DOI: https://doi.org/10.46296/yc.v9i17.0744

HALLAZGOS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA MODERNA

IT SECURITY FINDINGS FOR THE MODERN BUSINESS

Almeida-Zambrano Edison Ernesto [1]; Moreira-Moreira Cristhian Elías [2];
Flores-Lopez Angel Leandro [3]

[1] Universidad Laica Eloy Alfaro de Manabí. Manta, Ecuador.
Correo: edison.almeida@uleam.edu.ec. ORCID ID: https://orcid.org/0000-0002-1601-3450.

[2] Universidad Técnica de Manabí. Portoviejo, Ecuador.
Correo: tegcristhian1982@hotmail.com. ORCID ID: https://orcid.org/0000-0003-0253-8173

[3] Universidad Laica Eloy Alfaro de Manabí. Manta, Ecuador.
Correo: angel.flores@uleam.edu.ec. ORCID ID: https://orcid.org/0009-0005-5032-9976

Resumen

El estudio aborda los hallazgos de seguridad informática en el contexto de la empresa moderna, considerando la complejidad de los entornos digitales y la necesidad de articular factores técnicos, organizativos y culturales. El análisis parte de la identificación de riesgos y vulnerabilidades presentes en infraestructuras corporativas interconectadas, donde la dependencia de sistemas en la nube y dispositivos digitales incrementa la exposición a amenazas. La evaluación de estas dinámicas permite comprender la importancia de la gestión integral de riesgos como proceso estratégico. Se destacan las tecnologías emergentes como componentes transformadores en la protección de datos empresariales. La inteligencia artificial, el blockchain, la criptografía avanzada y los entornos de virtualización representan recursos clave en la prevención y mitigación de incidentes, al facilitar modelos predictivos, trazabilidad de la información y cifrado robusto. Estas herramientas configuran un modelo de seguridad adaptativo que supera el enfoque reactivo tradicional y promueve una defensa continua. Finalmente, se resalta la dimensión organizacional de la seguridad informática, concebida como una cultura que integra protocolos, capacitación y políticas corporativas. La consolidación de esta cultura requiere la participación activa de todos los miembros de la organización y la alineación con marcos de gobernanza que fortalezcan la coherencia de las prácticas.

Palabras claves: Seguridad informática, empresa moderna, ciberseguridad, tecnologías emergentes, cultura organizacional.

Abstract

The study addresses computer security challenges in the context of a modern company, considering the complexity of digital environments and the need to articulate technical, organizational and cultural factors. The analysis starts from the identification of risks and vulnerabilities present in interconnected corporate infrastructures, where the dependence of systems on the cloud and digital devices increases exposure to threats. The evaluation of these dynamics allows us to understand the importance of integral risk management as a strategic process. Emerging technologies stand out as transformative components in the protection of business data. Artificial intelligence, blockchain, advanced encryption and virtualization environments represent key resources in preventing and mitigating incidents, facilitating predictive models, providing information and robust encryption. These tools configure an adaptive security model that overcomes the traditional reactive approach and promotes continuous defense. Finally, the organizational dimension of computer security is highlighted, conceived as a culture that integrates protocols, training and corporate policies. The consolidation of this culture requires the active participation of all members of the organization and alignment with governance frameworks that strengthen the coherence of practices.

Keywords: Computer security, modern company, cyber security, emerging technologies, organizational culture.
Información del manuscrito:
Fecha de recepción: 16 de junio de 2025.
Fecha de aceptación: 29 de agosto de 2025.
Fecha de publicación: 19 de septiembre de 2025.

1. Introducción

La transformación digital ha reconfigurado los sistemas empresariales, generando nuevas oportunidades de innovación y, al mismo tiempo, exponiendo a las organizaciones a riesgos sin precedentes en el ámbito de la seguridad informática. La creciente dependencia de redes interconectadas, infraestructuras en la nube y plataformas digitales ha convertido la información en uno de los activos más valiosos de la empresa moderna. En este contexto, la protección de los datos se posiciona como un eje central en la sostenibilidad de los modelos de negocio.

El estudio de la seguridad informática en entornos corporativos no se reduce al análisis de amenazas técnicas, sino que también abarca la comprensión de los factores organizativos y humanos que intervienen en la gestión de la información. Los hallazgos en este campo revelan que las vulnerabilidades suelen surgir tanto de fallas en los sistemas como de prácticas inadecuadas por parte de los usuarios, lo que plantea la necesidad de un enfoque integral.

Asimismo, el avance de tecnologías emergentes ha introducido soluciones que transforman la manera en que las empresas enfrentan los desafíos de la ciberseguridad. Herramientas basadas en inteligencia artificial, blockchain y criptografía avanzada ofrecen nuevos mecanismos de defensa que potencian la resiliencia digital.

