ANÁLISIS DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN SEDE SAN JOSÉ

JOSÉ ÁLVARO BASTIDAS SANDOVAL

Trabajo de grado aplicado

Directora

Ing. Jenny Fernanda Restrepo Santacruz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
ABRIL 2025

Dedicatoria

A Dios por derramar sus bendiciones en mi vida, y allanar los terrenos para que pudiera iniciar mi proceso formativo como especialista, por el don de la vida y su infinito amor derramado en cada instante de mi existencia. A mi amada esposa, por su paciencia, comprensión y aliento constante, por ser mi roca en los momentos difíciles y por creer en mí incluso cuando yo dudaba de mí mismo.

A mis hijos, cuyo amor puro e inagotable me motiva a ser un ejemplo para seguir, recordándome que cada logro es una semilla para un futuro prometedor, por ser el motor que me ha impulsado a ser un mejor hombre y lograr cosas inimaginables.

A mis padres, quienes con su amor incondicional y apoyo inquebrantable me enseñaron el valor del esfuerzo y la dedicación. A mis hermanos, por ser mi fuente de inspiración y por alentarme a nunca rendirme, recordándome que el conocimiento y la perseverancia son la clave para alcanzar nuestras metas.

A mis colegas y amigos, cuyo apoyo y colaboración fueron fundamentales en mi camino hacia la excelencia profesional, por compartir su conocimiento y experiencias, y por enriquecer mi visión de la seguridad informática.

Este logro no sería posible sin cada uno de ustedes. Esta victoria es también suya y espero que este trabajo sea un tributo a su constante aliento y fe en mí. Gracias por ser parte de mi viaje y por ser los pilares que me sostuvieron en los momentos más desafiantes.

Agradecimientos

Agradezco a las personas que han sido fundamentales en mi camino hacia la obtención del título de especialista en seguridad informática. A los docentes, gracias por su dedicación y orientación experta en cada etapa de este desafiante proceso. Sus valiosos consejos y comentarios han sido la piedra angular de este trabajo, a mis compañeros de formación, quienes, con su espíritu colaborativo y debates constructivos, han enriquecido mis perspectivas y han hecho de este viaje académico una experiencia memorable.

No puedo dejar de mencionar a mis colegas en la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, cuyo constante aliento y apoyo me han permitido equilibrar las demandas del trabajo y los estudios. su comprensión ha sido crucial para alcanzar este logro.

A mi familia, mi mayor pilar, gracias por su inquebrantable apoyo, amor y paciencia a lo largo de este desafiante trayecto. Su fe en mí ha sido mi principal motivación.

Finalmente, a todos aquellos cuyo nombre no menciono, pero cuya influencia ha dejado una huella en mi camino, les estoy enormemente agradecido. Su contribución ha sido invaluable y ha contribuido significativamente a mi crecimiento personal y profesional.

Gracias a cada uno de ustedes por ser parte de mi historia y por ayudarme a alcanzar este hito en mi vida académica y profesional.

Resumen

En un entorno como el nuestro dónde se tiene una sociedad cada vez más interconectada, la seguridad informática se ha convertido en un pilar fundamental para garantizar la continuidad de las operaciones y la protección de la información crítica. En este contexto, el presente proyecto se propone abordar uno de los desafíos más apremiantes de la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, sede San José: la evaluación y mejora de la seguridad en su infraestructura de red de telecomunicaciones. La infraestructura de red de esta institución educativa es el cimiento sobre el cual descansan una amplia gama de servicios telemáticos vitales para el aprendizaje, la administración y la colaboración. Sin embargo, la creciente complejidad de las amenazas cibernéticas y las vulnerabilidades identificadas en esta infraestructura plantean riesgos significativos que deben abordarse de manera proactiva. Este proyecto se constituye como una hoja de ruta hacia la mejora de la seguridad informática en la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, mediante un enfoque riguroso que abarca desde la identificación de amenazas hasta la elaboración de recomendaciones y medidas de mitigación. La metodología, diseñada con cuidado y basada en las mejores prácticas de seguridad informática, servirá como guía para proteger los activos de información, garantizar la disponibilidad de los servicios y preservar la integridad de los datos. En el desarrollo de este proyecto se trabajará incansablemente para evaluar los riesgos de seguridad, proponer soluciones efectivas y empoderar a la institución para mantenerse a la vanguardia en la protección de su infraestructura de red y la seguridad de sus servicios telemáticos.

Palabras clave*:* Activos de información, Clasificación, Controles, Confidencialidad, Integridad, Disponibilidad, Seguridad

Abstract

In an increasingly connected and technology-dependent world, cybersecurity has become a fundamental pillar to ensure the continuity of operations and the protection of critical information. In this context, the current project aims to address one of the most pressing challenges of the INSTITUTION OF HIGHER EDUCATION OF POPAYÁN, San José campus: the evaluation and improvement of security in its telecommunications network infrastructure. The network infrastructure of this educational institution is the foundation upon which a wide range of telematic services crucial for learning, administration, and collaboration rely. However, the growing complexity of cyber threats and vulnerabilities identified in this infrastructure pose significant risks that must be proactively addressed. This project serves as a roadmap towards improving cybersecurity at the INSTITUTION OF HIGHER EDUCATION OF POPAYÁN, employing a rigorous approach that spans from threat identification to the development of recommendations and mitigation measures. The methodology, carefully designed and based on cybersecurity best practices, will serve as a guide to protect information assets, ensure service availability, and preserve data integrity. In the development of this project, relentless efforts will be made to assess security risks, propose effective solutions, and empower the INSTITUTION OF HIGHER EDUCATION OF POPAYÁN to stay at the forefront of protecting its network infrastructure and the security of its telematic services.

Keyword: Information assets, Classification, Controls, Confidentiality, Integrity, Availability, Security

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

Glosario

CONTROL DE ACCESO: Forma de limitar el acceso a un sistema o a recursos físicos o virtuales. En informática, el control de acceso es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a los sistemas, recursos o información[1].

EVALUACIÓN DE RIESGOS: Proceso que ayuda a las organizaciones a identificar, analizar y aplicar controles de seguridad en el lugar de trabajo. Evita que las vulnerabilidades y las amenazas se infiltren en la organización y protege los activos físicos e informativos de los usuarios no autorizados[2].

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Es un conjunto de políticas de administración de la información. El término se denomina en inglés “Information Security Management System” (ISMS)[3].

ACTIVOS INFORMÁTICOS: Recursos tecnológicos del entorno de la información comunicativa que forman parte de las empresas y tienen como objetivo la difusión de información[4].

PRUEBAS DE PENETRACIÓN: Una prueba de penetración, o "pen test", es una prueba de seguridad que lanza un ciberataque simulado para encontrar vulnerabilidades en un sistema informático[5].

RIESGOS DE SEGURIDAD: Un riesgo en ciberseguridad es la existencia de una amenaza, o ciber-amenaza, que tenga consecuencias negativas para los sistemas de información de la empresa[6].

---

[1] Ciberseguridad. (2019). *Control de acceso*. Ciberseguridad.com. https://ciberseguridad.com/normativa/espana/medidas/control-acceso/#%C2%BFQue_es_el_control_de_acceso.

[2] Escuela Europea de Excelencia. (2022, febrero). *Evaluación de riesgos de seguridad de la información: 7 pasos para asegurar el cumplimiento de ISO 27001*. Escuela Europea de Excelencia. https://www.escuelaeuropeaexcelencia.com/2022/02/evaluacion-de-riesgos-de-seguridad-de-la-informacion-7-pasos-para-asegurar-el-cumplimiento-de-iso-27001/.

[3] Firma-e. (s.f.). ¿Qué es un SGSI – *Sistema de Gestión de Seguridad de la Información?* Firma-e | Proyectos y formación. https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/.

[4] Castejón, P. (2021, mayo 24). *Activos informáticos: Las 7 claves que tienes que conocer.* Perito Judicial Group. https://peritojudicial.com/activos-informaticos/#:~:text=1.-,Qué%20son%20los%20activos%20informáticos,ejemplo%20de%20hardware%20y%20software.

[5] IBM. (s.f.). *¿Qué son las pruebas de penetración?* IBM in Deutschland, Österreich und der Schweiz. https://www.ibm.com/mx-es/topics/penetration-testing.

[6] Ciberseguridad. (s.f.). *¿Qué es un riesgo en ciberseguridad? Definición y tipos*. Ciberseguridad Tips. https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas/#Que_es_un_riesgo_en_ciberseguridad.

SEGURIDAD INFORMÁTICA: Conjunto de tecnologías, procesos y prácticas diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado[7].

VULNERABILIDAD: Debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes[8].

CIBERSEGURIDAD: La ciberseguridad implica proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos frente a ataques malintencionados. También se conoce como seguridad de la información tecnológica o electrónica. Este término abarca diversos contextos, desde el ámbito empresarial hasta la informática móvil, y se puede dividir en varias categorías comunes[9].

INFRAESTRUCTURA DE RED: La infraestructura de red es un componente de la infraestructura TI que abarca el hardware, software, sistemas y dispositivos necesarios para la transmisión de datos dentro de una organización. Esta infraestructura permite la conexión entre usuarios, dispositivos, aplicaciones e Internet, entre otros[10].

TELECOMUNICACIONES: Las telecomunicaciones se refieren a la ciencia y práctica de transmitir información mediante medios electromagnéticos, utilizando técnicas y materiales especializados. Esta información puede ser textual, de audio, de video o una combinación de estos. Hoy en día, el concepto incluye diversas tecnologías como radio, televisión, telefonía, redes informáticas, Internet,

---

[7] HubSpot. (2023, mayo 8). *Seguridad informática: Qué es, tipos y características*. Blog de HubSpot. https://blog.hubspot.es/website/que-es-seguridad-informatica#:~:text=La%20seguridad%20inform%C3%A1tica%20es%20el,da%C3%B1o%20o%20acceso%20no%20autorizado.

[8] Banco Santander. (s.f.). *Vulnerabilidad*. Banco Santander. https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica,%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

[9] Kaspersky. (2024, mayo 24). *¿Qué es la ciberseguridad?* Kaspersky Latam. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

[10] Paessler. (s.f.). *Infraestructura de red siempre a la vista con PRTG*. Paessler.com. https://www.paessler.com/es/network-infrastructure?utm_term=&utm_campaign=1635204137&utm_content=&utm_source=google&utm_medium=cpc&utm_adgroup=96974539650&utm_device=c&gad_source=1&gclid=CjwKCAjwko21BhAPEiwAwfaQCPGrGgydM988XqzE1USNZEMOUnwpW_8d8TKUO148pTwGvKGEgmF8TRoCdVAQAvD_BwE

radionavegación, GPS y telemetría[11].

AMENAZA DE CIBERSEGURIDAD: Una amenaza de ciberseguridad se refiere a cualquier circunstancia o evento que pueda tener un impacto negativo en las operaciones, funciones, reputación, marca o percepción de una empresa. Además, puede comprometer el acceso, integridad y valor de los datos, así como afectar a las personas, procesos y tecnologías que los gestionan[12].

FIREWALL: Un firewall es un sistema de seguridad de red que controla el tráfico de Internet entrante, saliente o dentro de una red privada. Este sistema, que puede ser un software o una combinación de hardware y software, bloquea o permite el paso de paquetes de datos de manera selectiva. Su principal objetivo es prevenir actividades maliciosas y evitar accesos no autorizados a la red[13].

IDS: Un IDS es una herramienta de seguridad de red que supervisa el tráfico y los dispositivos en busca de actividades maliciosas, comportamientos sospechosos o violaciones de las políticas de seguridad establecidas[14].

IPS: Un IPS es un sistema que ayuda a las organizaciones a identificar y bloquear proactivamente el tráfico malicioso. Los productos que incorporan tecnología IPS se pueden implementar en línea para monitorear el tráfico entrante e inspeccionarlo en busca de vulnerabilidades y exploits[15].

---

[11]Concepto. (s.f.). *Telecomunicaciones - Qué son, historia, tipos, impacto en la sociedad*. Concepto.de. https://concepto.de/telecomunicaciones/

[12] Hewlett Packard Enterprise (HPE). (s.f.). *¿Qué es una amenaza de ciberseguridad?* Recuperado el 26 de julio de 2024, de https://www.hpe.com/lamerica/es/what-is/cybersecurity-threats.html#:~:text=Una%20amenaza%20de%20ciberseguridad%20se,imagen%20percibida%20de%20una%20empresa.

[13] Kaspersky. (2024, mayo 7). *¿Qué es un firewall? Definición y explicación*. https://latam.kaspersky.com/resource-center/definitions/firewall.

[14] IBM. (2023, abril 19). *¿Qué es un sistema de detección de intrusiones (IDS*)? https://www.ibm.com/es-es/topics/intrusion-detection-system.

[15] Fortinet. (s.f.). *¿Qué es un IPS (Sistema de Prevención de Intrusiones)?* Recuperado el 26 de julio de 2024, de https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips.

INTRODUCCIÓN

En el vertiginoso mundo digital actual, donde la conectividad es la columna vertebral de la enseñanza y la colaboración, las instituciones educativas enfrentan desafíos cada vez más complejos en lo que respecta a la seguridad de la información y la integridad de sus infraestructuras de red. En este contexto dinámico, la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, sede San José, no es ajena a los obstáculos que surgen en la protección de la red interna de telecomunicaciones frente a las constantes amenazas cibernéticas y las vulnerabilidades físicas y lógicas.

Existe una dependencia crítica en la cual se tiene la intervención de un tercero para el manejo de la red interna de telecomunicaciones que acude a respaldar los servicios telemáticos esenciales para la excelencia académica y administrativa dentro de la institución, lo que ha permitido evidenciar una serie de desafíos alarmantes que podrían comprometer la integridad, confidencialidad y disponibilidad de la información. La coexistencia de múltiples métodos de autenticación y el acceso compartido a la red inalámbrica, junto con la carencia de medidas de seguridad física en los gabinetes de distribución, han creado un panorama de riesgos inminentes que exigen una respuesta proactiva y efectiva

Consciente de la importancia crítica de salvaguardar la infraestructura de red y telecomunicaciones de la institución, este proyecto aplicado se propone analizar exhaustivamente los riesgos de seguridad informática que acechan a la institución. Al abordar estas vulnerabilidades desde una perspectiva holística y proponer estrategias concretas para su mitigación, buscando mantener a la universidad a la vanguardia en el entorno digital en constante evolución, fortaleciendo su capacidad de adaptarse a los cambios.

A través de un enfoque integral, este proyecto pretende establecer las bases para el fortalecimiento de una infraestructura de red robusta, resistente y segura, que garantice la continuidad de las operaciones académicas, administrativas y que salvaguarde la integridad de la información vital para la comunidad universitaria.

PLANTEAMIENTO DEL PROBLEMA

ANTECEDENTES DEL PROBLEMA

La relevancia de garantizar la seguridad informática en ámbitos educativos ha sido ampliamente investigada y analizada en la literatura académica. El incremento de la dependencia de la tecnología y las redes de comunicaciones en entornos educativos ha subrayado la importancia vital de proteger plenamente la integridad, disponibilidad y confidencialidad de la información frente a amenazas y vulnerabilidades cada vez más complejas.

Según una publicación de la revista edu “Asegurar la confidencialidad, integridad y disponibilidad de la información en un mundo tecnológico se han convertido en los ejes principales a garantizar al interior de cualquier organización. De hecho, actualmente, el sector educativo tiene el desafío de evitar la vulnerabilidad, fortalecer el acceso, monitorear y garantizar la adecuada gestión de los equipos, reduciendo las posibilidades de ser víctimas de ataques cibernéticos”[16].

Claramente, las universidades y demás centros educativos deben asumir una gestión responsable de la información que involucra a su comunidad educativa, incluyendo a estudiantes, profesores y personal administrativo. Por consiguiente, las instituciones de educación superior tienen un rol crucial en la promoción de una cultura de seguridad y la implementación de políticas que fomenten la capacitación de las personas, además de la identificación, desarrollo y aplicación de tecnologías para reforzar los sistemas de prevención ante posibles ataques informáticos perpetrados por ciberdelincuentes[17].

En una noticia publicada en la página del periódico el espectador, se menciona como en el año 2015, un estudiante de último semestre de la universidad de los Andes en Bogotá, “violó la plataforma de notas de su universidad y modificó algunas de sus calificaciones” [18]. En la misma noticia se menciona que “la Unidad de Delitos Informáticos de la DIJIN adelanta indagaciones por denuncias de otras

---

[16] Anónimo. (2023, octubre 24). *Los retos de seguridad informática que enfrentan las instituciones de educación en Colombia*. Revista Edu.co. Disponible en https://revistaedu.co/secciones/tematicas-educativas/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-de-educacion-en-colombia/2660/.

[17] Anónimo. (2023, octubre 24). *Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior*. Revista MODUM. Disponible en https://revistas.sena.edu.co/index.php/Re_Mo/article/view/4543.

[18] Anónimo. (2023, octubre 24). *Universidades, víctimas de “hackers”.* ELESPECTADOR.COM. Disponible en https://www.elespectador.com/judicial/universidades-victimas-de-hackers-article-560884/.

universidades, en las que no solo estudiantes, sino también empleados del área de admisiones y registro están involucrados"[19]. Lo que deja en evidencia que las instituciones de educación superior están expuestas ataques realizados por miembros de la misma institución, los cuales aprovechan que tienen acceso a la infraestructura de red de alguna forma, dejando en evidencia la clara necesidad de implementar medidas de mitigación de ataques informáticos.

La CCN (Centro Criptológico Nacional), en un documento llamado "Riesgos y amenazas en productos fuera de soporte: prevención y protección" dice:

La existencia de tecnología y productos fuera de soporte en los sistemas de la organización puede suponer un riesgo para su seguridad. Un producto no soportado por su fabricante no experimentará nuevas actualizaciones y los posibles fallos de seguridad que puedan aparecer no serán corregidos, de forma que contribuirá a incrementar la superficie de exposición a la ciberamenaza[20]. Lo anterior indica que la presencia de tecnologías y productos obsoletos en los sistemas de una institución representa un riesgo significativo para su seguridad. La falta de actualizaciones y parches de seguridad puede dejar vulnerabilidades sin corregir, ampliando así el potencial de exposición a ataques. Por lo tanto, es crucial mantener una infraestructura tecnológica actualizada y respaldada por el fabricante para garantizar la protección efectiva de los datos.

La INSTITUCIÓN ha experimentado un notable avance en la incorporación de tecnologías de la información para apoyar tanto sus funciones académicas como administrativas. Este progreso ha incrementado la dependencia de la infraestructura tecnológica, haciendo cruciales la seguridad y la gestión eficiente de los recursos tecnológicos para el funcionamiento diario de la institución. Sin embargo, esta dependencia ha aumentado la exposición a diversos riesgos y amenazas que podrían poner en peligro la confidencialidad, integridad y disponibilidad de la información.

A lo largo del tiempo, la sede San José ha enfrentado varios incidentes relacionados con su infraestructura de red y telecomunicaciones, como interrupciones del servicio de Internet, brechas de seguridad que han comprometido información sensible y fallos de hardware que han causado la pérdida de datos importantes. Estos problemas han afectado la operatividad de la institución y han resaltado la necesidad de implementar medidas de seguridad más robustas y eficaces. La falta

---

[19] Anónimo. (2023, octubre 24). *Universidades, víctimas de "hackers".* ELESPECTADOR.COM. Disponible en https://www.elespectador.com/judicial/universidades-victimas-de-hackers-article-560884/ (Óp. cit., p. 17).

[20] CCN-CERT. (2021). *Riesgos y amenazas en productos fuera de soporte: prevención y protección*. https://www.ccn-cert.cni.es/es/informes/abstracts/5726-riesgos-y-amenazas-productos-fuera-de-soporte/file?format=html.

de procedimientos adecuados de respaldo y recuperación de datos, junto con la vulnerabilidad a ataques cibernéticos como phishing y ransomware, subraya la urgencia de abordar estos desafíos de manera proactiva.

La institución debe adherirse a diversas normativas nacionales e internacionales que supervisan la seguridad de la información y la protección de datos personales, como la Ley de Protección de Datos Personales y el Reglamento General de Protección de Datos (GDPR). El cumplimiento de estas regulaciones es crucial no solo para evitar posibles sanciones legales, sino también para mantener la confianza de estudiantes, personal y demás partes interesadas en la capacidad de la institución para salvaguardar la integridad de sus datos. Reforzar las políticas internas de seguridad, proporcionar capacitación continua al personal y adoptar tecnologías avanzadas para la detección y respuesta ante incidentes son pasos fundamentales para mitigar los riesgos identificados y asegurar la continuidad de las operaciones institucionales.

Todos los puntos mencionados resaltan la relevancia de realizar una evaluación minuciosa de los riesgos de seguridad informática en contextos educativos, con el propósito de salvaguardar la estabilidad de la infraestructura de red y sistemas de comunicaciones. Se considera fundamental aplicar políticas de seguridad robustas, implementar controles de acceso eficaces y adoptar sistemas de gestión de riesgos proactivos para asegurar la permanente protección de la información esencial y la disponibilidad de los servicios telemáticos en instituciones educativas.

FORMULACIÓN DEL PROBLEMA

La INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, sede San José, es una institución educativa que depende en gran medida de su infraestructura de red de telecomunicaciones para el funcionamiento de sus servicios telemáticos. Sin embargo, se han identificado varias vulnerabilidades y riesgos de seguridad informática que ponen en peligro la integridad y disponibilidad de esta infraestructura. Una de ellas es que la red WiFi de la universidad está siendo compartida por estudiantes, administrativos y visitantes, lo que puede llevar a un uso inadecuado y riesgos de seguridad. Los estudiantes tienen acceso mediante un portal cautivo, lo que implica la creación de credenciales en un directorio activo, credenciales que en muchas ocasiones son compartidas entre varios usuarios. Los administrativos utilizan su propio dominio en el directorio activo y por las dinámicas institucionales comparten sus credenciales con docentes y administrativos para que puedan hacer uso de los equipos de cómputo, y los visitantes se autentican directamente en la controladora WiFi. Esta diversidad de usuarios y métodos de autenticación aumenta la complejidad de la gestión y la seguridad de la red.

Por otra parte, los gabinetes que alojan dispositivos de distribución, como Switches, carecen de seguridad física, como cerraduras. Esto permite un acceso no

autorizado a estos dispositivos y sus componentes, incluyendo cables de red, estabilizadores de voltaje y fuentes de energía, la manipulación no autorizada de estos elementos puede causar intermitencias y fallas en el servicio, sin mencionar que algunos de los sistemas de información y software de administración de servicios están virtualizados en servidores que ejecutan sistemas operativos obsoletos, como Windows 7, que ya no cuentan con soporte. Esto los hace vulnerables a fallas y amenazas de seguridad que podrían interrumpir la disponibilidad de los servicios críticos de la universidad.

De acuerdo con lo anterior, con el desarrollo del presente proyecto aplicado se busca dar respuesta a la siguiente pregunta problema: ¿Cómo el análisis de los riesgos de seguridad informática en la infraestructura de red y telecomunicaciones de la Institución de Educación Superior de Popayán sede San José, puede permitir la proposición de estrategias y medidas efectivas para fortalecer la seguridad informática?

JUSTIFICACIÓN

La realización de un análisis de riesgos actuales de seguridad informática en la infraestructura de red de telecomunicaciones de la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, sede San José, se fundamenta en la necesidad crítica de preservar la integridad, disponibilidad y confidencialidad de los servicios telemáticos ofrecidos por la institución. Esta justificación se basa en los siguientes puntos:

La institución depende en gran medida de su infraestructura de red para ofrecer servicios educativos, administrativos y de información críticos. Cualquier interrupción en la disponibilidad de estos servicios afecta negativamente a estudiantes, profesores, personal administrativo y la comunidad en general. En una red de telecomunicaciones tan grande y compleja como la que está siendo objeto de estudio de este trabajo, se requiere la identificación de múltiples vulnerabilidades y riesgos actuales en la infraestructura de red, como la compartición de redes inalámbricas, la falta de seguridad física en gabinetes de dispositivos y la obsolescencia de sistemas operativos, lo que resalta la urgencia de abordar estos problemas antes de que puedan ser explotados por amenazas cibernéticas o incidentes no autorizados.

