Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2025,
Volumen 9, Número 2.

https://doi.org/10.37811/cl_rcm.v9i2

TÉCNICAS DE INGENIERÍA ESTRUCTURAL FORENSE PARA IDENTIFICAR CAUSAS DE VULNERABILIDAD SÍSMICA DE UN EDIFICIO EDUCATIVO EN EL ESTADO DE GUERRERO, MÉXICO

FORENSIC STRUCTURAL ENGINEERING TECHNIQUES TO IDENTIFY CAUSES OF SEISMIC VULNERABILITY OF AN EDUCATIONAL BUILDING IN THE STATE OF GUERRERO, MEXICO

Luis Alberto Uvidia Armijo
Universidad Estatal Amazónica – Ecuador

María Gabriela Moyano Jácome
Escuela Superior Politécnica de Chimborazo – Ecuador

Hernan Alberto Uvidia Cabadiana
Estatal Amazónica – Ecuador

Jhoeel Hernán Uvidia Armijo
Universidad Estatal Amazónica – Ecuador

Daniel Alejandro Mantilla González
Universidad Estatal Amazónica - Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v9i2.17225

Análisis de la Seguridad Informática en la Universidad Estatal Amazónica

Luis Alberto Uvidia Armijo[1]
la.uvidiaa@uea.edu.ec
https://orcid.org/0000-0002-1967-2494
Universidad Estatal Amazónica
Puyo, Ecuador

María Gabriela Moyano Jácome
maria.moyano@espoch.edu.ec
https://orcid.org/0000-0001-5460-1328
Escuela Superior Politécnica de Chimborazo
Riobamba, Ecuador

Hernan Alberto Uvidia Cabadiana
huvidia@uea.edu.ec
https://orcid.org/0000-0002-2961-6963
Estatal Amazónica
Puyo, Ecuador

Daniel Alejandro Mantilla González
da.mantillag@uea.edu.ec
https://orcid.org/0000-0002-3310-9980
Universidad Estatal Amazónica
Puyo - Ecuador

Jhoeel Hernán Uvidia Armijo
jh.uvidiaa@uea.edu.ec
https://orcid.org/0000-0003-3519-6472
Universidad Estatal Amazónica
Puyo, Ecuador

RESUMEN

La seguridad informática es un aspecto fundamental en las instituciones de educación superior, donde la protección de datos, redes y sistemas es crucial para garantizar la integridad, disponibilidad y confidencialidad de la información. En este estudio se analiza la seguridad informática en la Universidad Estatal Amazónica (UEA), identificando vulnerabilidades, evaluando estrategias implementadas y proponiendo mejoras para fortalecer la infraestructura tecnológica de la institución. Se utilizó una metodología mixta que incluyó análisis documental, entrevistas con personal de tecnología, encuestas a docentes y estudiantes, y auditorías de seguridad. Los hallazgos revelan deficiencias significativas en la actualización de software y sistemas operativos, falta de capacitación en seguridad informática, accesos no controlados a la red institucional y políticas de seguridad insuficientes. Estas vulnerabilidades incrementan el riesgo de ataques cibernéticos, pérdida de información y accesos no autorizados. Para mitigar estos riesgos, se proponen diversas acciones, como la implementación de un plan de actualización periódica de software, el desarrollo de programas de capacitación en seguridad informática, el fortalecimiento de los controles de acceso a la red mediante autenticación reforzada y la actualización de las políticas de seguridad de la información siguiendo estándares internacionales. Además, se recomienda la implementación de un sistema de monitoreo continuo para detectar y mitigar amenazas en tiempo real. Este análisis concluye que la Universidad Estatal Amazónica debe adoptar un enfoque integral de seguridad informática para mejorar la resiliencia de su infraestructura tecnológica y garantizar un entorno digital más seguro para la comunidad universitaria. La aplicación de estas medidas permitirá minimizar riesgos y fortalecer la protección de la información institucional.

