en Colombia, y otras regulaciones sectoriales, se ha convertido en un componente esencial dentro del marco de auditoría.

El auditor ya no se limita a revisar documentos o políticas, sino que debe tener la capacidad de verificar técnicamente el ciclo de vida de los datos: desde su recolección y almacenamiento, hasta su procesamiento, transferencia y eliminación segura.

Además, se espera que el auditor evalúe la existencia y eficacia de controles como: el consentimiento informado y explícito de los titulares, la seudonimización o cifrado de la información personal, los protocolos de atención a incidentes de seguridad de datos, el cumplimiento del principio de minimización de datos y finalidad específica.

De igual manera, el auditor desempeña un rol preventivo y educativo, al fomentar una cultura de privacidad dentro de las organizaciones. Esto implica capacitar a los responsables del tratamiento, supervisar los flujos de información entre áreas o terceros, y evaluar si se están respetando los derechos fundamentales de los usuarios, como el derecho al olvido, la rectificación o la portabilidad de sus datos.

Por tanto, la auditoría de protección de datos ya no es opcional, ni exclusivamente legal, sino una herramienta clave para asegurar la transparencia, mitigar riesgos reputacionales y construir confianza entre la organización y sus partes interesadas.

Competencias Necesarias en los Auditores de Ciberseguridad

Los auditores en ciberseguridad, deben contar con competencias que le permitan desarrollar de manera efectiva la labor, desde un punto técnico como el conocimiento en criptografía, que comprende los conocimientos básicos de cifrados y cómo ayudan a la protección de datos sensibles; familiarizarse con las amenazas cibernéticas comunes, como malware, phishing, ransomware, ataques de ingeniería social; y por supuesto, la normatividad que indica los requisitos regulatorios para la protección y minimización de riesgos cibernéticos.

Aunque no sea un experto en todas las áreas técnicas, es crucial que entienda cómo los sistemas de información y la seguridad de la información, son esenciales al negocio en marcha.

Con referencia a lo anterior, las competencias técnicas son necesarias, pero deben ser combinadas con las habilidades profesionales, para garantizar la mitigación de riesgos cibernéticos, y el cumplimiento de la normativa, obstaculizando la materialización de las amenazas y/o evitar sanciones legales.

En efecto, se consideran diferentes tipos de auditoría de ciberseguridad, según la funcionalidad y especialidad a analizar. Entre ellas se encuentran las auditorías de cumplimiento normativo, el hacking ético y los ejercicios de red team. Estas

últimas se clasifican como auditorías ofensivas, ya que tienen un enfoque más intrusivo y están orientadas a simular con realismo las acciones de un atacante real sobre la organización (Tendero López, 2022).

Luego entonces, dependiendo del tipo de auditoría (por ejemplo, cumplimiento normativo, hacking ético o red team), se exigirá mayor profundidad técnica o habilidades estratégicas específicas.

La constante actualización, la formación especializada y la comprensión integral del entorno tecnológico y organizacional son claves para garantizar la efectividad y relevancia del rol del auditor en la protección de los activos digitales de una organización.

Normativas y Marcos Regulatorios para la Auditoría de Ciberseguridad

Los marcos normativos y regulatorios constituyen la base sobre la cual se estructuran las auditorías de ciberseguridad, ya que proporcionan criterios estandarizados para evaluar la protección de los activos digitales.

Entre ellos, la norma ISO/IEC 27001 se destaca como una de las más reconocidas a nivel internacional, al ofrecer lineamientos claros para diseñar, implementar y auditar sistemas de gestión de la seguridad de la información (SGSI).

Por otro lado, el marco COBIT 2019 aporta principios y prácticas para fortalecer la gobernanza y el control de las tecnologías de la información dentro de las organizaciones.

Así mismo, el Reglamento General de Protección de Datos (GDPR), aunque aplicable en el contexto europeo, ha tenido repercusión global, especialmente en lo que respecta al manejo responsable de datos personales, impactando directamente las políticas de ciberseguridad.

En el contexto latinoamericano, y particularmente en Colombia, la regulación también ha avanzado.