La implementación de medidas de seguridad informática adecuadas es esencial para cumplir con las regulaciones y normativas relacionadas con la privacidad de datos, protección de la información y seguridad cibernética que pueden aplicar a la universidad, sin mencionar que un incidente de seguridad informática puede tener un impacto significativo en la reputación de la institución. Normativas como la Ley 1581 de 2012 sobre Protección de Datos Personales en Colombia, la Ley 1273 de 2009 sobre Delitos Informáticos, y regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) en caso de tener datos de ciudadanos europeos, son ejemplos de los marcos normativos que deben ser considerados. Identificar las brechas en el cumplimiento de estas normativas y la implementación de medidas correctivas no solo protege a la institución legalmente, sino que también refuerza la confianza de la comunidad académica y los stakeholders externos. La adopción de prácticas de seguridad sólidas y la mitigación de riesgos ayudarán a proteger la imagen y la confianza de la comunidad académica y los stakeholders externos. Por otra parte, la implementación de medidas de seguridad proactivas y la identificación de vulnerabilidades permiten a la universidad asignar recursos de manera eficiente, reduciendo los costos potenciales asociados a incidentes de seguridad y reparaciones de emergencia.

Por último, es importante tener en cuenta que el entorno de seguridad informática está en constante evolución, con nuevas amenazas y vulnerabilidades emergiendo regularmente. Este proyecto proporcionará una base sólida para adaptarse a estos cambios y mantener un alto nivel de seguridad. Además, la evaluación continua de riesgos y la actualización de las políticas de seguridad permiten a la institución

anticiparse a las amenazas futuras y responder de manera efectiva, garantizando la resiliencia de su infraestructura tecnológica y la continuidad de sus operaciones críticas.

OBJETIVOS

OBJETIVO GENERAL

Analizar los riesgos de seguridad informática en la institución de educación superior de Popayán sede San José.

OBJETIVOS ESPECÍFICOS

Examinar los activos de información que conforman la infraestructura de red y telecomunicaciones de la institución, mediante técnicas que permitan la recopilación de datos para establecer un inventario actualizado

Identificar para cada activo las amenazas y vulnerabilidades potenciales en la infraestructura de red y telecomunicaciones de la Institución de Educación Superior de Popayán sede San José, a través de la realización de pruebas de penetración y análisis de seguridad.

Evaluar la probabilidad y el impacto de ocurrencia de los riesgos identificados, a través de la verificación de los controles aplicados y las políticas de seguridad de la información existentes en la Institución.

Proponer estrategias y medidas de control basadas en los resultados de la evaluación para el fortalecimiento de la seguridad de en la institución.

MARCO REFERENCIAL

ANTECEDENTES

La seguridad informática en entornos educativos y organizacionales ha sido objeto de estudio en numerosas investigaciones y publicaciones recientes. Estos antecedentes proporcionan una comprensión sólida del panorama actual de la seguridad informática y ofrecen información valiosa sobre las tendencias, desafíos y mejores prácticas en la protección de la infraestructura de red y telecomunicaciones.

Enfrentar los desafíos inherentes a la seguridad informática en una entidad demanda un esfuerzo considerable, sin lugar a duda. Ya sea que la inquietud provenga de fallos internos de seguridad o de ser víctimas de un ataque malicioso, una realidad cada vez más presente, las empresas deben permanecer en constante vigilancia para proteger su información confidencial21.Es evidente que salvaguardar la información confidencial en el entorno empresarial requiere una atención constante y una estrategia proactiva. Tanto los riesgos internos como los ataques maliciosos externos plantean desafíos significativos en términos de seguridad de datos. Por lo tanto, las organizaciones deben comprometerse a mantener una vigilancia constante y a implementar medidas eficaces para proteger su información valiosa y mantener la confianza del cliente.

Por otra parte, como indica Díaz, Javier, “Fomentar los procesos de seguridad de la información implementados en las Instituciones de Educación Superior. Promover buenas prácticas e implementación de estándares de seguridad”22, lo que indica que impulsar la mejora continua de los procesos de seguridad de la información en las Instituciones de Educación Superior se presenta como una prioridad esencial. Promover e inculcar el cumplimiento de estándares de seguridad, junto con la adopción de buenas prácticas, emerge como una estrategia clave para garantizar la protección efectiva de los datos sensibles y salvaguardar la integridad de la infraestructura educativa en el contexto de un entorno digital cada vez más complejo.

De acuerdo con los hallazgos de la Asociación Nacional de Facultades y Escuelas de Ingeniería (ANFEI), que actualmente representa a 213 Instituciones de Educación Superior afiliadas en México, el más reciente informe sobre el estado de las Tecnologías de la Información y la Comunicación (TIC) en estas instituciones

---

[21] Fortra. (2023, octubre 25). *Principales desafíos de seguridad de datos y cómo abordarlos*. Disponible en https://www.fortra.com/es/blog/principales-desafios-de-seguridad-de-datos-y-como-abordarlos.

[22] Díaz, J. (2023, octubre 25). *Ciberseguridad*. https://www.metared.org/ar/ciberseguridad.html.

revela que el 76% de ellas han implementado una política de seguridad bajo la supervisión del encargado de Tecnologías de la Información (TI)[23].

En general, la seguridad de la información en los contextos educativos y empresariales ha sido objeto de una amplia investigación reciente, lo que ha arrojado luz sobre la importancia crítica de mantener una vigilancia constante y una estrategia proactiva. En este sentido, se reconoce la necesidad de abordar los riesgos internos y externos que plantean desafíos significativos para la integridad de los datos confidenciales y la confianza del cliente. Asimismo, se destaca la importancia de fomentar los procesos de seguridad de la información en las Instituciones de Educación Superior, mediante la promoción de buenas prácticas y la adopción de estándares de seguridad, como una estrategia esencial para salvaguardar la infraestructura educativa en un entorno digital cada vez más complejo. Además, los resultados recientes de la Asociación Nacional de Facultades y Escuelas de Ingeniería (ANFEI) evidencian la creciente implementación de políticas de seguridad en las Instituciones de Educación Superior, bajo la supervisión de los responsables de Tecnologías de la Información (TI).

MARCO CONCEPTUAL

SEGURIDAD INFORMÁTICA: Práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes[24].

MATRIZ DE RIESGOS INFORMÁTICOS: La matriz de riesgos es una herramienta del ámbito de la gestión que busca determinar cuáles son los riesgos más importantes para la seguridad y salud general de los trabajadores y activos de una empresa u organización. Se plantea en una clásica matriz para que su llenado sea simple, pero requiere de un arduo análisis de las distintas actividades que se desarrollan en la empresa[25].

VIRTUALIZACIÓN: Utiliza el software para imitar las características del hardware y

[23] ANFEI. (2021). *Asociación Nacional de Facultades y Escuelas de Ingeniería*. Disponible en https://www.anfei.mx/miembros/.
[24] Kaspersky. (2023, octubre 25). *¿Qué es la ciberseguridad?* latam.kaspersky.com. Disponible en https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.
[25] Anónimo. (2023, octubre 25). *Matriz de riesgos: Qué es y cómo se hace una*. Ciberseguridad. Disponible en https://ciberseguridadtips.com/matriz-de-riesgos/#Que_es_una_matriz_de_riesgos.

crear un sistema informático virtual. Esto permite a las organizaciones de TI ejecutar más de un sistema virtual, y múltiples sistemas operativos y aplicaciones, en un solo servidor[26].

HACKING ÉTICO: Uso de habilidades y herramientas de hacking para evaluar la seguridad de un sistema informático o de una red, de manera legal y ética, con el objetivo de identificar y corregir posibles vulnerabilidades antes de que sean explotadas por hackers malintencionado[27].

RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN: Los riesgos de la seguridad de la información implican posibles situaciones o actos que podrían comprometer la privacidad, exactitud y accesibilidad de los datos. Estos riesgos pueden surgir de diversas fuentes, tanto dentro como fuera de una organización, e incluyen una variedad de amenazas que pueden impactar en los sistemas de información y la información confidencial. [28].

COMPONENTES DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN: los componentes clave son las amenazas, debilidades y repercusiones. Las amenazas pueden originarse internamente, como actos intencionales o negligencia por parte del personal, o externamente, como ataques informáticos y programas maliciosos. Las debilidades engloban fallas técnicas en el hardware o software, así como errores humanos como la falta de formación en seguridad. Las repercusiones incluyen impactos financieros, como los costes de recuperación de incidentes, operativos, como la interrupción de servicios, y de reputación, afectando la confianza de los usuarios y la imagen de la organización.[29].

NORMA ISO/IEC 27001: 2013: Es un estándar reconocido a nivel mundial que aborda de manera sistemática la gestión de la seguridad de la información. Su principal objetivo es salvaguardar datos sensibles a través de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando su confidencialidad, integridad y disponibilidad. Aplicable a organizaciones de cualquier tamaño o sector, consta de 11 cláusulas esenciales que van desde el contexto organizacional y el liderazgo hasta la evaluación del rendimiento y la

---

[26] Anónimo. (2023, octubre 25). *Virtualization Technology & Virtual Machine Software: ¿What is Virtualization?* VMWare. Disponible en https://www.vmware.com/es/solutions/virtualization.html#:~:text=La%20virtualización%20utiliza%20el%20software,aplicaciones,%20en%20un%20solo%20servidor.

[27] U-tad. (2023, octubre 25). *¿Qué es el hacking ético?* U-tad. Disponible en https://u-tad.com/hacking-etico#:~:text=El%20hacking%20ético%20se%20define,sean%20explotadas%20por%20hackers%20malintencionados.

[28] American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7ª ed.). https://doi.org/10.1037/0000165-000.

[29] ISO/IEC. (2024). ISO/IEC 27001: *Information technology - Security techniques - Information security management systems - Requirements*. International Organization for Standardization.

mejora continua. El análisis de riesgos es central en ISO/IEC 27001: 2013, requiriendo que las organizaciones identifiquen y mitiguen amenazas y vulnerabilidades a través de evaluaciones regulares. Además, ofrece un conjunto de controles de seguridad que pueden implementarse para fortalecer áreas críticas como políticas de seguridad, gestión de activos, control de acceso y seguridad física. Adoptar esta norma no solo protege activos de información, sino que también facilita el cumplimiento de normativas legales y reglamentarias, asegurando la continuidad del negocio frente a posibles amenazas.[30].

Marco teórico

El desarrollo de la seguridad informática ha evolucionado significativamente en las últimas décadas en respuesta al crecimiento exponencial de la tecnología y la conectividad. A medida que las organizaciones y las instituciones educativas han adoptado cada vez más infraestructuras de red complejas y servicios telemáticos, se ha vuelto crucial comprender la evolución histórica de la seguridad informática y su relevancia en la protección de los sistemas de información.

La seguridad informática tuvo sus orígenes con la interconexión de equipos y el desarrollo de redes informáticas en la década de 1950, coincidiendo con el establecimiento de las primeras redes de computadoras y la creación de módems. Fue durante la década de 1960 que la seguridad cibernética empezó a tomar la estructura que se reconoce en la actualidad[31].

Antes de la invención de Internet, la comunicación digital se realizaba a través del telégrafo, que se desarrolló en 1840. Este dispositivo transmitía señales eléctricas a lo largo de cables conectados entre dos puntos, utilizando el código Morse para interpretar la información.[32]. Durante la década de 1990, con la expansión de las redes informáticas, se comprendió la importancia de resguardar las comunicaciones de red y los datos transferidos en estas redes. La introducción de cortafuegos y sistemas de detección de intrusiones representó un hito significativo en la evolución de la seguridad informática, proporcionando a las entidades herramientas para resguardar sus redes contra amenazas externas.

En los primeros años del siglo XXI, con la rápida propagación de redes inalámbricas y el incremento de ciberataques a gran escala, se acentuó la importancia de

[30] ISO/IEC. (2013). ISO/IEC 27001: *Information technology - Security techniques - Information security management systems – Requirements*. International Organization for Standardization.
[31] Prieto, E. (2023, enero 23). *¿Cuál es la historia de la Ciberseguridad?* Saint Leo University. Disponible en https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad.
[32] Anónimo. (2023, octubre 25). *Historia de internet*. Facultat d'Informàtica de Barcelona. Disponible en https://www.fib.upc.edu/retro-informatica/historia/internet.html.

establecer políticas de seguridad completas y proactivas. La adopción extendida de normativas de seguridad como ISO 27001: 2013 y el enfoque en la gestión de riesgos se volvieron pilares esenciales para preservar la integridad y disponibilidad de los datos en la infraestructura de red y telecomunicaciones.

En el presente, y ante el incremento de dispositivos conectados a la red y el nacimiento de amenazas complejas, las instituciones se enfrentan a desafíos para resguardar sus recursos de información, lo que convierte a la seguridad informática en una práctica necesaria para proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales[33], es así como las entidades tienen la obligación de salvaguardar la información para preservar la confianza de los clientes y cumplir con las regulaciones.

A nivel nacional, Colombia ha reconocido la importancia de la seguridad informática a medida que las infraestructuras digitales se desarrollan y las amenazas se diversifican. El gobierno colombiano, mediante políticas como la Estrategia Nacional de Ciberseguridad, ha impulsado la creación de marcos legales y normativos para mejorar la seguridad. Esta estrategia incluye la promoción de buenas prácticas en la protección de información sensible y el fortalecimiento de las capacidades ante ataques. Las instituciones colombianas, tanto públicas como privadas, deben adaptarse a estos lineamientos para garantizar la continuidad de sus operaciones y proteger los datos de los ciudadanos. Además, la implementación de metodologías como el análisis de riesgos se está expandiendo para evaluar de manera más profunda los riesgos a los que se enfrentan las organizaciones nacionales.

En el ámbito local, en el departamento del Cauca y específicamente en la ciudad de Popayán, las instituciones educativas y empresas están adoptando medidas para mejorar la seguridad informática y mitigar los riesgos asociados con el uso de tecnologías emergentes. La Institución de educación, como otras organizaciones en la región, se enfrenta a desafíos particulares debido al crecimiento de la digitalización y la interconexión de sus redes. El análisis de riesgos a nivel local se enfoca en identificar amenazas específicas para las infraestructuras tecnológicas que las instituciones utilizan. Metodologías como el análisis de riesgos cualitativo y cuantitativo se están aplicando para evaluar el impacto de las amenazas, lo que permite a las entidades implementar estrategias de mitigación adecuadas, adaptadas a las características locales del entorno y los recursos disponibles. Este enfoque asegura que, además de cumplir con normativas internacionales, se consideren las particularidades del contexto local en las estrategias de ciberseguridad.

---

[33] Amazon Web Services, Inc. (2023, octubre 25). *¿Qué es la ciberseguridad?* - Explicación de la ciberseguridad. AWS. Disponible en https://aws.amazon.com/es/what-is/cybersecurity/.

MARCO LEGAL

La protección de la infraestructura de red y telecomunicaciones en entornos educativos está sujeta a una serie de regulaciones y normativas legales que buscan salvaguardar la integridad, confidencialidad y disponibilidad de los datos. Estas leyes y estándares legales son fundamentales para garantizar el cumplimiento normativo y promover prácticas de seguridad efectivas en la gestión de la información.

En Colombia, la Ley 1581 de 2012, Ley de Protección de Datos Personales, establece los principios y las obligaciones que las organizaciones deben seguir para proteger la información personal de estudiantes, profesores y personal administrativo. Esta ley enfatiza la importancia de obtener consentimiento informado y garantizar la seguridad de los datos almacenados y transmitidos a través de la red.

La Resolución 20001 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, establece directrices específicas para la implementación de medidas de seguridad en la gestión de redes y telecomunicaciones. Esta resolución destaca la necesidad de proteger la infraestructura de red contra amenazas cibernéticas y establece requisitos para la implementación de firewalls, sistemas de detección de intrusos y controles de acceso.

A nivel internacional, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea tiene implicaciones significativas para las instituciones educativas que gestionan datos de ciudadanos europeos. El GDPR establece estándares estrictos para el procesamiento y la protección de datos personales, y exige la implementación de medidas de seguridad adecuadas para prevenir el acceso no autorizado y el uso indebido de la información.

Además, estándares internacionales como ISO 27001: 2013 y COBIT proporcionan directrices detalladas sobre la implementación de políticas de seguridad de la información y la gestión de riesgos en entornos educativos y organizacionales. Estos estándares legales y de cumplimiento son esenciales para garantizar la protección efectiva de la infraestructura de red y telecomunicaciones y promover una cultura de seguridad informática sólida en la institución.

MARCO CIENTÍFICO O TECNOLÓGICO

El progreso de la protección de la información en contextos educativos y organizacionales ha estado fuertemente vinculado al continuo avance de tecnologías y enfoques científicos innovadores. El panorama científico y tecnológico actual se apoya en una serie de principios y recursos esenciales que han demostrado ser cruciales en la defensa efectiva de la infraestructura de redes y

telecomunicaciones.

Con el incremento de la exposición en línea y las demandas de seguridad de Internet, la criptografía ha evolucionado en un campo diversificado. La aplicación de enfoques criptográficos modernos, como la codificación asimétrica y simétrica, ha tenido un papel central en la preservación de la confidencialidad de los datos enviados a través de redes. “Estas técnicas científicas avanzadas posibilitan la protección de la integridad de la información y aseguran la autenticación confiable de usuarios y dispositivos en la red”[34], según lo señalado por JEAN JACQUES, gerente de marketing de aplicaciones en Arrow Electronics.

Cómo se discute en la investigación de Anderson y Stoll, “el desarrollo de firewalls y sistemas de detección y prevención de intrusiones ha evolucionado significativamente”[35], Estos progresos tecnológicos han brindado a las entidades recursos eficaces para supervisar y gestionar el flujo de datos en las redes, detectar acciones perniciosas y evitar posibles ataques informáticos.

“La implementación de sistemas de gestión de eventos de seguridad (SIEM) ha demostrado ser crucial en la detección temprana y la respuesta a incidentes de seguridad”[36], Como se expresa en el estudio de Brown y Jones, dichos sistemas científicos y tecnológicos sofisticados permiten que las entidades recopilen y examinen datos de diversas fuentes en tiempo real, lo que posibilita una mayor comprensión de los modelos de tráfico y las conductas irregulares en la red.

“El uso de técnicas de virtualización y contenedores seguros ha ganado popularidad en entornos educativos y organizacionales”[37], como se señala en el estudio de Smith y Johnson, estas tecnologías posibilitan un manejo eficaz de los recursos, mientras crean un entorno protegido y seguro para la ejecución de aplicaciones y servicios cruciales de la red.

En términos generales, la base del marco científico y tecnológico actual radica en la aplicación de métodos avanzados de codificación, el progreso en sistemas de vigilancia y protección contra intrusiones, la integración de sistemas de manejo de eventos de seguridad y la utilización estratégica de técnicas de virtualización para asegurar la salvaguarda efectiva de la infraestructura de red y las telecomunicaciones en entornos educativos y empresariales.

---

[34] Jacques, J. (2016). *Detalles sobre la criptografía moderna*. Arrow. Disponible en https://www.arrow.com/es-mx/research-and-events/articles/modern-cryptography.
[35] Anderson, J., & Stoll, C. (2017). *Computer security: Principles and practice.*
[36] Brown, A., & Jones, B. (2019). *Journal of Information Security.*
[37] Smith, R., & Johnson, T. (2020). *International Journal of Network Security.*

DISEÑO METODOLÓGICO

La metodología de análisis de riesgos es un proceso fundamental para identificar, evaluar y mitigar los riesgos asociados con el uso de tecnologías de la información en las organizaciones. En este contexto, el análisis de riesgos se convierte en una herramienta estratégica para proteger los activos de información y asegurar la continuidad de las operaciones frente a posibles amenazas. Esta metodología se puede abordar desde diferentes enfoques, pero en este caso se optará por una combinación de métodos cualitativos y cuantitativos, lo que permite obtener una visión más completa y precisa de los riesgos involucrados.

La utilización de un enfoque cuantitativo en el análisis de riesgos se fundamenta en la necesidad de medir de manera objetiva los impactos potenciales de las amenazas, así como la probabilidad de que estas se materialicen. Este tipo de análisis proporciona un marco numérico que facilita la priorización de riesgos, permitiendo a las organizaciones asignar recursos de forma eficiente para mitigar aquellos riesgos que presentan un mayor impacto y probabilidad. Además, el enfoque cuantitativo permite obtener resultados más concretos, los cuales son fácilmente comunicables a las partes interesadas, como directivos o responsables de la toma de decisiones.

Por otro lado, el enfoque cualitativo complementa al cuantitativo al considerar aspectos más subjetivos que pueden no ser fácilmente medibles en términos numéricos. Factores como la reputación de la organización, el impacto en la moral de los empleados o las consecuencias sociales de un incidente de seguridad son elementos clave que, aunque difíciles de medir de manera exacta, deben ser evaluados. Esta aproximación proporciona una perspectiva más amplia, permitiendo capturar riesgos que podrían no ser identificados mediante un análisis exclusivamente numérico.

En conjunto, la combinación de ambos enfoques permite obtener un análisis de riesgos más equilibrado y adaptable, adecuado para abordar los desafíos de seguridad informática en un entorno cada vez más dinámico y complejo.

El enfoque de este proyecto está basado en la metodología de gestión de riesgos. Esta se centra en la identificación, evaluación y mitigación de riesgos en el ámbito de la seguridad informática. Algunas de las fases clave de esta metodología incluyen:

fase de preparación

Establecer los objetivos específicos del proyecto, incluyendo la identificación de amenazas y vulnerabilidades, y la propuesta de medidas de mitigación.

Reunir un equipo multidisciplinario que incluya expertos en seguridad informática, administradores de red y otros profesionales relevantes.

Recopilar documentación existente, como políticas de seguridad, inventario de activos de red y configuraciones de dispositivos.

Fase de evaluación de la infraestructura actual

La metodología seleccionada para la fase de evaluación de la infraestructura actual se basa en principios reconocidos y probados en la gestión de la seguridad informática. Esta metodología es adecuada debido a su enfoque sistemático y exhaustivo, lo cual es esencial para garantizar una evaluación completa y precisa de la infraestructura de red de la institución, en la sede San José. Al seguir los siguientes pasos, se puede asegurar que todos los aspectos críticos de la infraestructura de red sean evaluados de manera coherente y detallada, permitiendo identificar y mitigar posibles riesgos y vulnerabilidades. A continuación, se presentan los pasos requeridos para la fase de evaluación:

Identificar y documentar todos los activos de red, incluyendo hardware, software y datos críticos.

Revisar y analizar las configuraciones de red, incluyendo la configuración de dispositivos como switches, routers y controladoras Wifi.

Evaluar las políticas de seguridad informática existentes para determinar su efectividad y coherencia con los objetivos del proyecto.

Realizar pruebas de penetración controladas para identificar vulnerabilidades y debilidades en la infraestructura.

Fase de identificación de riesgos

Enumerar todas las amenazas potenciales que podrían afectar a la infraestructura de red, considerando amenazas internas y externas.

Identificar las vulnerabilidades específicas en la infraestructura que podrían ser explotadas por las amenazas identificadas.

Evaluar el impacto potencial de cada amenaza en términos de confidencialidad, integridad y disponibilidad de los servicios.

Fase de evaluación de riesgos

Establecer la probabilidad de que cada amenaza se materialice en un evento adverso.

Evaluar las consecuencias potenciales de cada evento adverso, considerando el impacto financiero, operativo y reputacional.

Calcular el riesgo para cada amenaza multiplicando la probabilidad por las consecuencias estimadas.

Fase de mitigación de riesgos

Proponer medidas específicas para mitigar los riesgos identificados. Esto puede incluir mejoras en políticas de seguridad, cambios en configuraciones de red, actualizaciones de software, y capacitación del personal.

1. ACTIVOS DE INFORMACIÓN QUE CONFORMAN LA INFRAESTRUCTURA DE RED

La INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN ha sido consciente de la importancia crítica de salvaguardar los activos de información. La recolección de estos para reforzar los sistemas de gestión e incrementar la protección a la integridad de las bases de datos se realizó a través de un cuidadoso proceso de levantamiento. Este esfuerzo estratégico, diseñado para identificar y evaluar en detalle los distintos tipos de datos y activos digitales que a su vez son críticos para la eficiente operación. Mediante este proceso, la Institución ha sentado las bases para la implementación de medidas de seguridad informática más robustas y la promoción de una cultura organizacional centrada en la protección y el manejo responsable de la información sensible.

