UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Creada Ley No. 10 – Registro Oficial 313 de Noviembre 13 de 1985

PROYECTO INTEGRADOR

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERAS EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA

AUDITORIA DE SEGURIDAD INFORMATICA A EQUIPOS INFORMATICOS DE LA UNIDAD EDUCATIVA FISCO MISIONAL JUAN PABLO II LA BRAMADORA"

AUTOR

CARMEN CAPITU MENDOZA ARMENDARIZ

TUTOR

ING. MINAYA MACIAS RENELMO WLADIMIR MG.

2026

CERTIFICADO DE TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante **MENDOZA ARMENDARIS CARMEN CAPITU**, legalmente matriculado/a en la carrera de Ingeniería en Tecnología de la Información, período académico 2025(2)-2026(1), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es "**AUDITORÍA DE SEGURIDAD INFORMÁTICA A EQUIPOS INFORMÁTICOS DE LA UNIDAD EDUCATIVA FISCO MISIONAL JUAN PABLO II LA BRAMADORA**".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 27 de Julio de 2026.

Lo certifico,

Wladimir Minaya Macias, Mg.Sc.
Docente Tutor
Área: Tecnología de la Información

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
Uleam
COMISIÓN ACADÉMICA
EL CARMEN - MANABÍ

DECLARACIÓN DE AUTORÍA

DECLARACIÓN DE AUTORÍA

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de Titulación, cuyo tema es: "AUDITORÍA DE SEGURIDAD INFORMÁTICA A LOS EQUIPOS INFORMÁTICOS DE LA UNIDAD EDUCATIVA FISCO MISIONAL JUAN PABLO II – LA BRAMADORA", corresponde exclusivamente a Carmen Capitu Mendoza Armendáriz con C.I. 2350985418, y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Carmen Capitu Mendoza Armendáriz
C.I. 2350985418

CERTIFICDO DE TRIBUNAL

CERTIFICADO DE TRIBUNAL

Universidad Laica "Eloy Alfaro" De Manabí Extensión En El Carmen

Carrera De Ingeniería En Tecnologías De La Información

TRIBUNAL DE SUSTENACIÓN

Título del Trabajo de Titulación:

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LOS EQUIPOS INFORMÁTICOS DE LA UNIDAD EDUCATIVA FISCO MISIONAL JUAN PABLO II – LA BRAMADORA

Modalidad:

Proyecto Integrador

Autor:

Carmen Capitu Mendoza Armendáriz

Tutor:

Ing. Minaya Macias Renelmo Wladimir, MG

Tribunal de Sustentación:

- **Presidente:** Ing. Mora Marcillo Alex Bladimir, Mg

- **Miembro:** Ing. Pozo Hernández Clara Guadalupe, Mg

- **Miembro:** Ing. Arca Zavala Jefferson Omar, Mg

Fecha de Sustentación:

27 de agosto del 2026

DEDICATORIA

En primer lugar, a **Dios**, por sostenerme cuando las fuerzas parecían agotarse, por iluminar cada decisión, abrir puertas cuando todo parecía incierto y recordarme que, después de cada dificultad, siempre existe una nueva oportunidad para seguir adelante. Sin su infinita misericordia, este logro no habría sido posible.

A mis padres, **Efrén** y **Angélica**, quienes han sido el ejemplo más grande de amor, dedicación y entrega. Cada sacrificio que realizaron, cada palabra de aliento y cada enseñanza se transformaron en la base sobre la que hoy construyo este importante logro. A mis hermanos, **Arlyn** y **Snayder**, por acompañarme en cada etapa de este recorrido

Con inmenso amor dedico este logro a mis abuelos, **Segundo (†)** y **Ninfa**. Sus consejos, su nobleza y la manera en que me enseñaron a valorar las cosas sencillas dejaron una huella imborrable en mi corazón. Aunque uno de ellos hoy me acompaña desde el cielo, siento su presencia en cada paso que doy y en cada meta alcanzada. Este triunfo también honra su memoria y el legado que dejaron en mi vida.

A mis más grandes bendiciones, mis hijos, **Santiago** y **Zeneth**, quienes son la razón de mi esfuerzo y la inspiración que dio sentido a cada paso de este camino. Ustedes llegaron a mi vida para enseñarme que el amor es la fuerza más grande para superar cualquier obstáculo y que, por difícil que parezca el camino, siempre existe un motivo para seguir adelante.

También quiero expresar mi gratitud hacia aquellas personas que formaron parte de mi historia y que, en distintos momentos, caminaron a mi lado brindándome confianza, ánimo y apoyo sincero,

guardo con cariño cada enseñanza compartida, de todas ellas aprendemos algo valioso. Hoy solo permanece el agradecimiento por haber coincidido en el momento indicado.

A mi esposo, **Adrián Loor**, porque Dios permitió que nuestros caminos se encontraran en el momento indicado. Gracias por acompañarme con amor, paciencia y dedicación a lo largo de este camino, por creer en mis capacidades y por sostener mi mano cuando el cansancio y las dudas aparecían. Tu apoyo constante, tus palabras de aliento y la confianza que siempre depositaste en mí me dieron la fortaleza para seguir adelante. Este logro no solo representa el fruto de mi esfuerzo, sino también el de una persona que decidió caminar conmigo y hacer de este sueño una meta compartida.

Finalmente, a mis compañeras de vida que la universidad me regaló, **Jessenia** y **Juanis**. Lo que comenzó como una coincidencia entre aulas terminó convirtiéndose en una amistad que valoro profundamente. Con ustedes descubrí que aún existen personas capaces de alegrarse sinceramente por los logros ajenos, de brindar una palabra de aliento sin esperar nada a cambio y de permanecer presentes tanto en los días de felicidad como en aquellos en los que las fuerzas parecían desaparecer. Cada conversación, cada risa, cada desvelo, cada abrazo y cada recuerdo compartido hicieron que este recorrido fuera mucho más llevadero y, sobre todo, inolvidable. Espero que la vida nos permita seguir celebrando juntas muchos éxitos más. A todas las personas que, de una u otra forma, dejaron una huella en mi historia, los llevo en el corazón

Carmen Capitu Mendoza Armendariz

AGRADECIMIENTO

La culminación de este trabajo de titulación representa el cierre de una etapa llena de aprendizajes, desafíos y crecimiento personal. Por ello, deseo expresar mi más sincero agradecimiento a todas las personas e instituciones que, de una u otra manera, contribuyeron a que este sueño pudiera hacerse realidad.

A la **Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen**, por brindarme la oportunidad de formarme como profesional y por ofrecerme un ambiente académico donde adquirí los conocimientos, valores y experiencias que hoy forman parte de mi desarrollo personal y profesional.

A la **carrera de Tecnología de la Información**, por proporcionarme una formación sólida y de calidad. Mi reconocimiento a cada uno de los docentes en especial a mi querida Ing. Roció Mendoza quien me ayudó cuando más lo necesité, con sus consejos, cariño, y paciencia una de las mejores personas como amiga docente y compañera de aula mi mayor estimación, cariño para ella. que, con profesionalismo, dedicación y compromiso, compartieron sus conocimientos, fomentando en mí el pensamiento crítico, la responsabilidad y el deseo constante de superación.

Expreso un especial agradecimiento al **Ing. Wladimir Minaya**, director de este trabajo de investigación, por el tiempo, la orientación y la confianza que depositó en mí durante el desarrollo de esta tesis. Sus recomendaciones, experiencia y acompañamiento fueron esenciales para fortalecer este proyecto y culminarlo con éxito.

Carmen Capitu Mendoza Armendariz

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La digitalización creciente de los procesos académicos y administrativos en las instituciones educativas ha aumentado la exposición a amenazas cibernéticas, indicando también la necesidad de reforzar la seguridad de la infraestructura tecnológica. En este sentido, la presente investigación se realizó en la Unidad Educativa Fisco Misional Juan Pablo II - La Bramadora, a fin de contribuir a la protección de sus activos informáticos mediante la evaluación del nivel de seguridad existente. El objetivo general consistió en realizar una auditoría de seguridad informática a los equipos informáticos y la infraestructura tecnológica de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora, con el propósito de evaluar su nivel de seguridad, identificar vulnerabilidades y riesgos existentes y proponer un plan de medidas correctivas y preventivas. La investigación tuvo un enfoque mixto, con tipo de estudio descriptivo y de campo, apoyándose en la observación directa, entrevistas, encuestas, checklists y análisis técnico de los equipos, utilizando metodologías y marcos referenciales para la auditoría y la gestión de riesgos en las tecnologías de la información. Los resultados mostraron deficiencias relacionadas con la actualización de sistemas operativos, gestión de parches, políticas de seguridad, copias de seguridad, protección antivirus y capacitación del personal, permitiendo clasificar y priorizar problemas de riesgos detectados. Como resultado se diseñó un plan de mejora orientado al fortalecimiento de la confidencialidad, integridad y disponibilidad de la información. Se concluye que la auditoría permitió diagnosticar de manera objetiva el estado de seguridad informática de la institución y constituye una herramienta fundamental para la toma de decisiones y el establecimiento de una cultura de mejora continua en ciberseguridad.

ABSTRACT

The increasing digitization of academic and administrative processes in educational institutions has heightened exposure to cyber threats, highlighting the need to strengthen the security of technological infrastructure. Accordingly, this research was conducted at the *Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora* to help protect its IT assets by assessing its current security level. The primary objective was to perform an information security audit of the institution's computing equipment and technological infrastructure in order to evaluate security levels, identify existing vulnerabilities and risks, and propose a plan of corrective and preventive measures. The study employed a mixed-methods approach—combining descriptive and field research—and relied on direct observation, interviews, surveys, checklists, and technical equipment analysis, utilizing established methodologies and frameworks for IT auditing and risk management. The results revealed deficiencies regarding operating system updates, patch management, security policies, backups, antivirus protection, and staff training, enabling the classification and prioritization of identified risks. Consequently, an improvement plan was designed to strengthen the confidentiality, integrity, and availability of information. The study concludes that the audit provided an objective assessment of the institution's information security status and serves as a vital tool for decision-making and fostering a culture of continuous improvement in cybersecurity.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Preámbulo

En el mundo tecnológico actual, los centros escolares se hacen más dependientes de la tecnología de la información y la comunicación (TIC) para sus tareas escolares y administrativas. Esta digitalización trae consigo mejoras en eficiencia y alcance del aprendizaje, pero también abre camino a nuevos riesgos y a amenazas cibernéticas para los centros educativos. A nivel mundial se han notificado números alarmantes de incidentes de seguridad. Durante el año 2020 se registraron más de mil fallas en datos importantes que expusieron más de 20 mil millones de registros además de causar pérdidas económicas por 6 billones de dólares en todo el mundo (Navia & Zambrano-Romero, 2021).

La actividad educativa no escapa de esta circunstancia; por el contrario, se ha transformado en una presa deseada para aquellos que atacan por varios motivos, como pueden ser las redes débiles, la presencia de muchísimos usuarios, la valiosidad de unos datos privados y un escaso recurso para la seguridad (Revista 360º, 2025). Informes recientes indican que en 2024 el sector educativo latinoamericano llegó a tener más de 2.700 ataques cada semana por instituto, sobrepasando incluso a áreas críticas como la salud o la banca (Molina-Granja et al., 2025). En países avanzados siguen patrones similares: en Reino Unido, el 71% de las escuelas secundarias y el 97% de las universidades tuvieron por lo menos un problema serio en ciberseguridad en el último año, mucho más que el 50% del área empresarial (Revista 360º, 2025). Destas cifras se deduce la alta probabilización de los centros educativos de ser blanco de ciberataques, los cuales pueden llegar a interrumpir las clases de manera sistemática y poner en riesgo la información de los estudiantes.

En este aspecto proteger la infraestructura en tecnología de los colegios es muy importante para garantizar un ambiente seguro de estudio. La seguridad informática de la escuela trata de proteger los datos confidenciales y garantizar un buen ambiente para alumnos, profesores y personal de oficina, previniendo problemas cibernéticos que pongan en riesgo la integridad, acceso y privacidad de la información del colegio (Morales-Sáenz et al., 2025). Pero muchas escuelas no tienen las herramientas y prácticas para frenar de luchar estas nuevas amenazas. La falta de políticas integrales sobre seguridad en línea o ciberseguridad provoca lagunas que los atacantes pueden usar.

Lo anteriormente enunciado remite a la necesidad que se suscita de realizar una revisión del estado de la seguridad de la información en instituciones educativas de tipo privado con el objeto de localizar vulnerabilidades y sugerir mejoras. En ese contexto se desarrolla el siguiente proyecto de investigación, que consiste en realizar una auditoría de seguridad informática a los equipos de cómputo de la Unidad Educativa Fisco Misional Juan Pablo II - La Bramadora, como medida preventiva para fortalecer la seguridad de su infraestructura tecnológica ante amenazas presentes y futuras.

1.2 Presentación del tema

En terminos simples, una auditoría de seguridad informática es una forma organizada de revisar y evaluar la seguridad de los sistemas y activos tecnológicaos de una organización. Buscan vulnerabilidades, debilidades en los controles y peligros de seguridad para dar recomendaciones que ayuden a reducir riesgos y mejorar la postura de seguridad de la organización (Navia & Zambrano-Romero, 2021). Es básicamente una mirada profunda del estado de la estructura tecnológica (ordenadores, programas, redes, datos) buscando vulnerabilidades que pueden ser aprovechadas por amenazas internas o externas.

En una institución educativa como el Colegio Juan Pablo II - La Bramadora, la auditoría contempla la magnitud del actual paquete informático (ordenadores de aula, laptops para la oficina, servidores en el lugar, dispositivos de red, etc.) y las formas de uso y metodologías de protección. Lo que se persigue es examinar qué tan seguros son estos elementos tecnológicos frente a riesgos como pueden ser programas maliciosos, entradas no permitidas, pérdida de datos o cortes de servicio educativo. Esto conlleva, por ejemplo, asegurarse de que el software de seguridad (antivirus, firewalls) esté actualizado, las configuraciones de red sean sólidas, las políticas de claves sean adecuadas, haya sistemas de respaldo de datos y los usuarios sepan de prácticas de ciberseguridad. Al hacer esta auditoría, se usa un procedimiento ordenado y estricto, de acuerdo con normas y marcos del sector. Las investigaciones recientes destacan el beneficio de usar marcos internacionales en auditorías informáticas -como COBIT para gobierno de tecnología o MAGERIT para manejo de riesgos - porque su integración mejora el sistema y protección de las tecnologías, reduce peligros y aseguran la duración de las infraestructuras informáticas (Minaya et al., 2024).

1.3 Ubicación y contextualización de la problemática

La Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora se localiza en la provincia ecuatoriana de Manabí (El Carmen), en un espacio de tipo rural. Una escuela de extensión misional de Fe y Alegría, que acoge alumnos y alumnas de la comunidad educativa La Bramadora. En estos años, este centro escolar ha comenzado a incorporar, además, recursos informáticos tanto en sus procesos pedagógicos como en los administrativos: cuenta con un alumnado donde hay un aula de computación, y en la administración académica un equipo de oficina y probablemente también conectividad para facilitar la información, así como tener contactos con plataformas institucionales educativas. Esta integración tecnológica ha actualizado

las prácticas educativas, pero también ha abierto nuevas puertas a desafíos de seguridad de la información.

Al contextualizar la problemática, desde luego, hay que tener en cuenta las especificidades de este contexto educativo. Por ser una institución rural y de propósito, puede que no cuente con muchos fondos económicos y técnicos para invertir en seguridad. Por lo general, en los centros educativos de esta clase no existe una unidad de TI y el apoyo lo dan docentes o especialistas que también tienen otras responsabilidades. Esto significa que cosas importantes como actualizar software, aplicar parches de seguridad o configurar equipos de red o cuentas de usuario no siempre reciben la atención necesaria. Pero también la falta de capacitación del personal en ciberseguridad y la ausencia de políticas formales de seguridad TI incrementan la superficie de ataque.

Algunos estudios indican que el área de educación tiene características que hacen más fácil ser afectado por amenazas en internet. Entre estas se halla la gran cantidad de personas con diferentes niveles de conocimiento: alumnas, alumnos, profesoras, profesores y directoras y directores de las comunicaciones escolares; incluso están también la variability dispositivos que se conectan, muchas veces propios y vulnerables (Revista 360º, 2025). En la escuela Juan Pablo II es habitual que tanto alumnas y alumnos como profesoras y profesores utilicen ordenadores de laboratorio o sus memorias USB o dispositivos en las instalaciones incrementando la superficie de ataque y la oportunidad de incorporar software dañino si no hay ningún tipo de control. Las limitaciones a los recursos económicos frecuentes en la educación pública/misionera hacen que la escuela no tenga medidas sofisticadas de seguridad (p. ej., sistemas de detección de intrusos, filtrado de contenido o seguridad automatizadas) (Revista 360º, 2025).

También afecta el entorno local y su cultura: al ser una escuela religiosa en área rural, puede existir falta de conocimientos sobre riesgo digital. Tal vez hasta ahora no han pasado (por

lo menos no de forma evidente) problemas serios como sustracciones de datos o ataques informáticos, dando una falsa sensación de seguridad. No obstante, la falta de incidentes no quiere decir que el riesgo es bajo; incluso se sabe que muchos ataques digitales en pequeñas escuelas no se notan ni comentan por la falta de mecanismos de vigilancia ((Zambrano, 2024). En resumen, el problema se sitúa en un ambiente en el que la infraestructura y el uso de TIC del colegio Juan Pablo II - La Bramadora han avanzado más rápidamente que sus prácticas de protección y gestión de riesgos, generando una brecha entre las necesidades de seguridad y la capacidad actual de la institución para abordarlas.

1.4 Planteamiento del problema

La situación planteada propone un problema que se convierte en central: la infraestructura tecnológica y los equipos informáticos de la Unidad Educativa Juan Pablo II - La Bramadora tienen un nivel de seguridad desconocido o insuficiente que puede dejarlos expuestos ante amenazas cibernéticas, comprometiendo no sólo la información sino también la continuidad de las actividades educativas. En lo que sigue, se presenta una problematización, origen y estado de aquél.

1.4.1 Problematización

La **pregunta fundamental** que guía esta investigación puede formularse de la siguiente manera: ¿Cómo garantizar la seguridad informática de los equipos de cómputo de la Unidad Educativa Juan Pablo II - La Bramadora frente a las crecientes amenazas y vulnerabilidades detectadas, mediante la realización de una auditoría de seguridad que permita identificar los riesgos y proponer medidas de mitigación efectivas*?* La problematización requiere descomponer esta cuestión en sus dimensiones clave:

La posible presencia de problemas en los sistemas informáticos de la escuela. Estos problemas pueden ser desde fallos técnicos (sistemas y antivirus desactualizados, contraseñas muy fáciles o usadas en muchos sitios, configuraciones malos de WiFi) hasta las partes humanas y procesos (falta de conciencia de seguridad, usuarios sin saber los peligros del phishing o malware, falta de pasos para responder a problemas) La mezcla de estos problemas crea un lugar bueno para incidentes de seguridad. Por ejemplo, si un equipo no tiene los arreglos seguros aplicados, un atacante podría usar una vulnerabilidad conocida para tomar el control; si maestros y estudiantes no están educados en ciberseguridad, ellos podrían caer en un correo malicioso que le toma contraseñas.

Hay un coste que un incidente de seguridad acarrearía en el ámbito de la educación, así como la pérdida o el cambio de datos privados (notas, libros de alumnado, datos administrativos). No sólo pondría en peligro la ley de protección de datos personales, sino que se arriesgaría la confianza de la comunidad del centro escolar. Tambien, el fallo de los sistemas (virus, sabotae, fallas) detendría el flujo de las clases y proceso escolares causando demoras y afectando la calidad de educación. Estudios hechos en instituciones de educación universitaria encontraron que los vacios en ciberseguridad pueden dañar incluso el éxito de tareas escolares y el ánimo de estudiantes; por ejemplo, estudiantes que pierden información escolar o tienen pausas en lugares en líneas sienten ansiedad y trabajan menos (Molina-Granja et al., 2025). Aunque el tamaño una escuela secundaria es menor que el de una universidad, el idea es igual; la inseguridad informática pone en peligro la labor de enseñar.

El problema se basa en que actualmente la unidad educativa no tiene idea de qué tan vulnerable es su infraestructura ante un ataque. No se tiene un diagnóstico ni inventario de riesgos, por lo que la dirección escolar no tiene información para hacer una toma de decisiones en cuanto

a la protección de sus equipos e información. Y esto da paso a otras preguntas más concretas: ¿Cuáles son las vulnerabilidades que pueden ser más críticas en los equipos del colegio?; ¿Qué probabilidades hay de que se produzcan y con qué daños?; ¿Qué soluciones de seguridad deberían priorizarse para proteger la seguridad, la confidencialidad y la disponibilidad de la información escolar? La investigación va dando cuenta de estas preguntas, ya que el primer paso para solucionar una problemática es reconocerla.

A menudo, la problematización se enfoca en mejorar la seguridad de la infraestructura TIC en la escuela superando las barreras entre el estado actual y un estado futuro donde los riesgos están controlados. Hay una responsabilidad ética y legal de proteger los datos personales como información de niños y documentos de la escuela (Morales-Sáenz et al., 2025). Por lo tanto, el problema no es sólo técnico; sino que afecta a asuntos legales (cumplir leyes de protección de datos), administrativos (seguir con un negocio) y sociales (confianza de padres y alumnos en la institución). Este estudio busca resolver este problema mediante una auditoría que diagnostique y establezca las bases para su solución.

1.4.2 Génesis del problema

La génesis del problema se puede atribuir a diversos factores históricos y estructurales de la institución. En primer lugar, la incorporación de tecnología informática a la Unidad Educativa Juan Pablo II - La Bramadora fue un proceso gradual y reactivo, posiblemente provocado por la necesidad de modernizar la educación y los requerimientos administrativos (por ejemplo, informes en línea al Ministerio, uso de software ofimático en el aula, etc.). Pero esta adopción tecnológica no fue acompañada de una planificación de ciberseguridad paralela. Es decir, se priorizó equipar el colegio con computadoras e internet para fines pedagógicos inmediatos, pero no se generaron políticas ni inversiones paralelas para sostener esos activos digitales (Revista 360º, 2025).

Otra causa importante en la génesis es la falta de actualización y mantenimiento preventivo de los sistemas. Tradicionalmente, la escuela no ha tenido personal de planta dedicado a la administración de TI; las actualizaciones de software, cambio de contraseñas, revisión de registros de seguridad, etc., se harían sólo esporádicamente o cuando algo obviamente fallaba (por ejemplo, formatear equipos después de una infección de virus, cambiar alguna configuración después de una falla). Esta actitud reactiva y no proactiva hizo que con el tiempo se fueran acumulando vulnerabilidades sin corregir. De hecho, se sabe que la falta de auditorías periódicas y evaluaciones de riesgos permite que las vulnerabilidades de seguridad persistan hasta que alguien las aprovecha (Zambrano, 2024). En la Unidad Educativa Fiscomisional Juan Pablo II - La Bramadora, nunca se ha realizado una auditoría completa de seguridad informática; por lo tanto, vulnerabilidades que se introdujeron hace años (por ejemplo, equipos con sistemas operativos desactualizados, contraseñas administrativas por defecto) pueden existir hasta el día de hoy.

Además, la misma naturaleza cambiante de las amenazas cibernéticas es parte del origen del problema. Hace 10 años los riesgos para una escuela rural conectada a la red se podrían considerar bajos o reducidos a virus informáticos comunes. De hecho, históricamente el malware tipo virus ha sido la mayor amenaza para las computadoras de pequeñas empresas (Zambrano, 2024). Pero el panorama de amenazas se ha vuelto más complejo: ahora hay ransomware, ataques de phishing dirigidos, robo de datos personales para fraude, por nombrar algunos. Muchos de estos ataques ya ni siquiera se fijan en el tamaño o en el lugar del centro educativo (lo mismo da que sea una gran universidad o un pequeño colegio), cifrando bases de datos críticas. La escuela Juan Pablo II, no posee una preparación inicial para afrontar amenazas avanzadas, sino partiendo de defensas legadas insuficientes para los riesgos de hoy en día.

En síntesis, el problema surge por la diferencia temporal que siempre ha existido entre la adopción de tecnología y la adopción de medidas de seguridad en la institución. Una cultura organizacional poco sensibilizada en ciberseguridad, aunado a restricciones presupuestarias y falta de personal especializado, crearon el ambiente perfecto para que las vulnerabilidades se multiplicaran sin ser resueltas. A esta causa estructural se suma el factor externo: los ciberdelincuentes han ampliado su objetivo hacia el sector educativo, ya que saben que suelen tener pocas defensas (Revista 360º, 2025). Se puede concluir que el problema de inseguridad informática en la Unidad Educativa Juan Pablo II - La Bramadora no es un problema que apareció de la noche a la mañana, sino que es el resultado de años de negligencia y falta de medidas de seguridad en sus sistemas informáticos.

1.4.3 Estado actual del problema

a Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora dispone de un laboratorio de computación equipado con 37 computadoras, destinadas principalmente al desarrollo de actividades académicas y al uso de recursos digitales por parte de los estudiantes. Del total de equipos existentes, 32 computadoras se encuentran operativas y 5 están fuera de funcionamiento, lo que significa que aproximadamente el 86,5% de los equipos está disponible para su utilización, mientras que el 13,5% permanece inoperativo. Esta situación evidencia la necesidad de evaluar no solo las condiciones de seguridad de los equipos en funcionamiento, sino también su estado tecnológico general, mantenimiento, actualización de software y mecanismos de protección.