La seguridad informática en la empresa moderna también se relaciona con la construcción de una cultura organizacional que promueva prácticas responsables y protocolos claros de actuación. Este trabajo se desarrolla bajo la premisa de que la protección digital constituye un proceso estratégico donde convergen innovación tecnológica, gestión de riesgos y participación activa de toda la organización.

2. Dinámicas de riesgo y vulnerabilidad en entornos corporativos digitales

La seguridad informática en el ámbito empresarial se ha convertido en un eje prioritario debido a la creciente complejidad de los sistemas digitales y la interconexión global que caracteriza a la economía

contemporánea. La exposición constante a amenazas cibernéticas ha generado un panorama donde los riesgos y vulnerabilidades deben analizarse de manera sistemática, considerando tanto factores técnicos como organizativos (Acurio et al., 2024). Las empresas modernas, al depender de infraestructuras digitales, sistemas en la nube y redes interconectadas, enfrentan escenarios en los que la integridad de los datos se convierte en un recurso estratégico de alto valor.

El estudio de las dinámicas de riesgo revela que las vulnerabilidades no se limitan únicamente a la configuración de hardware o software, sino que también abarcan procesos internos, prácticas laborales y el comportamiento humano dentro de las organizaciones. La ingeniería social, el acceso no autorizado y la explotación de debilidades en protocolos de seguridad constituyen vectores comunes que afectan a las estructuras empresariales (Arencibia-Pardo & Peña-Rodríguez, 2024). A su vez, el incremento de dispositivos conectados amplía la superficie de ataque, generando nuevas oportunidades para actores maliciosos.

La identificación de riesgos en estos entornos implica la aplicación de metodologías de evaluación que integran monitoreo continuo, análisis predictivo y la utilización de inteligencia artificial para detectar patrones inusuales en los flujos de información (Andrade Farias, 2024). Tales prácticas permiten construir un mapa detallado de amenazas que facilita la toma de decisiones estratégicas.

La comprensión de estas dinámicas no solo evidencia la necesidad de adaptar sistemas de defensa avanzados, sino que también resalta la importancia de establecer una cultura organizacional centrada en la gestión de riesgos, donde la seguridad informática sea asumida como un proceso integral que atraviesa todas las áreas de la empresa.

3. Tecnologías emergentes aplicadas a la protección de datos empresariales

El avance tecnológico ha impulsado la aparición de herramientas innovadoras que transforman la manera en que las empresas resguardan su información crítica.

Estas tecnologías emergentes proporcionan mecanismos que van más allá de los sistemas tradicionales de defensa, integrando inteligencia artificial, blockchain, criptografía avanzada y entornos de virtualización como recursos clave en la seguridad informática contemporánea (Gaviria-Lopera et al., 2023).

La inteligencia artificial y el aprendizaje automático permiten el desarrollo de sistemas de detección y respuesta automatizada que identifican actividades anómalas en tiempo real. A través del análisis de grandes volúmenes de datos, estas soluciones generan modelos predictivos que anticipan ataques y ofrecen respuestas rápidas ante incidentes (López-Anchala & Ordóñez-Parra, 2024). Por otra parte, la tecnología blockchain introduce esquemas de almacenamiento descentralizado que refuerzan la integridad y la trazabilidad de la información, dificultando su manipulación no autorizada.

La criptografía de última generación se presenta como otro pilar en la protección empresarial, garantizando la confidencialidad de los datos mediante algoritmos robustos y técnicas de cifrado que resisten intentos de descifrado sofisticados. Asimismo, las plataformas de virtualización y entornos de nube segura brindan a las empresas la posibilidad de aislar procesos críticos y minimizar el impacto de posibles intrusiones (Olaniyi et al., 2024).

El despliegue de estas tecnologías requiere de una articulación estratégica con los sistemas ya existentes, garantizando su compatibilidad y eficacia en la mitigación de riesgos. Al mismo tiempo, su aplicación refleja la evolución hacia un modelo de seguridad informática que no se limita a la reacción ante incidentes, sino que adopta un enfoque preventivo y adaptativo.

De esta manera, las tecnologías emergentes se consolidan como componentes esenciales en la configuración de un ecosistema digital empresarial resiliente, en el que la protección de datos constituye una prioridad fundamental.

4. Estrategias organizacionales y cultura de ciberseguridad en la empresa moderna

La seguridad informática en el contexto empresarial trasciende el plano estrictamente técnico para convertirse en un componente organizacional que involucra políticas, prácticas y procesos orientados a consolidar una cultura de ciberseguridad. Esta cultura se manifiesta en la capacidad de las empresas para integrar la seguridad en cada nivel de su estructura, desde la alta dirección hasta los colaboradores que interactúan diariamente con los sistemas digitales (Apriani et al., 2024).