1.1 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Para una correcta clasificación de los activos de información, es significativo tener presente la norma ISO 27001: 2013 ya que es un estándar internacionalmente reconocido que proporciona un marco para gestionar la seguridad de la información. Su aplicación garantiza que las organizaciones implementen un sistema de gestión de seguridad de la información (SGSI) robusto y efectivo, además la ISO 27001: 2013 es fundamental porque establece un enfoque sistemático ya que es la norma guía de las organizaciones en la identificación, evaluación y gestión de riesgos de seguridad de la información, asegurando que se apliquen controles adecuados para mitigar estos riesgos[38].

La ISO 27001: 2013 promueve la revisión y mejora constante de las políticas y procedimientos de seguridad, adaptándose a las nuevas amenazas y cambios en el entorno[39], lo que genera confianza y reputación, gracias a la certificación ISO 27001: 2013 se demuestra a clientes, socios y otras partes interesadas que la organización toma en serio la seguridad de la información, mejorando la confianza y la reputación de la entidad[40].

Por otro lado, las recomendaciones del MINTIC son fundamentales dentro del contexto colombiano, especialmente para la institución, ya que ofrecen pautas

[38] ISO. (2013). ISO/IEC 27001:2013 - *Information technology -- Security techniques -- Information security management systems -- Requirements*. International Organization for Standardization.
[39] ISO. (2013). ISO/IEC 27001:2013 - *Information technology -- Security techniques -- Information security management systems -- Requirements*. International Organization for Standardization.
[40] ISO. (2013). ISO/IEC 27001:2013 - *Information technology -- Security techniques -- Information security management systems -- Requirements*. International Organization for Standardization.

precisas que se alinean con la normativa y las necesidades locales. Al combinar estas recomendaciones con la ISO 27001: 2013, la universidad no solo asegura que la clasificación de sus activos de información cumpla con los más altos estándares internacionales, sino que también garantiza que estas prácticas estén en sintonía con las exigencias y particularidades del entorno regulatorio nacional. Esta integración es crucial para proteger adecuadamente los datos y asegurar la continuidad operativa, cumpliendo tanto con las expectativas globales como con las obligaciones legales locales.

Con el propósito de efectuar una clasificación óptima de los activos de información, se toman las directrices de la ISO 27001: 2013 y las recomendaciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), las cuales sugieren clasificar los activos "con base a tres elementos fundamentales: confidencialidad, integridad y disponibilidad"[41], como se detalla a continuación:

1.1.1 Clasificación de acuerdo a la confidencialidad

La confidencialidad implica que la información no esté accesible ni sea divulgada a personas, entidades o procesos no autorizados. La definición se ajusta a las particularidades de los activos gestionados por la universidad y consta de tres (4) niveles en consonancia con los tipos de información especificados en la Ley 1712 del 2014.

Tabla 1. Esquema de clasificación por confidencialidad

Tipo de información	Descripción
Información pública reservada	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
Información pública clasificada	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros

[41] MINTIC. (2016). *Guía para la gestión y clasificación de activos de información*. Ministerio de Tecnologías de la Información y Comunicaciones. https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf.

	sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
Información pública	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información pública reservada.

Fuente: MINTIC. Guía para la gestión y clasificación de activos de información

1.1.1.1. Proceso realizado en la institución para la clasificación de acuerdo a la confidencialidad

En la Institución de educación superior de Popayán, el proceso de clasificación de los activos de información basado en la confidencialidad se desarrolló de la siguiente manera:

Identificación de información sensible: Se llevó a cabo una identificación exhaustiva de toda la información gestionada por la institución, destacando aquellos datos que podrían tener un impacto significativo si fueran divulgados sin autorización.

Asignación de niveles de confidencialidad: Cada tipo de información fue clasificado según los siguientes niveles:

Información pública reservada: Información accesible solo para ciertos procesos de la entidad cuya divulgación no autorizada podría tener consecuencias legales, operativas, de reputación o económicas negativas.

Información pública clasificada: Información accesible a todos los procesos internos cuya divulgación no autorizada podría perjudicar los procesos de la institución.

Información pública: Información que puede ser divulgada sin restricciones, sin

riesgo de daño.

No clasificada: Activos de información que aún no han sido clasificados se tratan como información pública reservada.

Documentación y etiquetado: Todos los activos de información fueron documentados y etiquetados según su nivel de confidencialidad para asegurar un manejo adecuado.

1.1.2 Clasificación de acuerdo con la integridad

En la norma ISO 27000 se describe que “la integridad se refiere a la exactitud y completitud de la información”. Esto implica asegurarse de que la información no sea alterada de manera no autorizada o accidental, y que se mantenga precisa y completa a lo largo de su ciclo de vida. En la guía de MINTIC denominada “Guía para la gestión y clasificación de activos de información”, Se sugiere utilizar la siguiente estructura de clasificación en tres niveles:

Tabla 2. Esquema de clasificación por integridad

Clasificación	Descripción
A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: MINTIC. Guía para la gestión y clasificación de activos de información

1.1.2.1 Proceso realizado en la institución para la clasificación de acuerdo a la integridad

Para garantizar la integridad de los activos de información, se siguió el siguiente procedimiento:

Revisión de la información: Se realizó una revisión detallada de la exactitud y completitud de los datos, identificando posibles riesgos de alteración no autorizada.

Asignación de niveles de integridad: Se establecieron los siguientes niveles:

Alta (A): Información cuya alteración podría tener un impacto severo legal, económico, o de reputación.

Media (M): Información cuya alteración podría tener un impacto moderado.

Baja (B): Información cuya alteración tendría un impacto no significativo.

No clasificada: Activos de información no clasificados se tratan como de alta integridad.

Controles de integridad: Se implementaron controles específicos para mantener la integridad de la información, incluyendo procedimientos de auditoría y validación de datos.

1.1.3 Clasificación de acuerdo con la disponibilidad

La disponibilidad de la información implica que debe ser accesible y utilizable por una entidad o proceso autorizado cuando se necesite, tanto en el presente como en el futuro, junto con los recursos necesarios para su uso.

Aquí se muestra la siguiente estructura de clasificación de tres niveles:

Tabla 3. Esquema de clasificación por disponibilidad

CLASIFICACIÓN	DESCRIPCIÓN
1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus

	funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente*:* MINTIC. Guía para la gestión y clasificación de activos de información

1.1.3.1 Proceso realizado en la institución para la clasificación de acuerdo con la disponibilidad

El proceso de clasificación de la disponibilidad de los activos de información se llevó a cabo de la siguiente manera:

Evaluación de necesidades de acceso: Se evaluó la necesidad de acceso a la información en diferentes escenarios operativos, considerando tanto el presente como el futuro.

Asignación de niveles de disponibilidad: Se establecieron los siguientes niveles:

Alta (1): Información cuya indisponibilidad podría tener un impacto legal, económico, o de reputación severo.

Media (2): Información cuya indisponibilidad podría tener un impacto moderado.

Baja (3): Información cuya indisponibilidad afecta la operación normal sin implicaciones graves.

No clasificada: Activos no clasificados se tratan como de alta disponibilidad.

Implementación de medidas de disponibilidad: Se implementaron sistemas de respaldo y recuperación de datos, así como monitoreo constante para asegurar la disponibilidad continua de la información.

1.1.4 Etiquetado de activos de información

Para realizar el etiquetado de los activos de Información se toman las directrices sugeridas en la “Guía para la gestión y clasificación de activos de información de MINTIC”, el conjunto de directrices son las siguientes:

Se etiquetarán todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad[42].

Se etiquetará el nivel de clasificación con relación a Confidencialidad, Integridad y Disponibilidad[43].

Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA[44].

Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente diligenciar la clasificación de la siguiente forma: Clasificación Confidencialidad - Clasificación Integridad - Clasificación Disponibilidad[45].

Para los activos clasificados en confidencialidad como información pública reservada se podría utilizar la etiqueta IPR, información pública clasificada IPC e información pública, IPB[46].

Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B[47].

Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3[48].

1.1.4.1 Proceso realizado en la institución para etiquetado de activos de información

El etiquetado de los activos de información en la Institución de Educación Superior de Popayán se realizó conforme a las siguientes directrices, asegurando la identificación precisa y clara de cada activo:

Aplicación de etiquetas: Todos los activos de información fueron etiquetados con base en los esquemas de confidencialidad, integridad y disponibilidad.

Formatos de etiquetas: Se utilizaron formatos específicos para cada nivel de clasificación, asegurando que la información relevante sea visible y comprensible para los usuarios autorizados.

---

[42] Ibíd., p. 32
[43] Ibíd., p. 32
[44] Ibíd., p. 32
[45] Ibíd., p. 32
[46] Ibíd., p. 32
[47] Ibíd., p. 32
[48] Ibíd., p. 32

Confidencialidad: IPR para Información Pública Reservada, IPC para Información

Pública Clasificada, IPB para Información Pública.

Integridad: A para alta, M para media, B para baja.

Disponibilidad: 1 para alta, 2 para media, 3 para baja.

Manejo de información no etiquetada: Cualquier activo de información que no estuviera etiquetado se trató como no clasificado, siguiendo los niveles más altos de protección hasta que se completara su clasificación formal.

1.2 Metodología

1.2.1 Diseño de la investigación

En este estudio, se empleó una metodología mixta que combina técnicas cualitativas y cuantitativas para obtener una comprensión integral de los activos de información en la institución. La metodología se dividió en dos fases: la primera, centrada en la revisión de documentos y literatura existente sobre seguridad informática y gestión de activos de información; la segunda, en la recopilación de datos primarios a través de instrumentos específicos.

1.2.2 Instrumentos de recopilación de datos

1.2.2.1 Revisión documental

En la fase inicial, se llevó a cabo una revisión exhaustiva de documentos internos y externos, así como de literatura académica relacionada con la seguridad informática en entornos educativos. Esta revisión proporcionó una base sólida para comprender los conceptos clave y las mejores prácticas en la gestión de activos de información.

1.2.2.2 Entrevistas estructuradas

Se diseñó un conjunto de entrevistas estructuradas que se llevaron a cabo con personal clave de la institución, incluyendo responsables de tecnología, seguridad informática y administradores de sistemas. Las entrevistas se centraron en aspectos como la identificación de activos, políticas de seguridad, control de acceso y desafíos de seguridad específicos.

1.2.2.3 Cuestionario

Se desarrolló un cuestionario detallado dirigido a diferentes departamentos y niveles jerárquicos dentro de la institución. El cuestionario abarcó temas como la infraestructura de red y telecomunicaciones, hardware y software utilizados, políticas de seguridad percibidas y cualquier experiencia pasada con incidentes de seguridad.

1.2.2.4 Matriz análisis de riesgos

En el marco del desarrollo del presente trabajo de grado, se implementó una matriz de análisis de riesgos como herramienta fundamental para identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información. Esta matriz se diseñó bajo los lineamientos establecidos por la norma ISO 27001:2013, que proporciona un enfoque sistemático para la gestión de la seguridad de la información, y MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), que ofrece un marco metodológico para la evaluación de riesgos en entornos organizacionales.

La combinación de estos dos marcos normativos permite estructurar un proceso robusto y adaptado a las necesidades específicas del proyecto, asegurando una evaluación integral de los riesgos y la implementación de controles adecuados para mitigarlos.

El procedimiento para la utilización de la matriz de análisis de riesgos se llevó a cabo en varias etapas, las cuales se describen a continuación:

Como primer paso se realizó la definición del Alcance, donde se establecieron los límites del análisis, identificando los activos de información críticos, los procesos involucrados y los objetivos de seguridad que se buscaban proteger, posteriormente se realiza la identificación de activos y amenazas donde se realizó un inventario detallado de los activos de información, incluyendo hardware, software, datos y recursos humanos. Posteriormente, se identificaron las amenazas potenciales que podrían afectar a estos activos, considerando tanto fuentes internas como externas.

Como tercer paso se realizó la evaluación de vulnerabilidades en la cual se analizaron las vulnerabilidades asociadas a cada activo, considerando factores como la exposición, la probabilidad de ocurrencia y el impacto potencial. Este análisis permitió priorizar los riesgos en función de su criticidad. Terminada la evaluación de vulnerabilidades se desarrolló el cálculo del nivel de riesgo utilizando la metodología MAGERIT, este cálculo se realiza para cada combinación de activo, amenaza y vulnerabilidad y se basó en la estimación de la probabilidad de ocurrencia y el impacto potencial, asignando valores cuantitativos o cualitativos según correspondiera.

Por último, se realizó el plan de tratamiento por medio de la selección de controles con base en los resultados de la evaluación, se seleccionaron los controles de seguridad más adecuados para mitigar los riesgos identificados. Estos controles se alinearon con los requisitos de la ISO 27001:2013, asegurando su efectividad y conformidad con estándares internacionales.

La matriz de análisis de riesgos no solo sirvió como una herramienta de evaluación, sino también como un componente integral de la metodología del trabajo. Su aplicación permitió estructurar el proceso de investigación, proporcionando una base sólida para la toma de decisiones y la formulación de recomendaciones. Además, la integración de la ISO 27001:2013 y MAGERIT aseguró que el análisis fuera tanto riguroso como adaptable a las particularidades del proyecto.

1.2.2.4 Procedimiento

La implementación de la metodología se desarrolló en tres fases: preparación, recopilación de datos y análisis. En la preparación, se obtuvo la aprobación de la institución, se definieron objetivos y se realizó una revisión documental alineada con la ISO 27001:2013 y MAGERIT.

La recopilación de datos incluyó entrevistas semiestructuradas y la distribución de un cuestionario validado para identificar riesgos y vulnerabilidades. El análisis combinó técnicas cualitativas (análisis de contenido) y cuantitativas (herramientas estadísticas) para evaluar los activos de información. Este enfoque permitió una comprensión integral de la seguridad de la información, contrastando perspectivas y validando hallazgos. Los resultados se documentaron en un informe que sirvió de base para recomendaciones específicas, como la implementación de controles, mejora de políticas y capacitación del personal, fortaleciendo así la gestión de riesgos en la institución.

1.3 Levantamiento de activos de información

Reconociendo la importancia crítica de salvaguardar los activos de información y con el objetivo de fortalecer los sistemas de gestión y mejorar la protección de la integridad de los datos, se llevó a cabo un meticuloso proceso de levantamiento de activos de información. Este esfuerzo estratégico se ha centrado en identificar y clasificar de manera exhaustiva los distintos tipos de datos y recursos digitales que son vitales para el funcionamiento efectivo de la institución. Por lo cual, para la evaluación de la infraestructura actual, se ha seguido un enfoque sistemático basado en la metodología MAGERIT y la norma ISO 27001: 2013. Esta evaluación se centra en identificar y documentar todos los activos de información críticos.

Es importante mencionar que la implementación de la metodología MAGERIT, nos proporciona un marco detallado y sistemático para la gestión de riesgos, lo que permite una evaluación exhaustiva y precisa de la seguridad de la información, además de una alineación con la norma ISO 27001: 2013, lo que facilita la integración y cumplimiento de estándares internacionales de seguridad, permitiéndole ser adaptable a diferentes tipos de organizaciones y tamaños, lo que permite personalizar la evaluación de riesgos según las necesidades específicas de la institución.

1.3.1 Implementación de la Metodología MAGERIT

Identificación de activos: Se han catalogado todos los activos de información, incluyendo hardware, software y datos críticos, creando un inventario detallado que abarca todos los componentes esenciales.

Evaluación de amenazas: Se han identificado y documentado las posibles amenazas que podrían afectar a cada activo, considerando tanto amenazas internas como externas.

Análisis de vulnerabilidades: Se ha realizado un análisis exhaustivo de las vulnerabilidades presentes en la infraestructura, evaluando tanto las debilidades técnicas como las humanas que podrían ser explotadas.

Evaluación del impacto: Se ha evaluado el impacto potencial de cada amenaza sobre los activos, determinando la gravedad de las consecuencias en caso de que se materialicen los riesgos.

Priorización de riesgos: Los riesgos identificados han sido priorizados en función de su probabilidad de ocurrencia y el impacto potencial, permitiendo enfocar los esfuerzos de mitigación en los riesgos más críticos.

Definición de medidas preventivas y correctivas: Se ha desarrollado un plan de acción para mitigar los riesgos, estableciendo controles y procedimientos adecuados para prevenir incidentes de seguridad y corregir vulnerabilidades detectadas.

1.3.1.1 Clasificación de los activos de información

Dentro del proceso de clasificación de los activos de información es indispensable iniciar con la identificación inicial, la cual se presenta a continuación:

Tabla 4. Información inicial para la identificación de activos de información

Objetivo	Analizar los riesgos de seguridad informática en la institución de educación superior de Popayán sede San José
Alcance	Aplica para los activos de la institución de educación superior de Popayán sede San José
Nombre de la entidad	INSTITUCIÓN DE EDUCACIÓN SUPERIOR POPAYÁN
Actividad Comercial	Prestación de servicios relacionados con la educación
Contexto legal	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
Enfoque metodológico	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**

Fuente: Autoría Propia

1.3.1.2 Identificación de los roles y las responsabilidades del propietario y/o custodio del activo de información.

La Guía 4 de MINTIC establece un marco claro para la gestión de la seguridad de la información en las organizaciones, detallando los roles y responsabilidades de los diferentes actores involucrados, especialmente del propietario y el custodio del activo de información. Según esta guía, el propietario del activo es responsable de definir su clasificación, establecer las políticas de acceso, uso y protección de la información, y asegurarse de que se cumplan las normativas relacionadas. Por otro lado, el custodio se encarga de implementar las medidas técnicas y operativas para proteger el activo, garantizar su integridad y disponibilidad, y asegurar que se realicen copias de seguridad y auditorías regulares. Ambos roles deben trabajar de manera colaborativa para proteger los activos de información, cumpliendo con los principios de seguridad establecidos por la Guía 4 y otras normativas vigentes[49].

En la siguiente tabla se presentan los actores involucrados con los activos de información.

49 Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). (2016). *Guía 4: Roles y responsabilidades*. Recuperado de https://gobiernodigital.mintic.gov.co/692/articles-5482_G4_Roles_responsabilidades.pdf.

Tabla 5. Actores involucrados

Nombres	Dependencia	Funciones
Director-GSI	GEERENCIA DE SISTEMAS DE INFORMACION	Coordinar la implementación de sistemas informáticos, garantizar la seguridad de la información, gestionar la mejora continua de los procesos tecnológicos de información y mantener la comunicación con otras áreas sobre necesidades.
Desarrollador-GSI	GEERENCIA DE SISTEMAS DE INFORMACION	Desarrollar, implementar y mantener aplicaciones y sistemas informáticos, realizar pruebas de software, asegurar la funcionalidad de los sistemas de información, realizar actualizaciones y optimizaciones de aplicaciones y proporcionar soporte técnico.
Director-GTI	GERENCIA DE TECNOLOGIAS DE LA INFORMACION	Definir y gestionar la estrategia de tecnología de la institución, supervisar proyectos de infraestructura tecnológica, garantizar la seguridad y disponibilidad de los sistemas informáticos, gestionar presupuestos y recursos tecnológicos, y coordinar equipos de trabajo en el área tecnológica.
Profesional de virtualización y redes-GTI	GERENCIA DE TECNOLOGIAS DE LA INFORMACION	Gestionar y mantener la infraestructura de redes y servidores, administrar entornos virtualizados, asegurar la disponibilidad de las redes internas y externas, realizar configuraciones y optimizaciones en sistemas de red, y proporcionar soporte técnico en temas de redes y virtualización.

Auxiliar de soporte-GTI	GERENCIA DE TECNOLOGIAS DE LA INFORMACION	Proporcionar soporte técnico a usuarios, gestionar incidencias tecnológicas, mantener equipos de cómputo en buen estado, asegurar el funcionamiento de hardware y software, instalar y configurar equipos y sistemas, y asistir en la implementación de nuevas tecnologías.
Director-GTH	GESTION DEL TALENTO HUMANO	Coordinar la gestión de recursos humanos, supervisar procesos de contratación, formación y desarrollo, gestionar la nómina y bienestar del personal, implementar políticas de recursos humanos, y promover el desarrollo organizacional.
Director-Comunicaciones	COMUNICACIONES INSTITUCIONALES	Desarrollar e implementar la estrategia de comunicación interna y externa, gestionar la imagen institucional, coordinar campañas de comunicación, supervisar el uso de medios digitales y redes sociales, y asegurar la correcta comunicación entre la comunidad educativa y los stakeholders externos.
Director-Calidad	ASEGURAMIENTO DE LA CALIDAD	Supervisar los procesos de calidad dentro de la institución, asegurar el cumplimiento de normativas y estándares, gestionar auditorías internas, coordinar la implementación de planes de mejora, y asegurar la calidad en los servicios educativos y administrativos.

Director-Investigación	INVESTIGACION	Coordinar y promover actividades de investigación en la institución, gestionar proyectos de investigación, buscar fuentes de financiamiento para investigaciones, asesorar a investigadores y estudiantes en proyectos, y promover la innovación y transferencia de conocimiento.
Tesorero	TESORERIA	Gestionar los recursos financieros de la institución, supervisar la elaboración de presupuestos, coordinar pagos y cobros, gestionar la tesorería y fondos de la institución, asegurar la correcta gestión de flujos de caja, y preparar informes financieros.

Fuente: Autoría Propia

Una vez realizado el levantamiento de activos de información, utilizando la metodología MAGERIT, se ha procedido a la clasificación de los activos, lo que ha permitido establecer una estructura organizada para su gestión y protección. Este proceso ha involucrado no solo la identificación de los activos críticos para la organización, sino también la definición de los roles y responsabilidades de los propietarios y custodios de cada activo de información. A continuación, se presenta una tabla que detalla el levantamiento de estos activos, proporcionando una herramienta clara para la gestión continua y la mejora de las políticas de seguridad de la información.

A continuación, se presenta la tabla de levantamiento de información de activos según metodología MAGERIT y norma ISO 27001:2013.

Tabla 6. Inventario de activos de información

No.	DATOS DEL ACTIVO DE INFORMACION			
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo	Descripción
1	Servidor base de datos institucional	Director-GSI	SERVICIOS	Sistema de gestión de datos de manera eficiente y segura, permite almacenar, organizar y recuperar la información contenida en sus tablas.
2	Servidor base de datos Software Gestión Comercial	Director-GTI	SERVICIOS	La base de datos del Software gestión comercial almacena y organiza la información estructurada (como registros financieros, inventarios, clientes, productos, etc.).
3	Servidor base de datos Software Gestión Comercial (Modulo de contabilidad, tesorería, pagos, activos)	Tesorero	SERVICIOS	Sistema de gestión empresarial (ERP), es una solución que integra diversas funcionalidades para la administración de procesos empresariales, como finanzas, inventarios, recursos humanos, compras, ventas, entre otros.
4	Servidor de aplicaciones	Director-GSI	SERVICIOS	Entorno para ejecutar aplicaciones de manera centralizada. Este tipo de servidor es responsable de la gestión y ejecución de las aplicaciones web
5	Servidor de dominio Administrativos	Profesional de virtualización y redes-GTI	SERVICIOS	Servidor que administra y controla el acceso a los recursos de una red dentro del dominio administrativos
6	Servidor de dominio	Profesional de virtualización y redes-GTI	SERVICIOS	Servidor que administra y controla el acceso a los recursos de una red dentro

	estudiantes y docentes			del dominio de docentes y estudiantes
7	Servidor DHCP	Director-GTI	SERVICIOS	Asigna de manera automática direcciones IP y otros parámetros de red a dispositivos.
8	Router (Core)	Profesional de virtualización y redes-GTI	HARDWARE	Se encarga de gestionar el tráfico principal dentro de una red, tomando decisiones de enrutamiento rápidas y eficientes para garantizar la conectividad de todo el sistema de red.
9	Firewall	Profesional de virtualización y redes-GTI	HARDWARE	Herramienta de seguridad que actúa como una barrera de protección entre una red interna y una red externa, controlando y monitoreando sistemas y redes de accesos no autorizados, ataques y otras amenazas externas.
10	Software Administrativos	Director-GSI	SOFTWARE	Sistema de Información de Registro Estudiantil para personal de registro académico.
11	Software Estudiantes	Director-GSI	SOFTWARE	Sistema de Información de Registro Estudiantil para estudiantes.
12	Software Docentes	Director-GSI	SOFTWARE	Sistema de Información de Registro Estudiantil para personal de docentes.
13	Software Admisiones	Director-GSI	SOFTWARE	Sistema de Información de Registro Estudiantil para personal de mercadeo y admisiones.
14	Página web calidad	Director-Calidad	SOFTWARE	Micrositio web donde reposa toda la información, formatos y documentación, referentes

				al Sistema de Gestión de la Calidad
15	Repositorio institucional	Director-Investigación	SOFTWARE	Plataforma digital en la que la institución almacena, organiza, preserva y distribuye su producción académica, científica y/o institucional.
16	Página Web	Director-Comunicaciones	SOFTWARE	Sitio web oficial creado para proporcionar información relevante sobre las actividades, servicios, misión, visión, valores y otros aspectos importantes.