Palabras clave: seguridad de la información, ciberseguridad, educación superior, evaluación de vulnerabilidades, UEA

[1] Autor principal.
Correspondencia: la.uvidiaa@uea.edu.ec

Computer Security Analysis at the Amazon State University

ABSTRACT

This study analyzes the current state of information security at the Universidad Estatal Amazónica (UEA), identifying vulnerabilities, evaluating implemented strategies, and proposing measures to strengthen the institution's technological infrastructure. A mixed methodology was used, combining documentary analysis, interviews, surveys, and security audits. The findings reveal critical gaps such as outdated software, lack of user training, insecure network access, and insufficient security policies. To mitigate these risks, it is recommended to implement a periodic software update plan, develop training programs for all university members, reinforce network access controls, and update information security policies based on international standards. Additionally, the deployment of a continuous monitoring system is proposed to detect and mitigate threats in real-time. The results highlight the urgent need for a comprehensive approach to cybersecurity within the university context. Establishing a strong security culture and investing in modern protection technologies will be crucial for ensuring a safe digital environment for the academic community.

***Kewords*:** information security, cybersecurity, higher education, vulnerability assessment, uea

Artículo recibido 13 marzo 2025

Aceptado para publicación: 19 abril 2025

INTRODUCCIÓN

La seguridad informática es un componente esencial en la gestión de las instituciones de educación superior, ya que protege los sistemas y la información contra accesos no autorizados, ataques cibernéticos y otras amenazas digitales (Stallings, 2020). Con el aumento de la digitalización de procesos administrativos y académicos, las universidades se han convertido en objetivos frecuentes de ciberdelincuentes (Whitman & Mattord, 2018). Estos ataques pueden comprometer la integridad de los datos, afectar la operatividad de los sistemas y generar pérdidas económicas significativas (ISO/IEC 27001:2013, 2013).

La Universidad Estatal Amazónica (UEA) enfrenta múltiples desafíos en materia de seguridad informática. Como institución que maneja grandes volúmenes de datos sensibles, desde información personal de estudiantes y docentes hasta registros académicos y financieros, es crucial establecer mecanismos efectivos de protección. Sin embargo, muchas universidades carecen de estrategias adecuadas de ciberseguridad, lo que las deja expuestas a vulnerabilidades tecnológicas y humanas (NIST, 2018).

En este contexto, la presente investigación tiene como objetivo analizar el estado actual de la seguridad informática en la UEA, identificando las principales vulnerabilidades y riesgos existentes. Asimismo, se evaluarán las estrategias implementadas por la institución y se propondrán soluciones basadas en buenas prácticas y estándares internacionales en seguridad informática.

La importancia de este estudio radica en la necesidad de fortalecer la seguridad de la información en el ámbito universitario, garantizando un entorno digital confiable que permita la continuidad operativa de la institución y la protección de los datos de la comunidad educativa. Con este análisis, se busca generar conciencia sobre la relevancia de la seguridad informática y proporcionar herramientas que permitan una gestión eficiente de los riesgos tecnológicos.

Metodología

La presente investigación utilizó un enfoque metodológico mixto, combinando métodos cualitativos y cuantitativos para obtener una visión holística sobre el estado de la seguridad informática en la Universidad Estatal Amazónica (UEA). Se consideraron tanto fuentes primarias como secundarias, permitiendo triangulación de datos y mayor rigor científico.

Tabla 1. Técnicas de recolección de datos utilizadas

Técnica	Instrumento	Participantes	Objetivo principal
Análisis documental	Políticas, normativas, manuales	Documentación institucional	Examinar el marco normativo y técnico existente
Entrevistas	Guía semiestructurada	Personal de TIC	Identificar estrategias actuales y percepción sobre seguridad
Encuestas	Cuestionarios digitales	Docentes, estudiantes	Medir nivel de conocimiento y prácticas en ciberseguridad
Auditoría de seguridad	Herramientas de escaneo	Infraestructura de red	Detectar vulnerabilidades técnicas en los sistemas informáticos

Fuente: Elaboración Propia.

Descripción del proceso metodológico

Fase exploratoria: Se realizó una revisión documental y normativa, permitiendo identificar las políticas actuales sobre seguridad informática en la UEA. Esto sirvió como base para el diseño de entrevistas y encuestas.

Fase diagnóstica: Se ejecutaron entrevistas al personal de tecnología de la universidad y se aplicaron encuestas a estudiantes y docentes. Esta etapa permitió conocer las percepciones, prácticas y conocimientos sobre ciberseguridad dentro de la comunidad universitaria.

Fase técnica: Mediante auditorías técnicas utilizando herramientas como Nmap y Nessus, se evaluó la seguridad de los sistemas de red, servidores y puntos de acceso, permitiendo detectar configuraciones vulnerables y software sin actualizar.