- Protecciones técnicas insuficientes: Los ordenadores tienen medidas de seguridad básicas, pero insuficientes. Por ejemplo, tal vez sólo algunos tengan antivirus y ni siquiera esté actualizado a las últimas definiciones, haciendo que los equipos sean vulnerables a un malware reciente; probablemente no exista la figura de un firewall perimetral, la red podría

estar protegida por el router doméstico que proporciona el ISP y con la configuración por defecto; también nos falta la figura de los sistemas de monitorización del tráfico o detección de intrusos que avisen de patrones anómalos de tráfico en la red, etc. Esta falta de profundidad de la seguridad tecnológica implica que ante un ataque o un malware que pueda propagarse en la red, hay escasas defensas para detenerlo o, a priori, para descubrirlo rápidamente.

- Vulnerabilidades de software y configuración: Como no existe un plan de gestión de parches, seguramente muchos equipos estarán funcionando con sistemas operativos desactualizados o incluso sin soporte (por ejemplo, PC con versiones antiguas de Windows). Por otro lado, el software instalado (navegadores, suites ofimáticas) puede no estar debidamente actualizado (su instalación puede ser, por ejemplo, tal vez un par de meses atrás, pero no tenemos garantías de que, por ejemplo, se vaya utilizando su versión) y estas vulnerabilidades son conocidas y constituyen puntos de acceso importante para los atacantes. En términos de configuración, puede haber puertos no necesitados abiertos, habrá ejecución de carpetas compartidas en la red local sin contraseña, o conjuntos de cuentas de administrador en los PCs que no incluyan una separativa de privilegios. Cada una de estas malas prácticas provoca que se aumenten las posibilidades de ataque.
- Humano y operativo: El personal docente y administrativo está consciente de la relevancia de la información, pero no ha sido capacitado en seguridad informática. Un estudio similar realizado en otra institución educativa con características similares encontró que la mayoría de los encuestados no habían recibido capacitación periódica en seguridad, lo que indica un área de mejora en la capacitación del personal (Zambrano, 2024). Podemos suponer que en Juan Pablo II - La Bramadora pasa lo mismo: no existen programas de concienciación

sobre cómo generar contraseñas seguras, cómo reconocer correos sospechosos, cómo manipular memorias USB de forma segura, etc. También puede ser que no existan manuales o protocolos definidos para el uso de los recursos TIC por parte de estudiantes y profesores (por ejemplo, políticas de uso aceptable, normas para la instalación de software, restricciones de acceso). Esto trae consigo riesgos como el uso inconsciente de software no autorizado o malicioso, o ser víctima de ataques de ingeniería social por estar poco alerta ante estafas (phishing, fraudes online, etc.) (Revista 360º, 2025).

- Falta de gestión de vulnerabilidades y backups: Hoy en día no se monitorean vulnerabilidades de forma proactiva y no existe un plan de remediación continuo (no hay patch management). Tampoco existe un plan de copias de seguridad: los backups se hacen manualmente y poco frecuentes o dependen de discos locales que pueden perderse o estropearse. De acuerdo con las buenas prácticas, la gestión de vulnerabilidades es un proceso continuo que se debe incorporar en cualquier programa de seguridad maduro para disminuir el riesgo cibernético (Humpiri et al., 2023); la ausencia de este proceso en la institución deja puertas abiertas de manera indefinida.
- Exposiciones de riesgos actuales: Aun cuando no se hayan reconocido públicamente incidentes, existen ciertas señales menores que se relacionan con cuestiones de seguridad. Por ejemplo, no es raro que determinados equipos empiecen a ir lentos o empiecen a tener comportamientos de lo más extraño que puedan hacer pensar que están infectados por un malware. Entrevistas informales han dejado entrever que, con el tiempo han ido llegando hasta los equipos de computación del laboratorio virus, requiriéndose formatear. A pesar de que todos los encuestados se pueden permitir el lujo de decir que no han presenciado

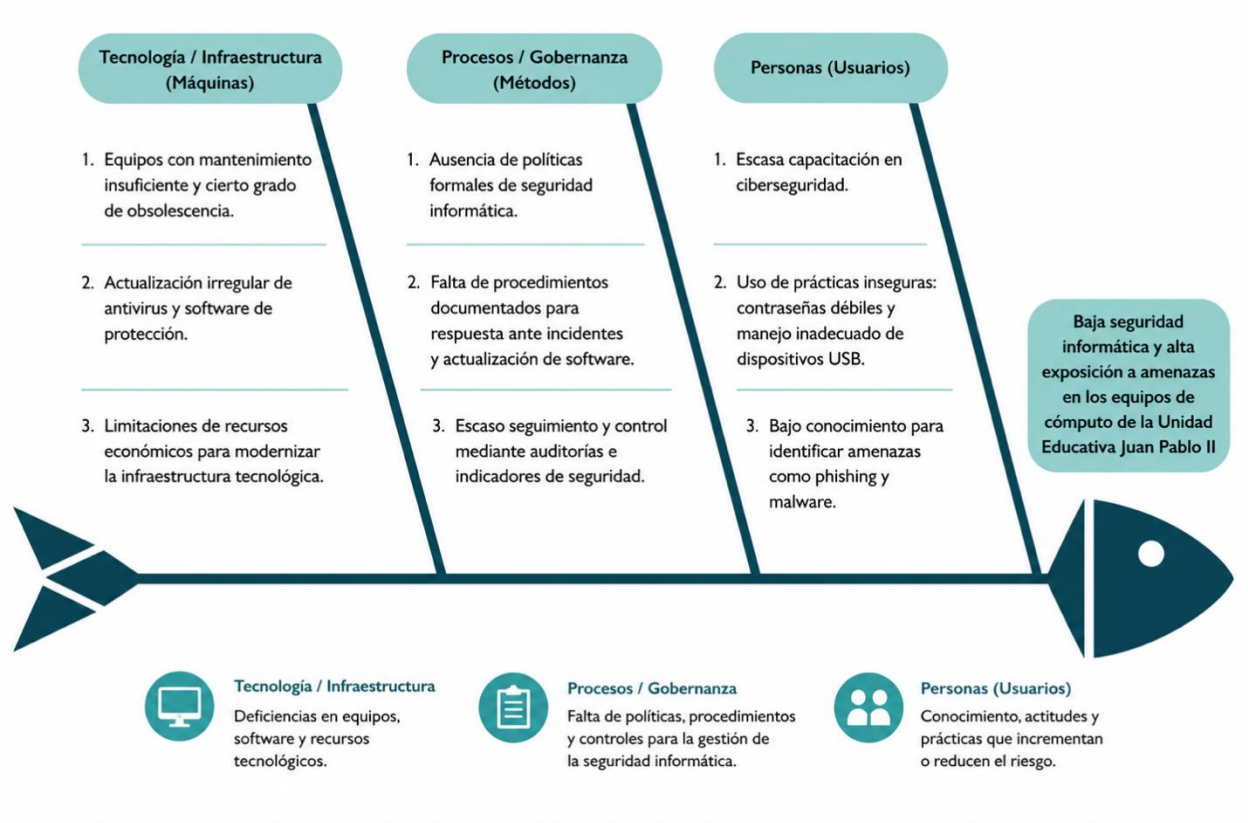
ningún incidente importante (Zambrano, 2024), esto puede referirse a que la falta de problemas sea el reflejo de una falta de percepción.

1.5 Diagrama causa – efecto del problema

Con base a al problema, efectos y causas detallados en secciones anteriores se presenta en la Figura 1 el diagrama causa-efecto:

Figura 1

Diagrama causa-efecto



Fuente: Elaborado por autora por medio del programa Canva

1.6 Objetivos

1.6.1 Objetivo general

Realizar una auditoría de seguridad informática a los equipos informáticos y la infraestructura tecnológica de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora.

1.6.2 Objetivos específicos

- Diagnosticar el estado actual de seguridad informática en la institución, mediante el levantamiento de información y evaluación de los sistemas y equipos de cómputo.
- Identificar las vulnerabilidades presentes en los equipos informáticos y la red de la unidad educativa, considerando aspectos de software, configuración y procedimientos, y evaluar los riesgos tecnológicos asociados mediante la determinación de su probabilidad de ocurrencia y el impacto potencial de posibles incidentes.
- Proponer un plan de mejora en seguridad informática, desarrollando un plan de acciones que incluya medidas técnicas, medidas administrativas y medidas de capacitación.

1.7 Justificación

El avance de este proyecto se justifica por varias razones tanto académicas como institucionales, sociales y tecnológicas. En primer lugar, desde un punto de vista práctico, la Unidad Educativa Juan Pablo II - La Bramadora enfrenta un riesgo claro en la seguridad de sus datos y sistemas, que se ha considerado alto para el sector educativo en general. Varias fuentes indican cuán importante es la ciberseguridad en la formación para proteger la información privada y hacer un espacio seguro para la comunidad estudiantil y profesorado (Morales-Sáenz et al., 2025). Al hacer una revisión de la seguridad informática, la escuela sabrá su estado y podrá actuar de manera adecuada. Si no se efectúa esta asistencia, la escuela estará ciega en temas de seguridad, con el riesgo de tener un evento feo que pare sus clases y muestre datos privados de los niños.

Desde el ámbito académico y científico, el proyecto que se lleva a cabo tiene su justificante de ser generador de conocimiento aplicado en un espacio poco estudiado como es el de la seguridad informática en instituciones educativas básicas rurales. A pesar de que existen diversas investigaciones enfocadas en la ciberseguridad orientada a empresas o universidades, escasean

notablemente los casos de estudio de la seguridad informática en el contexto de los colegios secundarios en la ruralidad. Esta investigación de máster hace que las líneas de investigación sean elevadas a otro nivel de rigor y profundización, de modo que los resultados y recomendaciones que se aportan puedan considerarse como pautas o formas de abordar la temática para otros centros con la misma realidad.

La justificación se sustenta con fuerza en función de los beneficios e impactos esperados. En un lado, a nivel institucional, la vez que se realicen las mejoras post auditoría la unidad educativa estará mucho más protegida, y se reducirá considerablemente la probabilidad de interrupciones por incidentes TI o la pérdida de información. Esto se traduce en eficiencia y disminución de costes en el medio plazo, dado que siempre sale a cuenta prevenir más que curar (en términos económicos y de tiempo). Pero también existe un deber ético y legal: en Ecuador ya es de aplicación la Ley Orgánica de Protección de Datos Personales (2021) y las instituciones que se ocupan de datos personales —como las educativas— tienen el deber de adecuar las medidas de seguridad.

1.8 Impactos esperados

El desarrollo y culminación exitosa de la auditoría de seguridad informática en la Unidad Educativa Juan Pablo II - La Bramadora generará una serie de impactos positivos, que pueden agruparse en tres dimensiones: tecnológica, social y ecológica.

1.8.1 Impacto tecnológico

El efecto de las nuevas tecnologías es mejorar significativa la forma en que se proporciona significativa a la infraestructura de las TIC de una organización. Gracias a las vulnerabilidades que se han encontrado y los pasos que se han dado para mitigarlos, el riesgo de problemas de ciberseguridad disminuirá mucho. En la realidad, los dispositivos serán más seguros contra virus,

malware y entradas no permitidas, lo que ayuda a que los sistemas que se usan para trabajar en clase sean más estables y confiables.

Se prevé también la sanción de la infraestructura de datos y de redes, es probable que las recomendaciones de la auditoría también incluyan la segmentación de la red de la escuela, reforzar la red WiFi con protocolos fuertes, realizar backups externos de forma regular, etcétera. A medio plazo, la escuela también podría introducir nuevas herramientas (por ejemplo, software de monitoreo, software de filtrado de contenido), que no se habían considerado hasta ahora. Es importante mencionar que la evidencia ha demostrado que las instituciones educativas con protocolos definidos y buenas prácticas de ciberseguridad reducen el número de ataques y mejoran la resiliencia de sus comunidades (Jiménez et al., 2025).

Desde la óptica de la gestión de TI, el cambio tecnológico supone establecer una cultura de mejora continua de la seguridad. La auditoría se encargará de establecer la base de un proceso cíclico: de evaluar, de mejoras y de volver a evaluar. La institución escolar establecerá la costumbre de revisar sus sistemas (auditorías internas anuales, seguimiento de alertas, revisión de logs), constituyendo así un gran avance con relación a la situación anterior. En otros términos, técnicamente la escuela pasará de ser reactiva a ser proactiva en la seguridad. De esta forma se apoya la sostenibilidad tecnológica ede futuro ya que los equipos y los sistemas operarán bajo controles que alargarán la vida útil y el rendimiento de los mismos. Por ejemplo, prevenir accidentes severos previene daños lógicos o físicos en los equipos; se ha apuntado que la aplicación de medidas de seguridad refuerza la infraestructura y puede alargar la vida útil de los equipos, disminuyendo la necesidad de reparaciones o sustituciones urgentes (Zambrano, 2024).

1.8.2 Impacto social

El efecto social de este plan se ve en la creacion de un entorno mas seguro y con fiable para la comunidad. A resguardar la informacion academica y personal de estudiantes y maestros, la escuela fortalece la confianza de todo el grupo (alumnos, papas, personal) en el uso de las tecnologías. Los estudiantes pueden usar las computadoras del colegio para hacer tareas, buscar información, y usar plataformas para el estudio con tranquilidad ya que se cuenta con procesos y reglas que protegen su información y privacidad. También, los padres estarán seguros de que la escuela cuida la información de sus hijos.

Además, el proyecto implica acciones de capacitación y sensibilización con impacto social directo: docentes, personal administrativo y estudiantes serán capacitados en seguridad digital y desarrollarán habilidades aplicables más allá de la escuela. Esta mayor conciencia en ciberseguridad capacita a las personas para protegerse también en otros ámbitos (por ejemplo, cuando navegan por internet en casa o en dispositivos móviles personales).

Vale la pena señalar que un ambiente seguro favorece el aprendizaje. Cuando se reducen al máximo las interrupciones técnicas y se salvaguarda la integridad de los materiales de estudio, los estudiantes pueden concentrarse en sus estudios con menos distracciones o preocupaciones. Incluso a nivel psicoeducativo, se ha verificado que la incertidumbre o ansiedad ante fallos tecnológicos habituales perjudica el rendimiento del estudiante (Molina-Granja et al., 2025).

1.8.3 Impacto ecológico

Aunque de manera inicial la conexión entre una auditoría de seguridad informática y el medio ambiente pueda parecer distante, hay impactos ambientales indirectos que resultan de una buena administración de la infraestructura tecnológica. Uno de los principales impactos ambientales que se esperan es la mejora en el uso y la vida útil de los equipos electrónicos. Con

buenas prácticas de seguridad y mantenimiento, los equipos duran más tiempo en funcionamiento antes de quedar obsoletos o inservibles (Zambrano, 2024).

Además, el proyecto promoverá entre sus recomendaciones prácticas como la optimización de recursos y la virtualización de procesos que antes se realizaban en papel. Aunque la seguridad es la principal finalidad, muchas medidas implican también una postura de uso racional de la tecnología. Por ejemplo, al consolidar servidores o migrar a la nube se puede disminuir el número de equipos físicos encendidos todo el día en la escuela, lo que lleva a usar menos energía.

Otro punto de vista ecológico es la conciencia ambiental en la disposición de aparatos. En un plano o política de seguridad integral, lo que suelen incluir la destrucción errónea de datos de los aparatos viejos es la situación de un proyecto que puede incluir guías para que, al renovar el parque tecnológico, la institución se adhiera a los protocolos de una disposición responsable (por ejemplo, donar aparatos que aún funcionan, reciclar piezas, en lugar de lanzarlas a una bolsa de basura). Además, en la literatura la relación entre ciberseguridad y sostenibilidad comienza a ser una men-ción en donde se establece que las organizaciones deben implementar una serie de estrategias que minimicen el impacto ambiental de sus operaciones TI, pero sin sacrificar la seguridad de la información (Rosso, 2023).

En definitiva, sin ser éste su principal objetivo, el proyecto tiene beneficios ambientales indirectos: alargar la vida útil de los equipos (generando menos residuos electrónicos), posible reducción del consumo de papel y energía gracias a sistemas más eficientes, prácticas responsables en el ciclo de vida de los recursos tecnológicos.

CAPÍTULO II

2 MARCO TEÓRICO DE LA INVESTIGACIÓN

2.1 Antecedentes históricos

La auditoría informática es una partida de la auditoría tradicional que evoluciona a medida que los sistema de cómputo se hacen más comunes en las organizaciones. Pero a medida que las organizaciones automatizaron tareas y manejaron data digital, se hizo evidente que la auditoría financiera tradicional no era suficiente para evaluar controles de datos intangible. Por lo tanto se generó la auditoría informática para abarcar todos los elementos del medio informático de una organización (Rodriguez & Calvarado, 2023). En los inicios de la misma, a mediados del siglo XX, las auditorías informáticas se encargaban de revisar los primeros sistemas de procesamiento electrónico de datos. Con el tiempo, su visión se amplió, dejando de ser sólo en la tarea de revisar números, para extenderse a los sistemas informáticos integrales los cuales revisan hardware, software, redes y procedimientos.

Es importante conocer que en el principio la auditoría de tecnología estaba unida a las revisiones de datos internas dentro de las empresas y a los números, porque una de sus primeras metas fue verificar la integridad de los registros informáticos (Ramos et al., 2022). Con más tecnologías de información apareciendo a fines del siglo 20, la auditoría de TI llegó a ser una materia, creando formas especiales para medir la defensa de sistemas informativos (INCIBE, 2023).

Hoy en día, la auditoría de seguridad de información es un sistema que se hace por expertos para notar, escribir y describir sobre vulnerabilidades en los activos tecnológicos (Jiménez et al., 2025). Esta nueva definición muestra cómo pasamos de revisar controles a una gestión proactiva de riesgos informáticos. En la escuela, los procesos de auditoría han cambiado mucho más

despacio que en el banco o gobierno; pero con la digitalización de la educación, los colegios están dándose cuenta de que necesitan revisiones informáticas para proteger la información de los estudiantes, asegurar que todo funcione bien en línea y seguir las reglas sobre privado.

De hecho, las auditorías de seguridad en centros educativos se están volviendo más comunes. A principios del siglo XXI pocas escuelas o universidades auditaban en forma comprensiva sus sistemas. Pero después de algunos incidentes de alto perfil y la proliferación de marcos internacionales de seguridad, los colegios y universidades están comenzando a adoptar auditorías informáticas regulares. Esto se ajusta a la tendencia: la auditoría de TI pasó de ser una práctica opcional a ser una obligatoria para certificar la integridad, confidencialidad y disponibilidad de la información en cualquier tipo de organización, incluyendo las educativas (Guaña-Moya, 2023).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

En los últimos años se han realizado diversas investigaciones sobre auditorías de seguridad informática. A continuación, se resumen cinco estudios recientes, priorizando el ámbito educativo y complementando con otros contextos relevantes, indicando para cada uno autor, año, título, objetivo, metodología, resultados y conclusiones principales:

Paladines Chuez (2023) – *"Auditoría de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre (periodo 2022)"*. Objetivo: Verificar el grado de acatamiento de normativas de seguridad informática en la infraestructura tecnológica de una institución educativa. Enfoque: estudio de caso de un enfoque mixto. Se realizó un diagnóstico institucional basado en la integración de cuestionarios y entrevistas a 18 profesorado y directivos en la elaboración de un diagnóstico institucional y de una auditoría técnica con la metodología MAGERIT de análisis de riesgo. Resultados: el grado de seguridad general fue

deficiente (43%). Se encontraron vulnerabilidades muy elevadas, así como un alto riesgo de robo de información (95%) y de infección por malware (83%), y se detectaron deficiencias frente a amenazas físicas (de robos, incendios, daños de aparatos), aunque con menor probabilidad. Conclusiones: La institución carecía de medidas sólidas de protección; se elaboró un informe de auditoría con una guía de recomendaciones para mitigar los riesgos detectados, enfatizando la necesidad de mejorar políticas de seguridad y actualizar controles.

Zhuño et al., (2022) – *"Auditoría informática a centros de estudios. Caso U.E. 'Nuestra Señora de Fátima'"*. Objetivo: Verificar el desempeño del equipamiento informático y el cumplimiento de las normas de TI en una escuela particular. Metodología: Auditoría informática integral con una aproximación técnico-administrativa; se revisaron componentes de hardware, de software y de redes, comprobándose la legalidad de los programas instalados en los equipos de cómputo. No existía un manual de auditoría informática, así que el proyecto elaboró una pauta para evaluar la situación del centro de computación y el entorno digital en el que desarrollan su actividad el profesorado y el estudiantado. Resultados: Se identificó la falta de políticas y procedimientos formales de control informático en la institución, así como de software pirata y un uso poco eficiente de los recursos tecnológicos. Conclusiones: El estudio resaltó la necesidad de implantar un manual de auditoría informática y mejorar la gestión de TI en la escuela, proponiendo recomendaciones para un mejor control del hardware, las redes y el personal técnico, a fin de crear un entorno computacional más seguro y acorde a las necesidades educativas.

Ramos et al., (2022) – "Auditoría informática para determinar las falencias del centro de cómputo de la U.E. Miguel Ángel León Pontón". Objetivo: Identificar las disfunciones que se presentan en las instalaciones, en los sistemas de cómputo y en el sistema de calificaciones de un centro de educación, a partir de lo cual se busca también la mejora en el uso de los recursos que

tiene a su disposición ese centro. Metodología: Método cualitativo-descriptivo. A partir de entrevistas realizadas a la persona responsable de llevar el laboratorio y a los estudiantes, observaciones directas en las instalaciones del centro de cómputo, aplicación de cuestionarios, y revisión de documentos técnicos (revisión de auditorías previas). La auditoría también consideró el rendimiento de las máquinas, así como la aplicación de algunos de sus reglamentos internos de TI. Resultados: Se detectó un conjunto de debilidades operativas y, posiblemente la más importante, la sobrecarga de los equipos provocaba lentitud e inconvenientes a la hora de llevar a cabo las tareas académicas. Por otra parte, se recibió información de que la infraestructura tecnológica instalada no era la correcta para albergar al software de gestión de calificaciones. Conclusiones: Se planteó entre las autoridades de la unidad educativa la posibilidad de equipar de nuevo a los equipos obsoletos a fin de que la experiencia de aprendizaje de los estudiantes mejorará.

Imbaquingo et al., (2020) – *"Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de la literatura"*. Objetivo: Definir aquellos impedimentos que existen en auditorías de IT de nivel internacional a partir de una revisión sistemática de investigaciones. Metodología: Revisión de literatura con un gran volumen de trabajos sobre la temática de problemas y relevancia de la auditoría informática. Resultados: Las dificultades principales para poner en práctica auditorías informáticas detectadas fueron (1) los elevados costes para auditorías exhaustivas, (2) los resultados obtenidos no son satisfactorios para el usuario final y (3) resultados desfavorables para la organización auditada. Conclusiones: Se estableció que incluso ante elevados costes o hallazgos desagradables. Las auditorías son necesarias para preservar los datos y aprender de las debilidades detectadas, aumentado la confianza en los sistemas auditados.

Rodríguez et al., (2023) – *"Frameworks utilizados para la auditoría de tecnologías de la información en las universidades"*. Objetivo: Identificar los frameworks que son más comunes en auditorías de TI en instituciones de educación superior, se realizó una revisión de publicaciones académicas con el periodo de tiempo de 2018 a 2022. Metodologías: Revisión sistemática de literatura. Resultados: Durante el periodo analizado se pudo verificar el predominio del framework COBIT 5 como el más utilizado para llevar a cabo las auditorías de TI en universidades, muy por encima de los demás frameworks. En segunda posición se encuentran prácticas sustentadas en ITIL v3, seguido de la adopción más reciente de COBIT 2019. Conclusiones: Las universidades suelen apegarse a los frameworks de gobernanza de TI consolidados para realizar sus auditorías, probablemente porque proporcionan una visión integral de todos los controles y procesos.. Sin embargo, el estudio sugiere que estándares especializados en seguridad podrían tener más cabida al presentarse una preocupación creciente por los riesgos cibernéticos en los entornos académicos.

2.1 Auditoría de Seguridad Informática

El control de la seguridad informática es un proceso completo que mira el nivel de protección de los sistemas de información de una empresa, analizando sus métodos, estructura y ajustes, y revisando si cumplen con las reglas de seguridad (Gómez, 2022). Su objetivo es hallar debilidades y fallos de seguridad que pueden ser usados por los atacantes, para proponer soluciones antes de que ocurran incidentes (Gómez, 2022).

En otras palabras, la auditoría de seguridad informática es el proceso exhaustivo de evaluación y control del sistema realizado por expertos, que permite poner de relieve y documentar todas aquellas vulnerabilidades que se hallan en redes de ordenadores, servidores, estaciones de trabajo, dispositivos o demás tecnologías del entorno (Tejada, 2023). El resultado de la auditoría se registra y se proporciona a los responsables, los cuales deberían analizar el resultado para

establecer las medidas correctivas y preventivas que tienen que realizarse en función de las recomendaciones.

2.2 Tipologías de auditorías de seguridad informática

Las auditorías de seguridad informática se pueden clasificar según su objetivo y su alcance; de las que existen, se presentan algunas de las más habituales (Ambit Iberia, 2021):

2.2.1 Auditorías internas vs. Externas

Las auditorías dentro de la empresa son hechas por personal de la misma compañía, y las subcontratadas son hechas por alguien ajeno. Las internas aportan conocimiento de la realidad local, pero pueden carecer de objetividad.

2.2.2 Auditorías técnicas o de infraestructura

Son revisiones que se concentran en secciones concretas de TI. Por ejemplo, exámenes de seguridad de límites de comunicación de la organización o auditorías de aplicaciones web, buscando fallas en los sitios o sistemas por internet. También entran aquí las pruebas de intrusión donde el examinador imita ataques reales para ver lo fuerte que son los sistemas ante accesos no permitidos. Los exámenes de cumplimiento normativo también son auditorías técnicas y verifican si los sistemas cumplen con normas o marcos dados.

2.2.3 Auditorías operativas o por objetivos

Se clasifican de acuerdo al objetivo que persiguen. Por ejemplo, auditorías forenses, auditorías de configuración y hardening, auditorías de eficacia de controles, etc. Estas revisiones pueden superponerse a las anteriores, pero tienden a abordar cuestiones específicas.

2.3 Principios, normas y marcos de referencia

La auditoría de seguridad informática se basa en estándares y mejores prácticas internacionales. Entre sus ideas principales están la objetividad, la evidencia, la confidencialidad y la periodicidad.

Para una auditoría hay patrones y marcos muy reconocidos. Algunos marcos, como por ejemplo ISO/IEC 27000 (familia de normas sobre cómo gestionar la seguridad de la información), COBIT (gestión y control de tecnologías), ITIL (gestión de los servicios técnicos), entre otros, se utilizan como pautas para lograr auditorías aceptables (Navia y Zambrano-Romero, 2021). Dichos marcos ofrecen patrones y chequeos para comprobar el estado de la empresa auditada. ISO/IEC 27001:2022, por ejemplo, expresa lo que se desea para poder llevar a cabo un Sistema de Gestión de Seguridad de la Información (SGSI); en una auditoría se comprueba el grado de cumplimiento con esos requerimientos.

En otro lado, COBIT 5 y COBIT 2019 son formas de manejar procesos de TI que tienen metas de seguridad y auditoría; de verdad, como se dijo en la parte anterior, COBIT ha sido uno de los métodos más usados en auditorías de TI universitarias hace poco (Rodríguez y otros, 2023). También, agencias como NIST dan manuales técnicos como el Formato de Ciberseguridad del NIST o la colección especial 800, que pueden ayudar a dar forma a las revisiones, porque explican qué controles se deben usar en áreas como gestión de identidades, protección de redes, respuesta a incidentes, etc.

En el ámbito académico, por ejemplo, se pueden mezclar estándares: ISO 27001/27002 para controles de seguridad específicos, COBIT para medir la gobernanza de TI institucional y marcos de NIST para pruebas técnicas específicas. Existen también marcos de trabajo abiertos guiados a pruebas de seguridad, uno de los cuales, OSSTMM, ha sido utilizado en investigación para conformar auditorías técnicas profundas exhaustivas (Navia & Zambrano-Romero, 2021). La

diversidad de estos marcos pone de manifiesto que la auditoría de las seguridad informática no es un proceso singular, sino que de ella se deriva una colección de prácticas guiadas por marcos de referencia mundiales para asegurar la constancia y el rigor de dicha evaluación.

2.4 Fases de una Auditoría Informática

Típicamente, una auditoría de seguridad de TI se desarrolla en fases o etapas secuenciales bien definidas. De acuerdo con la literatura estándar, las etapas de una auditoría informática comprenden:

2.4.1 Planificación y recopilación de información

Se decide cuáles partes de la auditoría serán revisadas y se recoge información antes de empezar. Esto trata de saber la arquitectura de la red, el inventario de activos, las reglas actuales y cualquier información del contexto que pueda ayudar a guiar el trabajo (Morales-Sáenz et al., 2025).

2.4.2 Análisis del entorno y control interno

Se necesita hacer una lista de redes, topologías y reglas, y analizar cómo es el control interno de la organización para aparatos tecnológicos. También aquí es común ver si se cumplen las reglas internacionales que son obligatorias (Molina-Granja et al., 2025)–por ejemplo, verificando si la empresa cuenta con la certificación ISO 27001 en vigor o si cumple con la normativa nacional de protección de datos.

2.4.3 Identificación de activos y software

Inventariar los sistemas operativos, aplicaciones y servicios que se utilizan (Montalvo & Quishpe, 2024). Estos datos son muy importantes para establecer los puntos débiles ya conocidas de esas plataformas. Se encuentran versiones del software, grado de parche, configuraciones importantes, usuarios con sus permisos y otros detalles.

2.4.4 Análisis y pruebas de vulnerabilidades

Es lo más importante de la parte técnica de la auditoría. Se trata de encontrar, comprobar y valorar fallos de seguridad en los sistemas (Rodríguez et al., 2023). Se pueden usar herramientas automáticas (scanners de puertos, analizadores de vulnerabilidades, scripts) y pruebas hechas a mano. Aquí entran en juego métodos como ética hacking, pruebas de penetración controladas, revisar configuraciones seguras, etc.

- Registro de hallazgos: El auditor apunta detalladamente cada hallazgo de puntos débiles o áreas para mejorar con pruebas sólidas y una explicación. Se puede usar una matriz de peligro para clasificar la criticidad da cada falla de seguridad.
- Informe de auditoría: Cuando terminan las pruebas, se crea un informe que muestra la seguridad de los bienes revisados durante la evaluación (Imbaquingo et al., 2020). Este informe suele tener alcances y formas, hallazgos con análisis (¿que se halló?, ¿cómo? ¿qué peligro tiene?), resultados amplios y varias con sugerencias claras (Paladines Chuez, 2023).
- Retroalimentación y seguimiento: Una vez dado el documento, el jefe a cargo de la organización tiene que mirar los resultados con el grupo auditor, hacer un esquema para solucionar las deficiencias y darle seguimiento.

2.5 Vulnerabilidades frecuentes Equipos Informáticos en Unidades Educativas

Estudios muestran que varias escuelas tienen problemas grandes de seguridad en sus sistemas. Un informe de seguridad en línea de escuelas, en España de 2020, dio a conocer que el 100% de los colegios revisados tenían debilidades importantes en sus ordenadores (Gaptain, 2021). Los principales motivos hallados fueron: (a) no tener suficientes recursos de tecnología, ni personal capacitado ni equipo actualizado; (b) ajustes inseguras en los sistemas (como redes

inalámbricas abiertas o mal protegidas, servidores sin endurencer); y (c) falta de profesionales en seguridad informática y revisiones régulares que aseguren un buen cuidado de la defensa (Gaptain, 2021).

Por otro lado, una vulnerabilidad típica son las políticas débiles o la indefinición de políticas. Si se contempla que no existen políticas de contraseñas, uso aceptable de Internet, control de software, copias de seguridad, etc., se genera un entorno para incidentes (Solís et al., 2023). Ésto es especialmente alarmante en las escuelas, donde casi no existen departamentos de TI y las políticas de seguridad son igual de débiles. Permitir que estudiantes o profesores instalen software libremente en los ordenadores, o que todos compartan la misma cuenta de usuario son prácticas que violan los principios básicos de seguridad.

En cuanto a los sistemas y equipos concretos, las vulnerabilidades comúnmente encontradas suelen ser: software desactualizado (softwares antiguos sin un parche de actualización), puertos abiertos o servicios innecesarios que se están ejecutando en los servidores o PCs del laboratorio (INCIBE, 2023).

2.6 Riesgos tecnológicos en el ámbito escolar

Las vulnerabilidades mencionadas se traducen en riesgos concretos. Entre los riesgos tecnológicos principales que enfrentan los equipos informáticos de unidades educativas están:

- Robo o fuga de información confidencial: Los colegios guardan información personal de alumnos (nombres, notas, expedientes) y profesores que puede ser robada por ciberdelincuentes. Con protecciones inadecuadas, es vulnerable a accesos no autorizados y fuga de estos datos. Un estudio publicado por Gaptain (2021) ya advertía de que la escasa ciberseguridad que existe en los colegios puede ser un riesgo para el robo de datos e incluso para la vulneración de la privacidad de alumnos y familias.

- Ataques de ransomware y el secuestro de sistemas. Este riesgo se ha ampliado a nivel global en la educación. Un atacante podría tomar medidas para encriptar los archivos de la escuela (las bases de datos de notas, los archivos administrativos) y pedir un rescate para restaurarlos. La falta de segmentación de la red o de backups confiables exacerba este riesgo. En 2022 se casi ha duplicado el número de escuelas atacadas por ransomware en todo el mundo en comparación con el año anterior, lo que demuestra que esta amenaza está en aumento (CYREBRO, 2024). Evidentemente, los centros que tienen redes poco seguras y usuarios sin capacitación son los objetivos más fáciles para este tipo de ataques.
- Interrupción de las actividades escolares: Un riesgo tecnológico siempre presente es que una falla de seguridad o incidente deje inoperativos los equipos o la plataforma virtual de clases. Por ejemplo, un virus propagado por la red puede inutilizar todos los ordenadores del laboratorio, o un ataque DDoS al sitio web del colegio puede cortar las comunicaciones.
- Maltrato y exposición a material inapropiado: Si en los equipos escolares no existen filtros de contenido o controles parentales, los alumnos se enfrentan a riesgos online. Esto se adentra en el terreno de la convivencia digital más que en el de la seguridad informática, pero es un punto: la seguridad informática educativa también es proteger a los menores de ciertos riesgos en línea.

2.7 Políticas de Seguridad Informática en Instituciones Educativas

Las políticas de seguridad son normas oficiales que definen cómo proteger la información y cómo deben actuar los usuarios con la tecnología (Molina-Granja et al., 2025). En los centros educativos a menudo fallan las políticas claras de seguridad informática. Muchos centros educativos no cuentan con políticas escritas sobre, por ejemplo, uso aceptable de Internet, restricciones de software, políticas de contraseñas, copias de seguridad regulares o respuesta a

incidentes de seguridad. La falta de estas directrices ya es una vulnerabilidad en sí misma (Solís et al., 2023). Cuando existen políticas, otro problema común es el incumplimiento por desconocimiento. Puede existir un reglamento de laboratorio de informática, pero si ni maestros ni alumnos lo conocen y lo aplican, de nada sirve. Por eso no es suficiente con generar políticas, hay que socializarlas, capacitar (Revista 360º, 2025).

Entre las políticas que todo centro educativo debe establecer se encuentran: política de contraseñas (complejidad mínima y cambio periódico, en especial para accesos administrativos), política de actualización de sistemas, política de backup, política de uso de dispositivos, política de seguridad física del hardware y política de respuesta a incidentes.

Un problema identificado en la literatura es que las autoridades educativas no siempre le dan la importancia que merecen a estas políticas. Calquier tipo de organización, incluyendo las universidades, se debería de preocupar por generar políticas explícitas, precisas y adaptadas a su contexto con el fin de salvaguardar sus sistemas (Montalvo & Quishpe, 2024). Un buen diseño de políticas trae beneficios inmediatos: disminuye la improvisación, define responsabilidades y crea una cultura de prevención. Desafortunadamente, muchas escuelas apenas han comenzado en los últimos años a codificar dichas políticas impulsadas por requisitos legales (protección de datos personales, por ejemplo) o después de incidentes de llamada de atención. No basta con establecer políticas, hay que velar por su cumplimiento y actualizarlas. Aquí es donde la auditoría vuelve a entrar en escena: una auditoría informática puede verificar con regularidad si las políticas de seguridad de la escuela se están implementando correctamente y si siguen siendo efectivas ante las nuevas amenazas.

Para finalizar, la protección de los sistemas informáticos en entornos educativos depende de políticas políticas robustas y de una correcta gestión de riesgos; sin políticas, la tecnología

queda expuesta a un uso no controlado; con políticas mal definidas o incumplidas, la protección se convierte en pura apariencia, pseudo-protección; la intersección generada por las vulnerabilidades técnicas y los errores humanos es el cuadro de situación que describe la actual ciberseguridad escolar y que debe ser tratado como cuestión prioritaria para proteger la información y la comunidad escolar.

2.8 Conclusiones relacionadas al marco teórico en referencia al tema planteado.

A modo de cierre de este marco teórico, se realiza una síntesis crítica de los conceptos e investigaciones revisadas, conectándolos con el objeto de estudio de la tesis:

La auditoría de seguridad informática se ha convertido en una práctica esencial para proteger los activos digitales de las organizaciones en la actualidad. Su historia nos muestra cómo han ido evolucionando desde simples controles contables hasta una gestión integral de riesgos tecnológicos. En el ámbito educativo, a pesar de que su incorporación es más reciente, cada vez existe mayor conciencia de que los centros educativos necesitan auditorías TI para afrontar el mundo digital. Varios autores señalan que la seguridad informática es ya una necesidad en la educación digital, con el desarrollo de soluciones integrales que impliquen el uso de estándares internacionales, mejores prácticas, análisis de riesgos y capacitación a los usuarios (Guaña-Moya, 2023). Dicho de otra manera, lograr que el entorno de aprendizaje sea seguro tecnológicamente entendido como un hecho de la calidad y resiliencia de los actuales sistemas educativos.

Los antecedentes revisados muestran puntos en común. De una parte se confirma que las auditorías realizadas en centros educativos muestran con frecuencia deficiencias severas desde el punto de vista de configuraciones inseguras o de ausencia de políticas que les expone a riesgos. La falta de recursos especializados y de cultura de seguridad es una característica común. De otra parte, estos estudios muestran un conjunto de metodologías y frameworks aplicables: por ejemplo,

los estudios presentan el uso de metodologías del análisis de riesgos o la referencia a normas como la ISO 27001 y frameworks como COBIT para estructurar la auditoría.

En particular, para la Unidad Educativa Juan Pablo II “La Bramadora”, el marco teórico plantea algunos nudos críticos a resolver: Las vulnerabilidades típicas en los colegios probablemente existan si nunca se ha hecho un diagnóstico. A su vez, los riesgos de robo de información, malware o interrupción de clases son concretos y pueden generar graves consecuencias. La literatura existente ya los advierte: investigaciones como la de Gaptain (2021) determinan que la combinación de defensas técnicas débiles y falta de capacitación de usuarios deja a las escuelas muy expuestas, por lo que es necesario actuar.

En el plano prescriptivo, en primer lugar, el marco conceptual insiste en que una auditoría de seguridad de este contexto en el que vemos información y comunicación, tecnología, red e Internet debería cubrir: evaluar el aspecto técnico más profundo posible + revisar políticas + realizar una formación en ciberseguridad. Abordando todos ellos se consigue una mejora sostenible (Rodríguez et al., 2023). Por cierto, ya hay propuesta, ya hay conocimiento orientador de la intervención a realizar: por ejemplo, la implementación de estándares que ya están recogidos (ISO/NIST) se la plantea como solución que es necesaria en ciertos estudios (Rodríguez et al., 2023), o la elaboración de unos manuales internos de auditoría para escuelas es recomendada (Zhuño et al., 2022).

2.9 Fundamentación teórica de la Metodología Integral de Auditoría y Gestión de Riesgos de Seguridad Informática (MIAGRSI)

Para el desarrollo de la propuesta se adopta la Metodología Integral de Auditoría y Gestión de Riesgos de Seguridad Informática (MIAGRSI), estructurada específicamente para orientar el proceso de evaluación de la infraestructura tecnológica de la Unidad Educativa Fisco Misional

Juan Pablo II – La Bramadora. La metodología integra principios de auditoría informática y gestión de riesgos, tomando como sustento los aportes de Gómez (2022), Humpiri et al. (2023) y Minaya et al. (2024), y organiza el proceso desde la planificación y levantamiento de información hasta la valoración de riesgos y formulación de medidas de tratamiento.

De acuerdo con Gómez (2022), la auditoría de seguridad informática constituye un proceso sistemático de evaluación mediante el cual se analiza el estado de los sistemas de información, los controles implementados y las posibles debilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Desde esta perspectiva, la auditoría permite obtener evidencias sobre las condiciones reales de seguridad de una organización y, a partir de los hallazgos encontrados, formular recomendaciones destinadas al fortalecimiento de sus controles.

Asimismo, Minaya et al. (2024) señalan que la auditoría informática puede apoyarse en metodologías y marcos especializados, entre ellos COBIT y MAGERIT, que permiten estructurar tanto la evaluación de los recursos tecnológicos como el proceso de identificación, análisis y tratamiento de los riesgos. Particularmente, el enfoque de gestión de riesgos resulta pertinente para este proyecto porque posibilita relacionar cada amenaza y vulnerabilidad identificada con su probabilidad de ocurrencia y con las consecuencias que podría generar sobre los activos tecnológicos de la institución.

En concordancia con lo anterior, Humpiri et al. (2023) destacan que la identificación y evaluación de vulnerabilidades constituye un componente fundamental de la seguridad cibernética, puesto que permite reconocer debilidades presentes en los activos digitales antes de que sean aprovechadas por una amenaza. Por esta razón, una evaluación de seguridad debe considerar no únicamente vulnerabilidades técnicas relacionadas con software desactualizado o configuraciones

incorrectas, sino también aquellas asociadas con procedimientos, controles y prácticas humanas que pueden incrementar la exposición al riesgo.

Para el contexto educativo, esta metodología adquiere especial relevancia debido a que las instituciones administran equipos, redes y datos utilizados permanentemente por estudiantes, docentes y personal administrativo. Zambrano (2024)evidencia la necesidad de implementar procesos de gestión de seguridad de la información en laboratorios de computación de instituciones educativas, considerando la identificación de activos, amenazas, vulnerabilidades y riesgos como elementos necesarios para establecer controles y medidas de protección acordes con las características del entorno institucional.

Con base en estos fundamentos, la metodología adoptada para la propuesta se desarrolla mediante una secuencia estructurada de auditoría y análisis de riesgos, integrada por las siguientes etapas: planificación de la auditoría, levantamiento de información, inventario y clasificación de activos, análisis del contexto, identificación de amenazas y vulnerabilidades, análisis de los riesgos, determinación de su impacto y probabilidad, valoración y priorización mediante una matriz de riesgos y, finalmente, formulación de medidas de tratamiento y mejora.

La elección de esta metodología responde directamente al propósito de la investigación, ya que permite transformar la información recopilada durante la auditoría en un diagnóstico técnico y posteriormente en decisiones de mejora. En consecuencia, los hallazgos no son considerados de manera aislada, sino que son analizados según el riesgo que representan para la institución, permitiendo priorizar aquellos que requieren una intervención inmediata y establecer acciones correctivas, preventivas y de capacitación.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

En este capítulo se explica el tipo de metodología utilizada para realizar la auditoría de seguridad informática en los equipos de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora, especificando los tipos de investigación y los métodos de investigación que se utilizaron para resolver el problema; además, se identificaron las fuentes de información de datos primarias y secundarias utilizadas en la investigación.

3.2 Tipos de Investigación

3.2.1 Investigación Documental

Para llevar a cabo la presente investigación ha sido necesario realizar una búsqueda exhaustiva de varias fuentes documentales como libros, artículos científicos, trabajos de titulación y tesis relacionados con la temática de la seguridad informática y la educación. Según Hernández-Sampieri (2017), la la investigación documental consiste en un proceso sistemático que tiene como propósito acceder a una serie de fuentes de información y su recopilación y organización.

3.2.2 Investigación de Campo

La investigación de campo permite recoger datos reales y de primera mano. El investigador fue a la Unidad Educativa Juan Pablo II – La Bramadora para recoletar datos clave.

3.2.3 Investigación Aplicada

Según Navia y Zambrano-Romero (2021), la investigación aplicada se orienta a la resolución real de la problemática, buscando generar un impacto directo mediante la utilización del conocimiento científico y técnico, priorizando la utilidad y aplicabilidad de los resultados para mejorar los procesos. Este enfoque se adoptó en el presente proyecto dado que el objetivo no es

únicamente estudiar o describir la situación de seguridad informática, sino proponer e implementar medidas concretas.

3.3 Métodos de Investigación

3.3.1 Método Mixto

El método de investigación adoptado es de enfoque mixto, el cual integra tanto el enfoque cuantitativo como el cualitativo en un mismo estudio En opinión de Hernández-Sampieri (2017), la combinación de métodos cuantitativos y cualitativos permite completar los datos cuantitativos con los datos cualitativos hallados, complementando así los primeros a partir de los segundos, de manera que permite una visión más completa del fenómeno que se investiga.

3.3.2 Método Deductivo

En la investigación se emplea también el método deductivo, el cual –según Hernández-Sampieri (2017) – consiste en aplicar principios o leyes generales a situaciones particulares, siendo un enfoque sistemático que permite derivar conocimientos específicos mediante procesos lógicos.

3.3.3 Método Analítico – Sintético

También se aplicó el método analítico-sintético, el cual combina dos etapas complementarias del pensamiento científico. Este método consiste, primero, en descomponer el problema en sus componentes básicos para comprenderlo mejor y, luego, en integrar esos elementos estudiados en una visión unificada que permita ofrecer soluciones coherentes al problema original.

3.4 Fuentes de Información de Datos

3.4.1 Fuente Primaria

La principal fuente de información de esta investigación la constituyen los datos recogidos directamente en la institución a través de la técnica de encuesta a los estudiantes, siendo una técnica

muy útil cuando necesitamos recoger información de un gran número de personas sobre sus opiniones, conocimientos o percepciones sobre un tema determinado. En este caso, se elaboró y aplicó una encuesta presencial a los estudiantes de la Unidad Educativa Juan Pablo II – La Bramadora, con preguntas cerradas tipo escala Likert, la cual fue aplicada en horario de clases con autorización de las autoridades institucionales.

3.4.2 Fuente Secundaria

Como fuente secundaria de información, se empleó la técnica de entrevista dirigida al personal de la institución. Según Sánchez & Hernández (2024), esta técnica propicia un entendimiento más rico del fenómeno de estudio al posibilitar que los participantes expresen con sus propias palabras sus vivencias y puntos de vista, algo particularmente valioso en temas institucionales donde las percepciones y experiencias individuales pueden variar ampliamente.

3.5 Estrategia Operacional para la Recolección de Datos

3.5.1 Población y muestra

La población objeto de estudio estuvo constituida por 50 miembros de la comunidad educativa de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora, vinculados con el uso y gestión de los recursos informáticos de la institución. Debido al reducido tamaño de la población, no se aplicó un procedimiento de muestreo, sino que se consideró la totalidad de sus integrantes, mediante un censo poblacional.

La población estuvo distribuida en 45 estudiantes pertenecientes a primero, segundo y tercero de Bachillerato, quienes hacen uso regular del laboratorio de cómputo y otros recursos tecnológicos de la institución, y 5 miembros del personal docente y administrativo.

Por tanto, la población total del estudio fue de 50 participantes.

3.6 Análisis de las herramientas para la recolección de datos

3.6.1 Encuesta

Para la recolección de datos cuantitativos se elaboró un cuestionario estructurado de 10 preguntas cerradas tipo Likert dirigido a los estudiantes, para medir sus conocimientos y percepciones sobre seguridad informática y sus prácticas de uso de dispositivos tecnológicos y riesgos informáticos en la institución. El cuestionario fue validado previamente en una prueba piloto con uno o dos estudiantes y el tutor del proyecto para asegurar la comprensión de las preguntas y escalas utilizadas.

3.6.2 Entrevista

La entrevista se realizó con la persona encargada de la gestión de equipos y tecnología en la institución y además con personal administrativo que conozca los procesos de la institución, cubriendo así la perspectiva técnico-operativa y la perspectiva de gestión institucional. El carácter semiestructurado de la entrevista implicó que, aunque se contaba con un guion de preguntas previamente definido, el entrevistador pudo ahondar en temas emergentes o solicitar aclaraciones según las respuestas del entrevistado, garantizando así una conversación fluida pero enfocada en los temas de interés..

3.7 Estructura de los instrumentos de recolección de datos aplicados

Encuesta (para estudiantes): *Se empleó una escala Likert de cinco puntos, desde 1 (Totalmente en desacuerdo) hasta 5 (Totalmente de acuerdo):*

- **a)** "Estoy familiarizado con las políticas o normas de seguridad informática de la institución."
- **b)** "Soy capaz de identificar un correo electrónico sospechoso o intento de *phishing*."
- **c)** "Utilizo contraseñas seguras (combinación de letras, números, símbolos) y las cambio periódicamente."

d) “Considero que el laboratorio de computación de la institución cuenta con medidas de seguridad adecuadas.”

e) “He recibido capacitación o charlas sobre ciberseguridad en la institución.”

f) “En ocasiones comparto mis contraseñas o cuentas con compañeros de clase.”

g) “Conozco los riesgos de conectar dispositivos USB desconocidos o externos a las computadoras de la escuela.”

h) “Los programas y sistemas de las computadoras de la institución se mantienen actualizados y protegidos contra virus.”

i) “Me siento seguro/a al utilizar las computadoras e Internet de la institución.”

j) “Existen normas claras en la institución para el uso adecuado de los equipos informáticos y se cumplen.”

Entrevista (a personal docente/administrativo)*:*

a) ¿Qué *medidas de seguridad informática* se aplican actualmente en la institución para proteger los equipos y la información?

b) ¿Cómo evalúa el *nivel de conocimiento* acerca de la seguridad informática?

c) ¿La institución ha tenido incidentes de seguridad informática?

d) ¿Existen políticas o normas internas que regule el uso de los equipos tecnológicos?

e) ¿Cuáles son los principales riesgos informáticos que hoy enfrenta la institución?

f) ¿Qué medidas, capacitaciones o formación siente que harían falta para detener las posibles situaciones?

g) ¿La institución cuenta con los recursos suficientes para afrontar los incidentes?

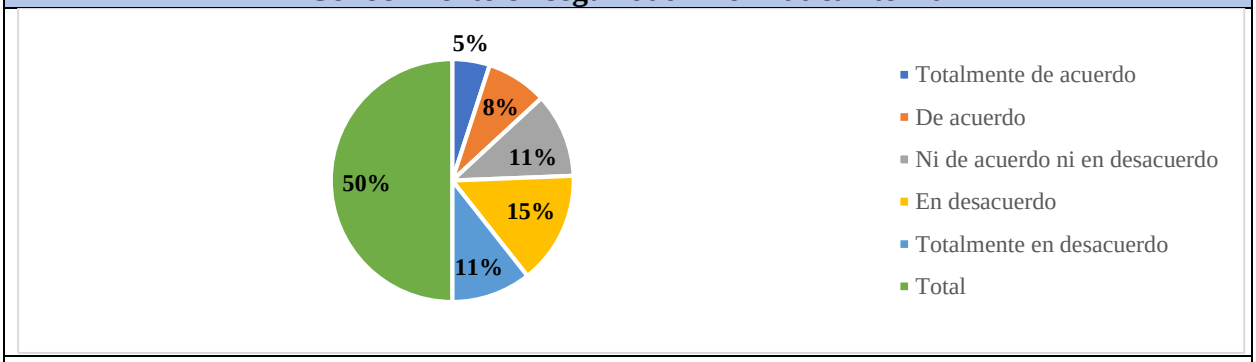
3.8 Plan de Recolección de Datos

Para la recolección de datos de este proyecto se siguió una planificación; las actividades de campo se realizaron el día lunes 15 de diciembre de 2025, a partir de las 10:00 a.m. en la Unidad Educativa Juan Pablo II – La Bramadora.

3.9 Análisis de encuesta aplicadas a estudiantes

Tabla 1

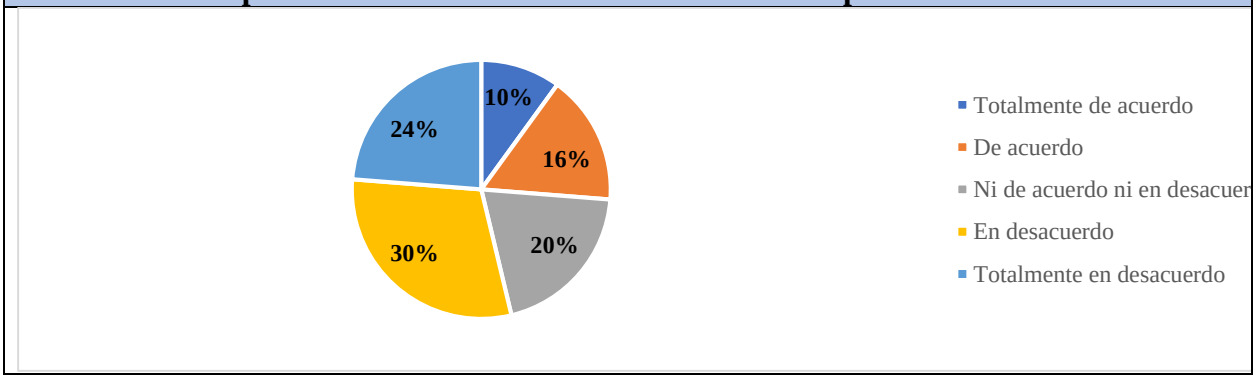
Conocimiento en seguridad informática

Conocimiento en seguridad informática-Item a

Los resultados evidencian un escaso nivel de apropiación normativa en el estudiantado, dado que más de la mitad de ellos/as afirmaron estar en desacuerdo con conocer políticas o normas relativas a la seguridad informática.

Nota: elaborado por autora.

Tabla 2

Capacidad de identificar correo electrónico sospechoso

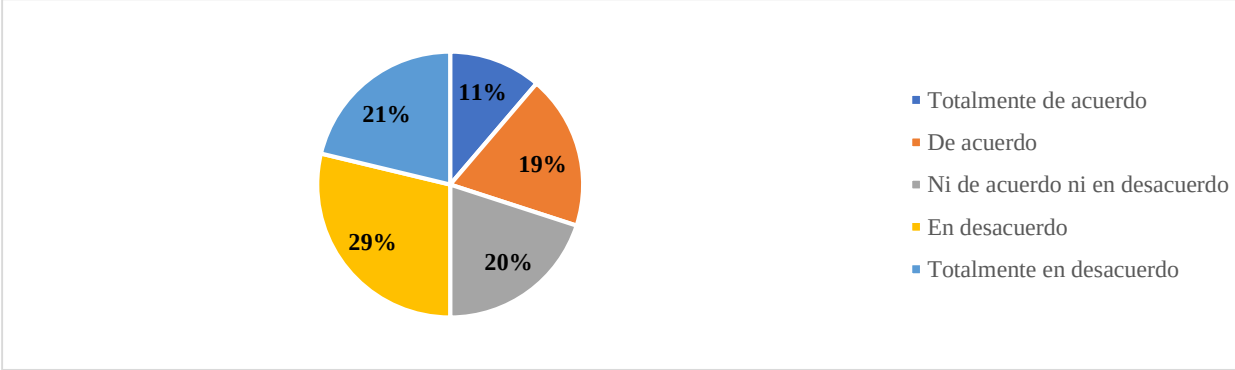
Capacidad de identificar correo electrónico sospechoso-Item b


La distribución observada muestra la poca capacidad de reconocer amenazas de la ingeniería social, especialmente correos fraudulentos o mensajes engañosos.

Nota: elaborado por autora.

Tabla 3

Uso de contraseñas seguras

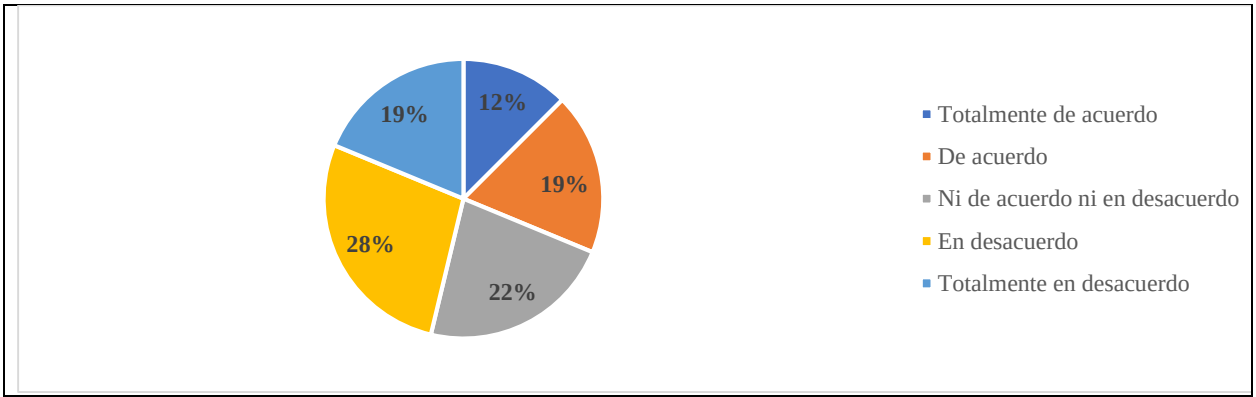
Uso de contraseñas seguras-Item c

Los hallazgos indican hábitos de autenticación de baja madurez. A pesar de que un pequeño grupo reporta prácticas razonables para el establecimiento y renovación de contraseñas, lo habitual sugiere que existe un cierto grado de debilidad del usuario en lo que es la autoprotección de la cuenta.

Nota: elaborado por autora.

Tabla 4

Seguridad del laboratorio de computación

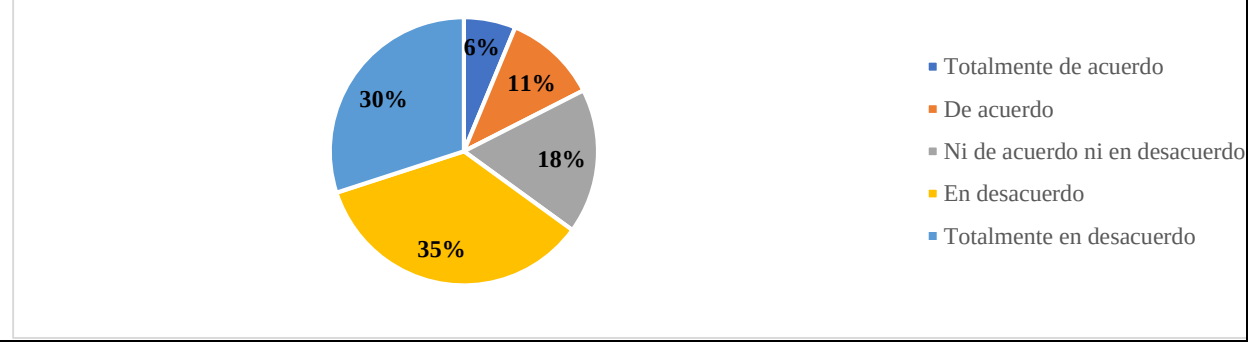
Seguridad del laboratorio de computación-Item d



La percepción respecto al propio laboratorio parece manifestar una impresión contextual fundamentalmente negativa lo que permite suponer hasta qué punto el estudiantado tiene conciencia de la existencia de controles perceptibles y considera que no constituyen lo suficiente.

Tabla 5

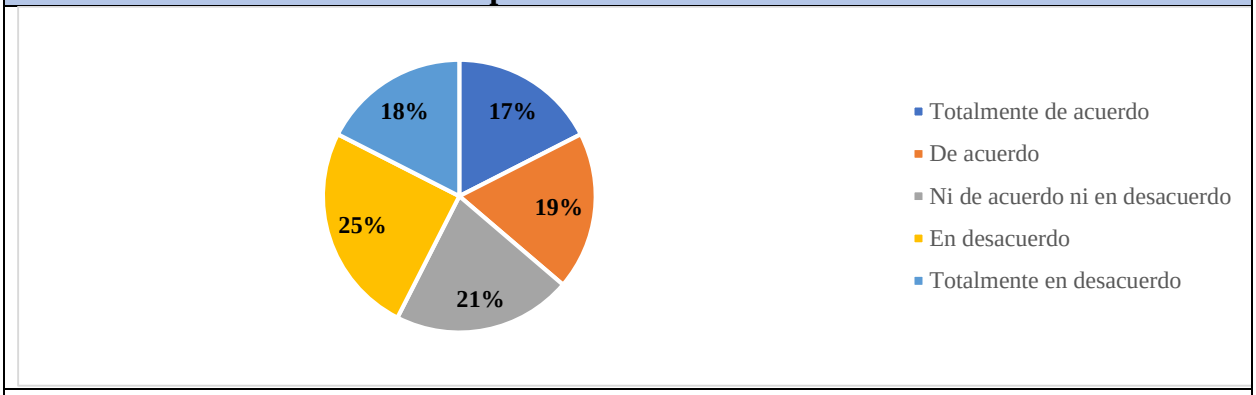
Capacitación en ciberseguridad

Capacitación en ciberseguridad-Item e

Este resultado es uno de los más recurrentes de la simulación, pues pone de manifiesto la no existencia de una estrategia sistemática de formación en ciberseguridad en la institución. La preponderancia del desacuerdo indica que la mayoría del alumnado no reconoce su participación en charlas, talleres o procesos de formación en ciberseguridad orientados a la prevención de riesgos digitales.

Nota: elaborado por autora.

Tabla 6

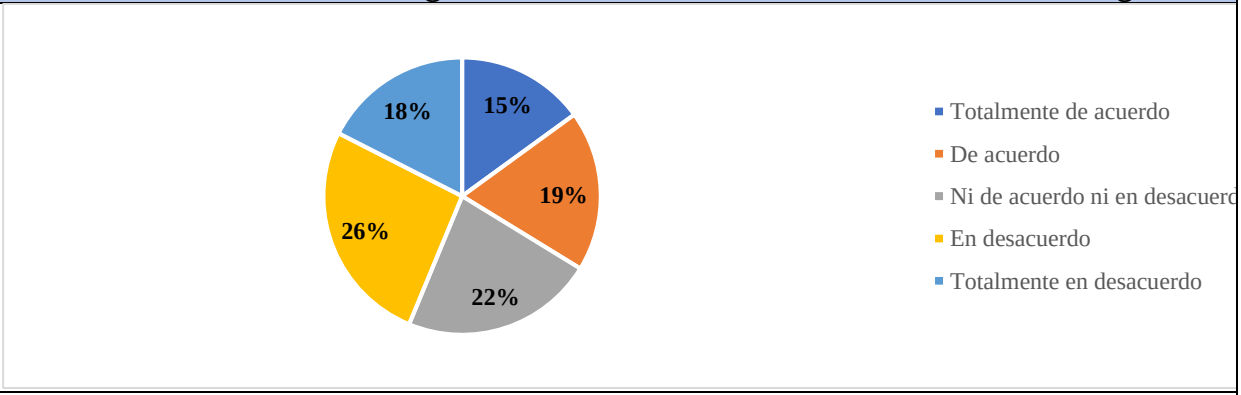
Frecuencia con la que los participantes comparten sus contraseñas con compañeros

Comparte credenciales-Item f

Dado que se trata de una afirmación negativa, el grado de acuerdo se constituye como una de las señales de la vulnerabilidad institucional. En este sentido, más de un tercio de este grupo admiten compartir credenciales con compañeros.

Nota: elaborado por autora.

Tabla 7

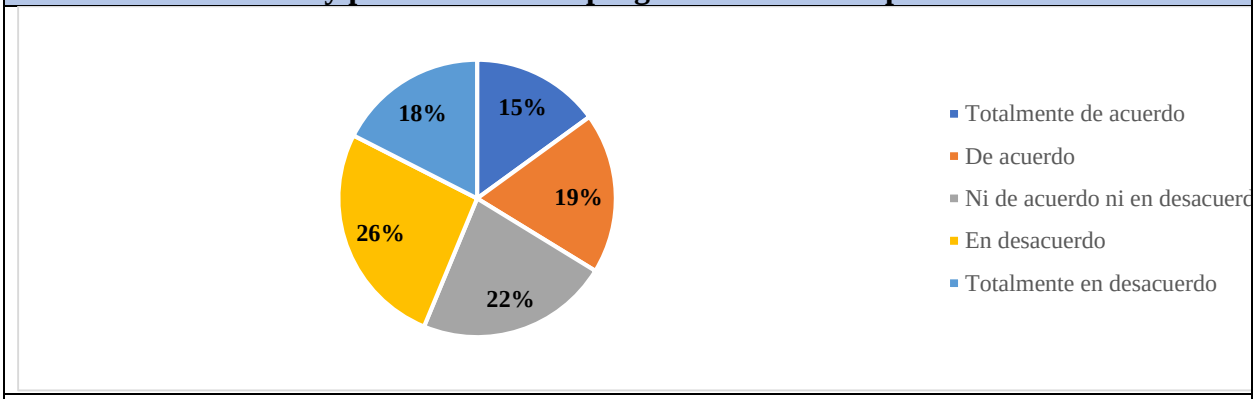
Conocimiento de los riesgos de conectar memorias USB desconocidas

Conocimiento de los riesgos de conectar memorias USB desconocidas-Item g

Los resultados evidencian un conocimiento dividido acerca de una de las rutas de infección víricas más habituales en los entornos escolares que implican la utilización compartida de equipos.

Nota: elaborado por autora.

Tabla 8

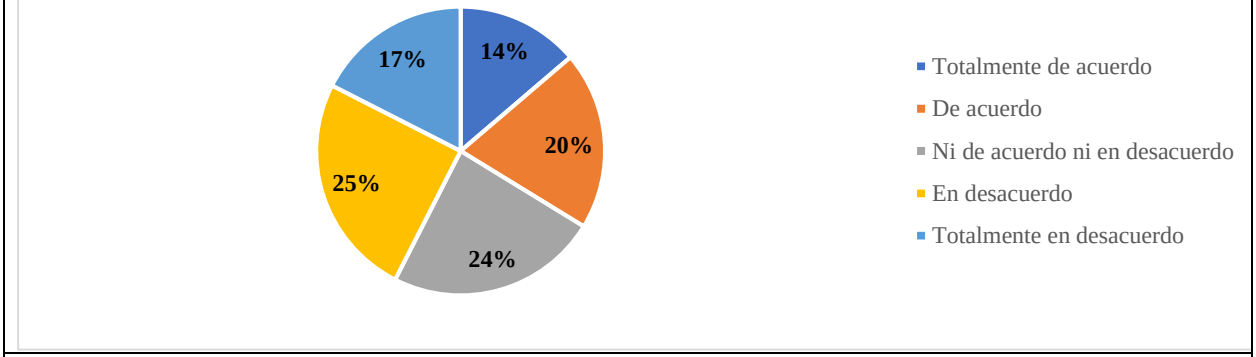
Actualización y protección de los programas de las computadoras

Actualización y protección de los programas de las computadoras-Item h

La apreciación de los estudiantes en torno a actualizaciones y protección de software es claramente negativa, confirmando la imagen de un mantenimiento más reactivo que preventivo.

Nota: elaborado por autora.

Tabla 9

Percepción de seguridad al utilizar las computadoras de la institución

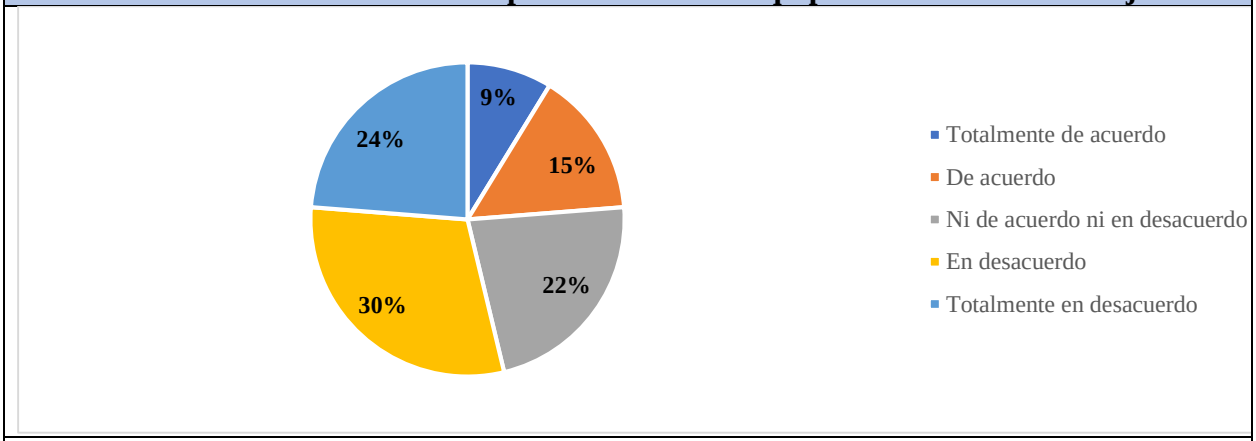
Percepción de seguridad al utilizar las computadoras de la institución-Item i

La idea de la seguridad subjetiva tiene un patrón intermedio, a lo cual se le puede dar consideraciones metodológicas. En comparación con otros indicadores que claramente muestran sus aspectos desfavorables, el primero no presenta una ruptura absoluta de la confianza.

Nota: elaborado por autora.

Tabla 10

Existencia de normas claras para el uso de los equipos informáticos

Existencia de normas claras para el uso de los equipos informáticos -Item j



La mayoría de estudiantes indican la ausencia de reglas claras, lo que hace inferir ausencia de la existencia de protocolos claramente establecidos.

Nota: elaborado por autora.

3.10 Entrevistas semiestructuradas simuladas

Tabla 11

Análisis cualitativo de las entrevistas

Item de pregunta de entrevista	Categoría	Resumen de la evidencia e interpretación
d	**Políticas institucionales**	No contándose la naturaleza de políticas formales de seguridad de la información, la vulnerabilidad aumentada en el contexto de gestión y estandarización de las prácticas que se reconocen como seguras.
f	**Capacitación**	La formación en materia de ciberseguridad es escasa y, por lo tanto, episódica.
a, e	**Infraestructura tecnológica**	El equipamiento informático está obsoleto y presenta mantenimiento irregular, lo que aumenta la vulnerabilidad ante fallos técnicos y amenazas de los dispositivos de cómputo.

c, e	**Gestión de riesgos**	La respuesta de la institución ante incidentes es reactiva, no contará con protocolos ni un sistema de gestión de incidentes formal en el ámbito de la gestión del riesgo.
b	**Cultura de seguridad**	Son prácticas habituales las inseguras como compartir credenciales y minimizar los riesgos de seguridad digitales, reflejándose la poca o baja conciencia en materia de ciberseguridad.
f	**Recursos tecnológicos**	Los límites de la planificación de actividades tanto presupuestarias como de recursos humanos dificultan que se llegue a realizar una buena capacidad de respuesta y una mejor capacidad preventiva ante un posible incidente.
a, e	**Protección de datos**	El manejo de datos sensibles presenta flaquezas inherentes a los controles de acceso y los respaldos.
f	**Necesidades de**	La constancia sobre la necesidad de la seguridad de la información, fortaleciendo sus programas de capacitación, protocolos, mantenimiento, auditorías y mejores prácticas de protección de la información

Nota: elaborado por autora.

3.11 Análisis integral de resultados

El análisis conjunto de las encuestas aplicadas a estudiantes y de las entrevistas realizadas al rector, docentes y responsable del laboratorio permitió comprobar que las principales causas planteadas en el diagrama de Ishikawa sí se encuentran presentes en la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora.

Los resultados demostraron que existen deficiencias en las dimensiones de infraestructura tecnológica, procesos de la institución, y factor humano, confirmándose la existencia de equipos con un mantenimiento escaso, ausencia de políticas formales de seguridad informática, una escasa capacitación en ciberseguridad y prácticas de uso que incrementan la exposición a las amenazas digitales.

Respecto a las causas asociadas a la gobernanza y a los procesos, tanto las entrevistas como las encuestas confirmaron que la institución no cuenta con procedimientos documentados para la gestión de la seguridad informática, para la respuesta ante incidentes, de actualización y control

periódicos de los equipos. También se verificó que las auditorías de seguridad no se realizan de forma sistemática y que el seguimiento de los indicadores de ciberseguridad es escaso. Estos resultados apoyan las causas que aparecen en el diagrama de Ishikawa y que se relacionan con la falta de planificación, control y medición, lo que pone de manifiesto que la gestión de la seguridad depende más bien de acciones correctivas y no de unas acciones de prevención institucionalizadas.

Con respecto al componente humano y al componente tecnológico, la evidencia recogida también nos permitió confirmar la mayoría de las causas inicialmente planteadas. Las encuestas mostraron divergencias respecto al conocimiento sobre buena utilización de las buenas prácticas de seguridad, acerca del uso de contraseñas, de la identificación de correos sospechosos, y sobre la utilización de dispositivos USB; mientras que las entrevistas nos indicaban limitaciones de recursos económicos, equipamiento con un cierto grado de obsolescencia y dificultades para mantener los sistemas de protección actualizados.

CAPÍTULO IV

4 MARCO PROPOSITIVO (ELABORACIÓN DE LA PROPUESTA)

4.1 Introducción

En el Marco Propositivo se elabora una serie específica de controles y acciones de remediación para el tratamiento de las vulnerabilidades diagnosticadas (Capítulo III) en la seguridad informática de la Unidad Educativa Fiscomisional Juan Pablo II - La Bramadora y tiene como finalidad la exposición es la ejecución de una auditoría basada en riesgos acordes con los estándares internacionales y metodologías consolidadas en el sentido de coadyuvar a la confidencialidad, la integridad y la disponibilidad de los activos de la información institucional. A partir del diagnóstico, se proponen controles de naturaleza técnica y organizativa para remediar los hallazgos reportados, entre ellos destacan por ejemplo la falta de políticas formales, el soporte insuficiente de controles de red y de los sistemas, la falta de copias de seguridad y la escasa capacitación. La implementación de estos controles traerá consigo una serie de beneficios: una reducción de las vulnerabilidades críticas, una disminución de los riesgos de malware, accesos no autorizados, o pérdida de información y permitirá la mejora de la gobernanza de las TI. Adicionalmente, un enfoque de riesgos permitirá asegurar que los recursos que se tienen son conducidos a tratar con las amenazas más significativas. Este enfoque, según ISO/IEC 27001, es un requisito esencial y abarca la identificación, la evaluación y el tratamiento de forma sistemática de los riesgos.

En términos generales, la auditoría de sistemas informáticos es "un instrumento clave para contribuir a que la transparencia y la confianza estén presentes en la esfera digital", pues exige la aplicación de normas y estándares que protegen los activos de la información y mejoran la gestión de riesgos. De hecho, se asocia la aplicación de normas internacionales (ISO 27000, COBIT,

MAGERIT, etc.) con el fortalecimiento de la postura de seguridad y con la aplicación de una solución completa para afrontar la manera de hacer frente a los problemas tecnológicos. Es por ello que, cada control propuesto en la presente propuesta se encuentra argumentado por las normas que le son devengadas: ISO 27001/27002 para los controles de seguridad, ISO 19011 para la dirección de la auditoría, MAGERIT para el análisis de riesgos y COBIT 2019 para la gobernanza de TI. En fin, este planteamiento sistemático no solo corrige deficiencias puntuales, sino que establece las bases para la mejora continua de la seguridad de la institución. En definitiva, el presente marco propositivo responde a los hallazgos del Capítulo III recopilando un plan coherente y especializado, muy similar al que podría elaborar una firma de consultoría, para incrementar los niveles de seguridad de la Universidad Fiscomisional Juan Pablo II – La Bramadora.

4.2 Determinación de recursos

La correcta ejecución de la propuesta de auditoría requiere la asignación de recursos humanos, tecnológicos y económicos adecuados. A continuación se identifican los principales actores y elementos necesarios, junto con su análisis de importancia.

- **Recursos Humanos**

Tabla 12

Recursos Humanos

Cargo / participante	Rol en la auditoría	Responsabilidades principales	Participación
Auditora	Responsable de la ejecución de la auditoría	Planificar y desarrollar la auditoría; recopilar y analizar evidencias; revisar los controles y procesos relacionados con TI; aplicar los criterios y	**Alta**

		metodologías seleccionados; identificar hallazgos y elaborar el informe de auditoría.	
Tutor académico	Supervisor y orientador metodológico	Brindar orientación durante el desarrollo de la auditoría; revisar la metodología, instrumentos y procedimientos aplicados; realizar observaciones y recomendaciones para garantizar la coherencia académica y metodológica del trabajo.	**Media**
Representante de la institución educativa	Facilitador de información institucional	Proporcionar la información y documentación requerida; facilitar el acceso a los datos necesarios para la auditoría; aclarar aspectos relacionados con los procesos institucionales y colaborar en la recopilación de evidencias.	**Media**

Cada uno de los participantes involucrados en el desarrollo de la auditoría cumple una función específica de acuerdo con el alcance del trabajo. La auditora es la responsable de planificar y ejecutar el proceso de auditoría, recopilar y analizar la información disponible, revisar las evidencias proporcionadas por la institución e identificar los principales hallazgos. Asimismo, tiene a su cargo la aplicación de los criterios y procedimientos definidos para el desarrollo del trabajo y la elaboración del informe correspondiente El tutor académico cumple una función de

orientación y supervisión metodológica durante el desarrollo de la auditoría. Su participación se centra en revisar los procedimientos aplicados, realizar observaciones y proporcionar recomendaciones que contribuyan a mantener la coherencia metodológica y académica del trabajo. Por su parte, la persona responsable de la institución educativa que facilitó la información actúa como enlace con el colegio y proporciona la documentación y los datos necesarios para desarrollar la auditoría. Además, facilita la comprensión de los procesos institucionales y atiende los requerimientos de información necesarios para sustentar el análisis y los hallazgos obtenidos.

- **Recursos tecnológicos**

Tabla 13

Recursos tecnológicos

Recurso tecnológico	Descripción	Función en el trabajo de titulación	Disponibilidad
Computadora portátil	Equipo informático de uso personal de la autora	Utilizada para redactar el trabajo de titulación, organizar la información recopilada, elaborar tablas y matrices y procesar los resultados obtenidos durante la auditoría.	Disponible
Microsoft Word	Software de procesamiento de textos	Utilizado para la redacción, edición, organización y presentación del documento final del trabajo de titulación.	Disponible
Microsoft Excel	Hoja de cálculo	Empleada para organizar y tabular los datos recopilados, realizar cálculos y estructurar las matrices utilizadas en el análisis de riesgos.	Disponible
Google Forms	Herramienta digital para elaboración y aplicación de formularios	Utilizada para apoyar la recopilación y organización de información obtenida mediante los instrumentos aplicados durante la investigación.	Disponible
Navegador web	Aplicación para acceso a recursos disponibles en Internet	Utilizado para realizar búsquedas bibliográficas, consultar documentación técnica y acceder a fuentes académicas relacionadas	Disponible

		con auditoría y seguridad informática.	
Internet	Servicio de conectividad	Permitió acceder a fuentes bibliográficas, plataformas académicas y recursos digitales necesarios para sustentar teórica y metodológicamente el trabajo.	Disponible
Canva	Plataforma de diseño gráfico	Utilizada para elaborar elementos gráficos incorporados en el trabajo, como el diagrama causa-efecto presentado en la investigación.	Disponible
Teléfono celular	Dispositivo móvil de apoyo	Empleado para la comunicación, registro y consulta de información durante las actividades relacionadas con el desarrollo del trabajo de titulación.	Disponible

La tabla presenta los principales recursos tecnológicos empleados para el desarrollo del trabajo de titulación y la ejecución de las actividades investigativas relacionadas con la auditoría de seguridad informática. Estos recursos facilitaron la redacción y organización del documento, la recopilación y procesamiento de la información, la elaboración de matrices y la consulta de fuentes académicas y técnicas. El uso de herramientas como la computadora portátil, Microsoft Word, Excel, recursos de Internet y plataformas digitales permitió sistematizar los datos obtenidos mediante los instrumentos de investigación y estructurar los resultados de manera ordenada. Asimismo, Canva sirvió de apoyo para la elaboración de elementos gráficos incorporados en el documento. En conjunto, estos recursos constituyeron herramientas de apoyo para desarrollar las diferentes etapas del trabajo de titulación y documentar adecuadamente el proceso de auditoría.

- **Recursos económicos**

Tabla 14

Recursos económicos

Actividad / recurso	Descripción	Cantidad	Costo estimado (USD)	Financiamiento

Computadora portátil	Equipo utilizado para la redacción, procesamiento de información y elaboración del trabajo	1	0,00*	Propio
Teléfono celular	Utilizado para comunicación, coordinación y apoyo en la recopilación de información	1	0,00*	Propio
Servicio de Internet	Conectividad para investigación bibliográfica, consulta de fuentes y uso de herramientas digitales	4 meses	25,00	100,00
Impresiones y copias	Impresión de instrumentos, borradores y documentación necesaria	1 rubro	30,00	30,00
Materiales de oficina	Hojas, carpetas, esferográficos y otros materiales empleados durante el proceso	1 rubro	20,00	20,00
Transporte	Movilización hacia la Unidad Educativa para el levantamiento de información y desarrollo de la auditoría	6 visitas	10,00	60,00
Energía eléctrica	Consumo asociado al uso de computadora y demás dispositivos durante el desarrollo del trabajo	4 meses	10,00	40,00
Total estimado				**250,00**

La tabla presenta los recursos económicos empleados para el desarrollo del trabajo de titulación, evidenciando que su ejecución se sustentó principalmente en recursos propios de la autora y en gastos operativos necesarios para llevar a cabo la investigación. La computadora portátil y el teléfono celular constituyeron herramientas disponibles previamente, por lo que no generaron costos adicionales de adquisición, mientras que los principales egresos estuvieron relacionados con el servicio de Internet, transporte, impresiones, materiales de oficina y consumo de energía eléctrica. En conjunto, estos recursos permitieron realizar el levantamiento y procesamiento de la información, la elaboración de los instrumentos, las actividades de campo y la redacción del documento final. Por tanto, el presupuesto presentado corresponde exclusivamente

a los recursos utilizados durante el proceso investigativo y no contempla los costos asociados con la futura implementación de las recomendaciones derivadas de la auditoría.

4.3 Etapas para el desarrollo de la propuesta

La propuesta metodológica se organiza en fases secuenciales, cada una con objetivos claros, fundamentos normativos, procedimientos, actividades, responsables, productos esperados, riesgos asociados y evidencias. A continuación se describen las 13 fases de la auditoría, inspiradas en ISO 19011, MAGERIT v3 y otras guías reconocidas, adaptadas al contexto de la institución.

4.3.1 Planificación de la auditoría

- **Objetivo:** Establecer la estructura general del programa de auditoría alineado a las normas (ISO 19011), definiendo alcance, objetivos, recursos y cronograma.
- **Fundamento:** ISO 19011 exige formular un *programa de auditoría* que incluya objetivos, criterios, alcance, recursos y calendario. Esto garantiza que la auditoría se planifique de forma coherente con el tamaño y riesgo del auditado, maximizando la eficiencia.
- **Procedimiento y actividades:**
    - Reunión inicial con la dirección (Rector y responsables de TI) para la fijación de los objetivos estratégicos hacia el objetivo de la auditoría.
    - Elaboración del Programa de Auditoría, documentando alcance (equipos informáticos, sistemas críticos, procesos académicos), criterios (normas ISO 27001, políticas internas), frecuencia y tipo de auditorías (interna/externa).
    - Designación de personal auditor por competencias (ver 4.1).
    - Elaboración de criterios de evaluación (checklists) en función de las normas ISO/IEC 27001:2022 y MAGERIT v3.

- **Responsables:** Auditor Líder (ISO 27001) que desarrolla el programa; Rector da el visto bueno al plan; área de TI colabora informando sobre la necesaria información de contexto.
- **Productos esperados:** Documento "Programa de Auditoría" que contiene objetivos, alcance, plan de actividades y recursos (véase tabla siguiente).
- **Riesgos asociados:** Constatar una subestimación del alcance, el hecho de que no se hayan incorporado los puntos de vista de los interesados claves.
- **Evidencia generada:** Programa de Auditoría formalizado (documento planificado) y actas de reunión de planificación.

Programa de Auditoría:

Tabla 15

Programa de auditoría informática

Programa de auditoría informática a equipos informaticos de la Unidad Educativa Fisco Misional Juan Pablo II La Bramadora"		
Objetivo • Confirmar el alcance de la auditoría y los criterios establecidos. • Verificar el cumplimiento de los controles de seguridad de la información conforme a las normas ISO/IEC 27001 e ISO 19011. • Identificar oportunidades de mejora en el Sistema de Gestión de Seguridad de la Información.		
Técnica y procedimiento	**Referencia a papel de trabajo**	**Tiempo**

1. Planificación de la auditoría: definir el objetivo, alcance, criterios, actividades y recursos necesarios para desarrollar la auditoría.	4.3.1	2 días
2. Levantamiento de información: recopilar evidencias mediante observación directa, entrevista, revisión documental e inspección de los equipos informáticos de la institución.	4.3.2	3 días
3. Inventario y clasificación de activos: identificar y registrar los activos tecnológicos objeto de evaluación, considerando su tipo, ubicación, función y nivel de criticidad.	4.3.3	2 días
4. Análisis del contexto: examinar las condiciones tecnológicas, físicas, organizacionales y humanas que pueden influir en la seguridad informática de la institución.	4.3.4	2 días
5. Aplicación de cuestionarios para la identificación de riesgos: utilizar los instrumentos definidos para identificar amenazas, vulnerabilidades y controles existentes.	4.3.5	3 días
6. Análisis de riesgos: analizar los riesgos identificados considerando las amenazas, vulnerabilidades, probabilidad de ocurrencia y posibles consecuencias.	4.3.6	3 días
7. Tabulación de los riesgos: organizar y sistematizar los resultados obtenidos durante la evaluación para facilitar su interpretación.	4.3.7	2 días

8. Determinación del impacto: establecer las consecuencias que podrían generar los riesgos identificados sobre los activos informáticos de la institución.	4.3.8	2 días
9. Valoración de riesgos: determinar el nivel de riesgo de acuerdo con los criterios establecidos en la metodología aplicada.	4.3.9	2 días
10. Elaboración de la matriz de riesgos: consolidar los riesgos identificados y valorados para establecer su nivel y facilitar la priorización de las medidas de tratamiento.	4.3.10	2 días
Elaborado por:	**Revisado por:**	
Fecha:	**Firma**:	

La elaboración de checklists específicos para ISO 27001 asegura que la evaluación de controles sea sistemática. Asimismo, la planificación contempla la gestión de riesgos del propio programa conforme a ISO 19011.

4.3.2 Levantamiento de información

- **Objetivo:** Recopilar información detallada sobre la operación de los sistemas y procesos de TI, así como las prácticas de seguridad vigentes.
- **Fundamento:** Una auditoría eficaz requiere combinar técnicas diversas (observación, entrevistas, revisión documental, inspección física y pruebas lógicas) para contrastar la documentación con la realidad. Esto se complementa con principios de recolección de

información de MAGERIT, que recomienda identificar fuentes de vulnerabilidad mediante estudio de procesos, personas y tecnología.

- **Procedimiento y actividades:**
    - **Diseño de instrumentos:** Se elaboraron seis cuestionarios de 20 preguntas cerradas para identificar los riesgos de incendio, malware–ransomware, intrusión externa, acceso no autorizado, robo de hardware y phishing. Cada instrumento incluyó respuestas "Sí/No" y un campo de observaciones.
    - **Aplicación de los instrumentos:** Los cuestionarios se aplicaron de manera presencial al personal relacionado con los activos tecnológicos evaluados, complementando las respuestas con la verificación directa de las condiciones existentes.
    - **Identificación de riesgos:** Con la información recopilada se determinaron las principales vulnerabilidades y controles existentes para cada activo y amenaza analizada.
    - **Tabulación de resultados:** Finalmente, las respuestas obtenidas fueron codificadas y organizadas para calcular los niveles de cumplimiento y exposición al riesgo de cada escenario evaluado.
- **Responsables:** Auditora de TI asumirán la mayoría de las tareas (observación, pruebas técnicas).
- **Productos esperados:** Informes parciales de observación, registros de evidencia recogida.
- **Objetivo:** Recopilar información sobre el estado y funcionamiento de los equipos informáticos de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora, así como identificar las prácticas y controles de seguridad aplicados en la institución.

Técnicas e instrumentos:

Tabla 16

Técnicas e instrumentos

Técnica	Instrumento	Objetivo	Evidencia obtenida
Verificación y observación directa	**Cuestionario estructurado para identificación del riesgo de incendio**, compuesto por 20 preguntas cerradas con opciones de respuesta Sí/No, campo de observación y valoración del riesgo.	Verificar los controles físicos, eléctricos y preventivos implementados para reducir la posibilidad de incendio y afectación del servidor principal, considerando sistemas de detección y extinción, instalaciones eléctricas, UPS, sobretensiones, extintores, señalización, monitoreo de temperatura, mantenimiento y protocolos de actuación.	Cuestionario aplicado con registro de controles existentes y ausentes, observaciones de campo y condiciones de vulnerabilidad relacionadas con la protección del servidor principal frente a incendios.
Verificación y observación directa	**Cuestionario estructurado para identificación del riesgo de malware–ransomware**,	Identificar la existencia y suficiencia de controles destinados a prevenir infecciones por malware y ataques de ransomware en	Registro de controles de protección implementados y vulnerabilidades detectadas en los

	compuesto por 20 preguntas cerradas con opciones Sí/No, campo de observación y valoración del riesgo.	las computadoras del Aula TIC, mediante la revisión de antivirus, actualizaciones, permisos de usuario, instalación de software, respaldos, dispositivos USB, firewall, monitoreo y mecanismos de recuperación.	equipos, incluyendo condiciones relacionadas con actualizaciones, privilegios de usuario, software, respaldos y mecanismos de prevención de malware.
Verificación y observación directa	**Cuestionario estructurado para identificación del riesgo de intrusión externa**, integrado por 20 preguntas cerradas con opciones Sí/No, campo de observación y valoración del riesgo.	Evaluar los controles de seguridad implementados en la red WiFi institucional para prevenir accesos externos no autorizados, considerando protocolos de seguridad, contraseñas, registro de dispositivos, filtrado, firewall, monitoreo, IDS/IPS, actualización de firmware, segmentación de red y pruebas de penetración.	Información sobre las medidas de protección de la red inalámbrica y registro de vulnerabilidades relacionadas con configuraciones, accesos, monitoreo, segmentación y mecanismos de detección de intrusiones.

Verificación y observación directa	**Cuestionario estructurado para identificación del riesgo de acceso no autorizado**, compuesto por 20 preguntas cerradas con opciones Sí/No, campo de observación y valoración del riesgo.	Examinar los controles de acceso lógico implementados en el Sistema de Gestión Académica, considerando credenciales individuales, robustez y caducidad de contraseñas, autenticación multifactor, permisos por roles, bloqueo de cuentas, registro de accesos, monitoreo, cifrado y auditorías.	Registro de controles de acceso existentes y debilidades identificadas en la gestión de credenciales, autenticación, privilegios, monitoreo y protección de la información del sistema.
Verificación y observación directa	**Cuestionario estructurado para identificación del riesgo de robo de hardware**, integrado por 20 preguntas cerradas con opciones Sí/No, campo de observación y	Determinar la existencia de medidas de seguridad física destinadas a prevenir la sustracción o pérdida de equipos tecnológicos, mediante la revisión del control de ingreso, videovigilancia, registro de visitantes, inventarios, identificación de equipos,	Evidencia sobre los controles físicos existentes, registros de inventario, medidas de vigilancia, restricciones de acceso y demás condiciones relacionadas con la protección física de los equipos tecnológicos.

	valoración del riesgo.	alarmas, políticas de préstamo, custodia e inspecciones periódicas.	
Verificación y observación directa	**Cuestionario estructurado para identificación del riesgo de phishing**, compuesto por 20 preguntas cerradas con opciones Sí/No, campo de observación y valoración del riesgo.	Verificar los controles implementados para prevenir ataques de phishing mediante el correo corporativo, considerando filtros antispam, autenticación multifactor, capacitación, campañas de concienciación, verificación de remitentes, análisis de enlaces y archivos, bloqueo de dominios, simulaciones y mecanismos de reporte y respuesta.	Registro de medidas preventivas implementadas y vulnerabilidades asociadas con autenticación, capacitación de usuarios, detección de correos fraudulentos, reporte de incidentes y respuesta frente a ataques de phishing.

Se elaboraron seis cuestionarios estructurados con 20 ítems cada uno, para un total de 120 ítems de verificación. Se optó por preguntas cerradas debido a que el propósito de los instrumentos no fue medir opiniones o niveles de satisfacción, sino comprobar la existencia o ausencia de determinadas condiciones y controles de seguridad. Cada instrumento mantuvo una estructura homogénea compuesta por los siguientes campos: número del ítem, pregunta, respuesta “Sí”,

respuesta “No”, observación y riesgo. La uniformidad estructural permitió aplicar un mismo procedimiento de registro y procesamiento a los seis escenarios evaluados.

Los ítems fueron redactados en forma interrogativa y orientados hacia condiciones observables o verificables. Por ejemplo, preguntas como “¿El cuarto del servidor cuenta con detectores de humo?”, “¿Los equipos tienen antivirus actualizado?”, “¿Existe autenticación multifactor?” o “¿Se realizan simulaciones de phishing?” permiten determinar directamente la presencia o ausencia del control analizado.

La columna Observación se incorporó como elemento complementario a la respuesta cerrada. Su finalidad fue registrar información relevante cuando una respuesta dicotómica no resultara suficiente para describir la condición encontrada. Por esta razón, en los instrumentos aplicados se registraron anotaciones como “No dispone”, “Protección parcial”, “Equipos desactualizados”, “No implementado” o “Requiere fortalecer capacitación y MFA”, según las condiciones identificadas durante la evaluación. Para facilitar el procesamiento de la información se utilizó una escala dicotómica de respuesta. Las alternativas “Sí” y “No” permitieron establecer si el control examinado se encontraba implementado o si existía una condición que requería atención.

Posteriormente, para efectos de tabulación, las respuestas fueron transformadas en valores numéricos. La presencia de una condición considerada segura se registró con un valor de 1, mientras que la condición asociada con riesgo se registró con un valor de 0. Asimismo, se contempló la categoría “No aplica”, destinada a aquellos ítems que, por las características del activo o del contexto evaluado, no correspondieran al escenario analizado.

4.3.3 Inventario y clasificación de activos

Tanto ISO 27001 como MAGERIT destacan la importancia de inventariar activos de información y sus soporte físicos. Un inventario completo es requisito para luego evaluar riesgos sobre cada activo. MAGERIT v3 propone clasificar activos como hardware, software, información, servicios y usuarios, asignando un valor según su rol en la misión educativa.

Tabla de inventario:

Tabla 17

Inventario y clasificación de activos

Código	**Activo**	**Tipo**	**Ubicación**	**Responsable**	**Criticidad**	**Valor para la institución**
A001	Servidor principal	Hardware	Sala de servidores	Ing. de Sistemas	Alta	Aloja base de datos de alumnos y administrativos
A002	PC Laboratorio TIC	Hardware	Aula 101	Docente TIC	Media	Soporta clases diarias y software educativo
A003	Red WiFi Institucional	Servicio (Red)	Plantel completo	Ing. de Redes	Alta	Conectividad esencial para docentes y alumnos

A004	SGA (software)	Software	Servidor local / nube	Coordinador Acad.	Alta	Gestión de notas, matrículas y datos confidenciales
A005	Base de datos de alumnos	Información	Servidor de BD	Ing. de Sistemas	Alta	Contiene datos personales y registros académicos
A006	Correo corporativo	Servicio (Cloud)	En la nube	Ing. de Sistemas	Media	Canal oficial de comunicación institucional

4.3.4 Análisis del Contexto

Durante la fase de levantamiento de información se realizó la inspección directa del laboratorio de computación de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora, con el propósito de verificar las condiciones físicas y tecnológicas de los activos incluidos en el alcance de la auditoría. La actividad permitió obtener evidencia directa sobre el estado de los equipos, las condiciones del espacio físico, los mecanismos de protección existentes y otros aspectos relacionados con la seguridad informática.

La inspección comprendió el laboratorio institucional, el cual dispone de 37 computadoras, de las cuales 32 se encuentran operativas y 5 fuera de funcionamiento. Estos datos coinciden con

la caracterización de la infraestructura tecnológica presentada previamente en el estado actual del problema.

Figura 2

Vista general del laboratorio de computación

Se realizo una evaluación del entorno físico donde se encuentran ubicados los equipos, tomando en cuenta también la ventilación, la seguridad del área, el control de humedad y los riesgos de ingresos no autorizados, además, se logró llegar a un análisis de la estructura organizacional del área, incluyendo los niveles de responsabilidad, los procesos aplicados y el nivel de seguridad, en el nivel tecnológico, se evaluó a los equipos utilizados, el sistema de autenticaciones seguras, la existencia de copias de seguridad o respaldos, las actualizaciones de software y las configuraciones de red, en cuanto al factor humano, se observó las buenas prácticas

de contraseñas seguras, los accesos de los usuarios, el manejo de dispositivos y el cumplimiento de las normativas internas.

Tabla 18

Cuestionario para cumplimiento de requisitos

Cuestionario para cumplimiento de requisitos Según normas ISO		**C1 Pag 1 de 5**	
Requisitos	**Preguntas**	**Cumplimiento (0,1,2)**	**Observación**
4. Contexto de la organización			
4.1 Comprensión de la organización y de su contexto	¿La institución ha identificado los riesgos que afectan la seguridad de la información?	**2**	Se dispone de una matriz de riesgos institucional.
	¿Se encuentran documentados los activos de información críticos?	**2**	Inventario de activos actualizado por el área de TI.
	¿Existe un inventario actualizado de los activos tecnológicos?	**2**	El inventario incluye servidores, equipos y red institucional.
4.2 Comprensión de las necesidades y	¿La Universidad ha identificado los requisitos de seguridad de usuarios	**1**	Existen lineamientos, pero no están

expectativas de las partes interesadas	y organismos reguladores?		documentados completamente.
	¿Se consideran los requisitos legales relacionados con la protección de datos personales?	**1**	Se cumplen parcialmente los requisitos legales vigentes.
4.3 Determinación del alcance del SGSI	¿Está definido el alcance del Sistema de Gestión de Seguridad de la Información?	**1**	El alcance no contempla todos los procesos institucionales.
	¿El alcance incluye servidores, red institucional, correo electrónico y Sistema de Gestión Académica?	**1**	Incluye los principales activos, pero no todos los servicios.
4.4 Sistema de Gestión de Seguridad de la Información	¿Existe documentación formal del SGSI?	**0**	No se evidencia un SGSI implementado conforme a ISO/IEC 27001.
	¿Se revisa periódicamente la eficacia del SGSI?	**0**	No existen auditorías internas periódicas del SGSI.

	¿Se han definido objetivos para mejorar la seguridad de la información?	**1**	Existen iniciativas, pero no indicadores de seguimiento.
5. Liderazgo			
5.1 Liderazgo y compromiso	¿La Dirección demuestra compromiso con la seguridad de la información?	**2**	Existe apoyo institucional para fortalecer la seguridad informática.
	¿Se asignan recursos suficientes para implementar controles de seguridad?	**1**	Los recursos son limitados para cubrir todas las necesidades.
5.2 Política de Seguridad de la Información	¿Existe una política institucional de seguridad de la información aprobada?	**1**	La política está en elaboración o actualización.
	¿La política es conocida por docentes, administrativos y personal de TI?	**0**	No se evidencia socialización formal de la política.

5.3 Roles y responsabilidades	¿Están claramente definidas las responsabilidades relacionadas con la seguridad informática?	**1**	Las funciones existen, pero no están formalizadas completamente.
	¿Existe un responsable del Sistema de Gestión de Seguridad de la Información?	**1**	Existe responsable de TI, pero no un responsable formal del SGSI.

Resumen de resultados

Valor	**Cantidad**
2 (Cumple)	**5**
1 (Cumple parcialmente)	**9**
0 (No cumple)	**3**
Elaborado por:	**Revisado por:**
Fecha:	**Firma**:

Cuestionario para cumplimiento de requisitos Según normas ISO	**C1 Pag 1 de 5**

Requisitos	Preguntas	Cumplimiento (0,1,2)	Observación
5. Control de Acceso			
5.1 Gestión de usuarios	¿Cada usuario dispone de credenciales individuales para acceder a los sistemas institucionales?	**2**	Cada funcionario posee un usuario institucional.
	¿Las cuentas de usuarios inactivos son eliminadas oportunamente?	**1**	Existen cuentas pendientes de desactivación.
	¿Existe un procedimiento formal para la creación y eliminación de usuarios?	**1**	El procedimiento no se encuentra completamente documentado.
5.2 Gestión de contraseñas	¿Se exige el uso de contraseñas seguras?	**1**	No todos los usuarios cumplen los criterios establecidos.
	¿Las contraseñas se cambian periódicamente?	**0**	No existe una política obligatoria de cambio periódico.

	¿Las contraseñas son almacenadas de forma segura?	**2**	Se utilizan mecanismos de cifrado en el sistema.
5.3 Autenticación	¿El Sistema de Gestión Académica utiliza autenticación multifactor (MFA)?	**0**	No se encuentra implementada autenticación multifactor.
	¿Se bloquean las cuentas después de varios intentos fallidos de inicio de sesión?	**2**	El sistema bloquea automáticamente el acceso.
	¿Las sesiones se cierran automáticamente por inactividad?	**1**	Solo algunos sistemas cuentan con esta configuración.
5.4 Gestión de privilegios	¿Los privilegios de acceso son asignados según el cargo del usuario?	**2**	Los permisos se administran por perfiles.
	¿Se revisan periódicamente los permisos asignados?	**1**	La revisión se realiza únicamente cuando existen cambios de personal.

	¿Existe segregación de funciones entre administradores y usuarios?	**2**	Los perfiles administrativos están diferenciados.
5.5 Registro y monitoreo	¿Se registran los accesos realizados al Sistema de Gestión Académica?	**2**	El sistema mantiene registros de auditoría.
	¿Los registros son revisados periódicamente?	**1**	No existe una revisión sistemática de los registros.
	¿Existe un procedimiento para reportar accesos sospechosos?	**1**	El procedimiento existe parcialmente, pero no está formalizado.

Resumen de resultados

Valor	**Cantidad**
2 (Cumple)	**6**
1 (Cumple parcialmente)	**7**
0 (No cumple)	**2**
Elaborado por:	**Revisado por:**
Fecha:	**Firma**:

Cuestionario para cumplimiento de requisitos Según normas ISO			**C1 Pag 1 de 5**
Requisitos	**Preguntas**	**Cumplimiento (0,1,2)**	**Observación**
7. Seguridad Física y Ambiental			
7.1 Protección de áreas seguras	¿El cuarto del servidor permanece con acceso restringido únicamente al personal autorizado?	**2**	El acceso se controla mediante personal autorizado.
	¿Existe un registro de ingreso y salida al cuarto del servidor?	**1**	El registro se realiza únicamente de forma manual.
	¿Se controla el ingreso de visitantes al área de servidores?	**1**	No existe un procedimiento formal para visitantes.
7.2 Protección de equipos	¿Los equipos críticos se encuentran protegidos contra robo o manipulación?	**2**	Los equipos permanecen en áreas restringidas.

	¿Los equipos cuentan con identificación patrimonial?	**2**	Todos los activos poseen código institucional.
	¿Se realizan inventarios periódicos de los equipos tecnológicos?	**2**	El inventario es actualizado por el área de TI.
7.3 Protección contra amenazas ambientales	¿El cuarto del servidor dispone de detectores de humo?	**2**	Existen detectores instalados.
	¿Existe un sistema automático de supresión de incendios?	**0**	No se dispone de un sistema automático contra incendios.
	¿Existe protección contra sobretensiones eléctricas?	**1**	La protección es parcial mediante UPS.
	¿Se realiza mantenimiento preventivo de las instalaciones eléctricas?	**2**	Se ejecuta mantenimiento programado.
7.4 Continuidad física	¿Existen extintores cercanos al área de servidores?	**2**	Los extintores se encuentran operativos.
	¿Se realizan inspecciones periódicas de los equipos de emergencia?	**1**	Las inspecciones no siguen un cronograma definido.

	¿Existe señalización de rutas de evacuación?	**2**	La señalización cumple con la normativa institucional.
	¿Se realizan simulacros de emergencia?	**1**	Se realizan ocasionalmente, sin planificación periódica.
7.5 Videovigilancia y monitoreo	¿El área de servidores cuenta con cámaras de vigilancia?	**2**	Se dispone de monitoreo mediante CCTV.
	¿Las grabaciones son revisadas periódicamente?	**1**	Solo se revisan cuando ocurre un incidente.

Resumen de resultados

Valor	**Cantidad**
2 (Cumple)	**9**
1 (Cumple parcialmente)	**6**
0 (No cumple)	**1**
Elaborado por:	**Revisado por:**

Fecha:	**Firma**:

Cuestionario para cumplimiento de requisitos Según normas ISO			**C1 Pag 1 de 5**
Requisitos	**Preguntas**	**Cumplimiento (0,1,2)**	**Observación**
6. Gestión de Riesgos			
6.1 Identificación de riesgos	¿La institución identifica periódicamente los riesgos de seguridad de la información?	**2**	Se dispone de una matriz institucional de riesgos.
	¿Los riesgos son evaluados considerando probabilidad e impacto?	**2**	Se emplean criterios definidos para la valoración.
	¿Los resultados de la evaluación son documentados?	**2**	Existe evidencia documental de la evaluación realizada.
6.2 Tratamiento de riesgos	¿Existe un plan de tratamiento para los riesgos identificados?	**1**	El plan requiere actualización y seguimiento.

	¿Se implementan controles para reducir los riesgos detectados?	**1**	Algunos controles han sido implementados parcialmente.
	¿Se realiza seguimiento a la eficacia de los controles?	**0**	No existe un procedimiento formal de seguimiento.
8. Seguridad Operacional			
8.1 Protección contra malware	¿Todos los equipos cuentan con antivirus actualizado?	**1**	Algunos equipos presentan antivirus desactualizados.
	¿Se realizan análisis periódicos contra software malicioso?	**1**	Los escaneos no se ejecutan con una frecuencia definida.
	¿Se restringe la instalación de software no autorizado?	**1**	Existen restricciones parciales para los usuarios.
8.2 Copias de seguridad	¿Se realizan copias de seguridad de la información institucional?	**2**	Se ejecutan respaldos periódicos.
	¿Las copias de seguridad son verificadas periódicamente?	**1**	La restauración no se prueba regularmente.

	¿Las copias se almacenan en un sitio seguro?	**2**	Se almacenan en infraestructura protegida.
8.3 Seguridad de la red	¿La red institucional cuenta con firewall?	**2**	El firewall protege la red perimetral.
	¿Se monitorean los intentos de acceso no autorizado?	**1**	El monitoreo se realiza únicamente cuando existen incidentes.
	¿La red inalámbrica utiliza mecanismos de cifrado seguros?	**1**	Utiliza WPA2; se recomienda migrar a WPA3.
8.4 Capacitación y concienciación	¿Se capacita periódicamente al personal sobre ciberseguridad?	**1**	Las capacitaciones no son continuas.
	¿Se realizan campañas de prevención de phishing?	**0**	No existen campañas institucionales permanentes.
	¿Los usuarios conocen el procedimiento para reportar incidentes?	**1**	El procedimiento es conocido únicamente por parte del personal.

Resumen de resultados

Valor	Cantidad

2 (Cumple)	**7**
1 (Cumple parcialmente)	**10**
0 (No cumple)	**2**
Elaborado por:	**Revisado por:**
Fecha:	**Firma**:

4.3.5 Ejecución de los cuestionarios para analizar riesgos

Una vez diseñados los cuestionarios que corresponden a las normas de seguridad informática, se aplicaron en los centros de cómputo. Dicha actividad fue llevada a cabo con el personal administrativo, los usuarios asignados con asiduidad de los equipos de la institución y los responsables del área de Tecnologías de la Información.

La aplicación de cuestionarios tuvo lugar en modo presencial a través de entrevistas directas y observaciones asistidas. Esto permitió que cada pregunta fuera interpretada mediante una lectura correcta de las mismas para asegurar la fidelidad de la información obtenida. Así mismo, durante la aplicación de los cuestionarios se resolvieron inseguridades en cuanto a los controles llevados a cabo, de la gestión de accesos, uso de contraseñas y de las prácticas operativas que pueden establecer vulnerabilidades en seguridad del entorno.

La aplicación de los cuestionarios permitió indicar la situación de cumplimientos de los requisitos en seguridad informática y determinar posibles brechas en el uso físico o lógico de la tecnología aplicada. Así mismo, esta aplicación proporcionó información valiosa sobre el

imaginario, hábitos y prácticas de uso, constituyendo un insumo valiosísimo para el proceso de análisis de riesgos.

4.3.5.1 Cuestionario de Identificación (Incendio)

Activo: Servidor principal

Indicador: Controles de prevención de incendios en el servidor principal.

Tabla 19

Cuestiomario de identificación de peligros (Incendio)

CUESTIONARIO PARA IDENTIFICAR RIESGO			**C1 Pág. 1 de 6**		
Nº	**Preguntas**	**Sí**	**No**	**Observación**	**Riesgo**
1	¿El cuarto del servidor cuenta con detectores de humo?	X			0
2	¿Existe sistema automático contra incendios?		X	No dispone	1
3	¿Las instalaciones eléctricas reciben mantenimiento periódico?	X			0
4	¿El servidor dispone de UPS?	X			0
5	¿Existe protección contra sobretensiones?		X	Protección parcial	1
6	¿Los cables eléctricos están en buen estado?	X			0
7	¿Se inspeccionan periódicamente los tableros eléctricos?	X			0
8	¿Existen extintores cercanos?	X			0

9	¿Los extintores están vigentes?	X			0
10	¿Existe señalización de evacuación?	X			0
11	¿El personal conoce el protocolo contra incendios?	X			0
12	¿Se realizan simulacros?	X			0
13	¿El cuarto permanece limpio?	X			0
14	¿Se almacenan materiales inflamables?		X	No existen	0
15	¿Existe monitoreo de temperatura?	X			0
16	¿Se realiza mantenimiento preventivo del servidor?	X			0
17	¿Existe registro de incidentes eléctricos?	X			0
18	¿Se revisan periódicamente los sistemas de protección?	X			0
19	¿El acceso al cuarto del servidor está restringido?	X			0
20	¿Los controles actuales son suficientes para prevenir incendios?		X	Requiere mejoras	1
Realizado Por:			**Revisado Por:**		
Fecha:			**Firma:**		

4.3.5.2 Cuestionario de Identificación (Malware - Ransomware)

Activo: Computadoras Aula TIC

Indicador: Controles para prevenir malware.

Tabla 20

Cuestiomario de identificación de peligros (Malware - Ransomware)

CUESTIONARIO PARA IDENTIFICAR RIESGO				C1 Pág. 2 de 6	
Nº	**Preguntas**	**Sí**	**No**	**Observación**	**Riesgo**
1	¿Los equipos tienen antivirus actualizado?	X			0
2	¿Todos los sistemas operativos están actualizados?		X	Equipos desactualizados	1
3	¿Existe política para instalar software?	X			0
4	¿Los usuarios tienen permisos restringidos?		X	Todos son administradores	1
5	¿Se bloquea software no autorizado?		X		1
6	¿Existe filtro de descargas peligrosas?		X		1
7	¿Se realizan respaldos periódicos?	X			0
8	¿Las copias son verificadas?	X			0
9	¿Se capacita a los usuarios?	X			0
10	¿Se restringe el uso de USB?	X			0
11	¿Existe monitoreo de incidentes?	X			0
12	¿Firewall activo?	X			0
13	¿Contraseñas robustas?	X			0
14	¿Antimalware institucional?	X			0
15	¿Se revisan periódicamente los equipos?	X			0
16	¿Existe registro de incidentes?	X			0
17	¿Existe plan de recuperación?	X			0

18	¿Software con licencia?	X			0
19	¿Se controla el acceso a Internet?	X			0
20	¿Los controles actuales son suficientes para evitar ransomware?		X	Persisten vulnerabilidades	1
Realizado Por:				**Revisado Por:**	
Fecha:				**Firma:**	

4.3.5.3 Cuestionario de Identificación (Intrusión Externa)

Activo: Red WiFi Institucional

Indicador: Controles de seguridad de la red inalámbrica.

Tabla 21

Cuestiomario de identificación de peligros (Intrusión Externa)

CUESTIONARIO PARA IDENTIFICAR RIESGO				**C1 Pág. 3 de 6**	
Nº	**Preguntas**	**Sí**	**No**	**Observación**	**Riesgo**
1	¿La red utiliza WPA3?		X	Usa WPA2	1
2	¿La contraseña es robusta?	X			0
3	¿Se cambia periódicamente?		X		1
4	¿Existe red para invitados?	X			0
5	¿Los dispositivos están registrados?		X		1
6	¿Existe filtrado MAC?		X		1
7	¿Firewall activo?	X			0

8	¿Se monitorean intentos de acceso?		X		1
9	¿Se revisan los registros?	X			0
10	¿Existe IDS/IPS?		X	No implementado	1
11	¿Firmware actualizado?	X			0
12	¿Se realizan pruebas de penetración?		X		1
13	¿Acceso administrativo restringido?	X			0
14	¿Autenticación segura?	X			0
15	¿Existe segmentación de red?	X			0
16	¿Se monitorea el tráfico?	X			0
17	¿Políticas de uso de red?	X			0
18	¿Se bloquean dispositivos desconocidos?		X		1
19	¿Existe monitoreo continuo?		X		1
20	¿Los controles actuales previenen intrusiones?		X	Riesgo alto	1
Realizado Por:				**Revisado Por:**	
Fecha:				**Firma:**	

4.3.5.4 Cuestionario de Identificación (Acceso No Autorizado)

Activo: Sistema de Gestión Académica

Indicador: Controles de acceso lógico.

Tabla 22

Cuestiomario de identificación de peligros (Acceso No Autorizado)

CUESTIONARIO PARA IDENTIFICAR RIESGO			C1 Pág. 4 de 6		
Nº	**Preguntas**	**Sí**	**No**	**Observación**	**Riesgo**
1	¿Cada usuario posee credenciales propias?	X			0
2	¿Se exigen contraseñas robustas?		X	Contraseñas débiles	1
3	¿Las contraseñas vencen periódicamente?		X		1
4	¿Existe autenticación multifactor?		X		1
5	¿Se bloquean cuentas tras intentos fallidos?	X			0
6	¿Permisos por roles?	X			0
7	¿Se revisan los permisos periódicamente?	X			0
8	¿Se eliminan cuentas inactivas?	X			0
9	¿Existe registro de accesos?	X			0
10	¿Se monitorean actividades sospechosas?	X			0
11	¿Administradores con cuentas independientes?	X			0
12	¿Recuperación segura de contraseñas?	X			0
13	¿Capacitación sobre seguridad?	X			0
14	¿Política de uso aceptable?	X			0
15	¿Auditorías del sistema?	X			0
16	¿Sesiones expiran automáticamente?	X			0
17	¿Información cifrada?	X			0
18	¿Respaldos del sistema?	X			0
19	¿Se realizan auditorías de acceso?	X			0

20	¿Los controles actuales impiden accesos no autorizados?		X	Debe fortalecerse MFA	1
Realizado Por:				**Revisado Por:**	
Fecha:				**Firma:**	

4.3.5.5 Cuestionario de Identificación (Robo de Hardware)

Activo: Base de datos de alumnos

Indicador: Seguridad física de los equipos.

Tabla 23

Cuestiomario de identificación de peligros (Robo de Hardware)

CUESTIONARIO PARA IDENTIFICAR RIESGO				**C1 Pág. 5 de 6**	
Nº	**Preguntas**	**Sí**	**No**	**Observación**	**Riesgo**
1	¿Los servidores permanecen bajo llave?	X			0
2	¿Existe CCTV?	X			0
3	¿Hay control de ingreso?	X			0
4	¿Existe registro de visitantes?	X			0
5	¿Los discos están cifrados?	X			0
6	¿Inventarios periódicos?	X			0
7	¿Etiquetas institucionales?	X			0
8	¿Existe alarma?	X			0
9	¿Se restringe la salida de equipos?	X			0

10	¿Existe política de préstamo?	X			0
11	¿Hay custodio responsable?	X			0
12	¿Inspecciones periódicas?	X			0
13	¿Respaldos externos?	X			0
14	¿Registro de incidentes?	X			0
15	¿Monitoreo de acceso?	X			0
16	¿Equipos asegurados físicamente?	X			0
17	¿Procedimiento ante robos?	X			0
18	¿Personal capacitado?	X			0
19	¿Inventario actualizado?	X			0
20	¿Los controles actuales previenen el robo de hardware?	X			0
Realizado Por:					**Revisado Por:**
Fecha:					**Firma:**

Resultado: probabilidad baja.

4.3.5.6 Cuestionario de Identificación (Phishing)

Activo: Correo Corporativo

Indicador: Controles para prevenir phishing.

Tabla 24

Cuestiomario de identificación de peligros (Phishing)

CUESTIONARIO PARA IDENTIFICAR RIESGO			**C1 Pág. 6 de 6**		
Nº	**Preguntas**	**Sí**	**No**	**Observación**	**Riesgo**
1	¿Existe filtro antispam?	X			0
2	¿Se utiliza autenticación multifactor?		X		1
3	¿Los usuarios reciben capacitación?	X			0
4	¿Se realizan campañas de concienciación?		X		1
5	¿Los usuarios verifican remitentes?	X			0
6	¿Existe botón para reportar phishing?		X		1
7	¿Se analizan enlaces sospechosos?	X			0
8	¿Se analizan archivos adjuntos?	X			0
9	¿Contraseñas robustas?	X			0
10	¿Cambio periódico de contraseñas?	X			0
11	¿Monitoreo de accesos?	X			0
12	¿Bloqueo de dominios maliciosos?	X			0
13	¿Existe política para el uso del correo?	X			0
14	¿Se realizan simulaciones de phishing?		X		1
15	¿Existe respaldo del correo?	X			0
16	¿Se registran incidentes?	X			0
17	¿Los usuarios conocen el procedimiento para reportar correos sospechosos?	X			0

18	¿El sistema se mantiene actualizado?	X			0
19	¿Existe respuesta ante incidentes?	X			0
20	¿Los controles actuales son suficientes para prevenir phishing?		X	Requiere fortalecer capacitación y MFA	1
Realizado Por:				**Revisado Por:**	
Fecha:				**Firma:**	

4.3.6 Aplicación de análisis de riesgo

Posteriormente, con los datos recolectados, se procedió a la aplicación del análisis de riesgos siguiendo una metodología sistemática basada en la identificación de activos, amenazas, vulnerabilidades y posibles impactos. Este análisis permitió establecer una visión detallada de los riesgos que afectan la seguridad informática, especialmente aquellos relacionados con accesos no autorizados, manipulación de equipos, pérdida de información, uso inadecuado de credenciales o ausencia de controles físicos y lógicos adecuados.

Para ello, se clasificaron los activos tecnológicos en categorías como: equipos de cómputo, servidores, sistemas de autenticación, documentación, información institucional y elementos físicos de protección. A continuación, se identificaron las amenazas probables como los ataques internos, las fallas eléctricas, los accesos indebidos, los robos de equipos y errores humanos, finalmente, así se evaluaron las vulnerabilidades asociadas, como las contraseñas débiles, falta de supervisión de accesos, carencia de cerraduras seguras o inexistencia de registros de ingreso.

Tabla 25

Resultados de identificación de peligros

Identificación de Riesgos	**R1** **Pág. 1 de 6**
Incendio debido a: • La inexistencia de un sistema automático de detección y supresión de incendios en el cuarto del servidor. • La protección insuficiente contra sobretensiones eléctricas. • La ocurrencia de cortocircuitos ocasionados por fallas eléctricas. • La ausencia de monitoreo permanente de temperatura en el servidor. • El deterioro del cableado eléctrico por falta de mantenimiento preventivo. • La inexistencia de un plan específico de respuesta ante incendios. • La falta de inspecciones periódicas del sistema eléctrico. • El riesgo de sobrecarga eléctrica. • La ausencia de redundancia en la infraestructura eléctrica. • La posibilidad de pérdida del servidor y de la información institucional.	
Realizado por:	Revisado por:
Fecha:	Firma:

Identificación de Riesgos	R1 Pág. 2 de 6
Malware (Ransomware) debido a: • La descarga de archivos de fuentes no confiables. • La apertura de archivos adjuntos maliciosos. • La inexistencia de restricciones para instalar software. • Equipos con sistemas operativos desactualizados. • Antivirus sin actualización permanente. • Ausencia de filtros de descargas. • Uso de memorias USB sin verificación. • Escasa capacitación de usuarios. • Falta de monitoreo continuo. • Posibilidad de cifrado de la información institucional.	
Realizado por:	Revisado por:
Fecha:	Firma:

Identificación de Riesgos	R1 Pág. 3 de 6
Intrusión externa debido a: • Configuraciones débiles de la red WiFi.	

• Contraseñas inalámbricas poco robustas. • No cambiar credenciales periódicamente. • Ausencia de monitoreo continuo. • No existe IDS/IPS. • Acceso de dispositivos no autorizados. • Deficiente segmentación de red. • Falta de pruebas de penetración. • Posible interceptación de información. • Robo o alteración de información institucional.

Realizado por:	Revisado por:
Fecha:	Firma:

Identificación de Riesgos	**R1** **Pág. 4 de 6**
Acceso no autorizado debido a: • Uso de contraseñas débiles. • Ausencia de autenticación multifactor. • Credenciales compartidas. • Deficiente administración de privilegios. • No revisar cuentas periódicamente.	

• Cuentas inactivas habilitadas. • Políticas débiles de credenciales. • Escasa capacitación. • Posible modificación de información. • Pérdida de confidencialidad, integridad y disponibilidad.

Realizado por:	Revisado por:
Fecha:	Firma:

Identificación de Riesgos	**R1** **Pág. 5 de 6**
Robo de hardware debido a: • Ingreso de personas no autorizadas. • Deficiente control físico. • Ausencia de monitoreo permanente. • Falta de procedimientos para préstamo. • Inventarios desactualizados. • Equipos sin identificación suficiente. • Ausencia de alarmas. • Deficiente control de visitantes. • Falta de inspecciones.	

• Pérdida de información almacenada.	
Realizado por:	Revisado por:
Fecha:	Firma:

Identificación de Riesgos	**R1** **Pág. 6 de 6**
Phishing debido a: • Recepción de correos fraudulentos. • Falta de autenticación multifactor. • Desconocimiento sobre ingeniería social. • No existen campañas de concienciación. • No se realizan simulaciones. • Apertura de enlaces maliciosos. • Contraseñas vulnerables. • Filtros de correo insuficientes. • Robo de credenciales. • Acceso no autorizado mediante cuentas comprometidas.	
Realizado por:	Revisado por:

Fecha:	Firma:

4.3.7 Tabulación de análisis de riesgos

Una vez obtenida la información del análisis de riesgos, se procedió a la tabulación y organización de los datos recopilados, cada uno de los riesgo identificados se los fue registrando en una matriz que permitió visualizar de una mejor manera, más clara y ordenada la relación entre amenazas, vulnerabilidades y activos, este proceso facilitó la comparación entre riesgos, destacando así a aquellos con una mayor relevancia para la seguridad institucional.

Basándonos en las normas ISO 27001 se ha evaluado los porcentajes de cumplimiento de controles mediante una tabla de evaluación la cual va del 0 al 2:

Tabla 26

Tabulación de análisis de riesgos

SI	1
NO	0
NO APLICA	2

PROBABILIDAD DE INCENDIO		
	Total	No aplica
Total de campos evaluados	20	0
Total seguro	17	0
Total riesgo	3	0
Porcentaje seguro	17*100/20=	85%
Porcentaje riesgo	3*100/20=	15%

Realizado por:	Revisado por:
Fecha:	Firma:

PROBABILIDAD DE MALWARE (RANSOMWARE)		
	Total	No aplica
Total de campos evaluados	20	0
Total seguro	15	0
Total riesgo	5	0
Porcentaje seguro	15*100/20=	75%
Porcentaje riesgo	5*100/20=	25%

Realizado por:	Revisado por:
Fecha:	Firma:

PROBABILIDAD DE INTRUSIÓN EXTERNA		
	Total	No aplica
Total de campos evaluados	20	0
Total seguro	11	0
Total riesgo	9	0
Porcentaje seguro	11*100/20=	55%
Porcentaje riesgo	9*100/20=	45%

Realizado por:	Revisado por:
Fecha:	Firma:

PROBABILIDAD DE ACCESO NO AUTORIZADO		
	Total	No aplica
Total de campos evaluados	20	0
Total seguro	16	0
Total riesgo	4	0
Porcentaje seguro	16*100/20=	80%
Porcentaje riesgo	4*100/20=	20%

Realizado por:	Revisado por:
Fecha:	Firma:

PROBABILIDAD DE ROBO DE HARDWARE		
	Total	No aplica
Total de campos evaluados	20	0
Total seguro	20	0
Total riesgo	0	0
Porcentaje seguro	20*100/20=	100%
Porcentaje riesgo	0*100/20=	0%

Realizado por:	Revisado por:
Fecha:	Firma:

PROBABILIDAD DE PHISHING		
	Total	No aplica
Total de campos evaluados	20	0
Total seguro	16	0
Total riesgo	4	0
Porcentaje seguro	16*100/20=	80%
Porcentaje riesgo	4*100/20=	20%
Realizado por:	Revisado por:	
Fecha:	Firma:	

Los resultados evidencian que el riesgo con mayor nivel de exposición corresponde a la intrusión externa, seguido por el malware. El robo de hardware presenta la menor probabilidad debido a la existencia de controles físicos implementados. Los hallazgos permiten priorizar el fortalecimiento de los controles de acceso lógico, seguridad perimetral, autenticación multifactor y programas de concienciación frente a ataques de ingeniería social.

4.3.8 Impacto de análisis de riesgos

El impacto del análisis de riesgos se determinó considerando las consecuencias potenciales que podría generar cada amenaza sobre los activos tecnológicos y la operación institucional. Se evaluaron aspectos como:

- Interrupción de actividades académicas o administrativas
- Pérdida de información confidencial o institucional
- Daños a equipos informáticos
- Accesos no autorizados
- Compromiso de datos personales
- Afectaciones a la disponibilidad y confiabilidad de los sistemas

En cada riesgo se evaluó la gravedad de cada uno de los daños que podría ocasionarse, haciendo una clasificándolo en la medida de bajo, medio o alto, el análisis permitió identificar situaciones que requieren atención humana inmediata, como accesos no autorizados a las salas docentes, falta de controles de ingreso y uso indebido de dispositivos externos. A partir de esto se establecieron cuáles son las prioridades y se definieron las acciones de mejora acordes a la realidad de la institución.

4.3.9 Valoración de riesgos

La valoración de riesgos se realizó combinando la probabilidad de ocurrencia y el impacto identificado para cada amenaza detectada durante la auditoría informática, conforme a los criterios de ISO/IEC 27001 e ISO 27005. Los riesgos fueron clasificados para establecer prioridades de tratamiento y definir acciones preventivas y correctivas.

Los niveles utilizados fueron:

- Muy bajo
- Bajo

- Medio
- Alto
- Muy alto

Tabla 27

Niveles de riesgos

Nivel		Probabilidad
1	Mas bajo	1%-10%
2		11%-30%
3		31%-50%
4		51%-75%
5	Mas alto	76%-100%

4.3.10 Matriz de riesgos

La matriz permitió representar el nivel de criticidad de cada riesgo identificado, priorizando aquellos con mayor probabilidad e impacto para orientar la implementación de controles.

Tabla 28

Especificaciones de riesgos

	Riesgo muy alto: Requiere medidas importantes preventivas urgentes
	Riesgo medio: Medidas preventivas obligatorias
	Riesgo bajo: Estudiar económicamente si es necesario
	Riesgo muy bajo: Se vigilará, aunque no requiere medidas preventivas

La matriz incluyó:

- Riesgos ubicados en el cuadrante de alta probabilidad y alto impacto, considerados críticos y prioritarios.
- Riesgos con probabilidad media y alto impacto, que requieren mitigación programada.
- Riesgos de baja probabilidad e impacto, cuya atención puede ser preventiva y planificada.
- Esta herramienta se convrtió en un recurso fundamental para apoyar la toma de decisiones en materia de seguridad informática y permitió orientar estrategias efectivas para el control de accesos.

Tabla 29

Evaluación de riesgos

Evaluación de riesgos

		LEYENDA					
		GRAVEDAD DEL IMPACTO					
		Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy alto (5)	
Aparición	Muy alto	5	5	10	15	20	25
(Probabilidad)	Alto	4	4	8	12	16	20
	Medio	3	3	6	9	12	15
	Bajo	2	2	4	6	8	10
	Muy bajo	1	1	2	3	4	5

4.3.10.1 Procesos (Ejemplo: estudio de factibilidad)

Como parte del proceso de auditoría, se llevó a cabo un estudio de factibilidad orientado a evaluar la viabilidad de implementar mejoras en los sistemas de control de accesos. Este estudio consideró aspectos técnicos, operativos, económicos y organizacionales relacionados con la adopción de nuevas medidas de seguridad.

Tabla 30

Cálculo de Impacto

Cálculo de Impacto	**R2 Pág. 1 de 1**

Riesgo	Confidencialidad	Integridad	Disponibilidad	Valor de impacto
Incendio	3	4	3	10
Malware	4	4	3	11
Intrusión externa	4	4	4	12
Acceso no autorizado	4	4	3	11
Robo de hardware	3	4	3	10
Phishing	4	3	3	10

Escala	**Descripción**
1	No afecta mayormente
2	Afecciones menores

	3	Paralización de la actividad, corto tiempo
	4	Afecciones mayores
	5	Efecto catastrófico
Realizado por:		Revisado por:
Fecha:		Firma:

Los resultados evidencian que los riesgos más críticos corresponden al malware, la intrusión externa y el acceso no autorizado, debido a su elevada probabilidad y alto impacto sobre la confidencialidad, integridad y disponibilidad de la información.

CAPÍTULO IV

5 EVALUACIÓN DE RESULTADOS

Tipo de Auditoría: Auditoría de Seguridad Informática.

Dirigido a: Rector(a) de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora.

Objetivo

- Evaluar el nivel de seguridad informática de los equipos de cómputo y la infraestructura tecnológica de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora, con base en buenas prácticas y estándares de seguridad de la información.

El presente capítulo tiene como finalidad presentar la propuesta de mejora derivada de los resultados obtenidos durante la auditoría de seguridad informática realizada a los equipos informáticos y a la infraestructura tecnológica de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora.

5.1 Objetivo de la propuesta

- Confirmar el alcance de la auditoría y los criterios establecidos.
- Verificar el cumplimiento de los controles de seguridad de la información conforme a las normas ISO/IEC 27001 e ISO 19011.
- Identificar oportunidades de mejora en el Sistema de Gestión de Seguridad de la Información

5.1.1 Alcance de la propuesta

La propuesta está dirigida a la infraestructura tecnológica de la Unidad Educativa Fisco Misional Juan Pablo II – La Bramadora y comprende la aplicación de las técnicas desarrolladas en

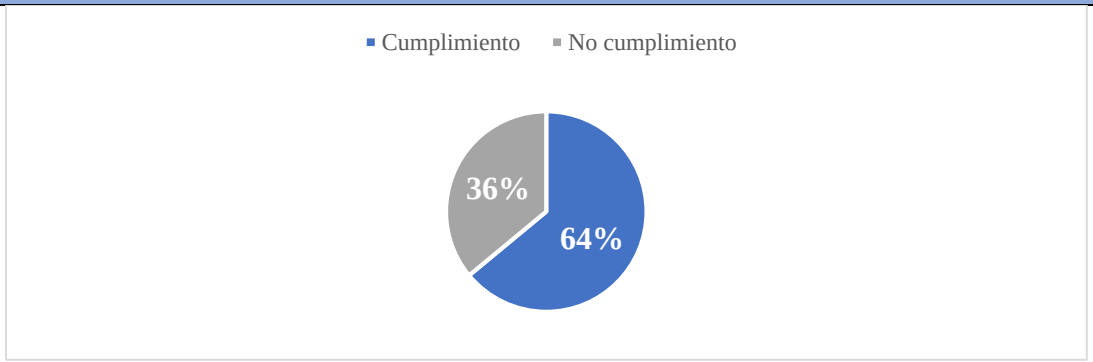
el programa para la identificación, análisis, evaluación y tratamiento de riesgos de seguridad informática. Se consideran los activos tecnológicos seleccionados, las amenazas y vulnerabilidades asociadas, la valoración de los controles existentes y la determinación de medidas de seguridad para su tratamiento. El análisis contempla los riesgos de incendio, malware–ransomware, intrusión externa, acceso no autorizado, robo de hardware y phishing, con la finalidad de fortalecer la protección de la infraestructura tecnológica y de la información institucional.

5.2 Hallazgos

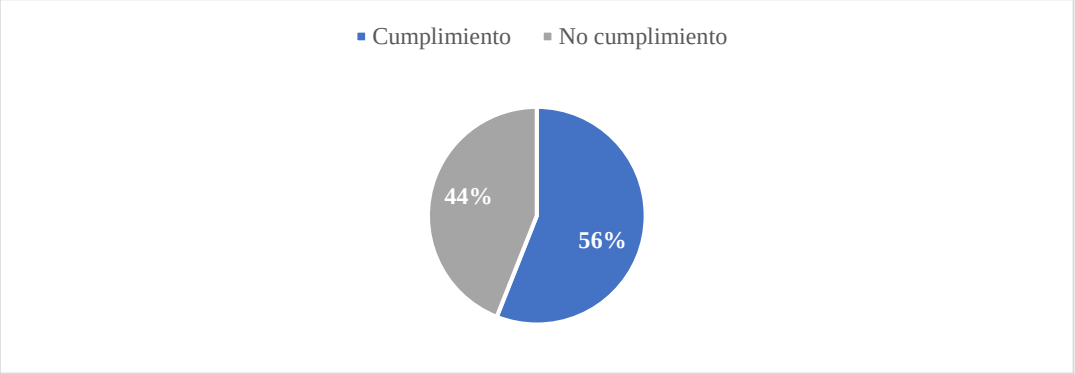
Una vez obtenidos los valores de probabilidad e impacto, se procedió a realizar la interpretación general del riesgo:

Tabla 31

Hallazgos obtenidos de evaluación

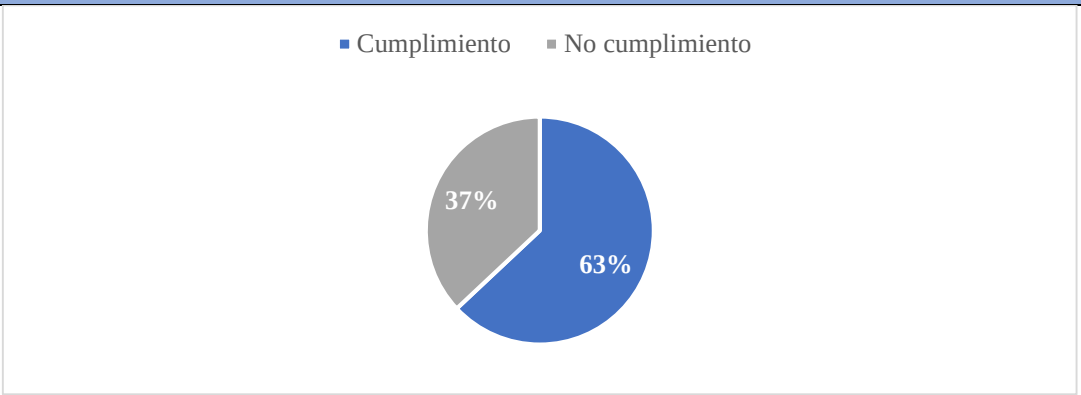
Evaluación de cumplimientos de requisitos ISO 27001

Estos resultados evidencian que la institución dispone de controles básicos de seguridad informática; sin embargo, aún existen oportunidades de mejora relacionadas con la formalización de políticas, fortalecimiento del Sistema de Gestión de Seguridad de la Información, monitoreo continuo y capacitación del personal.

Comprensión de la organización y su contexto



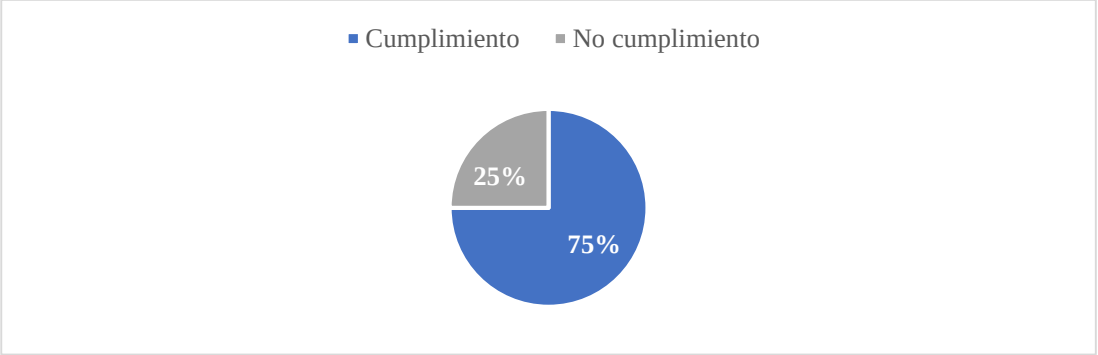
En lo que se refiere al requisito del contexto de la organización, se ha obtenido un 56 % de cumplimiento, lo cual pone de manifiesto que la organización ha ido desarrollando actividades como la identificación de riesgos, el inventario de activos y el compromiso institucional de la Seguridad Informática. Sin embargo, persisten debilidades en lo que respecta a la formalización del Sistema de Gestión de la Seguridad de la Información (SGSI), la completa definición del alcance y la documentación de políticas y responsabilidades.

Gestión del Control de Accesos



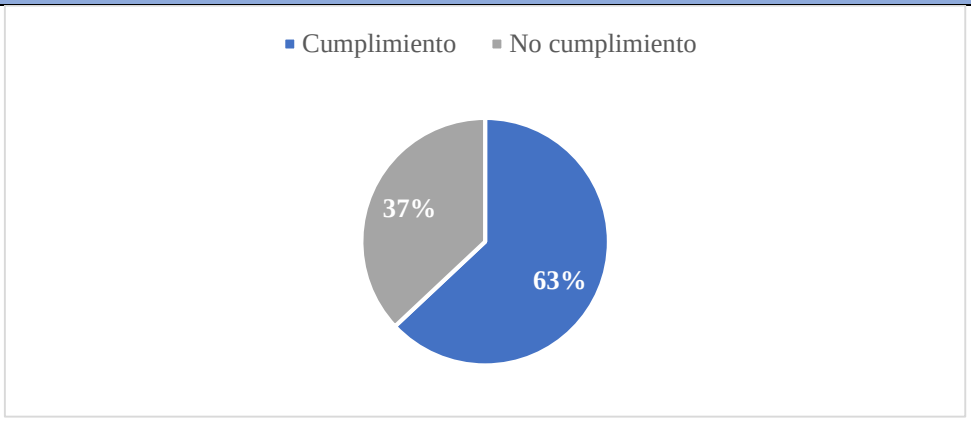
El control de accesos presenta un 63 % de cumplimiento, el cual indica que la organización tiene controles en relación con la asignación de usuarios, la administración de privilegios o registros de accesos, aunque también persisten importantes deficiencias como la no implementación de autenticación multifactorial.

Seguridad Física y Ambiental



La evaluación de la seguridad física y ambiental obtuvo un 75 % de cumplimiento, constituyéndose en uno de los requisitos con mejores resultados. La institución cuenta con controles adecuados sobre el acceso al cuarto de servidores, inventario de equipos, sistemas de videovigilancia y protección física de los activos tecnológicos.

Gestión de Riesgos y Seguridad Operacional

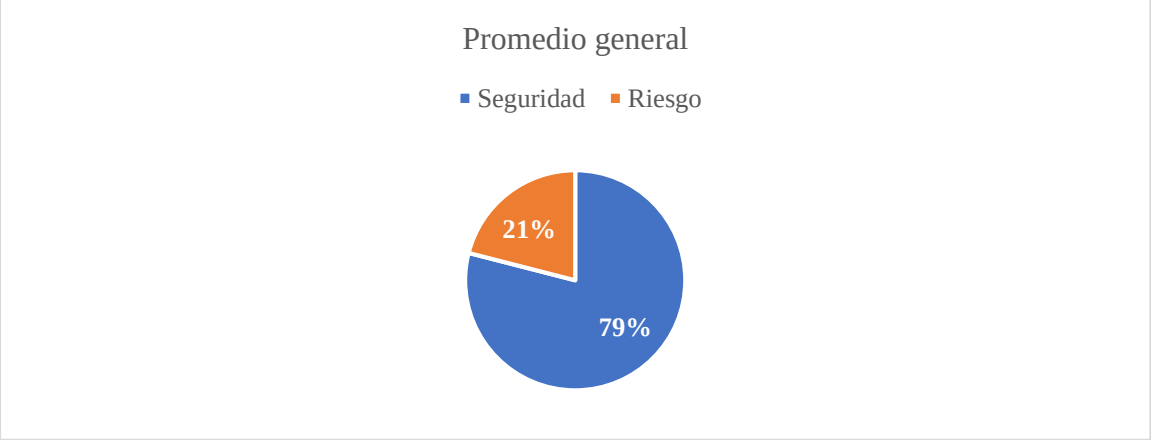


El requisito relacionado con la gestión de riesgos y la seguridad operacional alcanzó un 63% de cumplimiento, evidenciando que la institución realiza actividades de identificación y evaluación de riesgos y dispone de controles básicos de protección tecnológica.

5.3 Interpretación objetiva

Figura 3

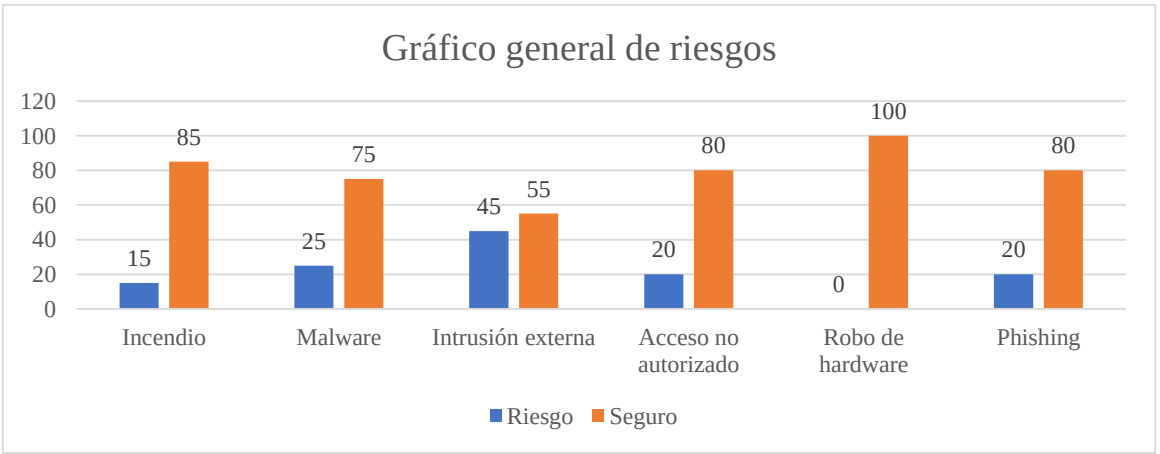
Promedio general



La Unidad Educativa Fiscomisional Juan Pablo II – La Bramadora presenta un nivel general de seguridad del 79%. Estos resultados demuestran que la institución dispone de controles físicos y lógicos que contribuyen a la protección de los activos tecnológicos; sin embargo, aún existen vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Figura 4

Gráfico genera de riesgos



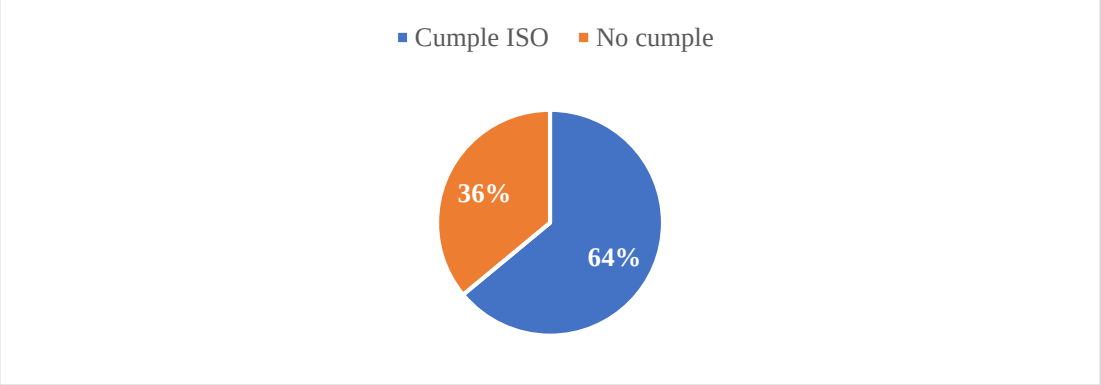
Los resultados evidencian que la intrusión externa constituye la amenaza con mayor nivel de exposición, alcanzando un 45 % de riesgo, seguida por el malware (25 %). Ambos riesgos representan las principales vulnerabilidades de la infraestructura tecnológica debido a la ausencia de algunos controles avanzados de seguridad.

5.4 Opinión de la Auditoría

Como resultado de la auditoría informática desarrollada, se concluye que la institución presenta un nivel de cumplimiento medio, alcanzando aproximadamente un 64% de conformidad con los controles evaluados de la norma y un nivel general de seguridad del 79% en los riesgos analizados.

Figura 5

Cumplimiento de ISO



5.5 Riesgos identificados y nivel de riesgo

Los riesgos identificados tuvieron la siguiente calificación:

Tabla 32

Riesgos y nivel de riesgos

Nº	Riesgo identificado	Activo afectado	Nivel de riesgo
1	Incendio	Servidor principal	Bajo
2	Malware (Ransomware)	Computadoras Aula TIC	Medio
3	Intrusión externa	Red WiFi institucional	Alto
4	Acceso no autorizado	Sistema de Gestión Académica	Bajo

5	Robo de hardware	Base de datos de alumnos	Muy bajo
6	Phishing	Correo corporativo	Bajo

5.6 Recomendaciones para riesgos con mayor puntuación

De acuerdo con los resultados obtenidos a partir de la auditoría informática, se recomienda: establecer un Sistema de Gestión de Seguridad de la Información en línea con la norma ISO/IEC 27001, robusteciendo así las políticas institucionales, los procedimientos de control y la documentación relativa a la seguridad informática.

Tabla 33

Plan de tratamiento del riesgo: Malware (Ransomware)

Riesgo	Nivel de riesgo	Objetivo del control	Actividades de control	Responsable	Recursos	Frecuencia	Indicador
Malware (Ransomware)	Medio	Reducir la probabilidad de infección y minimizar el impacto de un ataque de ransomware.	Actualizar el sistema operativo y el software de todos los equipos.	Responsable del laboratorio TIC	Conexión a Internet, licencias de software	Mensual	100 % de equipos actualizados.
			Instalar y mantener un antivirus con protección en tiempo real.	Responsable TIC	Antivirus institucional	Permanente	Equipos con antivirus activo.
			Implementar copias de seguridad periódicas de la información crítica en dispositivos externos o almacenamiento en la nube.	Rector y Responsable TIC	Disco externo o servicio en la nube	Semanal	Número de respaldos realizados.
			Capacitar a docentes y estudiantes sobre riesgos de malware, descargas inseguras y uso de memorias USB.	Rector y Docentes	Material de capacitación	Semestral	Porcentaje de personal capacitado (>90 %).

Tabla 34

Plan de tratamiento del riesgo: Intrusión externa

Riesgo	Nivel de riesgo	Objetivo del control	Actividades de control	Responsable	Recursos	Frecuencia	Indicador

Intrusión externa	Alto	Fortalecer la seguridad de la red inalámbrica para impedir accesos no autorizados.	Cambiar las credenciales predeterminadas del router y utilizar contraseñas robustas.	Responsable TIC	Router institucional	Inmediato y anual	Contraseña actualizada conforme a la política institucional.
			Configurar el protocolo de seguridad WPA3 (o WPA2 si el equipo no lo soporta).	Responsable TIC	Router WiFi	Permanente	Red protegida con cifrado seguro.
			Separar la red administrativa de la red destinada a estudiantes mediante segmentación o VLAN.	Responsable TIC	Equipos de red	Una sola implementación y revisión anual	Redes segmentadas correctamente.
			Deshabilitar WPS y servicios innecesarios del router.	Responsable TIC	Router	Permanente	Servicios inseguros deshabilitados.
			Revisar los registros de acceso y monitorear dispositivos conectados para detectar conexiones sospechosas.	Responsable TIC	Consola de administración del router	Mensual	Número de accesos no autorizados detectados y bloqueados.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIÓN

En relación con el objetivo específico orientado a analizar el diagnóstico -que centra en la situación actual- la encuesta permite contrastar un nivel institucional escaso, en relación a las políticas, la formación e incluso la claridad de la normativa. Solo un pequeño porcentaje del alumnado afirma conocer las normas de seguridad o poner de relieve que hay unas reglas definidas en relación con los equipos. En continuidad, las entrevistas permiten constatar que las indicaciones suelen transmitirse verbalmente, que no existen documentos formalizados ni los medios estables de seguimiento. El rector admite la necesidad de pasar de las impresiones globales hasta un diagnóstico técnico, mientras que en el caso de los docentes refieren una aplicación heterogénea en función de quién controle el uso del laboratorio.