Fuente: Autoría Propia

Para garantizar una gestión eficiente y segura de los activos de información, se realiza un inventario detallado que incluye todos los recursos críticos para la organización. El inventario se presenta en forma de matriz de activos (Ver el anexo C), lo que permite una visualización estructurada de los diferentes tipos de activos, su clasificación y la importancia de cada activo. Las siguientes tablas resumen la matriz de inventario de activos de información y brindan una base sólida para la toma de decisiones estratégicas relacionadas con la protección, control y optimización de estos activos de acuerdo con las políticas de seguridad establecidas.

Tabla 7. Clasificación general y número de activos

Tipo de activo	**Cantidad**
Tipo Dato	0
Tipo Claves Criptográficas	0
Tipo Servicio	7
Tipo Software	7
Tipo Hardware	2
Tipo Comunicaciones	0
Tipo Soporte de Información	0
Tipo Equipamiento Auxiliar	0
Tipo Instalaciones	0

Tipo Personal	0
Total	**16**

Fuente: Autoría Propia

Tabla 8. Clasificación de activos según su valor

Número de activos de clientes o terceros que deben protegerse	8
Activos de información que deben ser restringidos a un número limitado de empleados	16
Número de activos de información que deben ser restringidos a personas externas	10
Activos de información que pueden ser alterados o comprometidos para fraudes o corrupción	16
Número de activos de información que son muy críticos para las operaciones internas	16
Número de activos de información que son muy críticos para el servicio hacia terceros	16

Fuente*:* Autoría Propia

Tabla 9. Clasificación según impacto a la seguridad

Leve	3
Importante	2
Grave	11

Fuente*:* Autoría Propia

Tabla 10. Resumen de nivel de riesgo en los activos

Extremo	0
Alto	15
Medio	1
Bajo	0

Fuente: Autoría Propia

Tabla 11. Ubicación de los activos

Física	6
Electrónica	10

Fuente*:* Autoría Propia

Con el levantamiento de activos de información en la institución, se ha logrado obtener una visión detallada y actualizada de la infraestructura de red y telecomunicaciones. Este proceso exhaustivo no solo proporcionó un inventario preciso de los activos involucrados, si también ha permitido identificar aspectos cruciales para más adelante fortalecer la seguridad de la información en la institución. La colaboración y el compromiso de los equipos involucrados han sido fundamentales para el éxito de esta fase, sentando las bases para futuras estrategias de protección y gestión efectiva de los recursos tecnológicos. La información recopilada se erige como un valioso activo para la toma de decisiones informadas, respaldando la seguridad y continuidad de los servicios telemáticos.

2. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES A PARTIR DEL RIESGO EN LA INFRAESTRUCTURA DE RED Y TELECOMUNICACIONES DE LA INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN

Este capítulo se centra en un aspecto fundamental de la seguridad informática: la identificación de amenazas y vulnerabilidades dentro de la infraestructura de red y telecomunicaciones de la institución de educación superior de Popayán a partir del riesgo. Este proceso resulta esencial para salvaguardar los activos de información de la institución ante posibles riesgos, tales como ataques cibernéticos o fallas técnicas que puedan comprometer su operatividad. A través de una serie de pasos metodológicos, se busca identificar y evaluar tanto las amenazas, entendidas como los factores externos que podrían causar daño, como las vulnerabilidades, que son debilidades dentro de los sistemas susceptibles de ser explotadas.

Para abordar la identificación de amenazas y vulnerabilidades por lo general se emplean diversas normativas y marcos de referencia internacionales que brindan un enfoque estructurado para la gestión de riesgos en la seguridad de la información. En particular, las normas ISO/IEC 27001 y ISO/IEC 27005 las cuales proporcionan un enfoque robusto para la gestión de la seguridad de la información y la evaluación de riesgos, permitiendo a la organización identificar, analizar y tratar los riesgos de manera eficiente. Además, se hace uso la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), que es un enfoque estructurado para la evaluación y gestión de los riesgos en los sistemas de información. Desarrollada en España por el Instituto Nacional de Tecnologías de la Información (INTECO), MAGERIT está diseñada para ser aplicada en el ámbito de la gestión de la seguridad de la información, permitiendo a las organizaciones identificar, evaluar y tratar los riesgos relacionados con sus activos de información.

En este contexto, el del desarrollo del presente objetivo busca tener un plan de pruebas basado en metodologías que permitan identificar, analizar y comprender las amenazas y vulnerabilidades potenciales que podrían afectar la integridad y disponibilidad de los activos de información.

2.1 IDENTIFICACIÓN DE VULNERABILIDADES

Una vulnerabilidad es una debilidad o falla en un sistema, proceso o control que una amenaza puede aprovechar para causar daño. Durante esta fase, MAGERIT ayuda a identificar qué aspectos de la infraestructura tecnológica, las personas y los procesos tienen debilidades que pueden ser aprovechadas por las amenazas identificadas.

Aunque el proceso de identificación de vulnerabilidades en MAGERIT se desarrolla mediante la implementación de varias técnicas como el análisis de la infraestructura tecnológica, la revisión de los controles y procedimientos de seguridad, evaluación de la capacitación y concienciación del personal, detección de deficiencias operacionales y de procesos, y por último el uso de herramientas de escaneo de vulnerabilidades, para el desarrollo de este este punto se prioriza el uso de esta ultima la técnica para la identificación de vulnerabilidades en los activos de información por medio de herramientas especializadas.

2.1.1 Análisis de la infraestructura tecnológica

El proceso inicia con una revisión de los activos de información de tipo hardware, software y las redes para identificar problemas de configuración, errores en los controles de acceso, deficiencias en la seguridad del sistema operativo o aplicaciones que podrían ser explotadas por atacantes.

2.1.2 Revisión de los controles y procedimientos de seguridad

En la revisión de controles y procedimientos de seguridad se realiza una verificación de las políticas de seguridad existentes, las prácticas de administración de contraseñas, la capacitación del personal en ciberseguridad, el uso de tecnología de seguridad (Firewalls, antivirus, etc.) y otros controles internos. Las vulnerabilidades pueden incluir una mala configuración, falta de actualizaciones de seguridad o controles de acceso insuficientes.

2.1.3 Evaluación de la capacitación y concienciación del personal

Los factores humanos son una fuente importante de vulnerabilidad. Estos incluyen la falta de capacitación en seguridad o el manejo descuidado de información confidencial. En este caso, la vulnerabilidad no es técnica sino organizativa.

2.1.4 Detección de deficiencias operacionales y de procesos

La falta de protocolos de respuesta a incidentes, fallos en la gestión de cambios, o en la auditoría y monitoreo de actividades pueden constituir vulnerabilidades

críticas.

2.1.5 Uso de herramientas de escaneo de vulnerabilidades

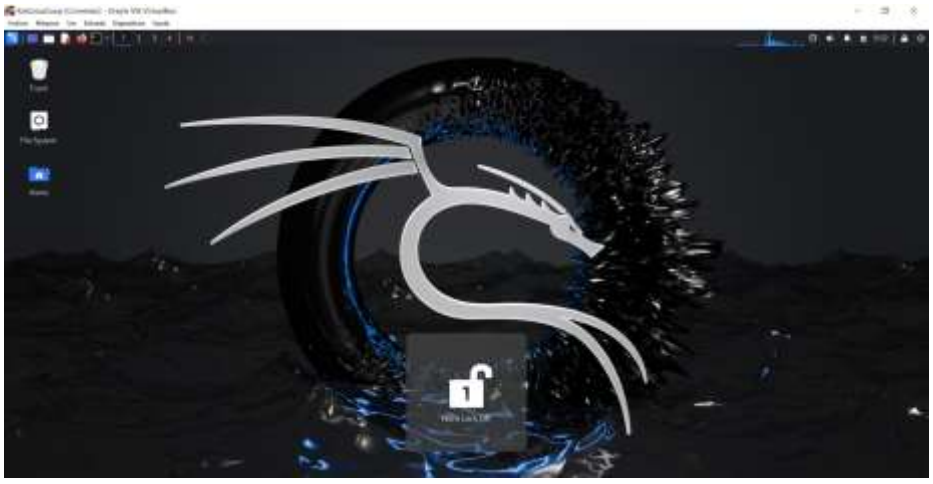
Para el escaneo de vulnerabilidades se emplearon herramientas automáticas de escaneo de vulnerabilidades, las cuales ayudaron a detectar posibles debilidades en los activos de información. A continuación, se presentan las herramientas utilizadas.

2.1.5.1 Kali Linux

Distribución de sistema operativo basada en Debían diseñada para pruebas de penetración, auditoría de seguridad y análisis forense digital. Con el paso de los años, se ha convertido en una de las herramientas más populares y completas de la comunidad de la ciberseguridad. Kali Linux es una plataforma potente y flexible diseñada para profesionales de la seguridad informática, piratas informáticos éticos y analistas de vulnerabilidades.

Una de las características clave de Kali Linux es su amplia colección de herramientas preinstaladas para todo, desde escaneo y explotación de vulnerabilidades de red hasta análisis de tráfico de red e ingeniería inversa. Estas herramientas incluyen utilidades como Metasploit, Wireshark, Nmap, Burp Suite y más, que le permiten realizar de todo, desde pruebas de penetración hasta investigaciones avanzadas de su red y entorno de sistema.

Figura 1. Entorno de la distribución Kali Linux



Fuente: Autoría Propia

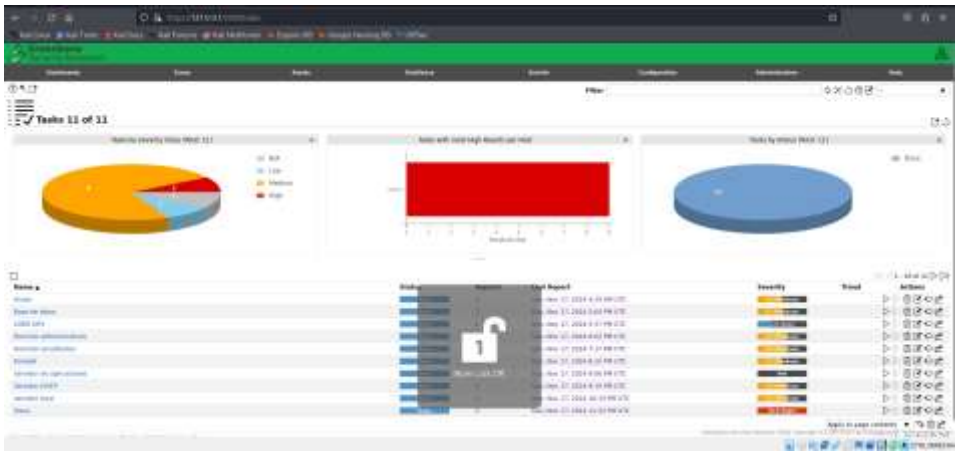
2.1.5.2 Greenbone Security Assistant (GSA)

Herramienta potente que ayuda a analizar y gestionar vulnerabilidades en sistemas y redes. Forma parte del conjunto de soluciones de Greenbone Networks que se especializa en herramientas de análisis de seguridad basadas en la plataforma OpenVAS (Open Vulnerability Assessment System). GSA proporciona una interfaz gráfica que permite administrar de manera eficiente análisis de seguridad, analizar resultados y generar informes detallados sobre posibles vulnerabilidades en los sistemas informáticos.

Una de las principales ventajas es su interfaz web intuitiva, que facilita la configuración y el uso del escaneo de vulnerabilidades sin conocimientos técnicos profundos. Esto lo hace accesible tanto para los profesionales de la seguridad como para los administradores de sistemas que desean evaluar la postura de seguridad de su infraestructura tecnológica. GSA le permite realizar una amplia gama de análisis, Desde detectar vulnerabilidades en aplicaciones web hasta evaluar la seguridad de redes y dispositivos conectados.

El proceso de análisis de GSA se basa en el uso de cámaras de escaneo (escáneres) para comprobar los sistemas y redes en busca de posibles debilidades, como errores de configuración, software obsoleto, fallas de seguridad conocidas y otras vulnerabilidades. Estos análisis se basan en una extensa base de datos CVE (vulnerabilidades y exposiciones comunes) y otros recursos que detectan vulnerabilidades con alta precisión. Además, GSA admite múltiples protocolos y tecnologías, incluidos SNMP, HTTP, SSH y más, lo que le permite cubrir una amplia gama de dispositivos y servicios.

Figura 2. Entorno de Greenbone Security Assistant (GSA).



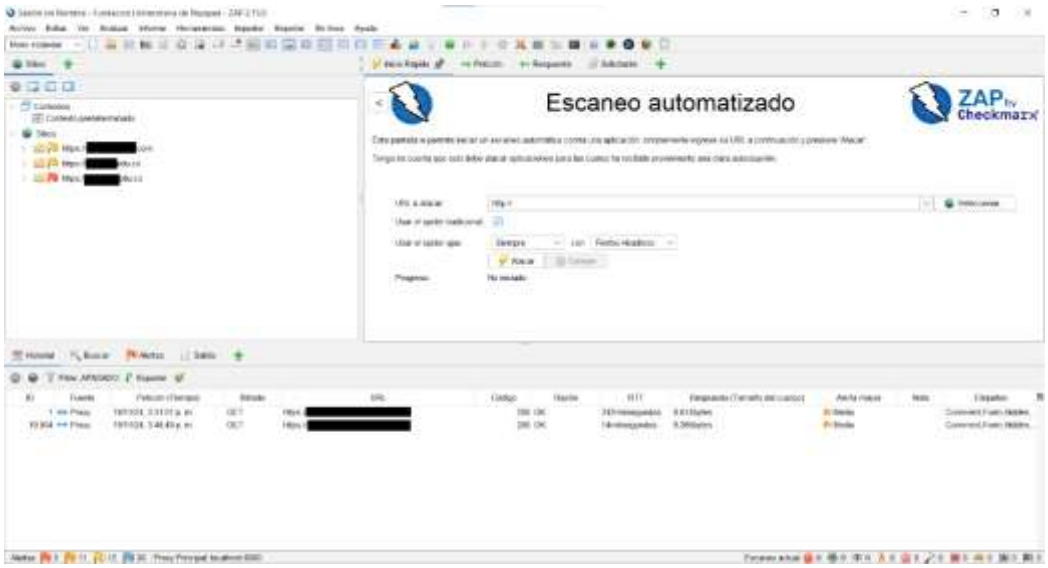
Fuente*:* Autoría Propia

2.1.5.3 ZAP (Zed Attack Proxy)

Herramienta de código abierto diseñada para realizar pruebas de penetración y auditorías de seguridad de aplicaciones web. Desarrollado por OWASP (Open Web Application Security Project), ZAP es una de las herramientas más populares y accesibles para identificar vulnerabilidades de seguridad en aplicaciones web. ZAP 2.15.0 para Windows incluye mejoras de funcionalidad, estabilidad y rendimiento, lo que la convierte en una opción sólida para las pruebas de penetración.

Una de las principales ventajas de ZAP es su interfaz gráfica intuitiva y sencilla que se puede utilizar sin configuraciones complejas. Permite realizar análisis de seguridad en aplicaciones web y obtener información detallada sobre posibles vulnerabilidades, como inyección SQL, secuencias de comandos entre sitios (XSS), problemas de autenticación y más.

Figura 3. Entorno de ZAP (Zed Attack Proxy).



Fuente*:* Autoría Propia

2.2 EVALUACIÓN DE VULNERABILIDADES

Este es un paso fundamental en la evaluación de riesgos en el enfoque MAGERIT, ya que su principal objetivo es descubrir debilidades en los activos de información que las amenazas puedan explotar. Una vulnerabilidad se define como cualquier debilidad o error en un sistema, proceso o control de seguridad que podría resultar en una amenaza que podría comprometer o alterar la integridad de un activo de información. Este proceso de identificación es fundamental para comprender el alcance de la exposición de un activo a posibles ataques,

de modo que se puedan tomar acciones correctivas antes de que se explote la vulnerabilidad.

El proceso de identificación de vulnerabilidades implica un análisis exhaustivo de los activos de información identificados en la fase previa de análisis de riesgos. El análisis cubre una revisión detallada de varios componentes clave del sistema de información, como configuraciones de hardware y software, procedimientos operativos y controles de seguridad existentes. Las vulnerabilidades pueden estar relacionadas con aspectos técnicos (como errores de configuración, falta de actualizaciones o parches, fallas de seguridad del software) y aspectos procedimentales (como falta de reglas de acceso adecuadas o procesos mal definidos).

2.1.2 Planificación de actividades

MAGERIT proporciona una planificación estructurada para identificar vulnerabilidades como parte del proceso de gestión de riesgos. La planificación es realizada de una manera ordenada y exhaustiva, asegurando que todos los aspectos relevantes del entorno técnico y operativo de la institución estén cubiertos.

Aunque MAGERIT no prescribe una lista de actividades específicas o una planificación detallada paso a paso de cada actividad para una organización, se utiliza un enfoque general para los métodos de identificación de vulnerabilidades, este incluye las siguientes actividades clave:

Tabla 12. Actividades en la planificación de la identificación de vulnerabilidades según MAGERIT.

Actividad	Descripción	Objetivo
Definir el alcance de la evaluación	Determinar los activos de información a evaluar, incluyendo hardware, software, redes y procesos.	Establecer claramente qué sistemas y activos serán objeto de la evaluación de vulnerabilidades.
establecer el contexto y el marco de seguridad	Definir las políticas y controles de seguridad actuales de la organización, además de cualquier norma o marco relevante (por ejemplo, ISO/IEC 27001).	Asegurar que la identificación de vulnerabilidades esté alineada con las políticas de seguridad y las normativas vigentes.
Identificación de activos críticos	Enumerar y clasificar los activos de información más importantes para la	Identificar los activos clave para enfocarse en aquellos que son más sensibles y

	organización, que requieren especial atención.	cruciales para la organización.
Análisis de amenazas y contexto operativo	Analizar las amenazas potenciales que pueden afectar a los activos identificados, como ciberataques, desastres naturales, etc.	Comprender las posibles amenazas que podrían explotar las vulnerabilidades y cómo se vinculan a los activos.
Selección de métodos y herramientas para identificar vulnerabilidades	Determinar las técnicas y herramientas a utilizar, como auditorías de seguridad, escaneos de vulnerabilidades, pruebas de penetración, etc.	Escoger las herramientas y métodos más adecuados para realizar una evaluación efectiva y exhaustiva.
recolección de información	Recolectar datos sobre los sistemas, configuraciones y aplicaciones mediante herramientas de escaneo o auditorías manuales.	Obtener información detallada sobre los activos y sus configuraciones para evaluar sus debilidades.
Realización de Evaluaciones Técnicas	Llevar a cabo evaluaciones técnicas utilizando escaneos de vulnerabilidades, pruebas de penetración y revisiones de código.	Identificar debilidades técnicas que puedan ser explotadas, como configuraciones incorrectas, software desactualizado, etc.
análisis de resultados y documentación	Analizar los resultados obtenidos de las pruebas y escaneos realizados, documentando las vulnerabilidades encontradas.	Crear un informe detallado que resuma las vulnerabilidades detectadas, clasificadas por nivel de riesgo.
Priorización de vulnerabilidades	Evaluar y clasificar las vulnerabilidades según su gravedad y el impacto potencial que podrían tener sobre la organización.	Determinar cuáles vulnerabilidades deben ser tratadas con mayor urgencia, según el nivel de riesgo asociado.
Planificación de tratamiento de vulnerabilidades	Desarrollar planes para corregir o mitigar las vulnerabilidades identificadas, mediante parches, mejoras en procesos o controles de seguridad.	Implementar soluciones para mitigar o eliminar las vulnerabilidades, minimizando el riesgo de explotación.

Fuente: Autoría Propia

2.1.3 Métodos para identificar vulnerabilidades según la metodología MAGERIT

El enfoque MAGERIT aborda este proceso de manera estructurada y detallada, proporcionando una variedad de métodos para identificar vulnerabilidades de manera precisa y efectiva. MAGERIT, como sistema de evaluación de riesgos, enfatiza la importancia de un análisis integral de los activos de información utilizando una variedad de herramientas y métodos, desde revisiones de configuración hasta auditorías de seguridad y pruebas de penetración. MAGERIT utiliza técnicas como el escaneo de vulnerabilidades, el análisis del código fuente y la auditoría no solo para identificar los problemas existentes sino también para priorizarlos en función de su potencial impacto. Esto facilita la toma de decisiones y la implementación de acciones correctivas. En este contexto, MAGERIT ofrece un enfoque que va más allá de identificar vulnerabilidades, sino que también proporciona la base para una planificación eficaz de su mitigación y tratamiento.

A continuación, se presenta una tabla que describe los métodos para identificar vulnerabilidades según la metodología MAGERIT:

Tabla 13. Métodos para identificar vulnerabilidades según la metodología MAGERIT.

Método	Descripción	Objetivo
Revisión de la Configuración de Sistemas (Hardware/Software)	Análisis detallado de las configuraciones del sistema informático tanto a nivel de hardware como de software. Esto incluye verificar si hay configuraciones incorrectas o inseguras.	Detectar configuraciones erróneas que puedan generar vulnerabilidades explotables por amenazas.
Auditorías de Seguridad	Análisis integral de las medidas y políticas de seguridad implementadas en la organización. Puede ser interno o externo.	Identificar fallos o debilidades en los controles de seguridad que puedan ser explotados.
Escaneos de Vulnerabilidades	Uso de herramientas especializadas, como Nessus o OpenVAS, para realizar escaneos automáticos en los sistemas en busca de vulnerabilidades conocidas.	Detectar vulnerabilidades conocidas y configuraciones inseguras mediante el uso de herramientas automatizadas.
Revisión de Código Fuente (en el caso de aplicaciones)	Inspeccione manual o automática del código fuente de una aplicación	Identificar errores de seguridad en el código que pueden ser

	nativa o aplicación web en busca de fallas de seguridad.	explotados, como inyecciones SQL o XSS.
Pruebas de Penetración (Pen Testing)	Simulación controlada de ciberataques reales para evaluar la seguridad del sistema. Los expertos intentan explotar las vulnerabilidades de forma controlada.	Detectar vulnerabilidades que no pueden ser encontradas fácilmente mediante escaneos o auditorías, simulando ataques reales.