La formulación de estrategias organizacionales en materia de seguridad informática implica el diseño de protocolos claros de actuación, planes de respuesta ante incidentes y sistemas de capacitación continua. Estos elementos permiten construir un marco en el que la prevención y la detección temprana de amenazas se integran a la rutina laboral. La creación de equipos especializados en ciberseguridad, acompañados de auditorías periódicas y simulaciones de ataques, fortalece la preparación empresarial frente a incidentes críticos (Al Kurdi et al., 2024).

La cultura de ciberseguridad, entendida como la internalización de prácticas responsables, se alimenta de procesos educativos que promueven la conciencia sobre los riesgos digitales. La capacitación de los empleados en el manejo seguro de información, la verificación de fuentes y la protección de credenciales constituye un factor decisivo en la reducción de vulnerabilidades asociadas al error humano.

Asimismo, la implementación de sistemas de gobernanza corporativa que incluyan comités de seguridad, métricas de desempeño y alineación con estándares internacionales refuerza la coherencia de las prácticas. Estas estrategias permiten que la seguridad informática se convierta en un valor compartido y transversal dentro de la organización (Sestino et al., 2025).

La construcción de una cultura sólida de ciberseguridad refleja la comprensión de que la protección digital no depende exclusivamente de tecnologías avanzadas, sino de la

convergencia entre estructuras organizativas, políticas internas y el compromiso activo de todos los miembros de la empresa.

5. Conclusiones

El análisis desarrollado muestra que los hallazgos de seguridad informática en la empresa moderna permiten comprender la magnitud de los desafíos que enfrentan las organizaciones en un entorno digital altamente interconectado. La identificación de riesgos y vulnerabilidades evidencia que las amenazas no se limitan a factores técnicos, sino que incluyen dimensiones humanas y organizativas, lo que exige un abordaje integral de la gestión de la seguridad.

Las tecnologías emergentes representan un aporte sustancial a la protección de datos empresariales. Su implementación posibilita la detección temprana de incidentes, la trazabilidad de procesos y el fortalecimiento de la confidencialidad de la información. Estas herramientas transforman la ciberseguridad en un proceso dinámico y preventivo, que se adapta de manera continua a la evolución de las amenazas.

Por otra parte, la consolidación de estrategias organizacionales y de una cultura de ciberseguridad constituye un factor clave en la resiliencia empresarial. La capacitación constante, la creación de protocolos de actuación y la integración de sistemas de gobernanza refuerzan la capacidad de respuesta de las empresas ante escenarios críticos. La seguridad informática se convierte así en un valor compartido que permea todas las áreas de la organización.

Bibliografía

Acurio, J. V. L., León, Á. R. E., Morocho, R. A. R., & Viteri, H. A. S. (2024). Evaluación de los controles de seguridad a través de auditorías informáticas: Desafíos en la era moderna. *Pro Sciences: Revista de Producción, Ciencias e Investigación, 8*(54), 79-90.

Al Kurdi, B., Alquqa, E. K., Nuseir, M. T., Alzoubi, H. M., Alshurideh, M. T., & AlHamad, A. (2024). Impact of cyber security and risk management on green operations: Empirical evidence from security companies in the UAE. En

Cyber security impact on digitalization and business intelligence: Big cyber security for information management: Opportunities and challenges (pp. 151-167). Cham: Springer International Publishing.

Andrade Farias, D. A. (2024). *Auditoría informática a la gestión de seguridad de la información a "YERAY Electrodomésticos"* (Tesis doctoral).

Apriani, D., Afrijaldi, R., Auliya, N., & Darmawan, A. A. (2024). Operating system and server integration for business effectiveness. *IAIC Transactions on Sustainable Digital Innovation (ITSDI), 5*(2), 91-99.

Arencibia-Pardo, F. R., & Peña-Rodríguez, B. (2024). Seguridad informática en la industria moderna, un enjambre de retos y estadísticas. *Formación Estratégica, 10*(2), 119-137.

Gaviria-Lopera, J. F., Villamizar-Jaimes, A. E., Soto-Durán, D. E., & Reyes-Gamboa, A. X. (2023). Buenas prácticas en la gestión en seguridad informática: Caso de estudio en la educación media. *Revista Ibérica de Sistemas e Tecnologias de Informação, (E60),* 567-580.

López-Anchala, K. A., & Ordóñez-Parra, Y. L. (2024). Auditoría y ciberseguridad en el sector comercial: Evaluación de resiliencia ante amenazas digitales [Audit and cyber security in the commercial sector: Assessing resilience to digital threats]. *Revista Multidisciplinaria Perspectivas Investigativas, 4*(especial), 14-27.

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion protocols: Strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. *Journal of Engineering Research and Reports, 26*(6), 31-49.

Sestino, A., Kahlawi, A., & De Mauro, A. (2025). Decoding the data economy: A literature review of its impact on business, society and digital transformation. *European Journal of Innovation Management, 28*(2), 298-323.