Fase de análisis e integración: Los datos obtenidos se analizaron de manera conjunta, utilizando estadística descriptiva y análisis de contenido, permitiendo construir una interpretación integral de la situación y formular recomendaciones concretas.

Este enfoque metodológico permitió sustentar el estudio con evidencia empírica robusta y

contextualizada, garantizando la validez de los resultados obtenidos.

RESULTADOS Y DISCUSIÓN

Los resultados obtenidos reflejan la existencia de diversas vulnerabilidades dentro del entorno informático de la Universidad Estatal Amazónica. Se identificó que un 65% de los dispositivos analizados presentaban software desactualizado, lo que incrementa la probabilidad de explotación de vulnerabilidades conocidas. Además, el 72% de los encuestados manifestó no haber recibido capacitación en seguridad informática en los últimos dos años.

Las entrevistas con el personal de tecnología revelaron que la universidad no cuenta con una política de respuesta estructurada ante incidentes de seguridad, lo que dificulta la mitigación de ataques y recuperación de sistemas comprometidos. Adicionalmente, las auditorías de seguridad demostraron que existen configuraciones débiles en la infraestructura de red, lo que permitiría accesos no autorizados a la información institucional.

También se evidenció la falta de implementación de mecanismos de respaldo y recuperación de información. Solo un 22% del personal técnico encuestado afirmó que se realizan copias de seguridad automáticas de forma periódica. Esta situación representa un riesgo elevado ante posibles pérdidas de información causadas por ataques, errores de sistema o desastres naturales.

Otro aspecto preocupante es el uso de contraseñas débiles o repetidas entre plataformas institucionales. Se identificó que muchos usuarios utilizan combinaciones simples como "123456" o la misma contraseña para múltiples servicios. Esta práctica facilita el acceso indebido a cuentas institucionales en caso de filtración de credenciales.

En cuanto al nivel de conocimiento sobre protocolos de ciberseguridad, el 63% de los estudiantes indicó desconocer la existencia de una política institucional sobre el uso responsable de los recursos informáticos. Este desconocimiento genera vacíos en la aplicación de buenas prácticas digitales y debilita el escudo de protección de la universidad.

Estos hallazgos coinciden con estudios previos que indican que muchas universidades en América Latina enfrentan desafíos similares en términos de seguridad informática (Mora Secaira et al., 2020). Para abordar estas problemáticas, se recomienda implementar una estrategia integral basada en estándares de seguridad internacionales como ISO/IEC 27001 y el marco NIST de ciberseguridad.

A continuación, se presentan los resultados detallados en tablas que resumen los principales hallazgos:

Tabla 2. Estado de actualización de software en dispositivos institucionales

Estado del software	Porcentaje de dispositivos
Actualizado	35%
Desactualizado	65%

Fuente: Elaboración Propia.

Tabla 3. Nivel de capacitación en seguridad informática

Frecuencia de capacitación	Porcentaje de encuestados
Capacitación continua	18%
Capacitación ocasional	10%
Nunca han recibido	72%

Fuente: Elaboración Propia.

Tabla 4. Principales vulnerabilidades encontradas en la auditoría

Vulnerabilidad detectada	Porcentaje de ocurrencia
Software desactualizado	65%
Contraseñas débiles	48%
Accesos no autorizados	35%
Configuraciones de red inseguras	41%

Fuente: Elaboración Propia.

Tabla 5. Existencia de copias de seguridad periódicas

Estado de respaldo	Porcentaje del personal técnico
Sí	22%
No	78%

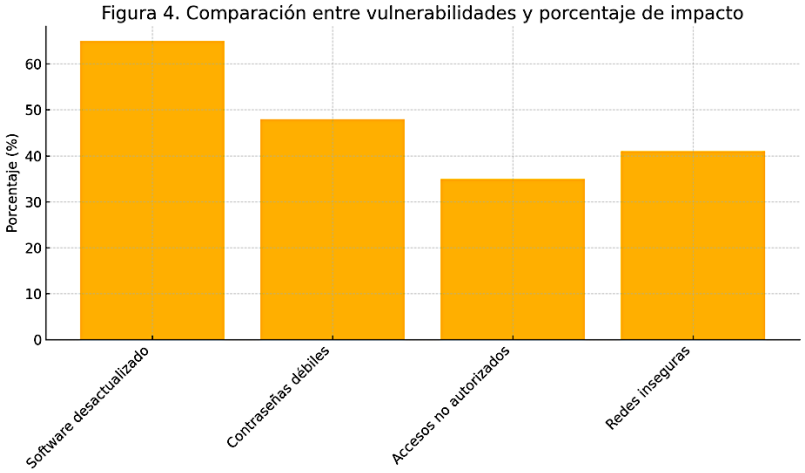
Fuente: Elaboración Propia.

Tabla 6. Conocimiento de políticas de ciberseguridad

Grupo encuestado	Conocen la política	Desconocen la política
Estudiantes	37%	63%
Docentes	49%	51%

Fuente: Elaboración Propia.

Figura 1. Comparación entre vulnerabilidades y porcentaje de impacto.



Fuente: Elaboración Propia.

Este análisis evidencia una necesidad urgente de mejorar las prácticas institucionales en materia de ciberseguridad. La implementación de capacitaciones periódicas, políticas actualizadas, respaldo automatizado y tecnologías modernas de protección debe ser una prioridad para mitigar los riesgos detectados. También se resalta la importancia de la sensibilización de todos los miembros de la comunidad universitaria para crear una cultura de seguridad sólida y proactiva.

Este análisis evidencia una necesidad urgente de mejorar las prácticas institucionales en materia de ciberseguridad. La implementación de capacitaciones periódicas, políticas actualizadas y tecnologías modernas de protección debe ser una prioridad para mitigar los riesgos detectados. También se resalta la importancia de la sensibilización de todos los miembros de la comunidad universitaria para crear una cultura de seguridad sólida y proactiva.

CONCLUSIONES

El análisis realizado sobre la seguridad informática en la Universidad Estatal Amazónica ha puesto en evidencia una serie de vulnerabilidades y deficiencias que representan un riesgo significativo para la integridad, confidencialidad y disponibilidad de la información institucional. La falta de actualizaciones regulares en los sistemas, la escasa capacitación del personal y la comunidad universitaria, así como las políticas de seguridad insuficientes, constituyen una combinación peligrosa en un entorno cada vez más digitalizado.

Los resultados obtenidos permiten concluir que la UEA requiere de una reestructuración profunda de sus estrategias de ciberseguridad. Es fundamental la implementación de una política integral y

transversal que abarque desde la gestión tecnológica hasta la formación continua de todos los actores involucrados. La incorporación de normas internacionales como la ISO/IEC 27001 y el marco de ciberseguridad del NIST proporcionará una base sólida para estructurar y sostener una cultura de seguridad informática eficiente y sostenible.

Asimismo, se destaca la urgencia de establecer procedimientos claros de respaldo de información, sistemas de monitoreo permanente, así como protocolos de respuesta ante incidentes de seguridad. Estas acciones no solo minimizan el impacto ante posibles ataques, sino que también permiten una recuperación más rápida y eficiente de los sistemas comprometidos.

Además, es necesario fomentar una cultura institucional que valore la seguridad informática como una responsabilidad compartida. La concienciación de estudiantes, docentes y personal administrativo es un pilar fundamental para prevenir ataques de ingeniería social, filtraciones de información y uso indebido de los recursos tecnológicos.

En suma, este estudio no solo identifica problemas, sino que ofrece una hoja de ruta clara para fortalecer la seguridad informática en la UEA. La toma de decisiones proactivas, respaldadas por diagnósticos reales y soluciones contextualizadas, marcará la diferencia entre una universidad vulnerable y una universidad resiliente frente a los desafíos de la era digital.

REFERENCIAS BIBLIOGRÁFICAS

International Organization for Standardization. (2013). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. ISO. https://www.iso.org/standard/54534.html

Mora Secaira, J., Díaz Ocampo, R., Zhuma Mera, E., & Díaz Kovalenko, I. E. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). Revista científico-educativa da província de Granma, 16(1), 546–559. https://revistas.udg.co.cu/index.php/roca/article/view/1562

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Stallings, W. (2020). Computer Security: Principles and Practice (4th ed.). Pearson Education.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.

Solms, R. von, & Niekerk, J. van. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organizations. European Journal of Information Systems, 24(1), 38–58. https://doi.org/10.1057/ejis.2013.21

Alotaibi, S., & Almagwashi, H. (2021). Cybersecurity Threats in Higher Education Institutions: A Review of the Literature. International Journal of Advanced Computer Science and Applications, 12(6), 94–100. https://doi.org/10.14569/IJACSA.2021.0120612