Fuente: Autoría Propia

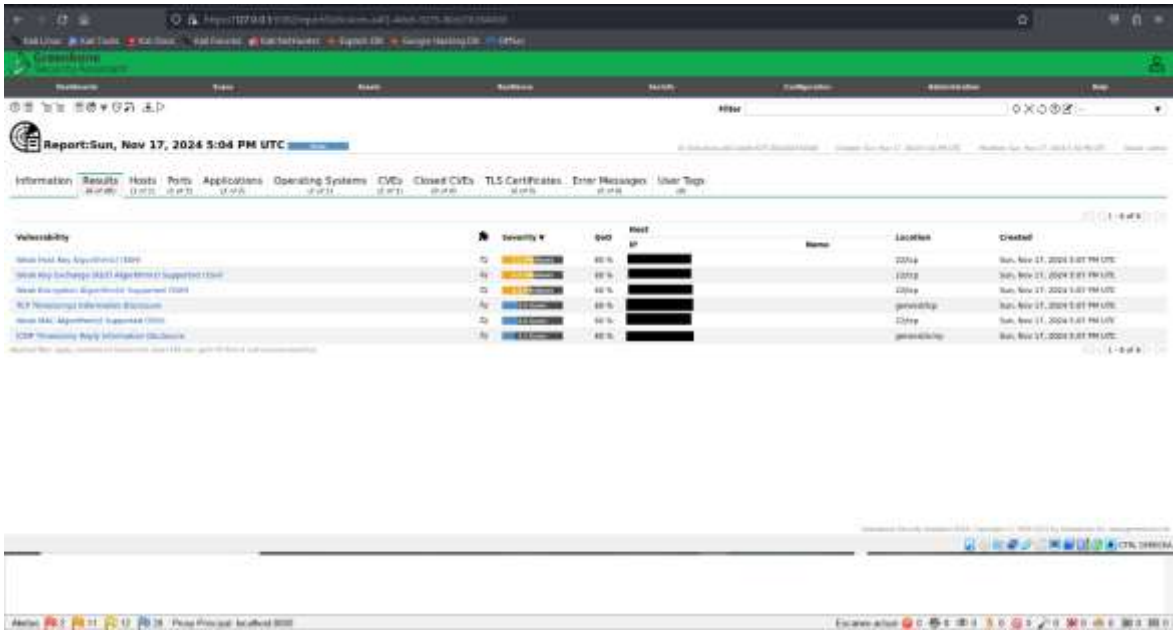
2.1.3.1 Escaneos de Vulnerabilidades

En el mundo de la seguridad informática, el escaneo de vulnerabilidades es un paso clave para identificar y mitigar riesgos potenciales para los activos de información. Para lograr una evaluación eficaz de las debilidades existentes, es indispensable el uso herramientas especializadas para realizar un análisis en profundidad de los activos de información. Algunas de las herramientas que se utilizaron en esta tarea incluyen Kali Linux, Greenbone Security Assistant (GSA) y OWASP ZAP, cada una con capacidades únicas para detectar vulnerabilidades específicas en diferentes niveles de la infraestructura.

El uso conjunto de estas herramientas proporciona una cobertura integral al identificar vulnerabilidades, entregando una descripción detallada de las debilidades que un atacante podría utilizar. Este enfoque multidimensional no sólo mejora la precisión de la detección de vulnerabilidades, sino que también guía la implementación de soluciones de seguridad efectivas para brindar una mayor protección a los activos de información.

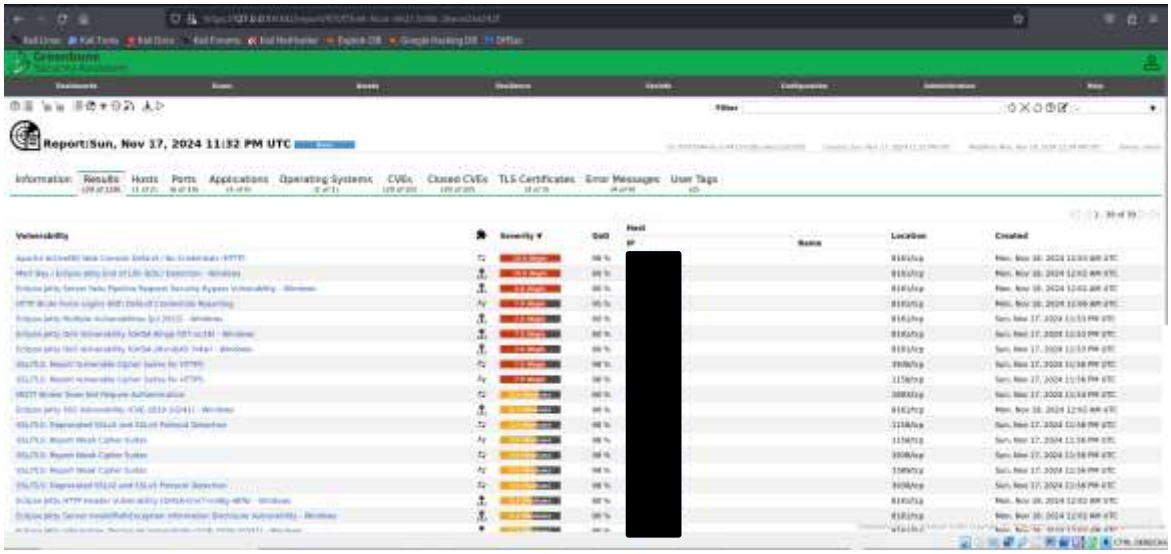
A continuación, se presentan los resultados obtenidos después de los escaneos para la identificación amenazas y vulnerabilidades en los activos de información:

Figura 4. Resultados del escaneo para la identificación de amenazas y vulnerabilidades al activo Bases de datos institucional.



Fuente: Autoría Propia

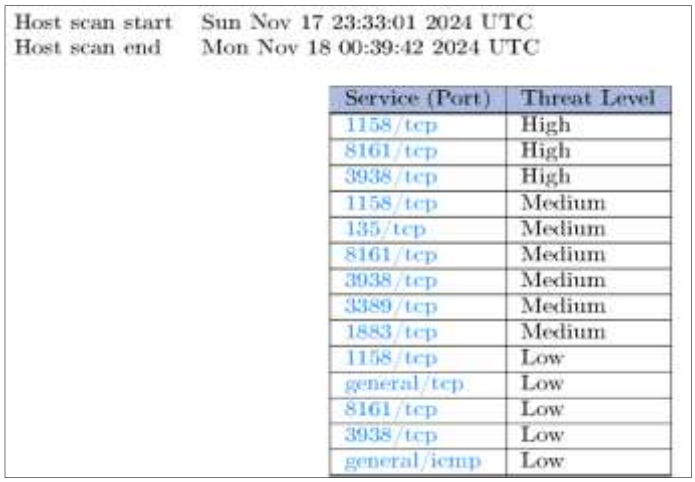
Figura 5. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el activo Bases de datos Software gestión comercial .



Fuente: Autoría Propia

Identificación de amenazas y vulnerabilidades para el Software Gestión Comercial (Modulo de contabilidad, tesorería, pagos, activos)

Figura 6. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en los modulos de Software gestión comercial.



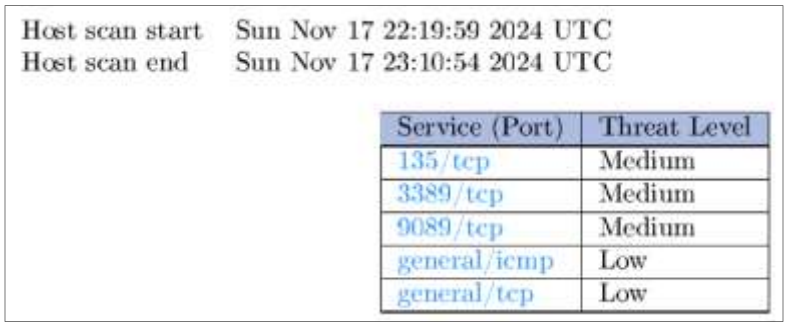
Host scan start	Sun Nov 17 23:33:01 2024 UTC
Host scan end	Mon Nov 18 00:39:42 2024 UTC

Service (Port)	Threat Level
1158/tcp	High
8161/tcp	High
3938/tcp	High
1158/tcp	Medium
135/tcp	Medium
8161/tcp	Medium
3938/tcp	Medium
3389/tcp	Medium
1883/tcp	Medium
1158/tcp	Low
general/tcp	Low
8161/tcp	Low
3938/tcp	Low
general/icmp	Low

Fuente: Autoría Propia

Identificación de amenazas y vulnerabilidades en el servidor de aplicaciones

Figura 7. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el servidor de aplicaciones.



Host scan start	Sun Nov 17 22:19:59 2024 UTC
Host scan end	Sun Nov 17 23:10:54 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
3389/tcp	Medium
9089/tcp	Medium
general/icmp	Low
general/tcp	Low

Fuente: Autoría Propia

Identificación de amenazas y vulnerabilidades en el servidor de dominio Administrativos

Figura 8. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el servidor de dominio de administrativos.

Host scan start	Sun Nov 17 18:03:24 2024 UTC
Host scan end	Sun Nov 17 19:12:48 2024 UTC

Service (Port)	Threat Level
3269/tcp	Medium
3389/tcp	Medium
135/tcp	Medium
636/tcp	Medium
9089/tcp	Medium
3269/tcp	Low
636/tcp	Low
general/icmp	Low
general/tcp	Low

Fuente: Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en el servidor de dominio estudiantes y docentes

Figura 9. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el servidor de dominio de estudiantes y docentes.

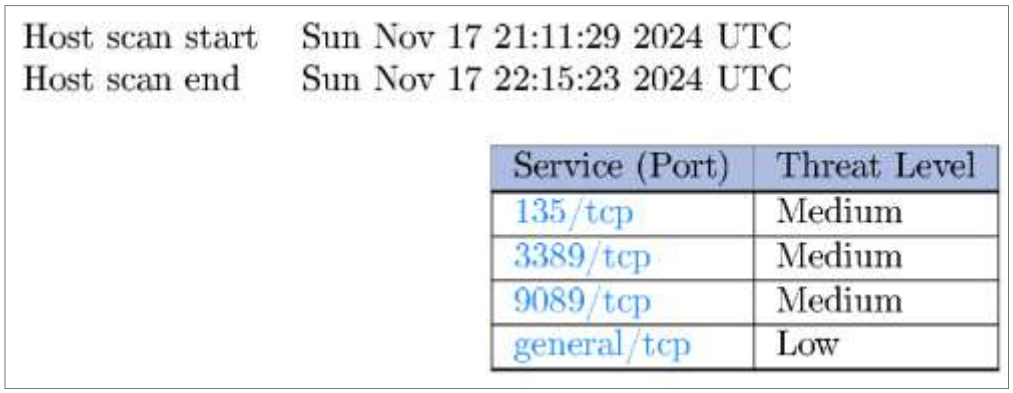
Host scan start	Sun Nov 17 19:18:05 2024 UTC
Host scan end	Sun Nov 17 20:07:39 2024 UTC

Service (Port)	Threat Level
636/tcp	Medium
3389/tcp	Medium
3269/tcp	Medium
9089/tcp	Medium
135/tcp	Medium
636/tcp	Low
3269/tcp	Low
general/icmp	Low
general/tcp	Low

Fuente: Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en el servidor DHCP

Figura 10. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el servidor DHCP.



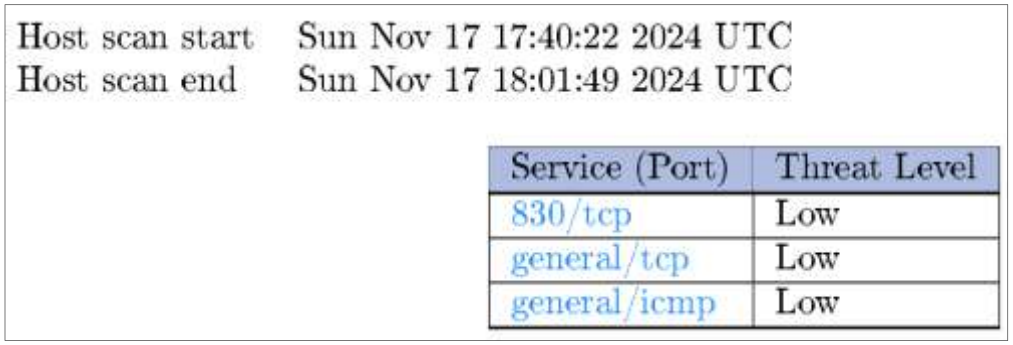
Host scan start Sun Nov 17 21:11:29 2024 UTC
Host scan end Sun Nov 17 22:15:23 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
3389/tcp	Medium
9089/tcp	Medium
general/tcp	Low

Fuente: Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en el Router Core

Figura 11. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el Router Core.



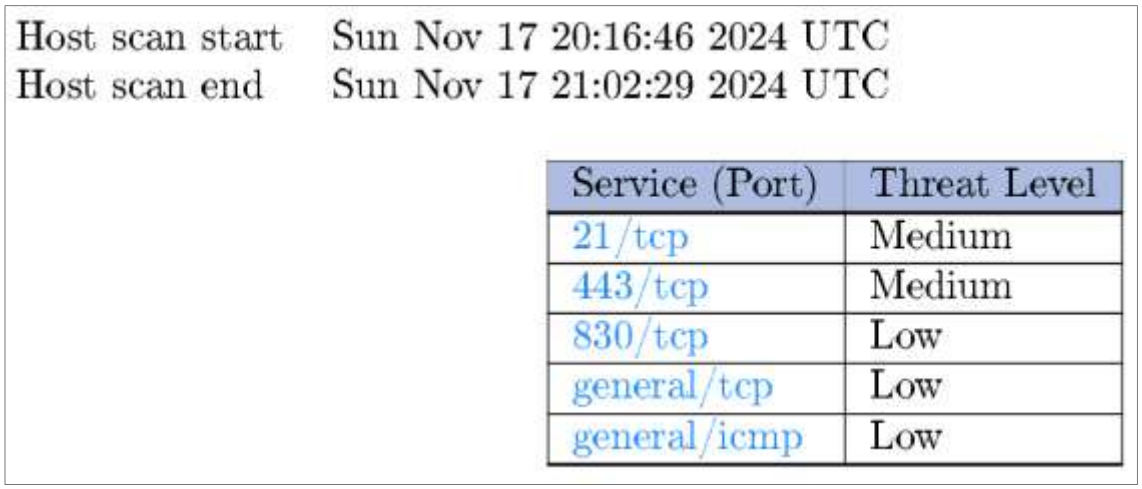
Host scan start Sun Nov 17 17:40:22 2024 UTC
Host scan end Sun Nov 17 18:01:49 2024 UTC

Service (Port)	Threat Level
830/tcp	Low
general/tcp	Low
general/icmp	Low

Fuente: Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en el Firewall

Figura 12. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el Firewall.



Host scan start Sun Nov 17 20:16:46 2024 UTC
Host scan end Sun Nov 17 21:02:29 2024 UTC

Service (Port)	Threat Level
21/tcp	Medium
443/tcp	Medium
830/tcp	Low
general/tcp	Low
general/icmp	Low

Fuente: Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en software Administrativos

Figura 13. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en software Administrativos.

Fuente: Autoría Propia

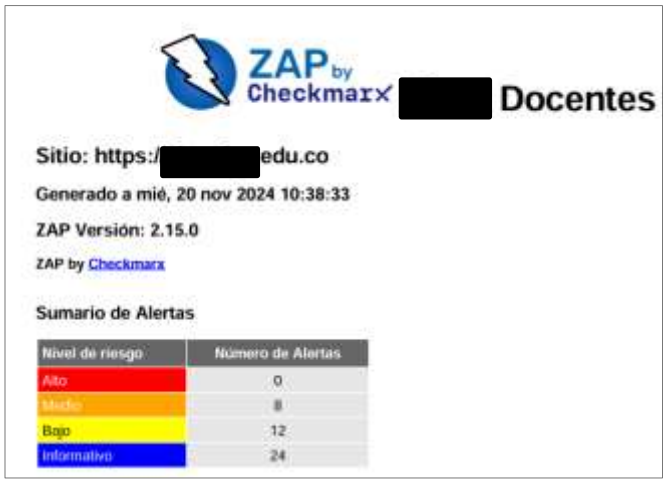
Identificación de análisis de amenazas y vulnerabilidades en software estudiantes

Figura 14. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en software estudiantes.

Fuente*:* Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en SOFTWARE Docentes

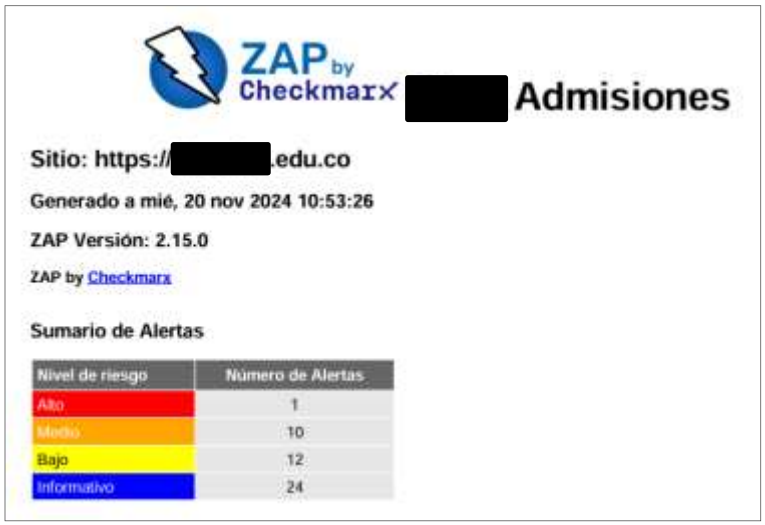
Figura 15. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en SOFTWARE Docentes.



Fuente*:* Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en SOFTWARE Admisiones

Figura 16. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en SOFTWARE Admisiones.



Fuente: Autoría Propia

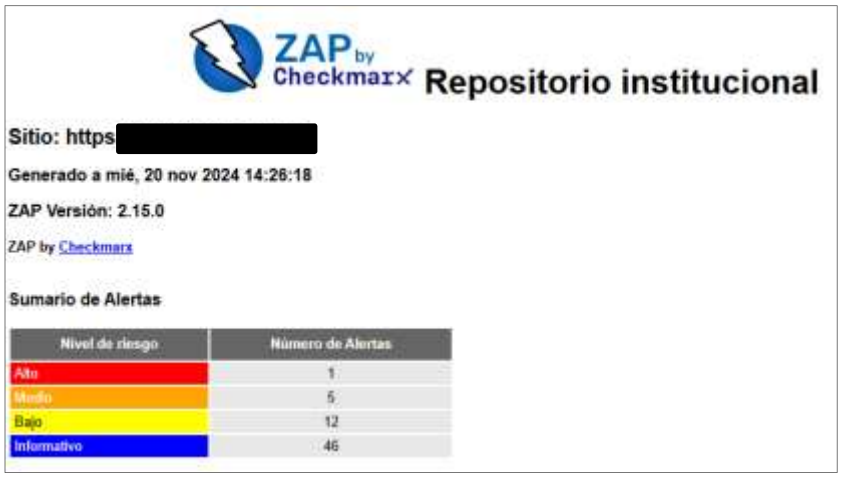
Identificación de análisis de amenazas y vulnerabilidades en el sitio web de calidad.

Figura 17. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el sitios web de calidad.

Fuente*:* Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en el repositorio institucional.

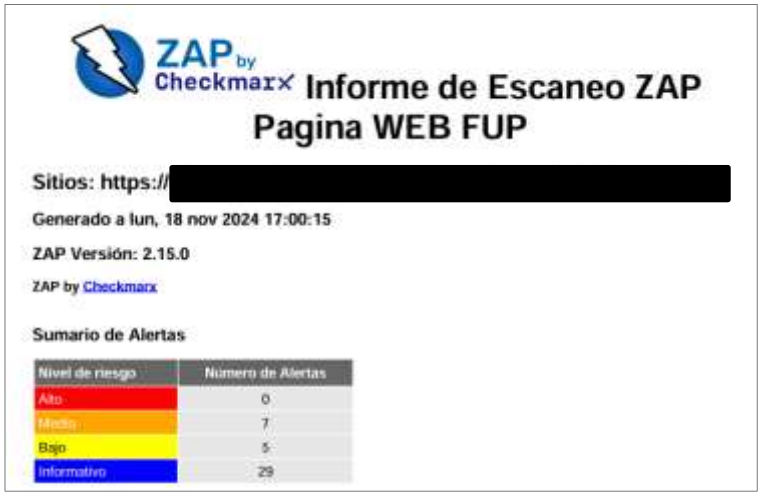
Figura 18. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el repositorio isntitucional.



Fuente: Autoría Propia

Identificación de análisis de amenazas y vulnerabilidades en el sitio web institucional.

Figura 19. Resultados del escaneo para la identificación de amenazas y vulnerabilidades en el sitio web institucional.



Fuente: Autoría Propia

2.3 Identificación de amenazas

La metodología MAGERIT define una amenaza como un evento, entidad o situación

que tiene el potencial de comprometer las propiedades de la información. Las amenazas pueden ser internas (por errores organizacionales o acciones maliciosas de los empleados) o externas (provocadas por causas externas, como ciberataques o desastres naturales). La identificación de amenazas implica un análisis exhaustivo de posibles fuentes que podrían dañar la propiedad de la institución.

2.2.1 Análisis de fuentes de amenazas

Esto incluye el estudio de eventos o situaciones que puedan impactar los activos, tanto naturales (por ejemplo, terremotos, incendios, etc.) como tecnológicos (como un ataque de Ransomware, Malware, etc.) y humanos (errores, negligencia o sabotaje interno).

2.2.2 Clasificación de las amenazas

MAGERIT agrupa las amenazas en categorías para facilitar el análisis, estas categorías son amenazas naturales (Terremotos, inundaciones, incendios), amenazas humanas (Ciberataques (hacking, phishing), fraudes internos, vandalismo), amenazas tecnológicas (fallos en software, fallos en hardware, problemas de interoperabilidad) y amenazas organizativas (Deficiencias en la gestión de seguridad, falta de formación).

2.2.3 Priorización

No todas las amenazas tienen el mismo nivel de impacto o probabilidad. MAGERIT utiliza técnicas de valoración para priorizar las amenazas según su probabilidad de ocurrencia y el impacto potencial sobre los activos de información.

2.4 Análisis de la interacción entre amenazas y vulnerabilidades

Una vez identificadas las amenazas y vulnerabilidades, MAGERIT también permite analizar sus interacciones. Es decir, evaluar qué vulnerabilidades específicas pueden explotar las amenazas identificadas y cómo se materializan los riesgos. Este análisis es necesario para priorizar los riesgos e identificar las amenazas que tienen más probabilidades de afectar los activos debido a las vulnerabilidades existentes.

A continuación, se presenta el cuadro donde se relacionan las amenazas y las vulnerabilidades encontradas:

Tabla 14. Interacción entre las amenazas y vulnerabilidades identificadas.

No. De Amenazas y Vulnerabilidades	Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades
1	SERVICIOS	Servidor base de datos institucional	[E4] Errores de configuración	El servidor SSH remoto admite los siguientes algoritmos de clave de host débiles: ssh-dss
2	SERVICIOS	Servidor base de datos institucional	[E4] Errores de configuración	El servidor SSH remoto admite los siguientes algoritmos de KEX débiles: diffie-hellman-group-exchange-sha1 y diffie-hellman-group1-sha1
3	SERVICIOS	Servidor base de datos institucional	[E4] Errores de configuración	El servidor SSH remoto está configurado para permitir/soportar algoritmos de cifrado débiles.
4	SERVICIOS	Servidor de bases de datos Software gestión comercial	[A19] Divulgación de información	Conjuntos de cifrados "vulnerables" aceptados por este servicio a través del protocolo SSLv3: TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

5	SERVICIOS	Servidor de bases de datos Software gestión comercial	[A11] Acceso no autorizado	La consola web Apache ActiveMQ no está protegida o utiliza credenciales predeterminadas como admin y user
6	SERVICIOS	Servidor de bases de datos Software gestión comercial	[E2] Errores del administrador	La versión MortBay/EclipseJetty en el host remoto ha llegado al final de su vida útil (EOL)
7	SERVICIOS	Servidor de bases de datos Software gestión comercial	[E2] Errores del administrador	Eclipse Jetty Server es propenso a vulnerabilidades de evasión de seguridad.
8	SERVICIOS	Servidor de bases de datos Software gestión comercial	[E2] Errores del administrador	Inicio de sesión en la aplicación web remota utilizando credenciales predeterminadas.
9	SERVICIOS	Servidor de bases de datos Software gestión comercial	[A11] Acceso no autorizado	CVE-2022-2047: El análisis de URI no válido puede generar un HttpURI.authority no válido.