Con relación al objetivo que abarca la identificación de las vulnerabilidades existentes en los equipos informáticos y la red institucional, los resultados tanto cuantitativos como cualitativos coinciden nuevamente. La encuesta muestra porcentajes negativos en el alcance de la existencia de software debidamente actualizado y con protección, en la valoración de que existen medidas de seguridad adecuadas en el laboratorio y en una valoración máxima de los sistemas de gestión de las contraseñas por parte de los estudiantes. La pregunta negativa en relación a la posibilidad del compartir las credenciales hace entender que un porcentaje importante del alumnado recurre a esa práctica. De la entrevista realizada, el responsable del laboratorio aporta una explicación de las operativas que hacen posible esa vulnerabilidad: existencia de equipos viejos, antivirus a veces no uniformizados, actualizaciones irregulares, infecciones recurrentes por memorias USB y diagnóstico y mantenimiento que se llevan a cabo de una forma más bien reactiva.

Respecto a la intención de evaluar los riesgos tecnológicos relacionados con las vulnerabilidades detectadas, la triangulación deja ver la existencia de las debilidades, pero también su posible impacto. Por ejemplo, la baja capacidad para identificar el phishing más la falta de reconocida capacitación por parte de los estudiantes y del personal intensificaría el riesgo de comprometer credenciales o permitir accesos no autorizados a las cuentas institucionales. De forma análoga, la baja capacitación en el uso de dispositivos USB y el constante recuerdo a infecciones previas en el laboratorio intensificarían las probabilidades de incidentes de malware con efectos sobre la disponibilidad y la continuidad de los servicios.

La triangulación también permite interpretar correctamente una constatación que podría parecer contradictoria si se contempla aisladamente: una parte del estudiantado no considera seguro el entorno tecnológico, pero otra sí manifiesta cierta sensación de seguridad a la hora de emplear los equipos de computación institucionales. Las entrevistas desvelan esta contradicción. Los docentes argumentan que gran parte del estudiantado asocia la seguridad con un funcionamiento inmediato, es decir, si el equipo enciende, permite realizar la tarea y pone de manifiesto ningún incidente evidente frente a ellos entonces lo deben percibir como seguridades. El rector advierte, no obstante, de que esta tranquilidad puede ser engañosa, ya que esa institución no cuenta con mecanismos formales de prevención, ni diagnósticos técnicos de periodicidad.

Finalmente, por lo que respecta al ámbito de lo que es presentarle el plan de mejora por lo que hace a la seguridad en la informática, el emparejamiento de ambos las herramientas puede resultar de gran utilidad. La encuesta tiene la capacidad de marcar en cuáles áreas hay que incidir para el alumnado: la de la formación, la de las normas, la de las actualizaciones, etc. Y las entrevistas van enlazando como debería articularse la intervención vistas desde la gestión de la institución: la de la formalización de las políticas, la del cronograma de mantenimiento preventivo,

la del control de memorias usb, la del refuerzo del acceso a información administrativa, la definición de unos protocolos frente a incidentes y la programación de unos programas de sensibilización periódicos.

6.2 RECOMENDACIONES

- Implementar el plan de tratamiento de riesgos elaborado a partir de los resultados de la auditoría, priorizando los riesgos clasificados con mayor nivel de criticidad. Para cada riesgo identificado deberán ejecutarse las medidas de tratamiento establecidas, asignar responsables, definir los recursos necesarios y establecer plazos para su cumplimiento.
- Establecer un programa de mantenimiento preventivo de forma permanente y gestión de vulnerabilidades que contemple el mantenimiento de los equipos informáticos, y la aplicación de actualizaciones de software de manera oportuna.
- Desarrollar un programa de formación y sensibilización continua en ciberseguridad para el personal docente, la administración y los estudiantes de la institución, que refuerce conocimientos sobre la utilización segura de las contraseñas, la detección de correos electrónicos fraudulentos, y la utilización correcta de dispositivos USB.
- Desarrollar la propuesta y ejecutar políticas de seguridad informática institucional que produzcan procedimientos claros en el manejo de equipos, control de accesos, administración de usuarios, copias de seguridad, clasificación de incidentes y protección de los datos personales, observando la normativa vigente.
- Generar un sistema periódico de copias de seguridad para garantizar la disponibilidad e integridad de la información institucional, generando las copias en soportes seguros que verifiquen periódicamente la correcta restauración de sus contenidos.

BIBLIOGRAFÍA

Ambit Iberia. (09 de febrero de 2021). *¿Qué es una auditoría de seguridad informática? Tipos y fases.* Obtenido de https://www.ambit-iberia.com/blog/qué-es-una-auditor%C3%ADa-de-seguridad-informática-tipos-y-fases#:~:text=Cuáles%20son%20los%20tipos%20de,auditor%C3%ADas%20de%20seguridad%20informática

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales (Registro Oficial Suplemento 459).* Registro Oficial Suplemento 459.

CYREBRO. (9 de abril de 2024). *Defender el aula: Amenazas a la ciberseguridad en los sistemas educativos.* Obtenido de https://www.cyrebro.io/es/blog/defender-el-aula-amenazas-a-la-ciberseguridad-en-los-sistemas-educativos/#:~:text=,casi%20el%20doble%20del

Gaptain. (15 de mayo de 2021). *Estudio Ciberseguridad y Convivencia escolar 2020.* Obtenido de Gaptain: https://gaptain.com/blog/estudio-ciberseguridad-y-convivencia-escolar-2020/#:~:text=Durante%20la%20revisión%20de%20la,centros%2C%20identificándose%20como%20principales%20causas

Gómez, Á. (2022). *Auditoría de seguridad informática.* Ediciones de la U.

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. *Revista Científica de la Investigación y el Conocimiento, 7*(1), 609-616.

Hernández-Sampieri, R. (2017). *Concepción o elección del diseño de investigación.* México: Mc Graw Hill Education.

Humpiri, M., Figueroa, E., Guillen, M., Cabel, D., Humpiri, R., & Huanca, J. (2023). Revisión sistemática: vulnerabilidades de seguridad cibernética en los activos digitales. *Ñawparisun-Revista de Investigación Científica de Ingenierías, 4*(2).

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jácome, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação, E32,* 427-440.

INCIBE. (10 de octubre de 2023). *Ciberseguridad en el sector educativo.* Obtenido de Instituto Nacional de Ciberseguridad: https://www.incibe.es/empresas/blog/ciberseguridad-en-el-sector-educativo#:~:text=Otro%20de%20los%20ataques%20por,de%20este%20tipo%20de

Jiménez, V., Tipanluisa, R., & León, C. (2025). Ciberseguridad en la educación superior: evaluación y estrategias de formación. *Technology Rain Journal, 4*(2).

Minaya, R., Mendoza, R., Mora, A., & Intriago, J. (2024). Análisis de las tecnologías y normativas en auditoría informática: un estudio de implementaciones basadas en COBIT y MAGERIT. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 6*(7), 366–380.

Molina-Granja, F., Cabezas-Heredia, E., Paredes, L., & Guambo-Vallejo, D. (2025). Ciberataques y rendimiento académico en educación superior: efectos psicoeducativos y estrategias de mitigación en contextos digitales latinoamericanos. *TESLA Revista Científica, 5*(1), e497-e497.

Montalvo, D., & Quishpe, L. (2024). Security Auditing and Information Assurance in Information Systems: A Practical Approach to Risk Identification and Mitigation. *Northern Reviews on Algorithmic Research, Theoretical Computation, and Complexity, 9*(12), 1-22.

Morales-Sáenz, F., Medina-Quintero, J., & Abrego-Almazán , D. (2025). Ciberseguridad en instituciones de educación superior: un análisis desde la perspectiva de la teoría de la motivación de protección. *IE Revista de Investigación Educativa de la REDIECH, 16*, e2271.

Navia, M., & Zambrano-Romero, W. (2021). Instrumento para la auditoría técnica de seguridad informática en pequeños proveedores de Internet. *Informática y Sistemas, 5*(2), 119–128.

Paladines Chuez, L. (2023). *Auditoría de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre en el periodo 2022.* Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador.

Ramos, I., Silva, A., & Girón, M. (2022). Auditoría informática para determinar las falencias del centro de cómputo, de la U.E. Miguel Ángel León Pontón. *Technology Rain Journal, 1*(1), e5.

Revista 360º. (20 de mayo de 2025). *El sector educativo en la mira de los ciberatacantes.* Obtenido de https://revista-360grados.com/el-sector-educativo-en-la-mira-de-los-ciberatacantes/#:~:text=Centroamérica%2015%20de%20mayo%20de,instituciones%20en%20todo%20el%20mundo

Rodríguez, R., Quispe, S., & Mendoza de los Santos, A. (2023). Frameworks Utilizados Para La Auditoría De Tecnologías De La Información En Las Universidades. *Revista Científica: BIOTECH AND ENGINEERING, 3*(1).

Rodriguez, V., & Calvarado, A. (2023). Dificultades e importancia de la auditoria informática. *Revista Científica: BIOTECH AND ENGINEERING, 3*(2).

Rosso, M. (2023). Revolución de la ciberseguridad en la cuarta revolución industrial. *Revista Ingeniería e Innovación del Futuro, 2*(2), 6-20.

Solís, B., Valderrama, H., Tejedor, E., & Vásquez, D. (2023). Seguridad de los Sistemas Informáticos Universitarios: Retos Pendientes. *Retos Pendientes. REICIT, 2*(2), 113-142.

Tejada, E. (2023). *Auditoría de seguridad informática. IFCT0109.* IC Editorial.

Zambrano, G. (2024). *SGSI Sistema de Gestión de Seguridad de la Información para el laboratorio de computación a la Unidad Educativa Alida Zambrano García [Trabajo de titulación, Universidad Laica "Eloy Alfaro" de Manabí, Extensión El Carmen]*. Repositorio ULEAM.

Zhuño, S., Heredia, S., & Paltan, D. (2022). Auditoria informática a centros de estudios. Caso U.E. "Nuestra Señora de Fátima". *Technology Rain Journal I, 1*(1), e2.

ANEXOS

ENCUESTA SOBRE SEGURIDAD INFORMÁTICA

Dirigida a: Estudiantes

Objetivo: Conocer el nivel de conocimiento, prácticas y percepción de los estudiantes respecto a la seguridad informática en la institución.

Instrucciones

Lee atentamente cada afirmación y marca con una X la opción que mejor represente tu nivel de acuerdo.

No hay respuestas correctas o incorrectas. La información será tratada de manera confidencial y utilizada únicamente con fines académicos.

Escala de valoración (Likert de 5 puntos)

Valor	Significado
1	Totalmente en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Totalmente de acuerdo

Datos generales (opcional)

Edad: _____

Curso / Grado: _____

Sexo: ☐ Femenino ☐ Masculino ☐ Prefiero no decir

Afirmaciones

Nº	Afirmación	1	2	3	4	5
1	Estoy familiarizado con las políticas o normas de seguridad informática de la institución.	☐	☐	☐	☐	☐

2	Soy capaz de identificar un correo electrónico sospechoso o intento de phishing.	☐	☐	☐	☐	☐
3	Utilizo contraseñas seguras (combinación de letras, números y símbolos) y las cambio periódicamente.	☐	☐	☐	☐	☐
4	Considero que el laboratorio de computación de la institución cuenta con medidas de seguridad adecuadas (antivirus, restricciones, etc.).	☐	☐	☐	☐	☐
5	He recibido capacitación o charlas sobre ciberseguridad en la institución.	☐	☐	☐	☐	☐
6	En ocasiones comparto mis contraseñas o cuentas con compañeros de clase.	☐	☐	☐	☐	☐
7	Conozco los riesgos de conectar dispositivos USB desconocidos o externos a las computadoras de la escuela.	☐	☐	☐	☐	☐
8	Los programas y sistemas de las computadoras de la institución se mantienen actualizados y protegidos contra virus.	☐	☐	☐	☐	☐
9	Me siento seguro/a al utilizar las computadoras e Internet de la institución.	☐	☐	☐	☐	☐
10	Existen normas claras en la institución para el uso adecuado de los equipos informáticos y se cumplen.	☐	☐	☐	☐	☐

ENTREVISTA SOBRE SEGURIDAD INFORMÁTICA INSTITUCIONAL

Dirigida a: Personal docente y administrativo

Tipo: Entrevista semiestructurada (preguntas abiertas)

Objetivo: Recopilar información sobre el nivel de conocimiento, la percepción institucional y las prácticas relacionadas con la seguridad informática en la institución.

Datos generales del entrevistado (opcional)

Cargo: _____

Área: ☐ Docente ☐ Administrativo

Años de experiencia en la institución: _____

Preguntas de la entrevista

1. **¿Qué medidas de seguridad informática se aplican actualmente en la institución para proteger los equipos y la información?**

2. **¿Cómo evalúa el nivel de conocimiento o concienciación de los docentes, estudiantes y personal administrativo acerca de la seguridad informática?**

3. **¿Han enfrentado incidentes de seguridad informática en la institución (por ejemplo, virus, accesos no autorizados o pérdida de datos)? ¿Cómo se manejaron dichas situaciones?**

4. **¿Qué políticas o normas internas existen para regular el uso de los equipos tecnológicos (computadoras, internet, cuentas de usuario) por parte de estudiantes y personal?**

5. **Desde su perspectiva, ¿cuáles considera que son los principales riesgos informáticos a los que está expuesta la institución en la actualidad?**

6. **¿Qué acciones, estrategias o capacitaciones cree que serían necesarias para mejorar la seguridad informática en la institución?**

7. **¿Considera que la institución cuenta con los recursos humanos, técnicos y presupuestarios suficientes para prevenir y responder adecuadamente a los incidentes de seguridad informática? ¿Por qué?**

CERTIFICADO ANTIPLAGIO

Certificado de análisis
Compilatio Magister+ | ULEAM-ECU

Compilatio3 Mendoza Capitu

ID : c7f282e6f3ccb9da4b647666d59bdefe5a2f29af

10%
Textos sospechosos

Nombre del fichero : Compilatio3 Mendoza Capitu.txt
Tamaño del archivo original : 1,13 MB
Número de palabras : 22.515

Depositante : RENELMO WLADIMIR MINAYA MACIAS
Fecha de depósito : 7 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 7 de agosto de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes 1%

Pasajes con similitudes a fuentes encontradas en diferentes colecciones.

Detección de IA 7%

Textos estilísticamente próximos a un texto generado por una IA.
Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.

Idiomas no reconocidos 2%

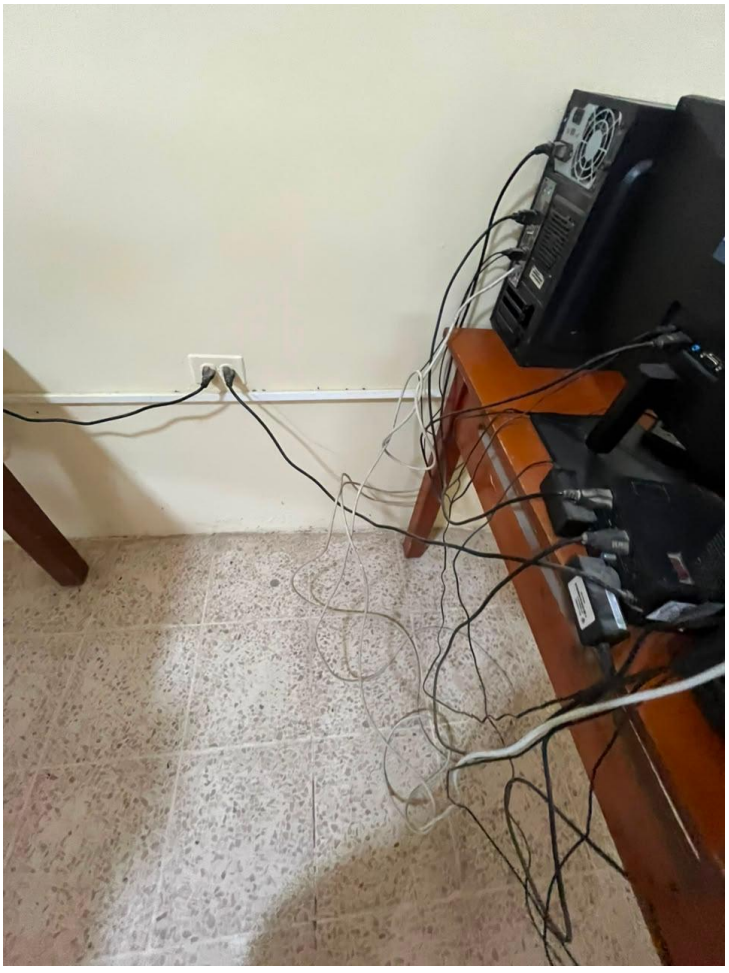
Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.
Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.

No incluido en el porcentaje de textos sospechosos :

Textos entre comillas 1%

Pasajes entre comillas, a menudo indicativos de una cita.

LABORATORIO EVALUADO




Google

GLOSARIO DE TÉRMINOS

Acceso no autorizado: Ingreso a un sistema, equipo, red o información por parte de una persona que no posee los permisos correspondientes para hacerlo.

Activo informático: Recurso tecnológico que posee valor para una organización y que debe ser protegido, como computadoras, servidores, bases de datos, sistemas, redes, dispositivos y archivos digitales.

Amenaza: Circunstancia, evento o agente con capacidad de aprovechar una vulnerabilidad y provocar daños en los sistemas, equipos o información de una organización.

Análisis de riesgos: Proceso mediante el cual se identifican y examinan las amenazas y vulnerabilidades asociadas a los activos informáticos, considerando su probabilidad de ocurrencia y las posibles consecuencias.

Antivirus: Software de seguridad destinado a detectar, bloquear, prevenir y eliminar programas maliciosos que puedan afectar un equipo informático.

Auditoría informática: Proceso sistemático de revisión y evaluación de los sistemas, equipos, infraestructura, procedimientos y controles tecnológicos de una organización para determinar su funcionamiento, seguridad y cumplimiento.

Auditoría de seguridad informática: Evaluación estructurada de los controles y mecanismos utilizados para proteger los activos tecnológicos, orientada a identificar vulnerabilidades, amenazas y riesgos y a establecer medidas para mejorar la seguridad.

Autenticación: Procedimiento mediante el cual un sistema verifica la identidad de un usuario antes de permitirle acceder a determinados recursos o información.

Autenticación multifactor (MFA): Mecanismo de seguridad que requiere dos o más formas de verificación de identidad antes de conceder acceso a un sistema.

Backup o copia de seguridad: Copia de información almacenada en una ubicación alternativa con el propósito de recuperarla en caso de pérdida, daño, eliminación accidental, ataque informático o falla tecnológica.

Ciberataque: Acción intencional realizada contra sistemas, redes, dispositivos o información digital con el objetivo de acceder, alterar, interrumpir, destruir o sustraer recursos tecnológicos.

Ciberseguridad: Conjunto de medidas, procedimientos, tecnologías y prácticas utilizadas para proteger sistemas, redes, dispositivos e información frente a amenazas y ataques digitales.

Checklist: Lista estructurada de verificación utilizada durante una auditoría para comprobar sistemáticamente el cumplimiento de determinados requisitos, controles o condiciones de seguridad.

COBIT: Marco de referencia para el gobierno y la gestión de las tecnologías de la información que permite establecer procesos, controles y objetivos orientados al adecuado manejo de los recursos tecnológicos.

Confidencialidad: Principio de seguridad de la información que garantiza que los datos sean accesibles únicamente para las personas, procesos o sistemas debidamente autorizados.

Contraseña robusta: Clave de acceso diseñada con características que dificultan su descubrimiento o vulneración, mediante una combinación adecuada de caracteres y evitando información fácilmente predecible.

Control de acceso: Conjunto de mecanismos y procedimientos empleados para determinar quién puede ingresar a un sistema y qué recursos o acciones tiene permitido utilizar.

Control de seguridad: Medida técnica, física, administrativa u organizativa implementada para prevenir, detectar, reducir o responder a riesgos relacionados con la seguridad de la información.

Credenciales: Información utilizada para comprobar la identidad de un usuario durante un proceso de autenticación, como nombre de usuario, contraseña u otros mecanismos de verificación.

Disponibilidad: Principio de seguridad que procura que la información, sistemas y servicios tecnológicos permanezcan accesibles y operativos cuando los usuarios autorizados los necesiten.

Firewall: Mecanismo de seguridad que controla el tráfico de una red de acuerdo con reglas previamente establecidas, permitiendo o bloqueando conexiones para reducir accesos o comunicaciones no autorizadas.

Firmware: Software integrado en un dispositivo de hardware que controla sus funciones básicas. Su actualización puede ser necesaria para corregir vulnerabilidades y mejorar la seguridad.

Gestión de parches: Proceso de identificación, instalación, control y seguimiento de actualizaciones destinadas a corregir errores y vulnerabilidades presentes en sistemas operativos y aplicaciones.

Gestión de riesgos: Proceso sistemático destinado a identificar, analizar, evaluar, tratar y supervisar los riesgos que pueden afectar los activos y objetivos de una organización.

Hardware: Conjunto de componentes físicos que conforman un sistema informático, como computadoras, servidores, routers, discos, periféricos y dispositivos de almacenamiento.

Impacto: Magnitud de las consecuencias que podría ocasionar la materialización de un riesgo sobre un activo, sistema, servicio o proceso institucional.

Incidente de seguridad: Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información y de los recursos tecnológicos.

Infraestructura tecnológica: Conjunto de equipos, redes, sistemas, dispositivos, software y demás recursos tecnológicos utilizados para apoyar los procesos y actividades de una institución.

Ingeniería social: Conjunto de técnicas utilizadas para manipular a las personas con el propósito de conseguir información confidencial, credenciales o acceso a recursos tecnológicos.

Integridad: Principio de seguridad orientado a garantizar que la información permanezca completa, correcta y protegida frente a modificaciones o eliminaciones no autorizadas.

Intrusión externa: Acceso o intento de acceso a una red, sistema o dispositivo institucional realizado desde el exterior sin la autorización correspondiente.

ISO/IEC 27001: Norma internacional que establece requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 19011: Norma internacional que proporciona directrices para la planificación, ejecución y gestión de auditorías de sistemas de gestión.

Logs o registros: Archivos que almacenan información sobre eventos y actividades realizadas en sistemas, aplicaciones o dispositivos y que pueden utilizarse para monitorear accesos e identificar comportamientos anómalos.

MAGERIT: Metodología para el análisis y gestión de riesgos de los sistemas de información que permite identificar activos, amenazas, vulnerabilidades e impactos y establecer medidas de tratamiento.

Malware: Software malicioso diseñado para infiltrarse, alterar, dañar, controlar o afectar el funcionamiento de equipos, sistemas o información.

Matriz de riesgos: Herramienta utilizada para organizar y representar los riesgos identificados de acuerdo con criterios como probabilidad e impacto, facilitando su clasificación y priorización.

Monitoreo: Supervisión continua o periódica de sistemas, redes y dispositivos con la finalidad de identificar anomalías, fallos, accesos sospechosos o posibles incidentes de seguridad.

Phishing: Técnica de ingeniería social mediante la cual un atacante intenta engañar a una persona, generalmente a través de mensajes o sitios falsos, para obtener contraseñas, datos personales u otra información sensible.

Plan de tratamiento del riesgo: Conjunto organizado de medidas, responsables, recursos, frecuencias e indicadores establecidos para reducir, controlar, evitar o gestionar los riesgos identificados.

Política de seguridad informática: Conjunto formal de normas, principios y directrices institucionales que establecen cómo deben utilizarse y protegerse los recursos tecnológicos y la información.

Probabilidad de ocurrencia: Estimación de la posibilidad de que una amenaza se materialice y produzca un incidente de seguridad.

Ransomware: Tipo de malware que bloquea el acceso a un sistema o cifra información y que normalmente busca exigir algún tipo de pago a cambio de restaurar el acceso.

Red informática: Conjunto de dispositivos interconectados que permiten compartir información, servicios y recursos tecnológicos.

Red WiFi: Red inalámbrica que permite conectar dispositivos y acceder a recursos tecnológicos mediante señales de radio, cuya configuración debe incorporar mecanismos adecuados de autenticación y cifrado.

Riesgo informático: Posibilidad de que una amenaza aproveche una vulnerabilidad y genere consecuencias negativas sobre los activos tecnológicos o la información.

Robo de hardware: Sustracción física no autorizada de equipos o componentes tecnológicos que puede ocasionar pérdidas económicas y comprometer la información almacenada.

Segmentación de red: División de una red informática en segmentos independientes con el propósito de controlar el tráfico, separar grupos de usuarios y reducir la propagación de amenazas.

Seguridad de la información: Conjunto de medidas destinadas a preservar principalmente la confidencialidad, integridad y disponibilidad de la información.

Seguridad informática: Disciplina orientada a proteger equipos, sistemas, redes y datos frente a accesos no autorizados, daños, alteraciones, pérdidas y otras amenazas tecnológicas.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto organizado de políticas, procesos, procedimientos, responsabilidades y controles utilizados para gestionar sistemáticamente la seguridad de la información dentro de una organización.

Software: Conjunto de programas, aplicaciones y sistemas operativos que permiten ejecutar funciones y tareas mediante dispositivos informáticos.

TIC: Siglas de Tecnologías de la Información y la Comunicación; comprende los recursos tecnológicos utilizados para procesar, almacenar, transmitir y comunicar información.

Tratamiento del riesgo: Proceso mediante el cual se seleccionan e implementan medidas destinadas a modificar y controlar un riesgo identificado.

VLAN: Red de área local virtual que permite separar lógicamente grupos de dispositivos dentro de una misma infraestructura física, contribuyendo a la segmentación y seguridad de la red.