Normativas como la Ley 1581 de 2012, que establece disposiciones generales para la protección de datos personales, y la Ley 1266 de 2008, sobre el manejo de información financiera y crediticia, representan pilares legales clave para la auditoría en entornos digitales.

Además, iniciativas lideradas por el MinTIC, como la Política Nacional de Seguridad Digital, buscan fortalecer el ecosistema de ciberseguridad a través de lineamientos que guíen tanto a entidades públicas como privadas.

Estos marcos no solo establecen responsabilidades legales, sino que también orientan la labor del auditor hacia una evaluación rigurosa, ética y alineada con los riesgos actuales del entorno digital.

El Futuro de la Auditoría de Ciberseguridad

El ahora de la auditoría de ciberseguridad se perfila como un proceso cada vez más inteligente, automatizado y adaptativo; a medida que las amenazas cibernéticas evolucionan con rapidez y sofisticación frente a un entorno digital dinámico; en consecuencia, el enfoque tradicional del auditor basado en revisiones periódicas resulta insuficiente.

En su lugar, se abre paso una auditoría continua y predictiva, capaz de anticiparse a los riesgos mediante el análisis de grandes volúmenes de datos y la detección de patrones anómalos en tiempo real.

La incorporación de inteligencia artificial y algoritmos de aprendizaje automáticos no solo optimiza la detección de vulnerabilidades, sino que transforma el rol del auditor en un agente estratégico de ciberdefensa. Así mismo, el avance de tecnologías como la computación en la nube, el Internet de las Cosas (IoT por sus

siglas en internet, que se refiere la conexión de objetos físicos a internet para que puedan intercambiar datos y funcionar de forma automática, sin intervención directa de personas) y la blockchain (es un sistema digital que guarda datos en bloques conectados entre sí, lo que hace que la información sea difícil de modificar y más segura) exige nuevas metodologías de evaluación, diseñadas para entornos distribuidos y altamente interconectados.

En este nuevo panorama, la auditoría no se limita a verificar el cumplimiento normativo, sino que se convierte en una herramienta clave para fortalecer la resiliencia digital de las organizaciones.

El auditor del futuro deberá combinar capacidades técnicas avanzadas con pensamiento crítico, visión anticipatoria y comprensión profunda del ecosistema digital, para responder eficazmente a los desafíos emergentes de la ciberseguridad.

Conclusiones

Los antecedentes revisados evidencian que el rol del auditor ha evolucionado hacia una función más técnica y estratégica, en la que debe integrarse a los procesos de transformación digital y liderar la evaluación de riesgos cibernéticos.

La adopción de tecnologías como la inteligencia artificial y la arquitectura de malla, así como el fortalecimiento de competencias digitales, se vuelve imprescindible.

La auditoría de ciberseguridad es esencial para garantizar la protección de los activos digitales de las organizaciones en un entorno cada vez más digitalizado y vulnerable a ciberataques.

Los auditores deben estar bien preparados, no solo con conocimientos técnicos, sino también con una capacidad para adaptarse a los rápidos cambios

tecnológicos. La formación continua y la adopción de marcos normativos y herramientas actualizadas son clave para enfrentar los desafíos emergentes.

En este contexto, la auditoría de ciberseguridad deja de ser una opción y se consolida como una función esencial para la sostenibilidad operativa y la confianza digital.

Su efectividad dependerá no solo del dominio de herramientas y marcos internacionales, sino de la capacidad del auditor para comprender la dimensión humana del riesgo, promover una cultura organizacional consciente de la ciberseguridad y adaptarse continuamente a un ecosistema digital en constante transformación. Así, el auditor del presente y del futuro no solo verifica, sino que protege, lidera e innova.

Finalmente, la auditoría en el mundo cibernético no sólo debe garantizar el cumplimiento normativo, sino también anticiparse a las amenazas y promover una cultura de seguridad digital en las organizaciones.