10	SERVICIOS	Servidor de bases de datos Software gestión comercial	[A11] Acceso no autorizado	CVE-2022-2048: Las solicitudes HTTP/2 no válidas pueden provocar la denegación de servicio.
11	SERVICIOS	Servidor de bases de datos Software gestión comercial	[E2] Errores del administrador	Eclipse Jetty es propenso a una vulnerabilidad de denegación de servicio (DoS).
12	SERVICIOS	Servidor de bases de datos Software gestión comercial	[A19] Divulgación de información	Cifrado de bloque de 64 bits 3DES vulnerable al ataque SWEET32 (CVE-2016-2183)
13	SERVICIOS	Servidor de bases de datos Software gestión comercial	[E2] Errores del administrador	Uso del protocolo SSLv2 y/o SSLv3 obsoleto en este sistema.
14	SERVICIOS	Servidor de aplicaciones	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Las actualizaciones de seguridad del proveedor no son de confianza.

15	SERVICIOS	Servidor de aplicaciones	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Los servicios DCE/RPC o MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose al puerto 135 y realizando las consultas correspondientes.
16	SERVICIOS	Servidor de aplicaciones	[E2] Errores del administrador	Aceptación de conjuntos de cefriados debiles. CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
17	SERVICIOS	Servidor de aplicaciones	[E2] Errores del administrador	Uso del protocolo obsoleto TLSv1.0 y/o TLSv1.1
18	SERVICIOS	Servidor de aplicaciones	[E2] Errores del administrador	El servicio SSL/TLS utiliza grupos Die-Hellman con fuerza insuficiente (tamaño de clave < 2048)
19	SERVICIOS	Servidor de aplicaciones	[E23] Errores de mantenimiento / actualización de equipos (hardware)	El servicio SSL/TLS remoto es propenso a una vulnerabilidad de denegación de servicio (DoS). (CVE-2011-1473, CVE-2011-5094).

20	SERVICIOS	Servidor de dominio Administrativos.	[A11] Acceso no autorizado	Conjuntos de cifrados SSL/TLS débiles. protocolo SSLv3: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA protocolo TLSv1.0: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLSv1.1: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLSv1.2: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_CON_RC4_128_SHA (CVE-2013-2566, CVE-2015-2808) (CVE-2015-4000).
21	SERVICIOS	Servidor de dominio Administrativos	[A24] Denegación de servicio	Puertos 3269/tcp, 3389/tcp, 135/tcp, 636/tcp, 9089/tcp: Uso del protocolo obsoleto SSLv2 y SSLv3 en este sistema. Además de TLSv1.0+, el servicio también proporciona el protocolo SSLv3 obsoleto y admite uno o más cifrados. Estos cifrados

					admitidos se pueden encontrar en el VT 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623 .1.0.802067).
	22	SERVICIOS	Servidor de dominio Administrativos	[A24] Denegación de servicio	Puertos 3269/tcp, 3389/tcp, 135/tcp , 636/tcp, 9089/tcp: Se pudo detectar el uso del protocolo TLSv1.0 y/o TLSv1.1 en desuso en este sistema. Además de TLSv1.2+, el servicio también proporciona los protocolos TLSv1.0 y TLSv1.1 en desuso y admite uno o más cifrados. CVE-2011-3389 Y CVE-2015-0204.

	23	SERVICIOS	Servidor de dominio Administrativos	[E2] Errores del administrador	Puertos 3269/tcp, 3389/tcp, 135/tcp, 636/tcp, 9089/tcp: El servicio SSL/TLS utiliza grupos Diffie-Hellman con una solidez insuficiente (tamaño de clave < 2048).
	24	SERVICIOS	Servidor de dominio Administrativos	[A11] Acceso no autorizado	Puertos 3269/tcp, 3389/tcp, 135/tcp, 636/tcp, 9089/tcp: Los servicios de Entorno informático distribuido/Llamadas a procedimientos remotos (DCE/RPC) o MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose al puerto 135 y realizando las consultas apropiadas.

	25	SERVICIOS	Servidor de dominio estudiantes y docentes	[A11] Acceso no autorizado	Conjuntos de cifrados SSL/TLS débiles. protocolo SSLv3: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA protocolo TLSv1.0: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLSv1.1: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA TLSv1.2: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_CON_RC4_128_SHA (CVE-2013-2566, CVE-2015-2808) (CVE-2015-4000)
	26	SERVICIOS	Servidor de dominio estudiantes y docentes	[A24] Denegación de servicio	Puertos 3269/tcp, 3389/tcp, 135/tcp , 636/tcp, 9089/tcp: Uso del protocolo obsoleto SSLv2 y SSLv3 en este sistema. Además de TLSv1.0+, el servicio también proporciona el protocolo SSLv3 obsoleto y admite uno o más cifrados. Estos cifrados admitidos se

					pueden encontrar en el VT 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623 .1.0.802067).
	27	SERVICIOS	Servidor de dominio estudiantes y docentes	[A24] Denegación de servicio	Puertos 3269/tcp, 3389/tcp, 135/tcp , 636/tcp, 9089/tcp: Se pudo detectar el uso del protocolo TLSv1.0 y/o TLSv1.1 en desuso en este sistema. Además de TLSv1.2+, el servicio también proporciona los protocolos TLSv1.0 y TLSv1.1 en desuso y admite uno o más cifrados. CVE-2011-3389 Y CVE-2015-0204.
	28	SERVICIOS	Servidor de dominio estudiantes y docentes	[E2] Errores del administrador	Puertos 3269/tcp, 3389/tcp, 135/tcp , 636/tcp, 9089/tcp: El servicio SSL/TLS utiliza grupos Diffie-Hellman con una solidez

				insuficiente (tamaño de clave < 2048).
29	SERVICIOS	Servidor de dominio estudiantes y docentes	[A11] Acceso no autorizado	Puertos 3269/tcp, 3389/tcp, 135/tcp, 636/tcp, 9089/tcp: Los servicios de Entorno informático distribuido/Llamadas a procedimientos remotos (DCE/RPC) o MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose al puerto 135 y realizando las consultas apropiadas.
30	SERVICIOS	Servidor DHCP	[A11] Acceso no autorizado	Los servicios de Entorno informático distribuido/Llamadas a procedimientos remotos (DCE/RPC) o MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose a los

					puertoss135/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, 49157/tcp, 49158/tcp, 49159/tcp, 49163/tcp
	31	SERVICIOS	Servidor DHCP	[A11] Acceso no autorizado	Conjuntos de cifrados "débiles" aceptados por este servicio a través del protocolo TLSv1.0: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA Conjuntos de cifrados "débiles" aceptados por este servicio a través del protocolo TLSv1.1: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA Conjuntos de cifrados "débiles" aceptados por este servicio a través del protocolo TLSv1.2: TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA

32	SERVICIOS	Servidor DHCP	[A24] Denegación de servicio	El servicio SSL/TLS remoto es propenso a una vulnerabilidad de denegación de servicio (DoS) CVE-2011-1473 CVE-2011-5094
33	HARDWARE	Router (Core)	[E2] Errores del administrador	El servidor SSH remoto está configurado para permitir/soportar algoritmos MAC débiles. cliente a servidor: umac-64-etm@openssh.com umac-64@openssh.com servidor a cliente: umac-64-etm@openssh.com umac-64@openssh.com
34	HARDWARE	Router (Core)	[E2] Errores del administrador	El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.
35	HARDWARE	Router (Core)	[E2] Errores del administrador	El host remoto responde a una solicitud de marca de tiempo ICMP.

	36	HARDWARE	Firewall	[A11] Acceso no autorizado	Puerto 21/tcp: Inicio de sesión FTP sin cifrar en texto claro. El servicio FTP remoto acepta inicios de sesión sin un comando 'AUTH TLS' enviado previamente
	37	HARDWARE	Firewall	[E2] Errores del administrador	Puerto 443/tcp: El certificado SSL/TLS del servidor remoto esta vencido. Expiró 2022-11-29 21:17:56. huella digital (SHA-1), huella digital (SHA-256)
	38	HARDWARE	Firewall	[A24] Denegación de servicio	SSL/TLS: vulnerabilidad de denegación de servicio por renegociación (CVE-2011-1473, CVE-2011-5094)
	39	HARDWARE	Firewall	[A24] Denegación de servicio	SSL/TLS: Certificado firmado mediante un algoritmo de firma débil
	40	SOFTWARE	SOFTWARE Administrativos	[A19] Divulgación de información	Inyección SQL avanzada - MySQL >= 5.0.12 AND basada en tiempo ciego (SELECT)
	41	SOFTWARE	SOFTWARE Administrativos	[A5] Suplantación de la identidad del usuario	Ausencia de Tokens Anti-CSRF No se encontraron

				tokens Anti-CSRF en formulario de envío HTML.
42	SOFTWARE	SOFTWARE Administrativos	[A11] Acceso no autorizado	Bypassing 403. Es posible saltarse los endpoints 403, la regla de scaneo envió un payload que hizo que la respuesta mostrara que era accesible (código de estado 200).
43	SOFTWARE	SOFTWARE Administrativos	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada
44	SOFTWARE	SOFTWARE Administrativos	[A11] Acceso no autorizado	Confusión de Ruta Relativa: El servidor web está configurado para servir respuestas a URL ambiguas de forma que se pueda confundir la "path relative" (ruta relativa) correcta de la URL
45	SOFTWARE	SOFTWARE Administrativos	[A18] Destrucción de información	Falta atributo de integridad de recursos secundarios
46	SOFTWARE	SOFTWARE Administrativos	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking: La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni XFrame-

					Options para proteger contra ataques de 'ClickJacking'.
	47	SOFTWARE	SOFTWARE Administrativos	[A15] Modificación deliberada de la información	La página incluye contenido mixto, es decir, contenido al que se accede a través de HTTP en lugar de HTTPS
	48	SOFTWARE	SOFTWARE Administrativos	[E8] Difusión de software dañino	Librería JS Vulnerable: La librería identificada bootstrap, versión 4.5.0 es vulnerable.
	49	SOFTWARE	SOFTWARE Estudiantes	[A11] Acceso no autorizado	Inyección SQL avanzada - MySQL > 5.0.11 consultas apiladas (SELECT - comment)
	50	SOFTWARE	SOFTWARE Estudiantes	[A11] Acceso no autorizado	Inyección SQL avanzada - MySQL >= 5.0.12 AND basada en tiempo ciego (SELECT)
	51	SOFTWARE	SOFTWARE Estudiantes	[A11] Acceso no autorizado	Inyección SQL avanzada: consultas apiladas de Oracle (DBMS_PIPE. RECEIVE_MESSAGE - comment)

52	SOFTWARE	SOFTWARE Estudiantes	[A11] Acceso no autorizado	Inyección SQL avanzada - PostgreSQL > 8.1 Y ciega basada en tiempo
53	SOFTWARE	SOFTWARE Estudiantes	[A8] Difusión de software dañino	Divulgación de Código Fuente - Inclusión de archivos
54	SOFTWARE	SOFTWARE Estudiantes	[A19] Divulgación de información	Inyección SQL avanzada - MySQL >= 5.0.12 AND basada en tiempo ciego (SELECT)
55	SOFTWARE	SOFTWARE Estudiantes	[A5] Suplantación de la identidad del usuario	Ausencia de Tokens Anti-CSRF No se encontraron tokens Anti-CSRF en formulario de envío HTML.
56	SOFTWARE	SOFTWARE Estudiantes	[A11] Acceso no autorizado	Bypassing 403. Es posible saltarse los endpoints 403, la regla de scaneo envió un payload que hizo que la respuesta mostrara que era accesible (código de estado 200).
57	SOFTWARE	SOFTWARE Estudiantes	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada

58	SOFTWARE	SOFTWARE Estudiantes	[A11] Acceso no autorizado	Confusión de Ruta Relativa: El servidor web está configurado para servir respuestas a URL ambiguas de forma que se pueda confundir la "path relative" (ruta relativa) correcta de la URL
59	SOFTWARE	SOFTWARE Estudiantes	[A18] Destrucción de información	Falta atributo de integridad de recursos secundarios
60	SOFTWARE	SOFTWARE Estudiantes	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking: La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni XFrame-Options para proteger contra ataques de 'ClickJacking'.
61	SOFTWARE	SOFTWARE Estudiantes	[A15] Modificación deliberada de la información	La página incluye contenido mixto, es decir, contenido al que se accede a través de HTTP en lugar de HTTPS
62	SOFTWARE	SOFTWARE Estudiantes	[E8] Difusión de software dañino	Librería JS Vulnerable: La librería identificada bootstrap, versión 4.5.0 es vulnerable.

63	SOFTWARE	SOFTWARE Docentes	[A5] Suplantación de la identidad del usuario	Ausencia de Tokens Anti-CSRF No se encontraron tokens Anti-CSRF en formulario de envío HTML.
64	SOFTWARE	SOFTWARE Docentes	[A11] Acceso no autorizado	Bypassing 403. Es posible saltarse los endpoints 403, la regla de scaneo envió un payload que hizo que la respuesta mostrara que era accesible (código de estado 200).
65	SOFTWARE	SOFTWARE Docentes	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada
66	SOFTWARE	SOFTWARE Docentes	[A11] Acceso no autorizado	Confusión de Ruta Relativa: El servidor web está configurado para servir respuestas a URL ambiguas de forma que se pueda confundir la "path relative" (ruta relativa) correcta de la URL
67	SOFTWARE	SOFTWARE Docentes	[A18] Destrucción de información	Falta atributo de integridad de recursos secundarios

68	SOFTWARE	SOFTWARE Docentes	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking: La respuesta no incluye Content-Security-Policy con la directiva 'frame-ancestors' ni XFrame-Options para proteger contra ataques de 'ClickJacking'.
69	SOFTWARE	SOFTWARE Docentes	[A15] Modificación deliberada de la información	La página incluye contenido mixto, es decir, contenido al que se accede a través de HTTP en lugar de HTTPS
70	SOFTWARE	SOFTWARE Docentes	[E8] Difusión de software dañino	Librería JS Vulnerable: La librería identificada bootstrap, versión 4.5.0 es vulnerable.
71	SOFTWARE	SOFTWARE Admisiones	[A8] Difusión de software dañino	Divulgación de Código Fuente - Inclusión de archivos
72	SOFTWARE	SOFTWARE Admisiones	[A5] Suplantación de la identidad del usuario	Ausencia de Tokens Anti-CSRF No se encontraron tokens Anti-CSRF en formulario de envío HTML.

73	SOFTWARE	SOFTWARE Admisiones	[A11] Acceso no autorizado	Bypassing 403. Es posible saltarse los endpoints 403, la regla de scaneo envió un payload que hizo que la respuesta mostrara que era accesible (código de estado 200).
74	SOFTWARE	SOFTWARE Admisiones	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada
75	SOFTWARE	SOFTWARE Admisiones	[A11] Acceso no autorizado	Confusión de Ruta Relativa: El servidor web está configurado para servir respuestas a URL ambiguas de forma que se pueda confundir la "path relative" (ruta relativa) correcta de la URL
76	SOFTWARE	SOFTWARE Admisiones	[A11] Acceso no autorizado	Error Desbordamiento de Enteros
77	SOFTWARE	SOFTWARE Admisiones	[A18] Destrucción de información	Falta atributo de integridad de recursos secundarios
78	SOFTWARE	SOFTWARE Admisiones	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking
79	SOFTWARE	SOFTWARE Admisiones	[E8] Difusión de software dañino	Format String Error (Error de formato de cadena)

80	SOFTWARE	Página web calidad	[A19] Divulgación de información	Advanced SQL Injection - MySQL >= 5.0.12 AND time-based blind (SELECT)
81	SOFTWARE	Página web calidad	[A19] Divulgación de información	Revelación PII: La respuesta contiene Información de Identificación Personal, como el número de CC, SSN y datos sensibles similares.
82	SOFTWARE	Página web calidad	[A5] Suplantación de la identidad del usuario	Ausencia de Tokens Anti-CSRF
83	SOFTWARE	Página web calidad	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada
84	SOFTWARE	Página web calidad	[A5] Suplantación de la identidad del usuario	Comprobación de Tokens Anti-CSRF
85	SOFTWARE	Página web calidad	[A11] Acceso no autorizado	Confusión de Ruta Relativa
86	SOFTWARE	Página web calidad	[A19] Divulgación de información	Divulgación de Proxy: Se detectaron o identificaron 1 servidor(es) proxy. Esta información ayuda a un posible atacante a determinar.
87	SOFTWARE	Página web calidad	[A19] Divulgación de información	Divulgación de Archivo de Backup

88	SOFTWARE	Página web calidad	[A15] Modificación deliberada de la información	Engaño de Web Cache
89	SOFTWARE	Página web calidad	[A7] Uso no previsto	Falta atributo de integridad de recursos secundarios
90	SOFTWARE	Página web calidad	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking
91	SOFTWARE	Página web calidad	[E8] Difusión de software dañino	Librería JS Vulnerable
92	SOFTWARE	Repositorio institucional	[A19] Divulgación de información	Revelación PII
93	SOFTWARE	Repositorio institucional	[A5] Suplantación de la identidad del usuario	Ausencia de Tokens Anti-CSRF
94	SOFTWARE	Repositorio institucional	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada
95	SOFTWARE	Repositorio institucional	[A18] Destrucción de información	Falta atributo de integridad de recursos secundarios
96	SOFTWARE	Repositorio institucional	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking
97	SOFTWARE	Repositorio institucional	[E8] Difusión de software dañino	Librería JS Vulnerable
98	SOFTWARE	Página Web	[A5] Suplantación de la identidad del usuario	Cabecera Content Security Policy (CSP) no configurada
99	SOFTWARE	Página Web	[A18] Destrucción de información	Falta atributo de integridad de recursos secundarios

100	SOFTWARE	Página Web	[A7] Uso no previsto	Falta de cabecera Anti-Clickjacking

Fuente*:* Autoría Propia

3. VALORACIÓN CUALITATIVA, CUANTITATIVA Y PROBABILIDAD DEL IMPACTO DE LOS RIESGOS IDENTIFICADOS EN LOS ACTIVOS DE INFORMACIÓN

3.1 NORMATIVAS Y METODOLOGÍAS INTERNACIONALES PARA LA GESTIÓN DE RIESGOS

3.1.1 ISO/IEC 27001 e ISO/IEC 2700

La norma ISO/IEC 27001 se centra en la implementación de un sistema de gestión de seguridad de la información (SGSI) que permite proteger sistemáticamente la información mediante la identificación, evaluación y tratamiento de riesgos. Además, ISO/IEC 27005 proporciona orientación específica para la gestión de riesgos de seguridad de la información, centrándose en la identificación de riesgos (Identificar amenazas y vulnerabilidades), que pueden afectar los activos de información y análisis y evaluación de riesgos (Evaluación y priorización cuantitativa basada en riesgos), Gestión de riesgos (Desarrollo de controles y estrategias para mitigar, transferir, aceptar o prevenir riesgos).

El uso de estas normas permite tener un enfoque estructurado en línea con las mejores prácticas internacionales para el desarrollo del presente objetivo.

3.1.2 Metodología MAGERIT

El Método de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) es un marco desarrollado por el Instituto Nacional de Tecnologías de las Comunicaciones (INTECO) de España. MAGERIT está diseñado para la gestión de riesgos en sistemas de información, permitiendo a las organizaciones identificar activos de información relevantes, descubrir amenazas y vulnerabilidades relacionadas, evaluar los riesgos en función de su impacto y probabilidad, determinar prioridades e implementar medidas para reducirlas o eliminarlas.

Este enfoque es particularmente útil para la infraestructura de redes y telecomunicaciones, donde la evaluación detallada de las amenazas permite una respuesta oportuna y eficaz.

3.2 Valoración del riesgo en activos de información

La metodología empleada no más que un enfoque estructurado para la evaluación de riesgos de los activos de información identificados, que incluye tres componentes

clave: probabilidad del riesgo, impacto del riesgo y evaluación del riesgo.

Una vez identificados los activos de información en el desarrollo del objetivo uno, es fundamental llevar a cabo un análisis de amenazas y vulnerabilidades que puedan afectar dichos activos. Las amenazas pueden ser internas (error humano, fraude, negligencia) o externas (ciberataques, desastres naturales, fallas técnicas), y las vulnerabilidades son debilidades en los sistemas, procesos o controles que estas amenazas pueden explotar. La combinación de amenazas y vulnerabilidades determinará el riesgo a evaluar.

A continuación, se exponen las escalas utilizadas para el análisis del riesgo a través de tablas, "siendo la escala siguiente adecuada para evaluar el valor de los activos, la extensión del impacto y la magnitud del riesgo".

Figura 20. Escalas utilizadas para el análisis parte 1.

PROBABILIDAD DEL RIESGO

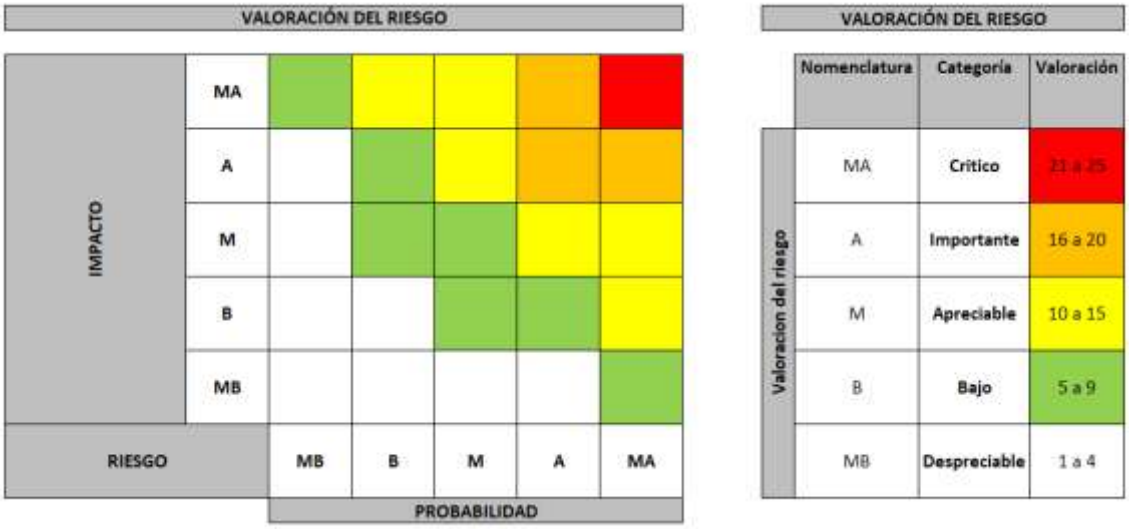
	Nomenclatura	Categoría	Valoración
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**muy raro**	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4
	M	**Medio**	3
	B	**Bajo**	2
	MB	**Muy Bajo**	1

Fuente*:* Matriz análisis de riesgos CSIRT Académico UNAD

Figura 21. Ecalas utilizadas para el análisis parte 2.



Fuente: Matriz análisis de riesgos CSIRT Académico UNAD

3.2.1 Evaluación de la probabilidad del riesgo

La probabilidad de riesgo se refiere a la probabilidad de que una amenaza aproveche una vulnerabilidad para causar daños a los activos de información. Para evaluar la probabilidad, se deben considerar varios factores, como la frecuencia de incidentes similares en el pasado, el entorno operativo, la madurez de los controles de seguridad implementados y la probabilidad de que ocurra la amenaza.

Escala de probabilidad (ejemplo):

Alta: La amenaza tiene alta probabilidad de materializarse (ocurre con frecuencia, es difícil de mitigar).

Media: La amenaza tiene una probabilidad moderada de ocurrir (ha sucedido ocasionalmente o está parcialmente mitigada).

Baja: La amenaza tiene baja probabilidad de ocurrir (es poco probable que se materialice, o está bien controlada).

Evaluación del impacto del riesgo: El impacto del riesgo se refiere a las consecuencias que tendría la materialización de una amenaza en un activo de información. Este impacto puede ser de diversa naturaleza: financiera, operativa, reputacional, legal o tecnológica. Para evaluar el impacto, se deben tener en cuenta las siguientes variables:

Impacto en la confidencialidad: ¿Cómo afectaría la divulgación no autorizada de la información?

Impacto en la integridad: ¿Qué efectos tendría una alteración o corrupción de los datos?

Impacto en la disponibilidad: ¿Cómo afectaría la pérdida de acceso o disponibilidad de la información?

Escala de impacto (ejemplo):

Alto: El impacto sería significativo y tendría consecuencias graves para la organización, como pérdida de datos críticos, grandes pérdidas financieras, daño a la reputación o sanciones legales.

Moderado: El impacto sería notable, pero no afectaría gravemente a la operatividad de la organización o a la integridad de los datos.

Bajo: El impacto sería mínimo, sin consecuencias graves para la organización.

Valoración del riesgo: La valoración del riesgo se realiza combinando la probabilidad del riesgo y su impacto potencial. Esta combinación permite determinar el nivel de riesgo asociado a cada amenaza, que puede ayudar a priorizar las acciones de mitigación.

Una forma común de calcular la valoración del riesgo es mediante una matriz de riesgo o una fórmula numérica. En la matriz de riesgo, se asignan valores numéricos a la probabilidad y el impacto, y luego se cruzan para obtener el nivel de riesgo.

Ejemplo de fórmula para valoración del riesgo:

$R=P\times I$

Donde:

R es el nivel de riesgo.

P es la probabilidad del riesgo (en una escala numérica).

I es el impacto del riesgo (en una escala numérica).

Dependiendo del valor de R, los riesgos se clasifican en categorías como:

Crítico: Nivel de riesgo muy alto, requiere acciones inmediatas de mitigación.

Alto: Nivel de riesgo considerable, requiere medidas de seguridad prioritarias.

Moderado: Riesgo manejable, pero se deben aplicar medidas de control preventivas.

Bajo: Riesgo mínimo, con poca probabilidad de ocurrir y bajo impacto si ocurre.

Priorización de los riesgos: Con los riesgos valorados y clasificados, se procede a priorizarlos en función de su nivel de riesgo. Los riesgos críticos y altos deben ser

tratados con urgencia, implementando medidas de mitigación, mientras que los riesgos moderados y bajos pueden ser gestionados con controles menos estrictos o monitoreados periódicamente.

Mitigación y control: Finalmente, una vez que los riesgos han sido priorizados, se deben implementar estrategias de mitigación para reducir tanto la probabilidad como el impacto de los riesgos más significativos. Esto puede incluir la implementación de controles técnicos (como firewalls, cifrado, etc.), procedimientos operacionales (como capacitación en seguridad, pruebas de penetración), y políticas organizativas (como gestión de accesos, gestión de incidentes).

Para la infraestructura de red y telecomunicaciones de la Institución de Educación Superior de Popayán, se implementó la "Valoración de los activos en Escala C.C eficiente" que es una herramienta clave para el análisis de activos de información dentro de una organización. Esta tabla proporciona una evaluación detallada de varias propiedades, centrándose en tres principios básicos: confidencialidad, integridad y accesibilidad. Esta métrica determina el nivel de riesgo asociado a cada activo, permitiendo al personal de seguridad informática priorizar acciones preventivas y correctivas. Cada evaluación es el resultado de un análisis integral de cómo cada activo podría verse afectado si se incumplen estos principios fundamentales, permitiéndole tomar decisiones informadas sobre la protección y gestión de los recursos más valiosos que existen en su empresa. Este enfoque integrado y personalizado tiene como objetivo controlar eficazmente el riesgo de la información y promover la resiliencia y la seguridad de la organización.

Tabla 15. Resumen de valoración del riesgo los activos en escala C.C Eficiente

Nombre del activo	Riesgo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valor
Servidor bases de datos institucional	ALTO	3	3	9	9	9	7
Servidor bases de datos Software Gestión Comercial	ALTO	3	3	9	9	9	7
Servidor software Gestión Comercial (Modulo de contabilidad, tesorería, pagos, activos)	MEDIO	3	3	9	9	3	5
Servidor de aplicaciones	ALTO	3	3	9	9	9	7

Servidor de dominio Administrativos	ALTO	3	3	6	9	6	6
Servidor de dominio estudiantes y docentes	ALTO	3	3	6	9	6	6
Servidor DHCP	ALTO	3	3	9	9	6	6
Router (Core)	ALTO	3	3	9	9	9	7
Firewall	ALTO	3	3	9	9	6	6
Software Administrativos	ALTO	6	3	9	9	6	7
Software Estudiantes	ALTO	6	3	9	9	6	7
Software Docentes	ALTO	6	5	9	6	6	7
Software Admisiones	ALTO	6	5	3	9	6	7
Página web calidad	ALTO	6	5	3	6	3	6
Repositorio institucional	ALTO	6	5	3	6	9	7
Página Web	ALTO	6	5	3	6	9	6

Fuente: Autoría Propia

3.3 Valoración cualitativa de los activos de información

En la valoración cualitativa de los activos de información se utiliza una tabla integral diseñada para evaluar y clasificar los activos de información claves dentro de la institución con el fin de garantizar una protección y gestión adecuadas. Esta tabla describe cada activo de información en detalle, comenzando con los datos esenciales del activo: nombre del recurso, proceso de propiedad y tipo específico. Esta identificación inicial proporciona una comprensión precisa del contexto en el que se utiliza y gestiona cada activo.

La valoración cubre una variedad de aspectos, incluidos factores críticos como la autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad, y factores que determinan el nivel de. Estos criterios son importantes para comprender el impacto potencial del compromiso o la pérdida de estas características. Además, se examina una serie de atributos específicos que ayudan a contextualizar aún más el papel del activo de información. Preguntas clave, como si el activo es de terceros o clientes que debe protegerse con mayor rigor, si está restringido a ciertos empleados o si es crítico para la operación interna o la relación con terceros, proporcionan un marco detallado para evaluar la sensibilidad y el nivel de acceso requerido. En función de estos criterios, se determina el grado de impacto que tendría un posible acceso no autorizado, alteración o uso indebido del activo, clasificando las consecuencias como leves, importantes o graves.

Por último, se establece la ubicación del activo, ya sea físico o electrónico, lo cual influye en las estrategias de protección y recuperación frente a posibles incidentes. La siguiente tabla proporciona una valoración exhaustiva y cualitativa de cada activo de información, permitiendo tomar decisiones informadas sobre sus políticas de seguridad y protección, garantizando la continuidad operativa y minimizando riesgos en la gestión de la información.

Tabla 16. Activos de información y valoración cualitativa

No.	DATOS DEL ACTIVO DE INFORMACION			DIMENSION					ATRIBUTOS								UBICACIÓN	
	Nombre del activo de información	Proceso propietario del activo	Tipo de Activo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes o corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que, en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:			Físico	Electrónico
															Leve	Importante	Grave		
1	Servidor base de datos institucional	Director-GSI	SERVICIOS	B	B	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X
2	Servidor base de datos Software Gestión Comercial	Director-GTI	SERVICIOS	B	B	MA	MA	MA	NO	SI	SI	SI	SI	SI			X		X

3	Servidor base de datos Software Gestión Comercial (Modulo de contabilidad, tesorería, pagos, activos)	Tesorero	SERVICIOS	B	B	MA	MA	B	SI	SI	SI	SI	SI	SI		X		X
4	Servidor de aplicaciones	Director-GSI	SERVICIOS	B	B	MA	MA	MA	NO	SI	SI	SI	SI	SI		X	X	
5	Servidor de dominio Administrativos	Profesional de virtualización y redes-GTI	SERVICIOS	B	B	MA	MA	A	NO	SI	SI	SI	SI	SI	X		X	
6	Servidor de dominio estudiantes y docentes	Profesional de virtualización y redes-GTI	SERVICIOS	B	B	MA	MA	A	NO	SI	SI	SI	SI	SI	X		X	
7	Servidor DHCP	Director-GTI	SERVICIOS	B	B	MA	MA	A	NO	SI	SI	SI	SI	SI		X	X	
8	Router (Core)	Profesional de	HARDWARE	B	B	MA	MA	MA	SI	SI	SI	SI	SI	SI		X	X	

		virtualización y redes-GTI																	
9	Firewall	Profesional de virtualización y redes-GTI	HARDWARE	B	B	MA	MA	A	SI	SI	SI	SI	SI	SI			X	X	
10	SOFTWARE Administrativos	Director-GSI	SOFTWARE	A	B	MA	MA	A	SI	SI	SI	SI	SI	SI			X		X
11	SOFTWARE Estudiantes	Director-GSI	SOFTWARE	A	B	MA	MA	A	SI	SI	SI	SI	SI	SI			X		X
12	SOFTWARE Docentes	Director-GSI	SOFTWARE	A	B	MA	MA	A	SI	SI	SI	SI	SI	SI			X		X
13	SOFTWARE Admisiones	Director-GSI	SOFTWARE	A	B	MA	MA	A	SI	SI	SI	SI	SI	SI			X		X
14	Página web calidad	Director-Calidad	SOFTWARE	A	B	MA	MA	B	NO	SI	SI	SI	SI	SI	X				X
15	Repositorio institucional	Director-Investigación	SOFTWARE	A	M	MA	A	MA	NO	SI	SI	SI	SI	SI	X				X

16	Página Web	Director-Comunicaciones	SOFTWARE	A	M	B	MA	MA	SI	SI	SI	SI	SI	SI	X		X

Fuente*:* Autoría Propia

3.4 VALORACIÓN CUANTITATIVA DE LOS ACTIVOS DE INFORMACIÓN

La valoración cuantitativa de activos de información en el contexto de la seguridad informática es un proceso clave para determinar el valor y el riesgo asociado a los recursos informáticos de una organización. A través de este enfoque, se asignan valores numéricos a los distintos activos de información, lo que permite medir de manera más precisa el impacto de posibles amenazas o vulnerabilidades sobre los mismos. Este proceso no solo considera el valor intrínseco de cada activo, sino también los posibles costos derivados de un incidente de seguridad, como pérdidas financieras, daños a la reputación o interrupciones operativas.

El objetivo principal de la valoración cuantitativa es proporcionar una base objetiva para la toma de decisiones, utilizando datos medibles como el coste de los activos, la probabilidad de un evento adverso, la gravedad del impacto y los costos asociados con su recuperación o mitigación. Además, este enfoque facilita la priorización de las acciones de seguridad, permitiendo a las organizaciones asignar recursos de manera eficiente para proteger los activos más críticos.

El resultado de la valoración cuantitativa es introducido en tablas o matriz que detallan el nivel de riesgo de cada activo, identificando aquellos que requieren mayor atención y los posibles recursos que deben invertirse en su protección. A través de este análisis, las organizaciones pueden optimizar sus estrategias de seguridad, asegurando una protección adecuada en función del valor de los activos y el riesgo que implican.

Este enfoque numérico es fundamental para la planificación estratégica de la seguridad informática, proporcionando una visión clara y detallada de los activos y su importancia relativa dentro de la infraestructura organizacional.

A continuación, se presenta la tabla resumen de la valoración cuantitativa realizada:

Tabla 17. Resumen de valoración cuantitativa de riesgos de los activos

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Servidor bases de datos institucional	IMPORTANTE	9	9	25	25	25	19
Servidor bases de datos Software gestión comercial	IMPORTANTE	9	9	25	25	25	19

Servidor software Gestión Comercial (Modulo de contabilidad, tesorería, pagos, activos)	APRECIABLE	9	9	25	25	9	15
Servidor de aplicaciones	IMPORTANTE	9	9	25	25	25	19
Servidor de dominio Administrativos	IMPORTANTE	9	9	25	25	20	18
Servidor de dominio estudiantes y docentes	IMPORTANTE	9	9	25	25	20	18
Servidor DHCP	IMPORTANTE	9	9	25	25	20	18
Router (Core)	IMPORTANTE	9	9	25	25	25	19
Firewall	IMPORTANTE	9	9	25	25	20	18
SOFTWARE Administrativos	IMPORTANTE	20	9	25	25	20	20
SOFTWARE Estudiantes	IMPORTANTE	20	9	25	25	20	20
SOFTWARE Docentes	IMPORTANTE	20	9	25	25	20	20
SOFTWARE Admisiones	IMPORTANTE	20	9	25	25	20	20
Página web calidad	IMPORTANTE	20	9	25	25	9	18
Repositorio institucional	CRITICO	20	15	25	20	25	21
Página Web	IMPORTANTE	20	15	9	25	25	19

Fuente: Autoría Propia

4. ESTRATEGIAS Y MEDIDAS DE CONTROL BASADAS EN LOS RESULTADOS DE LA EVALUACIÓN PARA EL FORTALECIMIENTO DE LA SEGURIDAD EN LA INSTITUCIÓN.

La seguridad de la infraestructura de red y telecomunicaciones es un aspecto crítico para la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN, especialmente en un entorno donde la interconexión digital y la dependencia de la tecnología son cada vez más significativas. En este capítulo se presenta el conjunto de estrategias y medidas de control que se derivan de los resultados obtenidos en la evaluación de riesgos llevada a cabo en los capítulos anteriores. La implementación efectiva de estas estrategias tiene como objetivo fortalecer la seguridad de la información y garantizar la protección de los activos clave de la institución frente a amenazas y vulnerabilidades identificadas. Este plan de tratamiento, desarrollado conforme a los principios y directrices de la norma ISO 27001:2013, establece las acciones específicas que la institución debe seguir para mitigar, gestionar o eliminar los riesgos relacionados con la seguridad de la información.

4.1 PLAN DE TRATAMIENTO

La norma ISO 27001:2013, que regula los sistemas de gestión de la seguridad de la información (SGSI), establece que, tras una exhaustiva identificación y evaluación de riesgos, es imprescindible elaborar un Plan de Tratamiento de Riesgos. Este plan debe ser completo, alineado con la política de seguridad de la institución y diseñado para abordar los riesgos de forma eficiente, asegurando que se implementen controles adecuados y proporcionales al nivel de riesgo identificado.

El proceso de tratamiento de riesgos debe ser diseñado para abordar tanto los controles ya existentes como aquellos que se deben añadir, con el fin de reducir los riesgos a niveles aceptables. Para ello, la norma sugiere que se consideren diversas opciones de tratamiento: mitigación, transferencia, aceptación y eliminación de los riesgos. La opción de tratamiento más adecuada dependerá de la naturaleza del riesgo, el costo asociado a su mitigación y el impacto potencial en la organización. Esta flexibilidad en el tratamiento de los riesgos permite que las soluciones sean adaptadas a las características y necesidades particulares de la institución.

El desarrollo de un plan de tratamiento efectivo involucra tres componentes clave, que a su vez se reflejan en la tabla que acompaña este capítulo, detallando las acciones propuestas para cada riesgo identificado. Estos componentes son:

El primer componente es el Objetivo, en el que se define claramente el propósito de cada control dentro del contexto de la seguridad de la información. El objetivo de cada acción esta alineado con las prioridades de la institución y con los resultados de la evaluación de riesgos, buscando proteger los activos de información más críticos.

El segundo componente es el Control por aplicar, en el cual se especifica el control específico que se implementará para mitigar el riesgo o cumplir con el objetivo

establecido. Este control es de naturaleza técnico, administrativo o físico, y está acorde con el nivel de riesgo identificado en la fase de evaluación.

Como ultimo componentes esta la Descripción de la aplicación del control, en el cual se detalla la forma en que el control debe ser implementado y gestionado dentro de la organización. Esto incluye las responsabilidades del personal encargado, los procedimientos a seguir, las herramientas necesarias y los plazos para su ejecución. La descripción debe ser lo suficientemente clara como para garantizar que los controles sean aplicados de manera efectiva, además de incluir indicadores de rendimiento o resultados esperados para medir la eficacia del control.

El propósito principal de este capítulo es asegurar que los riesgos previamente identificados sean tratados adecuadamente mediante el establecimiento de controles específicos que reduzcan las probabilidades de ocurrencia de amenazas y su impacto en la institución. De esta manera, el plan de tratamiento permite crear una estructura sólida de seguridad, estableciendo una respuesta coherente a los riesgos y ayudando a la institución a alcanzar sus objetivos de protección de la información. Además, el capítulo subraya la importancia de la revisión continua del plan, dado que los riesgos evolucionan constantemente, y las medidas de control deben adaptarse a los cambios en el entorno organizacional, tecnológico y de amenazas.

Es importante resaltar que existe un paso que la institución a través de los colaboradores encargados de la seguridad informática debe llevar a cabo en base al plan de tratamiento que se presentara, y es una evaluación continua para verificar su efectividad y realizar ajustes conforme se identifiquen nuevas amenazas o se produzcan cambios en los activos de información o procesos. De este modo, se logrará mantener la seguridad a largo plazo, garantizando que los activos más críticos continúen protegidos de manera adecuada y que los controles sean dinámicos, adaptándose a las necesidades de la institución en el futuro.

A continuación, se presenta una tabla resumen del plan de tratamiento, realizado en la matriz de análisis de riesgos que se puede consultar en el anexo C “Matriz de análisis de riesgos” pestaña APT.

Tabla 18. Resumen plan de tratamiento

Categoría	Amenazas y Vulnerabilidades	Controles Implementados	Acciones Recomendadas
4Bases de datos (Institucional y Software gestión comercial)	• Errores de configuración (E4): Algoritmos de clave de host y KEX débiles en SSH. Cifrados débiles en SSH. • Divulgación de información (A19): Uso de cifrados vulnerables (SSLv3, SWEET32). • Acceso no autorizado (A11): Credenciales predeterminadas en consolas web.	• Dominio A9 (Control de Acceso): Proceso formal de suministro de acceso. Gestión de contraseñas seguras. • Dominio A10 (Criptografía): Política de controles criptográficos. Deshabilitación de cifrados y protocolos obsoletos.	• Deshabilitar algoritmos de clave de host y KEX débiles en SSH. • Actualizar configuraciones para evitar cifrados vulnerables. • Cambiar credenciales predeterminadas y asegurar autenticación.
Servidores de aplicaciones y dominio	• Errores del administrador (E2): Uso de software obsoleto (Eclipse Jetty). Vulnerabilidades DoS en SSL/TLS. • Acceso no autorizado (A11): Cifrados débiles en TLS. • Denegación de servicio (A24): Uso de protocolos obsoletos (SSLv2, SSLv3).	• Dominio A10 (Criptografía): Política de controles criptográficos. Deshabilitación de SSLv2 y SSLv3. • Dominio A12 (Gestión de vulnerabilidades): Actualización de software y parches.	• Actualizar software obsoleto (Eclipse Jetty). • Deshabilitar protocolos obsoletos y cifrados débiles. • Filtrar tráfico en puertos vulnerables.
Firewall y Router	• Acceso no autorizado (A11): FTP sin cifrar. Algoritmos MAC débiles en SSH. • Errores del	• Dominio A10 (Criptografía): Reemplazo de certificados vencidos. Deshabilitación de algoritmos MAC débiles. • Dominio A13 (Controles	• Habilitar FTPS o AUTH TLS para FTP. • Deshabilitar algoritmos MAC débiles en SSH. • Obtener parches

	administrador (E2): Certificados SSL/TLS vencidos. Vulnerabilidades DoS en SSL/TLS.	de red): Filtrado de tráfico en puertos vulnerables.	para vulnerabilidades DoS.
(Softwares admisiones, administrativos, estudiantes, docentes, y Páginas web)	• Inyección SQL (A11): Vulnerabilidades en MySQL, PostgreSQL y Oracle. • Suplantación de identidad (A5): Falta de tokens Anti-CSRF. Cabecera CSP no configurada. • Divulgación de información (A19): Revelación de PII y código fuente.	• Dominio A14 (Desarrollo seguro): Validación de entradas. Protección contra inyecciones SQL. • Dominio A9 (Control de acceso): Validación rigurosa de parámetros de entrada.	• Implementar tokens Anti-CSRF. • Configurar cabeceras de seguridad (CSP, X-Frame-Options). • Validar y sanitizar entradas de usuario. • Actualizar librerías JS vulnerables.
Recomendaciones generales			• Actualización y parcheo: Mantener sistemas y aplicaciones actualizados. • Configuración segura: Deshabilitar protocolos obsoletos y usar cifrados fuertes. • Gestión de accesos: Políticas de contraseñas seguras y controles de autenticación. • Protección contra ataques comunes: Implementar medidas contra inyecciones SQL, CSRF, etc. • Monitoreo y auditoría: Establecer monitoreo

	continuo y auditorías periódicas.

Fuente: Autoría Propia

4.2 RECOMENDACIONES Y ACCIONES PROPUESTAS PARA MITIGAR AMENAZAS Y VULNERABILIDADES IDENTIFICADAS EN ACTIVOS NO CRÍTICOS PARA LA INSTITUCIÓN.

Dentro del desarrollo del objetivo dos del presente trabajo, se realizaron actividades que permitieron identificar amenazas y vulnerabilidades en activos que no son críticos para la institución, pero que si tienen relación con el manejo de la infraestructura de red. Estas amenazas si bien no registran un riesgo alto dentro de las valoraciones, es importante que la institución realice las acciones necesarias para eliminarlas o mitigarlas. Se recomienda leer el anexo D “Informe de análisis de amenazas y vulnerabilidades identificadas en activos no críticos”, para que se puedan implementar o identificar nuevas acciones a las que se recomiendan a continuación.

4.2.1 Actualización y parcheo de sistemas operativos

Implementar un plan de actualización y parcheo regular de sistemas operativos para garantizar que todos los y dispositivos de red estén protegidos contra las últimas amenazas. Por ejemplo, se debe programar actualizaciones y parcheo a los equipos de las salas de sistemas, y equipos de personal administrativo que aún tienen sistemas operativos a Windows 10.

Establecer políticas y procedimientos para monitorear y aplicar parches de seguridad de manera oportuna. Por ejemplo, se debe designar a un administrador de sistemas responsable de verificar y aplicar los parches de seguridad disponibles en todos los servidores y dispositivos de red.

4.2.2 Configuración segura de dispositivos de distribución de red

Realizar una revisión exhaustiva de la configuración de los equipos de distribución de red para asegurar que los puertos sensibles estén debidamente protegidos y que solo se permita el acceso autorizado. Por ejemplo, se debe configurar en el firewall una política que permita bloquear el acceso remoto a través del puerto 22 (SSH) desde direcciones IP externas no autorizadas.

4.2.3 Mejoras en la seguridad física

Instalar cerraduras y sistemas de control de acceso en los gabinetes de la infraestructura de red para prevenir el acceso no autorizado. Por ejemplo, se debe instalar una cerradura electrónica en el gabinete de la sala de servidores y configurar un sistema de control de acceso con tarjetas de proximidad para limitar el acceso solo al personal autorizado.

Implementar un sistema de control de acceso más granular y seguro en el centro de datos, con autenticación multifactorial y registros de acceso detallados. Por ejemplo, se debe actualizar el sistema de control de acceso del centro de datos para requerir la autenticación mediante tarjeta de proximidad y PIN, y registrar todas las entradas y salidas de personal en un registro de auditoría centralizado.

4.2.4 Gestión de identidad y acceso

4.2.4.1. Evaluación de la efectividad de los controles de autenticación y autorización

Realizar auditorías periódicas de los sistemas de autenticación para identificar posibles debilidades en la gestión de identidades y accesos. Esto incluye revisar las políticas de contraseñas, la asignación de privilegios y los registros de actividad de usuario.

4.2.4.2. Implementación de políticas de contraseñas seguras y autenticación multifactorial

Establecer requisitos estrictos para la creación y gestión de contraseñas, como longitud mínima, caracteres especiales y rotación regular. Además, implementar métodos de autenticación multifactorial, como el uso de tokens de seguridad o aplicaciones de autenticación móvil, para agregar una capa adicional de protección.

4.2.4.3. Auditoría regular de cuentas de usuario y privilegios de acceso

Realizar revisiones periódicas de las cuentas de usuario y los privilegios de acceso para garantizar que estén alineados con las políticas de seguridad de la organización. Esto implica revocar los privilegios innecesarios, monitorear los cambios en los roles y responsabilidades, y revisar los registros de actividad de usuario en busca de comportamientos anómalos.

4.2.5 Continuidad del negocio

4.2.5.1. Desarrollo de un plan de contingencia y recuperación ante desastres (DRP)

Crear un plan detallado que describa los procedimientos y recursos necesarios para mitigar los efectos de interrupciones en la infraestructura de red y telecomunicaciones. Esto incluye la identificación de riesgos, la asignación de roles y responsabilidades, y la definición de procesos de recuperación de datos y sistemas.

4.2.5.2. Pruebas regulares de los procedimientos de respaldo y restauración de datos

Realizar simulacros de recuperación ante desastres para validar la efectividad de los procedimientos de respaldo y restauración de datos. Estas pruebas deben incluir la restauración de datos desde diferentes tipos de copias de seguridad (por ejemplo, copias en la nube, copias locales) y la verificación de la integridad de los datos recuperados.

4.2.5.3. Implementación de redundancia de hardware y conectividad

Configurar sistemas redundantes y enlaces de comunicación para garantizar la disponibilidad continua de servicios críticos. Esto puede incluir la implementación de clústeres de servidores, la replicación de datos en tiempo real y la configuración de conexiones de red con conmutación por error automática.

4.2.6 Monitoreo y detección de amenazas

4.2.6.1. Implementación de herramientas de monitoreo de seguridad de red

Desplegar soluciones de monitoreo de seguridad de red que proporcionen visibilidad en tiempo real sobre el tráfico de red y las actividades de los usuarios. Estas herramientas pueden incluir sistemas de detección y prevención de intrusiones (IDS/IPS), sistemas de gestión de eventos e información de seguridad (SIEM) y sensores de red.

4.2.6.2. Establecimiento de políticas de registro y análisis de registros de eventos

Definir políticas claras de registro de eventos que especifiquen qué eventos deben registrarse, con qué nivel de detalle y durante cuánto tiempo deben conservarse los registros. Luego, realizar análisis periódicos de los registros de eventos para identificar patrones de tráfico sospechoso, intentos de acceso no autorizado y otras actividades maliciosas.

4.2.6.3 Desarrollo de capacidades de respuesta a incidentes

Establecer procedimientos y protocolos para responder de manera rápida y efectiva a incidentes de seguridad detectados. Esto incluye la asignación de roles y responsabilidades, la coordinación con equipos internos y externos, y la documentación detallada de los pasos a seguir durante la respuesta a incidentes.

CONCLUSIONES

La evaluación exhaustiva de la infraestructura de red y telecomunicaciones de la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN ha revelado la presencia de múltiples vulnerabilidades y riesgos de seguridad informática que podrían comprometer la integridad y disponibilidad de los servicios telemáticos. Estos hallazgos subrayan la necesidad crítica de implementar medidas de seguridad efectivas y proactivas para proteger los activos de información y garantizar la continuidad de las operaciones educativas y administrativas.

La diversidad de usuarios y métodos de autenticación en la red Wifi de la universidad representa un desafío significativo en términos de gestión y seguridad. La compartición de credenciales y el acceso no autorizado plantean riesgos de seguridad adicionales que deben abordarse mediante la implementación de políticas de acceso sólidas y la mejora de los mecanismos de autenticación.

La falta de seguridad física en los gabinetes que albergan dispositivos de distribución expone la infraestructura de red a riesgos de manipulación no autorizada y fallos en el servicio. La implementación de medidas de seguridad física, como cerraduras y controles de acceso, es esencial para proteger los componentes críticos de la infraestructura y garantizar la disponibilidad continua de los servicios.

La presencia de sistemas operativos obsoletos en algunos servidores expone a la universidad a amenazas de seguridad y a posibles interrupciones en los servicios críticos. La actualización y el reemplazo de estos sistemas operativos son cruciales para mantener la integridad y la seguridad de los datos, así como para mitigar los riesgos asociados con vulnerabilidades conocidas.

El desarrollo de un plan integral de gestión de riesgos, basado en una metodología rigurosa y en las mejores prácticas de seguridad informática, proporciona una hoja de ruta efectiva para proteger la infraestructura de red y telecomunicaciones de la universidad. La implementación de recomendaciones específicas y la adopción de medidas de mitigación contribuirán a fortalecer la postura de seguridad de la INSTITUCIÓN DE EDUCACIÓN SUPERIOR DE POPAYÁN y a salvaguardar la confidencialidad, integridad y disponibilidad de la información crítica.

RECOMENDACIONES

SISTEMA DE AUTENTICACIÓN MULTIFACTORIAL (MFA)

Esta recomendación tiene por objetivo reforzar la seguridad de las credenciales de los usuarios y prevenir accesos no autorizados, implementando un sistema de autenticación multifactorial robusto para la red Wifi de la universidad, con el fin de reforzar la seguridad de las credenciales de los usuarios y prevenir accesos no autorizados. Esto incluye la adopción de prácticas de gestión de identidades y accesos que aseguren una autenticación segura y personalizada para cada tipo de usuario.

Por lo anterior es importante que la institución siga las siguientes recomendaciones:

Evaluar las opciones de MFA que consiste en identificar proveedores y soluciones de MFA que se integren bien con la infraestructura existente de la universidad.

Seleccionar la solución adecuada en la cual se debe escoger una solución de MFA que ofrezca soporte para autenticación mediante dispositivos móviles, tokens físicos, y otros métodos seguros.

Desarrollo de políticas de gestión de identidades y accesos las cuales tienen como fin definir cómo se gestionan las identidades y accesos, asegurando autenticaciones personalizadas según el tipo de usuario (estudiantes, profesores, personal administrativo).

Implementación técnica con la cual se debe configurar la solución de MFA seleccionada en los sistemas de red Wifi y otros servicios críticos.

Capacitación y concientización con la realización de talleres y seminarios para educar a los usuarios sobre el uso del MFA, su importancia y cómo configurar y utilizar el MFA de manera efectiva.

POLÍTICAS DE GESTIÓN DE CONTRASEÑAS

Con las políticas de gestión de contraseñas se buscar en primera instancia prohibir el intercambio de credenciales y fomentar la creación de contraseñas seguras y únicas. Asimismo, se debe realizar una campaña de concientización para educar a los usuarios sobre las mejores prácticas de seguridad de contraseñas y la importancia de mantener la confidencialidad de sus credenciales.

Para la creación de las políticas se debe tener en cuenta lo siguiente:

Desarrollo de políticas de contraseñas, con la creación de políticas que especifiquen los requisitos de las contraseñas (longitud mínima, complejidad, periodicidad de cambio) y prohíban el intercambio de credenciales.

Lanzar campañas de concientización que permita educar a los usuarios sobre la importancia de las contraseñas fuertes y las mejores prácticas para su gestión.

Realizar la implementación técnica por medio de la configuración de los sistemas para hacer cumplir las políticas de contraseñas, utilizando herramientas que obliguen a la creación de contraseñas seguras y realicen verificaciones periódicas.

Monitoreo y auditoría constante con la implementar herramientas para monitorear el cumplimiento de las políticas de contraseñas y realizar auditorías regulares.

MEDIDAS DE SEGURIDAD FÍSICA

Con esta recomendación se busca restringir el acceso no autorizado a los dispositivos de distribución y proteger los componentes críticos de la infraestructura de red.

Implementar medidas de seguridad física, como cerraduras en gabinetes y salas de servidores, para restringir el acceso no autorizado a los dispositivos de distribución y proteger los componentes críticos de la infraestructura de red, dando prioridad a la identificación de todas las ubicaciones de los dispositivos críticos (salas de servidores, gabinetes de distribución) que necesitan protección física, implementar cerraduras seguras, sistemas de control de acceso y cámaras de vigilancia en las áreas identificadas, establecer políticas claras para el acceso físico, incluyendo quién tiene acceso y bajo qué condiciones, capacitar al personal en los procedimientos de seguridad física y en la importancia de estas medidas para la seguridad general de la red. Esto reducirá los riesgos de manipulación y posibles interrupciones en los servicios causadas por acciones malintencionadas o accidentales.

ACTUALIZACIÓN Y MIGRACIÓN DE SISTEMAS OPERATIVOS

Establecer un programa de actualización y migración de sistemas operativos obsoletos en los servidores a versiones más recientes y compatibles, con el fin de garantizar la estabilidad y seguridad de los sistemas de información crítica. Se deben programar actualizaciones regulares y realizar evaluaciones periódicas de la seguridad del sistema para identificar posibles vulnerabilidades y aplicar parches de seguridad de manera oportuna. Como pasos a seguir para la implementación de esta recomendación se presentan los siguientes:

Identificar todos los sistemas operativos actuales y determinar cuáles están obsoletos o cerca del fin de su soporte.

Desarrollar un plan para actualizar o migrar a versiones más recientes y compatibles, priorizando los sistemas más críticos.

Realizar pruebas piloto en un entorno controlado para asegurar que las actualizaciones no causen interrupciones no deseadas.

Realizar la actualización de los sistemas operativos de manera gradual, monitoreando de cerca los sistemas para detectar cualquier problema.

Establecer un calendario regular de actualizaciones y evaluaciones de seguridad para garantizar que los sistemas se mantengan actualizados y seguros.

SISTEMA DE MONITOREO Y DETECCIÓN DE INTRUSIONES

Implementar un sistema de monitoreo y detección de intrusiones que supervise de manera continua la actividad de la red y alerte sobre posibles amenazas y comportamientos anómalos. La adopción de soluciones de seguridad como firewalls avanzados, sistemas de prevención de intrusiones y sistemas de gestión de eventos de seguridad (SIEM) fortalecerá la postura de seguridad de la infraestructura y permitirá una respuesta rápida ante posibles incidentes de seguridad. Primero que todo la institución determinar las necesidades específicas de monitoreo y detección de intrusiones, para así investigar posibles opciones de herramientas de monitoreo y detección como firewalls avanzados, sistemas de prevención de intrusiones (IPS) y sistemas de gestión de eventos de seguridad (SIEM), se deben crear políticas que definan qué actividades y eventos deben ser monitoreados y cómo se debe responder a las alertas, capacitar al personal de TI en el uso de las nuevas herramientas y en los procedimientos de respuesta a incidentes y establecer un equipo dedicado para el monitoreo continuo de la red y realizar revisiones periódicas para ajustar las estrategias de detección y respuesta a incidentes.

REFERENCIAS BIBLIOGRÁFICAS

¿Qué es la ciberseguridad? (2023). *Kaspersky*. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

¿Qué es la gestión de identidades y accesos? Definiciones IAM, SSO, MFA e IDaaS. (2023). *IBM*. https://www.ibm.com/es-es/topics/identity-access-management

¿Qué es la seguridad informática? (2023). *UNIR Ecuador - Universidad Virtual*. https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

¿Qué es un riesgo en ciberseguridad? Definición y tipos. (2023). *Ciberseguridad*. https://ciberseguridadtips.com/que-es-un-riesgo-en-ciberseguridad-definicion-causas/#que_es_un_riesgo_en_ciberseguridad

¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? (2023). *Firma-e | Proyectos y Formación*. https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

¿Qué son las políticas de seguridad informática y por qué son importantes? (2023). *Informática para Empresas*. https://www.gadae.com/blog/politicas-de-seguridad-informatica/

¿Qué son las pruebas de penetración? (2023). *IBM*. https://www.ibm.com/mx-es/topics/penetration-testing

Amazon Web Services, Inc. (n.d.). *¿Qué es la ciberseguridad? - Explicación de la ciberseguridad.* AWS. https://aws.amazon.com/es/what-is/cybersecurity/

Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. (2023). *Revista Modum*. *Revistas SENA*. https://revistas.sena.edu.co/index.php/re_mo/article/view/4543

Andres, S., Kenyon, B., & Pack, E. B. (2004). *Security Sage's Guide to Hardening the Network Infrastructure.* Syngress. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&an=107438&lang=es&site=eds-live&scope=site

ANFEI. (2021). *Asociación Nacional de Facultades y Escuelas de Ingeniería.* https://www.anfei.mx/miembros/

Brown, A., & Jones, B. (2019). *Journal of information security.*

Carroll, J. (2022). *Infraestructuras seguras* [Objeto virtual de información (OVI)]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/53880

CCN-CERT. (2021). *Riesgos y amenazas en productos fuera de soporte: Prevención y protección* (pp. 1–16). https://www.ccn-cert.cni.es/es/informes/abstracts/5726-riesgos-y-amenazas-productos-fuera-de-soporte/file?format=html

Ciberseg1922. Amenazas y vulnerabilidades, ¿cuáles son sus diferencias? (2019, octubre 24). *Ciberseguridad*. https://ciberseguridad.com/amenzas/

Ciberseguridad. Control de acceso. (2019). *Ciberseguridad.com*. https://ciberseguridad.com/normativa/espana/medidas/control-acceso/#%C2%BFque_es_el_control_de_acceso

Control Objectives for Information and Related Technology (COBIT). (2019). *Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información (COBIT 2019).*

Copeland, M. (2017). *Cyber security on Azure: An IT professional's guide to Microsoft Azure Security Center.* Apress. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&an=1558534&lang=es&site=eds-live&scope=site

Díaz, J. (2023, octubre 25). *Ciberseguridad.* MetaRed. https://www.metared.org/ar/ciberseguridad.html

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92,* 101747. https://doi-org.bibliotecavirtual.unad.edu.co/10.1016/j.cose.2020.101747

Evaluación de riesgos de seguridad de la información: 7 pasos para asegurar el cumplimiento de ISO 27001: 2013. (2022). *Escuela Europea de Excelencia*. https://www.escuelaeuropeaexcelencia.com/2022/02/evaluacion-de-riesgos-de-seguridad-de-la-informacion-7-pasos-para-asegurar-el-cumplimiento-de-iso-27001:2013/

Ferre Bustos, J. S. (2020). *Pruebas de penetración en las redes de datos en cualquier entidad pública o privada.* Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/bitstream/handle/10596/40111/jsferrerb%20(1).pdf?sequence=

Fortra. (n.d.). *Principales desafíos de seguridad de datos y cómo abordarlos.* Fortra. https://www.fortra.com/es/blog/principales-desafios-de-seguridad-de-datos-y-como-abordarlos

Franco, D. A., Perea, J. L., & Puello, P. (2012). *Metodología para la detección de vulnerabilidades en redes de datos.* Información Tecnológica, 23(3), 113–119. https://doi-org.bibliotecavirtual.unad.edu.co/10.4067/s0718-07642012000300014

Gómez Vieites, Á. (2014). *Sistemas seguros de acceso y transmisión de datos* (pp. 63-72). https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/62465

Gonzalez, N., & Miers, C. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications, 1,* 11. https://link-springer-com.bibliotecavirtual.unad.edu.co/article/10.1186/2192-113x-1-11

Guaña Moya, J., et al. (2022). *Ataques de phishing y cómo prevenirlos.* En CISTI (Iberian Conference on Information Systems & Technologies) Proceedings, 17, 1–6. https://doi.org/10.23919/CISTI54359.2022.9823989

Infraestructura - MINTIC - Vive Digital. (2023). *Ministerio de Tecnologías de la Información y Comunicaciones*. https://mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-19449.html

Iza Sanhueza, S. (2023). *Desarrollo de un toolkit de pruebas de intrusión basado en OSSTMM.* Repositorio digital - EPN. https://bibdigital.epn.edu.ec/handle/15000/11460

Jacques, J. (2016). *Detalles sobre la criptografía moderna.* Arrow. https://www.arrow.com/es-mx/research-and-events/articles/modern-cryptography

John, A., & Stoll, C. (2017). *Computer security: Principles and practice.*

Kali Linux. (n.d.). *What is Kali Linux?* Kali Linux Documentation. https://www.kali.org/docs/introduction/what-is-kali-linux/

La importancia del cumplimiento normativo en ciberseguridad. (2023). *Datos 101*. https://www.datos101.com/blog/normativa-ciberseguridad-como-lograrlo/

Los retos de seguridad informática que enfrentan las instituciones de educación en Colombia. (2023). *Revista edu.co*. https://revistaedu.co/secciones/tematicas-educativas/los-retos-de-seguridad-informatica-que-enfrentan-las-instituciones-de-educacion-en-colombia/2660/

Martínez Lozano, J. (2019). *Creación de un ataque DDoS utilizando HTTP-GET flood a partir de la metodología Cyber Kill Chain.* ITeckne: Innovación e Investigación en Ingeniería, 41–47.

Matriz de riesgos: qué es y cómo se hace una. (2023). *Ciberseguridad*. https://ciberseguridadtips.com/matriz-de-riesgos/#que_es_una_matriz_de_riesgos

Mehta, P. (2022, abril 1). *¿Qué es prueba de penetración (pen test)? Definición en Computer Weekly*. *ComputerWeekly.es*. https://www.computerweekly.com/es/definicion/prueba-de-penetracion-pen-test

Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (2016). *Guía para la gestión y clasificación de activos de información.* Ministerio de Tecnologías de la Información y Comunicaciones. https://www.mintic.gov.co/gestionti/615/articles-5482_g5_gestion_clasificacion.pdf

Organización Internacional de Normalización (ISO). (2013). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos* (ISO 27001:2013).

Organización Internacional de Normalización (ISO). (2021). *Gobernanza de las organizaciones* (ISO 37000). https://www.iso.org/obp/ui

Organización Internacional de Normalización (ISO). (2022). *Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información* (ISO 27002).

OWASP. (2021). *OWASP Top Ten.* OWASP Foundation. https://owasp.org/www-project-top-ten/

Prieto, E. (2023, enero 23). *¿Cuál es la historia de la ciberseguridad?* Saint Leo University. https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad

PYMESEC. (n.d.). *ISSAF.* PYMSEC. https://pymesec.org/issaf/

Rincón, L. (2021). *Test de penetración para el estudio de vulnerabilidades a los ciberataques mediante técnicas de hacking ético en redes IPv4.* Revista Télématique, 20(2), 70–85.

Roba Iviricu, L., Vento Alvarez, J., & García Concepción, L. (2016). *Metodología para la detección de vulnerabilidades en las redes de datos utilizando Kali Linux.* Revista de Ingeniería, 334–344.

Seguridad informática: qué es, tipos y características. (2023, mayo 8). *Blog de HubSpot | Marketing, ventas, servicio al cliente y sitio web*. https://blog.hubspot.es/website/que-es-seguridad-informatica#:~:text=la%20seguridad%20inform%C3%A1tica%20es%20el,da%C3%B1o%20o%20acceso%20no%20autorizado.

Smith, R., & Johnson, T. (2020). *International journal of network security.*

Tori, C., & Pico, J. (2004). *Hacking ético.* 334 p. https://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://nebul4ck.files.wordpress.com/2015/08/hacking-etico-carlos-tori.pdf

u-tad. (2023, octubre 25). *¿Qué es el hacking ético?* u-tad. https://u-tad.com/hacking-etico#:~:text=el%20hacking%20ético%20se%20define,sean%20explotadas%20por%20hackers%20malintencionados.

Valderrama Guardia, J. (2017). *Pentesting "prueba de penetración" para la identificación de vulnerabilidades en la red de computadoras en la alcaldía del municipio de Cantón del San Pablo, Departamento del Chocó.* Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/18049/1077436201.pdf?sequence=1&isallowed=y

Vila, E., & Rrapaj, H. (2016). *An approach for hardening of network infrastructure.* Proceedings of the International Conference on Information Technologies, 2020. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&an=133494496&lang=es&site=eds-live&scope=site

Virtualization technology & virtual machine software: What is virtualization? (2023). *VMware*. https://www.vmware.com/es/solutions/virtualization.html#:~:text=la%20virtualizaci%C3%B3n%20utiliza%20el%20software,aplicaciones,%20en%20un%20solo%20servidor.

Vulnerabilidad. (2023). *Banco Santander*. https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=en%20inform%C3%A1tica,%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

Zhou, J. (2021). Construction of computer network security defense system based on big data. *2021 International Conference on Big Data Analysis and Computer Science (BDACS)*. https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/9516541/authors#authors

ANEXOS

Anexo A Cuestionario para levantamiento de activos de información.

CUESTIONARIO PARA LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN, PARA EL DESARROLLO DEL PROYECTO APLICADO COMO OPCION DE GRADO DE LA ESPECIALIZACION EN SEGURIDAD INFOMATICA DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA QUE LLEVA POR TITULO "ANÁLISIS DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE RED Y TELECOMUNICACIONES DE LA FUNDACIÓN UNIVERSITARIA DE POPAYÁN SEDE SAN JOSÉ"

Objetivo: Recopilar información detallada y específica sobre los activos de información en la Fundación Universitaria de Popayán, centrándose en dispositivos hardware, software, manejo de datos sensibles, políticas de seguridad, control de acceso, desafíos de seguridad y la infraestructura de red y telecomunicaciones.

1. Información general

Nombre del entrevistado:

Cargo y área de trabajo:

2. Tiempo en la institución:

¿Cuánto tiempo llevas trabajando en la Fundación Universitaria de Popayán?

3. Activos de información

Dispositivos hardware:

Enumera los principales dispositivos hardware que utilizas en tu área (computadoras, servidores, impresoras, etc.).

Software y aplicaciones:

¿Cuáles son las principales aplicaciones y software que utilizas para realizar tus actividades diarias?

Manejo de datos sensibles:

¿En tu área se maneja información sensible o confidencial? En caso afirmativo, ¿puedes proporcionar ejemplos?

4. Seguridad y acceso

Políticas de seguridad:

¿La Fundación Universitaria de Popayán tiene políticas de seguridad establecidas? ¿Puedes describirlas brevemente?

Control de acceso:

¿Cómo se gestiona el control de acceso a los activos de información en tu área?

5. Problemas o desafíos

Desafíos de seguridad:

¿Has enfrentado desafíos o problemas de seguridad en relación con los activos de información?

6. Infraestructura de red y telecomunicaciones

Redes y comunicaciones:

¿Cómo describirías la infraestructura de red y telecomunicaciones en la Fundación Universitaria de Popayán?

7. Recomendaciones

Recomendaciones:

¿Tienes alguna recomendación para mejorar la gestión de activos de información o la seguridad en la institución?

8. Cierre

Agradecemos tu colaboración. ¿Hay algún otro aspecto relevante sobre los activos de información en tu área que no haya sido cubierto en este cuestionario?

Anexo B Entrevista para levantamiento de activos de información.

ENTREVISTA PARA LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN, PARA EL DESARROLLO DEL PROYECTO APLICADO COMO OPCION DE GRADO DE LA ESPECIALIZACION EN SEGURIDAD INFOMATICA DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA QUE LLEVA POR TITULO "ANÁLISIS DE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE RED Y TELECOMUNICACIONES DE LA FUNDACIÓN UNIVERSITARIA DE POPAYÁN SEDE SAN JOSÉ"

Objetivo: Realizar un inventario actualizado de los activos de información utilizados en las distintas áreas.

Tus respuestas serán cruciales para garantizar un entendimiento preciso de la infraestructura de red y telecomunicaciones de la institución.

1. Información General

1.1. Cargo y Área de Trabajo

¿Cuál es tu cargo en la Fundación Universitaria de Popayán y cuál es tu área de trabajo?

1.2 Actividades Diarias

¿Podrías describir las principales actividades que realizas diariamente en tu área?

2. Activos de Información

2.1 Hardware

¿Cuáles son los principales dispositivos hardware que utilizas en tu área? (computadoras, servidores, impresoras, etc.)

2.2 Software

¿Qué software o aplicaciones son fundamentales para llevar a cabo tus tareas diarias?

2.3 Datos Sensibles

¿Manejas información sensible o confidencial en tu área? En caso afirmativo, ¿podrías proporcionar ejemplos?

3. Seguridad y Acceso

3.3 Políticas de Seguridad

¿La Fundación Universitaria de Popayán tiene políticas de seguridad establecidas? ¿Podrías describirlas brevemente?

3.4 Control de Acceso

¿Cómo se gestiona el control de acceso a los activos de información en tu área?

4. Problemas o Desafíos

¿Has experimentado desafíos o problemas de seguridad en relación con los activos de información?

5. Cierre

Agradezco tu colaboración. ¿Hay algún otro aspecto relevante sobre los activos de información en tu área que no haya sido cubierto en esta entrevista?

Anexo C Matriz de análisis de riesgos de activos de información.

https://docs.google.com/spreadsheets/d/1lPvUYWH53Uo7SxcXyi9NmvVbgqyPgN8U/edit?usp=sharing&ouid=107391233809811189768&rtpof=true&sd=true

Anexo D Informe de análisis de amenazas y vulnerabilidades identificadas en activos no críticos.

https://drive.google.com/file/d/1aSwKAWAk6ewuV62H0BuX469FSL_Nb96Q/view?usp=sharing