Referencias

1. Revista Finanzas y Negocios. (2022). Importancia del control interno y la tecnología en el emprendimiento. Universidad Latina de Panamá. https://revistas.ulatina.edu.pa/index.php/Finanzasynegocios/article/view/354

2. Infobae. (2024, noviembre 22). Récord histórico de ciberataques en todo el mundo y las pérdidas de billones de dólares de las empresas en 2025. https://www.infobae.com/tecno/2024/11/22/record-historico-de-ciberataques-en-todo-el-mundo-y-las-perdida-de-billones-de-dolares-de-las-empresas-en-2025/

3. Ayerbe, A. (2020). Ciberseguridad y su relación con la inteligencia artificial (ARI 128/2020). Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial.pdf

4. Forbes. (2024, febrero 28). Colombia es el país con más ataques de ciberseguridad en Latinoamérica. https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica

5. World Economic Forum. (2024). Riesgos globales 2024: 3 riesgos de los que no hablamos lo suficiente. https://es.weforum.org/stories/2024/02/riesgos-globales-2024-3-riesgos-de-los-que-no-hablamos-lo-suficiente/

6. PwC Colombia. (2024). Digital Trust Insights 2024. PwC. https://www.pwc.com/co/es/publicaciones/digital-trust-insights/2024/digital-trust-insights-2024-pwc-colombia.pdf

7. Saeed, S., Altamimi, SA, Alkayyal, NA, Alshehri, E. y Alabbad, DA (2023). Transformación digital y desafíos de ciberseguridad para la resiliencia de las empresas: problemas y recomendaciones. Sensors, 23 (15), 6666. https://www.mdpi.com/1424-8220/23/15/6666

8. Álvarez Carreño, Y. A., & Carrillo Naizaque, D. C. (2024). Inclusión de la inteligencia artificial generativa en la detección de ciberataques a usuarios del sector financiero en Colombia [Trabajo de grado, Universidad EAN]. Repositorio Institucional Universidad EAN. https://repository.universidadean.edu.co/server/api/core/bitstreams/8fa4b84b-fe9d-484e-aa1f-5ac101d88385/content.

9. Cristian Camilo Sánchez Orozco, Beatriz Elena Flórez Montoya (2024). Cyber-Security Mesh Architecture, estrategias para un despliegue en empresas colombianas. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia). http://revista.escolme.edu.co/index.php/cies/article/view/495

10. Sabillón, R., & Cano, J. J. (2019). Auditorías en ciberseguridad: Un modelo de aplicación general para empresas y naciones. Revista Ibérica de Sistemas e Tecnologias de Informação, 2019, (32). https://openaccess.uoc.edu/items/7692a1f2-6b07-4add-b92a-b70ab395b262#page=1

11. Teruel Carrera, D. (2023). Ciberseguridad en sistemas industriales [Trabajo de Fin de Grado, Universitat Oberta de Catalunya]. UOC Open Access.https://openaccess.uoc.edu/server/api/core/bitstreams/bbf53a38-40cc-4482-8e6e-143c352e5be3/content

12. Ghirardotti, M., & Renna, J. I. (2022). Auditoría externa y ciberseguridad. Auditar: Revista Argentina Exclusiva sobre Auditoría. https://sedici.unlp.edu.ar/bitstream/handle/10915/151367/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

13. La Torre, M., Botes, VL, Dumay, J., & Odendaal, E. (2021). Protegiendo un nuevo talón de Aquiles: el papel de los auditores en la práctica de la protección de datos. Revista de Auditoría Gerencial, 36 (2), 218-239. https://www.aasmr.org/jsms/Vol13/No.1/Vol.13.No.1.26.pdf

14. Tendero López, M. (2022). Un sistema para hacer auditorías de ataques tipo Mousejack [Trabajo de Fin de Grado, Universidad Complutense de Madrid]. https://docta.ucm.es/rest/api/core/bitstreams/265ed0e7-e7e1-4157-a29c-20c85701bfd1/content

15. International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 - Information security management systems. ISO. https://www.iso.org/standard/27001.

16. Information Systems Audit and Control Association (ISACA). (2019). COBIT 2019 Framework: Introduction and Methodology. ISACA. https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf