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 INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LOS EQUIPOS TECNOLOGICOS DE LA UNIDAD EDUCATIVA HORTENSIA VÁSQUEZ SALVADOR

AUTOR

CAMPOVERDE VÁSQUEZ WILSON ANDRÉS

TUTOR

A.S. MINAYA MACIAS RENELMO WLADIMIR, MG.

EL CARMEN, 2026

CERTIFICACIÓN DEL TUTOR

Uleam ELOY ALFARO DE MANABÍ	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 del estudiante **CAMPOVERDE VASQUEZ WILSON ANDRÉS**, 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 LOS EQUIPOS TECNOLÓGICOS DE LA UNIDAD EDUCATIVA HORTENSIA VASQUEZ SALVADOR**".

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

TRIBUNAL DE SUSTENTACIÓN

Universidad Laica Eloy Alfaro de Manabí

Extensión El Carmen

Carrera de Ingeniería en Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Título del Trabajo de Titulación:
AUDITORIA DE SEGURIDAD INFORMÁTICA A LOS EQUIPOS TECNOLÓGICOS DE LA UNIDAD EDUCATIVA HORTENSIA VÁZQUEZ SALVADOR.

Modalidad:
Proyector Integrador

Autor:
Campoverde Vásquez Wilson Andrés

Tutor:
A.S. Minaya Macias Renelmo Wladimir, Mgtr

Tribunal de Sustentación:

- **Presidente:** Ing. Mora Marcillo Alex Bladimir, Mgtr
- **Miembro:** Ing. Pozo Hernández Clara Guadalupe, Mgtr
- **Miembro:** Ing. Arca Zavala Jefferson Omar, Mgtr

Fecha de Sustentación:
24 Agosto de 2026

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 TECNOLOGICOS DE LA UNIDAD EDUCATIVA HORTENSIA VÁSQUEZ SALVADOR**, corresponde exclusivamente a: CAMPOVERDE VÁSQUEZ WILSON ANDRÉS con CI. 2300419153, y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Campoverde Vásquez Wilson Andrés
C.I. 2300419153

DEDICATORIA

En primer lugar, dedico este logro a Dios, por ser mi guía y fortaleza en cada etapa de este camino. Gracias por brindarme sabiduría, salud y la oportunidad de superar cada obstáculo. Su bendición y presencia constante me permitieron mantener la fe y la esperanza hasta alcanzar esta meta tan importante.

A mis padres, con todo mi amor y gratitud, por haber sido el pilar fundamental de mi vida. Gracias por cada sacrificio realizado para brindarme educación, por su apoyo incondicional, sus consejos y por creer siempre en mí. Este logro también les pertenece, porque sin ustedes no habría sido posible llegar hasta aquí.

A mi hermana, por regalarme uno de los momentos más especiales que marcaron el inicio de esta etapa. Aún recuerdo cuando, mientras yo me encontraba trabajando, decidiste inscribirme en la universidad y al llegar a casa me dijiste con una sonrisa: "Mañana comienzas clases". Ese gesto de confianza cambió mi vida y fue el primer paso para alcanzar este sueño. Gracias por creer en mí incluso antes de que yo mismo imaginara este camino.

Finalmente, me dedico este logro a mí mismo, por no rendirme jamás y demostrar que con esfuerzo, disciplina y perseverancia los sueños pueden hacerse realidad. Durante toda la carrera asumí el reto de trabajar y estudiar al mismo tiempo, enfrentando dificultades, sacrificios y momentos de cansancio. Hoy puedo decir con orgullo que cada esfuerzo valió la pena y que esta meta representa la recompensa de años de dedicación y constancia.

Wilson Andrés Campoverde Vásquez

AGRADECIMIENTO

En primer lugar, agradezco profundamente a Dios, por bendecirme con la vida, la salud, la fortaleza y la sabiduría necesarias para recorrer este camino. Gracias por iluminar cada una de mis decisiones, sostenerme en los momentos de dificultad y permitirme culminar esta importante etapa de mi formación profesional. Sin su guía y su infinita misericordia, este logro no habría sido posible.

A mis padres Mercy Vásquez y Oswaldo Campoverde, quiero expresarles mi más profundo agradecimiento por ser el ejemplo de esfuerzo, responsabilidad y perseverancia que ha guiado mi vida. Gracias por cada palabra de aliento, por confiar en mí incluso cuando el camino parecía difícil y por enseñarme que el trabajo honesto y la educación son las mejores herramientas para construir un mejor futuro. Este logro es también el resultado de todo lo que han sembrado en mí.

A mi hermana Andrea Campoverde, gracias por creer en mi futuro y por impulsarme a dar el primer paso hacia esta etapa tan importante de mi vida. Tu iniciativa de inscribirme en la universidad fue un acto de confianza que nunca olvidaré y que cambió el rumbo de mi historia. Agradezco cada consejo, cada palabra de motivación y el apoyo que me brindaste durante este proceso. Hoy puedo celebrar este logro gracias, en parte, a ese gesto que marcó el inicio de este gran sueño.

A mi novia Michelle Celi, gracias por acompañarme durante este proceso universitario con paciencia, comprensión y palabras de aliento. Agradezco tu apoyo incondicional en los momentos de cansancio, estrés y desánimo, así como tu confianza en que sería capaz de alcanzar esta meta. Tu compañía fue una motivación constante para seguir adelante y no rendirme. Te amo mucho.

A mis compañeros de la universidad, gracias por compartir conmigo esta etapa llena de aprendizajes, retos y experiencias. De manera muy especial, agradezco de todo corazón a mi amiga Jessenia Zambrano, por su amistad, apoyo constante y disposición para ayudarme en todo momento. Gracias por tus consejos, por compartir tus conocimientos, por colaborar en los deberes y por motivarme a seguir adelante. Tu ayuda fue invaluable durante toda la carrera y siempre la recordaré con mucho aprecio.

Wilson Andrés Campoverde Vásquez

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

Es hoy la tecnología una herramienta clave dentro de las instituciones educativas, sin embargo, no existe un control sobre los equipos y eso se convierte en un riesgo, en la Unidad Educativa Hortensia Vásquez Salvador, donde no se había realizado ninguna auditoría que permitiera conocer el estado real de sus 33 computadoras ni el nivel de protección de la información, por esta razón, el proyecto se planteó realizar una auditoría de seguridad informática, aplicando la metodología de MAGERIT, la cual se organizó por fases: definición del alcance, gestión de activos, identificación, análisis, evaluación, tratamiento de riesgo y monitorio.

La investigación fue bibliografía, de campo y aplicada, se usaron encuestas a los estudiantes y entrevista al docente, entre los hallazgos se detectaron debilidades como la falta de antivirus robusto, el uso sin control de dispositivos USB y la ausencia de políticas de seguridad, teniendo en cuenta que el malware resultó ser el riesgo más grave.

Finalmente se elaboró una guía rápida del sistema de gestión de seguridad de la información, adaptada a los recursos de la institución, que reúne políticas, roles, un protocolo de respuesta a incidente, con la finalidad de reducir riesgos y mantener la mejora continua.

ABSTRACT

Technology is currently a key tool within educational institutions; however, a lack of control over equipment poses a risk. At the Hortensia Vásquez Salvador Educational Unit, no audit had previously been conducted to determine the actual condition of its 33 computers or the level of information protection, consequently, this project proposed an information security audit using the MAGERIT methodology, organized into the following phases: scope definition, asset management, identification, analysis, evaluation, risk treatment, and monitoring.

The research combined bibliographic, field, and applied approaches, utilizing student surveys and teacher interviews. Findings revealed weaknesses such as the lack of robust antivirus software, uncontrolled use of USB devices, and an absence of security policies, with malware identified as the most serious risk.

Finally, a quick-reference guide for an information security management system tailored to the institution's resources was developed; it incorporates policies, roles, and an incident response protocol aimed at mitigating risks and fostering continuous improvement.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Preámbulo

Actualmente, la tecnología y la comunicación se ha vuelto sumamente importante en la educación, por eso, las escuelas y colegios han ido incorporando laboratorios de informática, porque son el espacio clave para aprender y fortalecer las destrezas digitales, en pocas palabras esto demuestra que la formación de los alumnos sea mucho más completa. No obstante, esta dependencia de la tecnología presenta múltiples desafíos en términos de seguridad informática, lo cual podría amenazar el funcionamiento apropiado y la integridad de los recursos institucionales.

Los laboratorios de computación, cuando son empleados por alumnos, docentes y personal administrativo, se ven expuestos a múltiples amenazas, entre ellas la entrada no autorizada a datos, la propagación de virus digitales, el uso indebido de dispositivos, la modificación o eliminación de información y la ausencia de supervisión en la configuración de sistemas operativos y redes.

Por otro lado, estas condiciones pueden generar fallas que afecten el trabajo administrativo y académico, como también pueden poner en peligro la seguridad y el acceso a la información.

Ante esto, es necesario crear un procedimiento de revisión de seguridad informática que sirva para observar cómo están los equipos, encontrar fallas y proponer soluciones para prevenir problemas, la idea es aprovechar mejor los recursos informáticos que tiene la institución educativa, asegurar la información, reforzar la protección del establecimiento.

De esta manera, el proyecto busca mejorar el manejo en la Unidad Educativa Hortensia Vásquez Salvador aportando buenas prácticas informática entre todos los que forman parte de la comunidad educativa.

1.2 Presentación del tema

Auditoría de seguridad informática a los equipos de la Unidad Educativa Hortensia Vásquez Salvador

1.3 Ubicación y contextualización de la problemática

Este proyecto se lleva a cabo en la Unidad Educativa Hortensia Vásquez Salvador, la cual está ubicada en el cantón Santo Domingo, parroquia Zaracay, provincia de Santo Domingo de los Tsáchilas, Ecuador, cabe mencionar que este plantel pertenece a la zona 4 del sistema educativo ecuatoriano y ofrece clases presenciales en horario de la mañana y tarde, con niveles en educación inicial básica, y bachillerato.

Asimismo, es una entidad enfocada en la formación académica, tecnológica y científica de sus estudiantes, con la idea que desarrollen habilidades que respondan a lo que pide el entorno actual. En este sentido, su meta es dar educación completa, basada en valores, conocimientos, destrezas que ayuden a los alumnos a pensar de manera critica e innovar, por esta razón la institución ha ido sumando varias herramientas tecnologías a su forma de enseñar, logrando así un modelo educativo modernos acorde a la actualidad.

Ahora bien, la entidad educadita cuenta con un laboratorio equipado con 33 computadoras, las cuales sirven para desarrollar proyectos, hacer investigaciones académicas y realizar las prácticas necesarias, sin duda este lugar es un recurso clave para que los estudiantes aprendan y además sirve para reforzar habilidades tecnológicas del personal administrativo, docentes lo cual apoya al proceso de enseñanza.

Finalmente, con este método de evaluaciones se podrá obtener información exacta sobre el rendimiento del laboratorio, encontrar errores técnicos, ubicar las normas básicas de seguridad, en base a los hallazgos, se propondrán mejoras y recomendaciones que garanticen un espacio adecuado para enseñar y aprender habilidades digitales y también optimizar los recursos tecnológicos.

1.4 Planteamiento del problema

A pesar de que la Unidad Educativa Hortensia Vásquez Salvador se ha puesto en marcha, desde el año 2013, un laboratorio de computación dotado con 33 equipos para mejorar la educación tecnológica, no se ha realizado ninguna auditoría de seguridad informática que examine el estado actual de sus sistemas y recursos. Esta falta de supervisión y evaluación ha generado potenciales vulnerabilidades, como accesos no autorizados, pérdida de datos y dificultades con la seguridad de la información, las cuales ponen en riesgo el desempeño adecuado e íntegro del laboratorio de computación.

1.4.1 Problematización

Es de total conocimiento que el progreso tecnológico ha propiciado un avance grandemente notorio en la gestión y utilización de recursos digitales en el ámbito educativo, todavía existen muchas organizaciones que afrontan carencias significativas en términos de seguridad informática. Uno de los problemas más notables es la insuficiencia de supervisión y control sobre el estado de los dispositivos tecnológicos, además de la falta de políticas claras para salvaguardar la información. Esta problemática ocasiona que los sistemas no operen correctamente, que se pierda información y que la vulnerabilidad a ataques cibernéticos se incremente, lo cual tiene un impacto directo en el avance de las actividades administrativas y académicas.

En este contexto, la falta de auditorías de seguridad informática y de cuidado preventivo genera un entorno inseguro para el manejo de la información institucional. La ausencia de evaluaciones técnicas oportunas dificulta la detección de las averías en los equipos, lo que acarrea un rendimiento insatisfactorio, interrupciones del servicio y una utilización ineficiente de los recursos tecnológicos, aparte de eso, como los usuarios no conocen sobre las practicas adecuadas digitales, aumenta el riesgo de incidentes a la integridad y disponibilidad de datos.

Dicho de otra forma, cuando la seguridad informática se maneja mal, la institución pierde capacidad para cuidar sus recursos digitales y esto a futuro repercute en todo el proceso educativo, esta situación preocupa a los docentes y al personal administrativo, pues no tienen sistemas estables ni confiables en los cuales apoyarse, por ende dificulta la ejecución de actividades pedagógicas y administrativas que dependen de la tecnología, limitando también el progreso hacia una cultura digital responsable que propicie la mejora continua.

1.4.2 Génesis del problema

La ausencia de supervisión técnica y revisión de los sistemas informáticos hace que aumente la probabilidad de que ocurran fallos en el sistema, se pierdan datos o haya vulnerabilidades de seguridad. Esto sucede porque se confía en métodos tradicionales para el mantenimiento y no se tienen herramientas concretas que aseguren la estabilidad, rendimiento y seguridad de la información, por esta razón a las instituciones se les hace difícil responder a las demandas tecnológicas y actuales y brindar un espacio digital seguro.

Además, este establecimiento educativo no tiene encargado del área, lo que limita a los usuarios del laboratorio usar los dispositivos de manera segura y complica el manejo de tareas y el buen uso de estas herramientas que tienen a la mano, como resultado de esta carencia esta falta afecta a la productiva y estanca en el avance de las habilidades del docente ye estudiante afectando así la eficiencia del trabajo académico.

Por no aplicar de manera suficiente las reglas y los procedimientos para revisar la seguridad informática, que permitan monitorear, identificar y optimizar el rendimiento de los dispositivos, es imposible mantener una infraestructura tecnológica actualizada y segura. Esta falta crea peligros para la protección de la información institucional, dificulta el desempeño de las tareas y obstaculiza el progreso de una sólida cultura digital segura en el ambiente educativo.

1.4.3 Estado actual del problema

En la Institución Educativa Hortensia Vásquez Salvador, es imprescindible el uso de dispositivos informáticos para progresar en las actividades académicas y administrativas; sin embargo, se detectan fallas en la supervisión y gestión de la seguridad de estos medios tecnológicos. La falta de una evaluación constante del estado de los dispositivos y de las medidas para proteger la información ha generado vulnerabilidades que podrían amenazar la integridad y el acceso a los datos.

Por lo que, la falta de protocolos y normas para revisar la seguridad informática dificulta el monitoreo del rendimiento y la detección temprana de fallos o riesgos, por ende esta carencia impacta en la calidad del servicio en la organización, ocasionando interrupciones en las labores del personal académico y administrativo, y disminuyendo la confianza en la utilización de las herramientas digitales.

Por otro lado, el mantenimiento manual y no programado de los dispositivos aumenta la probabilidad de que se pierdan datos, que haya un mal rendimiento y que se produzcan deterioros. Dificultan el aprovechamiento eficaz de los recursos informáticos con estas limitaciones, lo que limita la capacitación en competencias tecnológicas de los usuarios y dificulta el establecimiento de un entorno educativo seguro, productivo y alineado con las demandas tecnológicas actuales.

1.5 Diagrama causa -efecto del problema

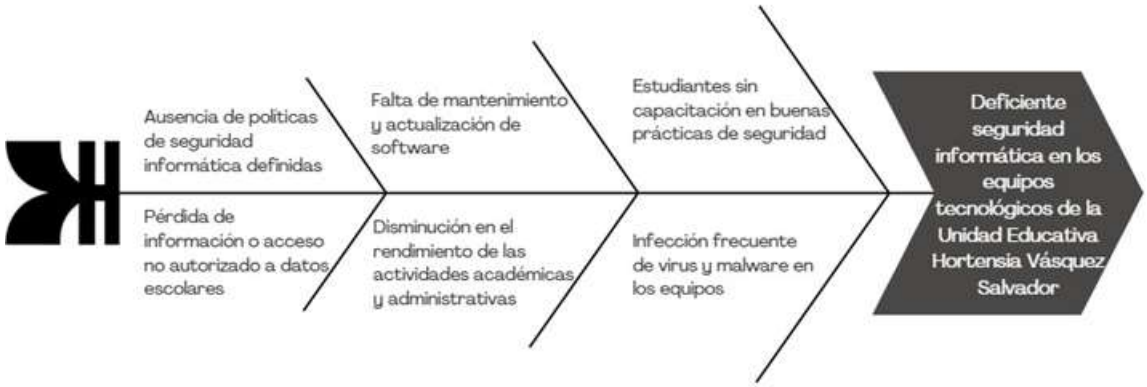


Ilustración 1 Diagrama causa-efecto del problema

1.6 Objetivos

1.6.1 Objetivo general

Realizar una auditoría de seguridad informática a los equipos tecnológicos del laboratorio de la Unidad Educativa Hortensia Vásquez Salvador

1.6.2 Objetivos específicos

- Analizar los fundamentos sobre una auditoría de seguridad informática, así como las normas, procedimiento y herramientas que esta involucra.
- Diagnosticar el estado actual del laboratorio computo, aplicando instrumentos como recolección de datos, encuestas y observación directa para detectar vulnerabilidades y riesgos existentes.

- Aplicar una metodología de auditoría de seguridad informática concreta a las circunstancias del laboratorio, estableciendo sus fases, técnicas y herramientas, con el fin de comprobar la efectividad de los controles de seguridad existentes.
- Plantear un plan de optimización a partir de los resultados de la auditoría, con el fin de fortalecer las prácticas, normas y procesos relacionados con la seguridad digital en el laboratorio de computación.

1.7 Justificación

La ciberseguridad es un elemento esencial en las instituciones educativas hoy en día, debido al incremento en el uso de herramientas digitales para tareas académicas y administrativas. Los dispositivos informáticos son una herramienta esencial para la educación, la capacitación y la gestión institucional en la Unidad Educativa Hortensia Vásquez Salvador.

Sin embargo, se ha identificado que es necesario examinar el nivel de seguridad, para garantizar que funcionen de manera correcta y que la información quede protegida.

Es por eso, que hacer una auditoría informática ayudará a detectar vulnerabilidades, estudiar riesgos asociados y proponer correcciones que refuercen la infraestructura tecnológica, de modo que se relacionan directamente con proteger la privacidad, el acceso a la información la integridad, previniendo perdida de datos o accenso no autorizados.

Por lo que, este estudio es importante porque fomentar que la tecnología se use de forma segura y adecuada en la educación, generando un entorno digital protegido y de prevención para docentes, estudiantes y personal administrativo, además los resultados que se obtenga servirán como base para tomar decisiones que ayuden a mejorar las políticas internas de seguridad y el cuidado de los dispositivos.

1.8 Impactos esperados

Aplicar una auditoría de seguridad informativa no busca únicamente fortalecer la gestión tecnológica en la organización, sino que además pretende impulsar un uso más consciente, seguro y provechoso de la tecnología.

Este procedimiento busca alcanzar progresos significativos en la protección de los datos, el rendimiento del hardware y la concienciación sobre la importancia de la

ciberseguridad. Se distinguen, a partir de esto, tres grandes categorías de efectos que surgen de esta iniciativa.

1.8.1 Impactos tecnológicos

La revisión de la seguridad digital permitirá detectar las vulnerabilidades y los riesgos existentes en los dispositivos tecnológicos de la organización, lo que mejorará su desempeño y garantizará la protección de los datos de igual forma, impulsará a que se apliquen reglas más efectivas para supervisar y cuidar los equipos, lo que hará que los activos informáticos tengan mayor durabilidad y sean más confiables de usar.

Como resultado, la auditoria permitirá poner en marcha los métodos y normas estandarizados para el mantenimiento preventivo y correctivo, evitando así que los problemas aparezcan una y otra vez, el grupo encargado tendrá la posibilidad de utilizar herramientas más eficaces para supervisar, lo que contribuirá a que se tomen decisiones basadas en información técnica actual y precisa.

1.8.2 Impacto social

La seguridad informática, desde el punto de vista social, promoverá un cambio positivo en la cultura digital de la Unidad Educativa Hortensia Vásquez Salvador. Al incorporar a los estudiantes, maestros y personal administrativo en prácticas de uso seguro de la tecnología se promueven principios de ética digital, responsabilidad y conciencia sobre la importancia de proteger la información institucional y personal.

Instruir en temas de ciberseguridad motivará a toda la comunidad educativa a participar activamente, lo que mejorará el sentido de pertenencia y colaboración en la correcta utilización de los recursos tecnológicos. Asimismo, un entorno digital seguro brinda a los usuarios confianza y transparencia, lo que les permite llevar a cabo sus labores administrativas y académicas sin el peligro de perder información, sufrir daños en los equipos o tener accesos no autorizados.

1.8.3 Impacto ecológico

La auditoría ayudará a que los dispositivos tecnológicos duren más, con lo que se evitará tener que sustituirlos tan a menudo y, en consecuencia, se producirá menos basura electrónica, siempre que se apliquen normas y prácticas eficaces de mantenimiento.

Asimismo, esta toma de conciencia promueve un uso eficaz de los recursos tecnológicos y energéticos, de acuerdo con los principios de la sostenibilidad del medio ambiente. De este modo, la organización no solo eleva la seguridad de su información, sino que también muestra su compromiso con la preservación del entorno natural.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes Históricos

2.1.1 Auditoría informática

En este escenario, la auditoría de ciberseguridad es un proceso sistemático que se ha creado para analizar cuán efectivos son los controles de seguridad al interior de una organización. Además, contribuye a detectar y tratar cualquier dificultad que pueda comprometer la confidencialidad, la integridad y la disponibilidad. A veces se asumen riesgos, lo que es más habitual en sistemas más recientes donde la inversión monetaria sobrepasa el riesgo de explotación vulnerable. (Menéndez Arantes, 2023)

En la actualidad, los equipos tecnológicos son herramientas fundamentales para desempeñarse tanto en el ámbito, laboral, estudiantil o simplemente uso personal, por lo tanto, implementar medidas de seguridad informática es la clave para proteger datos, por ello expertos en el tema implementan una serie de combinación de herramientas automatizada, pruebas manuales y habilidades individuales para identificar vulnerabilidades. (Mata, 2024)

La auditoría de los sistemas informáticos posibilita la evaluación de controles, el reconocimiento de riesgos y la garantía de un sistema tecnológico íntegro, lo cual mejora la seguridad y la gobernanza institucional. Su implementación garantiza que los recursos informáticos sean administrados de manera confiable y eficaz. (Laudon y Laudon, 2021)

2.1.2 Equipos Tecnológicos

Los antecedentes de los equipos tecnológicos se remontan a la segunda mitad del siglo XX, cuando los primeros sistemas informáticos comenzaron a integrarse en instituciones públicas y privadas como herramientas de apoyo administrativo.

En sus comienzos, estos equipos se caracterizaban por ser muy grandes, con capacidad limitada y costos de operación sumamente elevados, por lo que solamente las organizaciones con buenos recursos podían tenerlos, pero luego, con el desarrollo de la microelectrónica y la aparición de las computadoras personal en la década de 1980, la tecnología se hizo más

alcanzable, lo que permitió que de a poco llegara a escuelas, organismos del gobierno y empresas de distintos sectores.

Por lo tanto, Los dispositivos tecnológicos son herramientas o máquinas diseñadas por las personas que simplifican la ejecución de funciones concretas en áreas como la enseñanza, el sector industrial, las telecomunicaciones o la investigación. Contribuyen a manejar, guardar, enviar o producir datos o energía para abordar dificultades y optimizar procedimientos. (Health, 2023)

La evolución de los equipos tecnológicos ha estado marcada por una transición desde dispositivos básicos hacia sistemas complejos destinados a garantizar la eficiencia y continuidad de la información. La implementación de equipos de red, servidores, unidades de respaldo y sistemas permitió gestionar grandes volúmenes de datos y mejorar la disponibilidad institucional. (Rountree y Castrillo, 2021)

2.2 Antecedentes de Investigación

Auditoría informática a equipos tecnológicos a lo largo de los años a sido un tema clave para investigaciones ya que si bien es cierto con el pasar de los años las herramientas tecnológicas se han ido actualizando y por ello la implementación de una auditoría ha ayudado a salvaguardar la información de manera segura y oportuna, por lo tanto, a continuación, se presenta cinco investigaciones relevantes:

Estándares de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información

El objetivo de este documento es mostrar cómo se puede asegurar la integridad, la privacidad y la disponibilidad de los datos y recursos en los laboratorios dentro de la carrera de Tecnologías de la información, a través de un estudio que utiliza protocolos para defenderse contra riesgos tanto internos como externos, garantizando así la continuidad de las labores de investigación. Se detectó la implementación de protocolos de seguridad que incluyen medidas para evitar accesos no autorizados, como cámaras de vigilancia, sistemas de alarmas y cerraduras. Además, se identificaron debilidades en la gestión de contraseñas, el ingreso a los sistemas y la capacitación del personal en seguridad informática, lo que llevó a la conclusión de que algunos laboratorios presentaban estas vulnerabilidades. (Intriago et al., 2023)

Auditoría de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre en el periodo 2022

Esta investigación se centró en llevar a cabo una revisión de la seguridad de la información en la infraestructura tecnológica de la Unidad Educativa Antonio José de Sucre. El objetivo principalde este estudio fue elaborar un documento que permita analizar la adherencia a las normas de seguridad, detectando las problemáticas a través de encuestas y entrevistas, utilizando la metodología MAGERIT para examinar un laboratorio de computación. Como resultado, se determinó que los índices de seguridad se sitúan en un 43%, los riesgos críticos como el robo de información alcanzan un 95% y la presencia de virus en los dispositivos es del 83%, además de amenazas como el robo, incendios y daños a los equipos. Por último, se concluyó con la redacción de un informe y una serie de sugerencias para la mitigación de riesgos. (Paladines, 2023)

Auditoría de seguridad informática en los laboratorios de la Unidad Académica de Ciencias Empresariales de la UTMACH.

La lógica en las instituciones educativas de nivel superior en Ecuador se ve afectada por la incorporación de nuevas tecnologías de información y la internet. Estas herramientas presentan muchos beneficios, aunque también implican riesgos tanto físicos como lógicos, como el acceso indebido a datos sensibles y dificultades en la gestión de dispositivos electrónicos. Por lo tanto estos factores pueden dificultar la creación de ambientes de aprendizaje seguros y eficaces, ya que pueden causar perdida y afectar la calidad de los laboratorios de computación, por eso es clave establecer mecanismo que controlen, en este sentido se plantea reconocer las vulnerabilidades y proponer medidas para mejorar la seguridad y calidad debe ser prioridad, para así lograr espacios educativos seguros y funcionales para toda la comunidad (Reyes , 2018)

Diseño De Un Plan Estratégico De Seguridad Informática Para La Protección De Los Recursos Informáticos En El Laboratorio De Telecomunicaciones De La Carrera De Ingeniería En Computación Y Redes

Este estudio se centra en el desarrollo de un plan estratégico destinado a identificar y abordar una necesidad vinculada a la seguridad informática en el laboratorio de telecomunicaciones. La estrategia mejorará los métodos y normativas para salvaguardar los

recursos y equipos informáticos del laboratorio perteneciente al programa de Ingeniería en Computación y Redes. Hoy en día la Universidad Estantal del Sur de Manabí cuenta con varios equipos tecnológicos, y por esos mismo necesita aplicar acciones y normativas que aseguren que estos recursos estén siempre disponibles, por esto en esta investigación se usaron enfoques tanto cuantitativos como cualitativos, luego con los datos que se consiguieron , se armaron tablas que ayudaron identificar la necesidad y escoger la solución más efectiva.

Este proyecto se ejecuta según un cronograma previamente valorado y se ajusta al tiempo estipulado, además de contar con apoyo financiero del autor. (Romero y González, 2018)

Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la ESPAM MFL

Esta revisión se encarga de examinar la confiabilidad de los activos tecnológicos de información en la Escuela Técnica Superior Agropecuaria de Manabí, utilizando un enfoque metódico conforme a estándares internacionales. El proyecto se organiza en tres etapas, centrándose en la protección tanto física como lógica de dichos activos, a través de un estudio de los factores internos y externos involucrados en la evaluación, con el objetivo de identificar los aspectos más significativos. Esto permite destacar descubrimientos dentro de la institución, presentando los resultados derivados del monitoreo que sigue directrices generales de seguridad. El coeficiente de concordancia de Kendall muestra un 0,85 de coincidencia, con escaso control sobre los procedimientos aprobados, lo que sugiere la necesidad de implementar regulaciones de seguridad estrictas para reducir posibles amenazas a la infraestructura tecnológica. (Loor y Espinoza, 2014)

2.3 Definiciones Conceptuales

2.3.1 Auditoría de Seguridad Informática

Desde la perspectiva de Menéndez Silva (2022), expresa en su libro que una auditoría informática es:

Un procedimiento que permite evaluar y medir si el sistema de seguridad informativo implantado realiza sus funciones adecuadamente, permitiendo poner de manifiesto y mejorar

cualquier incidencia que se pueda presentar y que afecte a la triada CIA, confidencialidad, integridad y disponibilidad. (pág. 13).

La auditoría informática es una revisión que se lleva a cabo en el software, hardware, sistemas e información, con el objetivo de optimizar sus procedimientos. Esto permite evaluar la efectividad y el rendimiento en el uso de los recursos tecnológicos. (Yanza Chávez y Montoya Lunavictoria, 2022)

2.3.1.1 Ventajas

Del mismo modo Menéndez Silva (2022), acota que la auditoría informática brinda ciertos beneficios, por ello se debe realizar estas auditorías periódicas, por ello se menciona algunas ventajas:

Optimizar los procesos informáticos de negocio , detectar y conocer las vulnerabilidades existentes de forma que podamos eliminar o reducir el riesgo , permite actuar antes de que se materialice un incidente de seguridad, permite crear procedimiento de actuación en caso de sufrir el incidente, permite optimizar, mejorar y actualizar las políticas de seguridad existentes en la empresa, así como los procedimientos a seguir, evita multas y sanciones debidas al incumplimiento de leyes, buenas prácticas y normativas de protección de datos. (pág. 12).

Las auditorías de ciberseguridad deben realizarse al menos dos veces al año. Las auditorías de seguridad tienen varias ventajas, que son las siguientes:

Una auditoría de seguridad puede ayudarles a identificar sus puntos fuertes y débiles. Una vez que saben con qué trabajan y qué está en juego, pueden mitigar los riesgos, pueden ayudar a mejorar los programas de formación de concienciación de los empleados establecer un punto de partida y ayudar a construir bases sólidas, puede trazar una hoja de ruta para identificar a los empleados que necesitan formación adicional y recomendar excelentes oportunidades de tutoría garantiza la calidad para las partes interesadas, el aumento de la confianza entre proveedores e inversores y el cumplimiento sin problemas de las obligaciones de seguridad de las empresas de todo el mundo. (SentinelOne, 2025)

2.3.1.2.Código Deontológico de la Función de Auditoría

Con relación a Conrado Beatriz (2024), expresa que el código deontológico de la función de auditoria en seguridad informática establece una serie de principios éticos que guían

la conducta de los auditores y determinan como deben realizar su trabajo. Esto incluye normas sobre la confidencialidad, la objetividad, la integridad y la independencia en su labor, asegurando que los auditores operen de forma profesional y sus sesgos, por ello se debe basarse en principio de confidencialidad, integridad y objetividad. (pág. 14)

Por otro lado, Chicana Ester (2023), expresa que el código deontológico consiste en una serie de preceptos en los que se:

Determinan los derechos exigibles a ciertos profesionales cuando desempeñan su actividad con el fin de ajustar los comportamientos profesionales a unos principios éticos y morales adecuados. En el caso de la auditoría informática, existe una organización internacional que diseña los estándares de auditoría y control de sistemas de información aceptados por la comunidad general de auditoría. (pág. 12)

2.3.1.3. Relación de los Distintos Tipos de Auditoría en el Marco de los Sistemas de Información

Según CISA (2023), manifiesta que el mundo de la tecnología es muy extenso y variado y es imposible tener conocimiento de todo, por lo que existen especialistas en diferentes áreas relacionadas con IT y ciberseguridad, por lo que:

Existen multitud de tipos de auditorías en función del área. Una auditoria como has podido extraer de los puntos anteriores es un procedimiento sistemático, independiente y documentado donde obtenemos evidencias objetivas que determinan el grado de cumplimiento de los criterios previamente marcados en el plan de seguridad de la empresa y el nivel de cumplimiento legas en función de la información que se tiene que asegurar en cada caso, acorde a la POPD (Ley Orgánica de protección de Datos). Inicialmente las auditorías pueden ser de dos tipos:

1. Internas: cuando son realizadas por el personal de la propia empresa.
2. Externas: la auditoria la hace un agente externo a la empresa. A su vez pueden ser de dos tipos:
    - Auditoría externa de segundas partes: ocurre cuando un cliente quiere comprobar si sus proveedores cumplen los requisitos esperados (calidad y seguridad de los servicios, leyes, normas, procedimientos estipulados, ISO, etc.) De forma que contrata una entidad externa para la evaluación.

- Auditoria de terceros: en este caso, es una entidad certificadora, emitiendo un certificado final de cumplimiento si todo está conforme, por ejemplo, para que una empresa pueda obtener la certificación ISO 27001 debe someterse a una auditoría externa por parte de entidades como por ejemplo AENOR, que confirma si se cumplen con todos los requisitos establecidos en dicha ISO. (págs. 18,19)

2.3.2 Características y Capacidades del Equipo Auditor

Para llevar a cabo todas las actividades, no es necesario que sean desempeñadas por un solo auditor informático, sino que se recomienda seleccionar una serie de técnicos especializados que abarquen los conocimientos y capacidades suficientes para desarrollar todas las tareas de un modo global. El número de personas que formen el equipo auditor puede variar según las dimensiones de la organización, de los sistemas y de los equipos, pero, independientemente de la magnitud del equipo, sus miembros deberán estar suficientemente capacitados y deberán tener un alto sentido de la ética y la moralidad. Para seleccionar el equipo adecuado, en un primer lugar hay que pensar en profesionales con suficiente nivel para realizar una correcta coordinación del desarrollo de las tareas de la auditoria, siendo capaz de facilitar la información requerida en todo momento. (Chicano Tejada, 2023)

Por consiguiente, el equipo debe estar formado por profesionales con conocimientos básicos en cuanto a:

- Desarrollo de proyectos informáticos
- Gestión del departamento de sistemas
- Análisis de riesgos en sistemas informáticos
- Sistemas operativos
- Redes locales y telecomunicaciones
- Gestión de bases de datos
- Seguridad de bases de datos
- Seguridad física y del entorno
- Planificación informática
- Gestión de la seguridad de los sistemas
- Gestión de problemas, incidencias y camios en entornos informáticos
- Administración de datos
- Ofimática

- Permiso de acceso y encriptación de datos
- Comercio electrónico.

2.3.3 Fases Generales de una Auditoría

2.3.3.1 Planificación Inicial, Objetivos y Alcance

Se definen aspectos como el alcance de la auditoria, esto es sistemas a auditar, limites, se establecen ventanas horarias, en las que se va a realizar la auditoría, quien o quienes la van a realizar, el tipo de auditoría. En esta fase se establece también la duración de la auditoria que depende del tipo de auditoría a realizar, los equipos a auditar, así como del tipo de auditoría, si es de caja blanca, gris o negra. (Arantes, 2022, pág. 23)

2.3.3.2 Análisis de Riesgos y Amenazas

Desde la perspectiva Menéndez Silva (2022), menciona que en esta fase realizaremos un análisis de los riesgos y amenazas a los que está expuesta la empresa, identificando vulnerabilidades y el nivel de amenaza, evaluando las consecuencias en caso de que se materializase esa amenaza. (Arantes, 2022, pág. 23).

Los puntos a analizar serian:

- Analizar la seguridad del hardware, sistemas operativos, aplicaciones y redes
- Cumplimiento en cuando a políticas y procedimientos
- Cumplimiento de las normativas vigentes en cuanto a protección de datos y ciberseguridad.
- análisis de la formación del personal implicado en las tareas de seguridad informática de la empresa, teniendo en cuenta que este suele ser el eslabón más débil, generalmente por la falta de formación adecuada para el puesto.

2.3.3.3 Definir las Soluciones Necesarias

Con toda la información obtenida de la fase anterior e identificados los riesgos, proponer las soluciones adecuadas y objetivas para mitigar el riesgo o eliminarlo, estableciendo prioridades en función de la severidad del riesgo encontrada. En esta fase determinan las medidas a tomar, los tiempos necesarios para su implementación, el coste y se actualizan los protocolos en caso de que sea necesarios (revisiones). (Arantes, 2022, pág. 24)

2.3.3.4 Implantar los Cambios Necesarios

En áreas de incrementar la seguridad de la empresa y de gestionar los riesgos se deben implementar las soluciones aportadas en la fase anterior y realizar un calendario de implementación. Estos cambios suelen ser actualizaciones de software y hardware, aplicación de las correctas configuraciones, impartir formación adecuada a los empleados, actualizar las políticas de seguridad, adopción de nuevas tecnologías, instalación de software de seguridad como firewalls, IDS, IPS, sistemas de monitorización del tráfico de red, etc. (Arantes, 2022, pág. 24)

2.3.3.5 Monitorización y Evaluación de Resultados

Tras las modificaciones necesarios se hace necesario evaluar los resultados y monitorizar el correcto funcionamiento de los sistemas, para verificar si alcanzan el objetivo perseguido, aumentar el nivel de seguridad, en algunos casos, se vuelve a realizar todo el proceso de auditoria para verificar que realmente se ha cumplido los objeticos perseguidos a la hora de mejorar la seguridad y el cumplimiento. (Arantes, 2022, pág. 25)

2.3.4 Equipos Tecnológicos

Los equipos tecnológicos constituyen los elementos físicos que permiten el funcionamiento de los sistemas de información dentro de una organización. Estos dispositivos son considerados componentes esenciales de la infraestructura de tecnologías de la información (TI), pues soportan la ejecución de procesos operativos, administrativos y estratégicos. Según Laudon y Laudon (2020), los equipos tecnológicos representan el hardware que posibilita que un sistema informático procese información de manera eficiente y segura.

Asimismo, González (2021), indica que estos equipos abarcan todos los recursos físicos que se necesitan para manejar los datos de la institución, desde computadoras personales y hasta servidores especializados, además este autor resulta que adminístralos bien es fundamental para que las operaciones no se detengan.

En concordancia, la norma ISO/IEC 27001 (2022) define a los equipos tecnológicos como activos importantes que debe protegerse con control adecuado para así cuidar la integridad y disponibilidad de la información.

Por su parte, Bocanegra (2021), sostiene que los equipos tecnológicos deben verse como activos de TI, ya que su buen funcionamiento garantiza que los procesos del negocio sean estables y que los datos sean confiables procesamiento, resguardo y transmisión de información institucional.

2.3.4.1.Importancia de los equipos tecnológicos

La importancia de los equipos tecnológicos radica en su contribución directa al desempeño de los sistemas de información y a la continuidad de los procesos organizacionales. Según Laudon y Laudon (2020), estos componentes determinan la capacidad operativa de los sistemas informáticos, ya que influyen en la rapidez, precisión y disponibilidad de las actividades basadas en TI.

Romero (2022) resalta que los equipos tecnológicos se consideran activos estratégicos debido a que permiten ejecutar procesos críticos, almacenar información clave y garantizar la continuidad del negocio ante fallas o incidentes. Del mismo modo, la norma ISO/IEC 27002 (2022), enfatiza que una adecuada gestión y protección de estos equipos es esencial para asegurar la disponibilidad e integridad de los servicios tecnológicos.

2.3.4.2.Clasificación de las Equipos Tecnológicos

La clasificación de los equipos tecnológicos permite agruparlos según su función, características y su papel dentro de la infraestructura TI. Turban, Pollard y Wood (2021), establecen una clasificación basada en cuatro categorías: equipos de procesamiento, dispositivos de almacenamiento, equipos de comunicación y periféricos, cada uno con un rol específico en el soporte de los sistemas de información.

Por otra parte, la norma ISO/IEC 27002 (2022) plantea clasificarlos como activos físicos dentro de categorías como equipos de usuarios final, de red de procesamiento y medios de almacenamiento, subrayado en papel que juegan en el clico de vida de la seguridad de la información. Para completar esta idea, el NIST (2020), organiza los equipos tecnológicos en hardware de usuario, infraestructura de red, servidores, dispositivos móviles y sistemas especializados, haciendo énfasis en que son recursos diversos y críticos al mismo tiempo.

2.3.4.3.Tipología de Equipos Tecnológicos

2.3.4.3.1. Equipos de cómputo

Los equipos de cómputo constituyen la base operativa de la infraestructura tecnológica de cualquier organización, ya que permiten la ejecución de aplicaciones, el procesamiento de datos y la interacción directa del usuario con los sistemas de información corporativos. Estos dispositivos incluyen computadoras de escritorio, laptops y estaciones de trabajo, cada una diseñada para responder a diferentes niveles de demanda operativa. Según Laudon y Laudon (2021), los equipos de cómputo representan el acceso principal entorno digital; por lo tanto, gestionarlos correctamente es fundamental para que los procesos de la organización se desarrollen con eficiencia y sin interrupciones.

Las estaciones de trabajo y los equipos de alto rendimiento juegan un papel en actividades que exigen mucho procesamiento, como el diseño gráfico, el modelado 3D, el análisis de datos o la ingeniería asistida por computadora, es que estos dispositivos tienen arquitecturas más potentes, gráficos avanzados y procesadores preparados para trabajos pesado. Stallings (2022), señala que la evolución del hardware he hecho posible que las estaciones de trabajo incluyan características de computación avanzada, y gracias a eso, se han vuelto herramientas clave otros sectores donde la precisión y la velocidad de cálculos lo son todo.

El auge del teletrabajo y la movilidad empresarial ha hecho que las laptops y los dispositivos portátiles se vuelvan piezas centrales en el día a diade muchas organizaciones. Estos equipos permiten el acceso remoto a sistemas corporativos, facilitando la continuidad operativa y la flexibilidad del trabajo. Turban, Pollard y Wood (2021), afirman que la adopción de equipos móviles y portátiles ha transformado la dinámica del entorno laboral al proporcionar acceso ubicuo a información y aplicaciones críticas, incrementando la productividad y reduciendo barreras geográficas.

2.3.4.3.2. Equipos de red

De manera complementaria, los equipos de red incluyendo routers, switches, firewalls y puntos de acceso permiten la comunicación y transferencia segura de datos entre usuarios y sistemas, cumpliendo un rol estratégico dentro de la infraestructura tecnológica (Cisco Press, 2021). Asimismo, los servidores, ya sean físicos y virtualizados o en formato modulares, ofrecen capacidad de cómputo centralizada y se han vuelto la columna vertebral de los entornos empresariales de hoy (Tanenbaum y Wetherall, 2021).

El uso de tecnología de respaldo y recuperación, como servidores dedicados, cintas magnéticas moderna y sistemas híbridos, ha crecido bastante por el aumento de los ciberataques y porque cada vez dependemos más del almacenamiento digital, gracias a las

arquitectura de respaldo , se puede recupera la información cuando hay datos dañados ataques de ransomware o falla físicas, y es por eso que estos sistemas se han vuelto un pilar clave para que el negocio no se detenta (International Organization for Standardization 27002, 2022).

Sumando a esto, la integración de políticas de retención, recopilación y versionamiento refuerza la protección de los activos de información, lo que les permite a las organizaciones reaccionar con agilidad frente a eventos disruptivos (Oltsik, 2021). En este contexto, la planificación estratégica del respaldo constituye una buena práctica de gobernanza tecnológica.

2.3.4.3.3. Equipos servidores

Los servidores físicos siguen siendo fundamentales para organizaciones que requieren control total, alto rendimiento y mayor seguridad en el procesamiento de datos críticos. Estos equipos se caracterizan por ofrecer recursos dedicados y una arquitectura robusta orientada a la estabilidad operativa (Stallings, 2022).

Por su parte, la virtualización de servidores permite correr con varias máquinas virtuales en mismo hardware lo que aumenta la eficiencia y baja de costos de infraestructura, además, este enforque facilita juntar los recursos en un solo lugar y da más flexibilidad a la hora de repartir las cargas de trabajo (Marinescu, 2023).

Hoy en día, la gestión de servidores combina lo físico con los virtualizado mediante infraestructura convergentes que integran, en un solo sistema, el cómputo, el almacenamiento y la red. Este modelo mejora la escalabilidad y simplifica la administración tecnológica (Furht y Escalante, 2021).

2.3.4.3.4. Periféricos y dispositivos complementarios

Las impresoras siguen siendo dispositivos esenciales para la gestión documental, permitiendo producir información física de forma segura y eficiente. En los últimos años, estos equipos han incorporado funciones avanzadas de protección, administración remota y control de acceso para fortalecer la seguridad de los documentos corporativos (HP Inc., 2023).

Los escáneres juegan un papel clave en la digitalización de documentos, ya que facilitan pasar la información física a formatos electrónico que se pueden guardar y procesar más rápido, además la integración de tecnología OCR ha mejorado la precisión y la automatización al momento de capturar los datos (Epson, 2022)

Los proyectores continúan siendo periféricos importantes en entornos corporativos y educativos, ya que facilitan la comunicación visual y las presentaciones colaborativas. Su evolución hacia resoluciones más altas y conectividad inalámbrica ha mejorado la experiencia en salas de reuniones y espacios interactivos (BenQ, 2021).

2.3.5 Gestión de Riesgos

La gestión de riesgos es hablar de un proceso estratégico mediante el cual una organización identifica, analiza y responde de manera anticipada a los diversos peligros que amenazan las operaciones, activos e información. En vez de esperar a que ocurra una emergencia como un ciberataque y actuar de manera desesperada, la organización se adelanta calculando qué tan posible es que pase esa desgracia y cuánto dinero le costaría. A partir de ese análisis se definen medidas claras para prevenir riesgos de forma controlada. En definitiva, gestionar los riesgos no busca eliminar los peligros por completo, sino garantizar que se pueda tomar decisiones seguras, proteger su patrimonio y asegurar la continuidad de sus actividades. (Miranda, 2017)

2.3.6 Normas ISO/IEC 27001 e ISO/IEC 27002

La ISO/IEC 27001 es la norma internacional que establece los requisitos para crear, implementar y mantener un sistema de gestión de la seguridad de la información (SGSI). Su objetivo es ayudar a organizaciones de cualquier tamaño a proteger sus datos más valiosos frente a ciberataques y accesos no autorizados de forma ordenada. Por su parte, la ISO/IEC 27002 funciona como una guía práctica complementaria que detalla el cómo de cada control de seguridad listado en la ISO 27001, mientras que la norma principal menciona los controles brevemente, la 27002 dedica explicaciones a fondo sobre su objetivo. (Disterer, 2013)

La gran diferencia entre ambas radica en su función y en la posibilidad de obtener una certificación. La ISO 27001 define el marco general de gestión y es la única norma certificable, demostrando formalmente a clientes y socios que la empresa protege su información. En cambio, la ISO 27002 es simplemente un manual de consulta y buenas prácticas de uso opcional que orienta a los equipos técnicos en la implementación de las medidas, por lo que una empresa no puede certificarse directamente bajo este estándar.

2.3.7 Metodología MAGERIT

La metodología elegida en este trabajo es la MAGERIT la cuál funciona como una guía práctica para las instituciones y afianzar su seguridad digital. Lo que hace es ayudarles a poner en una balanza lo que más importa, entender sus vulnerabilidades ante posibles ataques, y calcular las consecuencias si algo sale mal. Con esto claro, las instituciones pueden aplicar

soluciones concretas ajustadas a la probabilidad real de que ocurra un problema. (Gómez et al., 2012). Para lograrlo, se despliega en una serie de fases clave:

- Planificación y Definición del Alcance
- Valoración de Activos
- Análisis de Riesgos
- Identificación de riesgos
- Evaluación de Riesgos
- Tratamiento y Gestión de Riesgos
- Monitoreo y Mejora Continua

Esta metodología le da un toque de orden a la toma de decisiones. Adiós a la improvisación: MAGERIT busca que se tome conciencia de sus riesgos reales, prepara a la empresa para superar auditorías sin sorpresas y genera herramientas muy útiles, como planes de seguridad bien estructurados, para saber exactamente dónde están parados en materia de protección TIC. Por último, no se trata de un solo esfuerzo, sino de un hábito de mejora continua. Al proteger pilares clave como la confidencialidad, la disponibilidad y la integridad de los datos, las empresas aprenden a convivir contra las sorpresas. Así, tras sondear el panorama, la dirección puede decidir con total claridad si un riesgo conviene reducirlo, pasárselo a un tercero o simplemente asumirlo. (Miranda, 2017)

2.4 Conclusiones del marco teórico

Lo plateado en este marco teórico permitió comprender que la auditoria de seguridad informática es un proceso sistemático y documentado, orientada evaluar el estado del equipo, los programas y los procedimientos de una organización, con el propósito de identificar vulnerabilidades, valorar riesgos y proponer mejoras.

Por otra parte, el análisis de las normas ISO/IEC 27001 e ISO/IEC 27002 y de la metodología MAGERIT permitió identificar un enfoque estructurado para la gestión de riesgos, basado en la valoración de los activos en las dimensiones de confidencialidad, integridad y disponibilidad.

En conclusión, los fundamentos teóricos analizados respaldan directamente la presente investigación, ya que brindan los conceptos, normas y procedimientos necesarios para efectuar una auditoría de seguridad informática a los equipos tecnológicos del laboratorio de la Unidad Educativa Hortensia Vásquez Salvador, y constituyen la base sobre la cual se diseñarán, en los siguientes capítulos, la metodología de evaluación y la propuesta de mejora.

CAPÍTULO III

3 Marco Investigativo

3.1 Introducción

El estudio cualitativo es un método que busca una comprensión detallada de una realidad social o humana desde el punto de vista de quienes participan, indagando en significados, vivencias y contextos mediante técnicas como entrevistas, observación y análisis de textos. Este método es inductivo, adaptable y centrado en la interpretación, con la finalidad de detallar e interpretar fenómenos complicados sin dar preferencia a la medición de variables. Por otro lado, el estudio cuantitativo es un método que se centra en la cuantificación de variables y en el análisis estadístico de la información, con el propósito de identificar conexiones, verificar hipótesis y conseguir hallazgos que se puedan aplicar a partir de muestras que representan a la población. Se distingue por su planificación rigurosa, imparcialidad y capacidad de ser reproducido. (Hernández y Klimenko, 2025)

Por lo tanto, en la presente investigación se usó una investigación cualitativa ya que se empleó la técnica de la entrevista en donde dicha información fue oportuna para el direccionamiento del presente trabajo, sin embargo, el uso de la investigación cuantitativa como es la técnica de las encuestas fue clave para determinar puntos importantes de la Unidad Educativa, dichos resultados fueron ordenados y tabulados para sacar datos estadísticos en relación con el estudio de la investigación.

3.2 Tipos de Investigación

3.2.1 Investigación Bibliográfica

La investigación a través de documentos o bibliográfica es una de las modalidades de investigación cualitativa que se ocupa de reunir, compilar y elegir datos provenientes de lecturas de documentos, revistas, libros, audios, videos, periódicos, artículos de investigaciones, memorias de eventos, y más. (Carmona y Reyes, 2020)

En el presente trabajo se utilizó investigación bibliográfica documental ya que se recopilo información oportuna y relevante en el marco teórico que permitió poder comprender un poco más de los hallazgos de la investigación.

3.2.2 Investigación de Campo

La exploración de terreno recoge información directamente del ambiente en el que se presenta el fenómeno analizado, a través de observaciones, diálogos o cuestionarios. Facilita la obtención de datos concretos y contextualizados, representando la realidad de los involucrados. Es crucial para indagaciones que necesitan información actual y específica sobre hábitos y situaciones locales. (Sandoval, 2022)

En la presente investigación sobre auditoria de seguridad informática en los equipos tecnológicos de la Unidad Educativa Hortensia Vázquez Salvador, se usó la investigación de campo para constatar directamente los sistemas y equipos de dicha unidad, mediante una inspección in situ, entrevistas al encargado de laboratorio y encuestas a una muestra de los estudiantes de tercero bachillerato.

3.2.3 Investigación Aplicada

En referencia a Castro et al. (2023) la investigación aplicada, “Se enfoca en centrar su atención en identificar necesidades, problemas u oportunidades del contexto para posteriormente, aplicar conocimientos y dar respuesta a estos requerimientos desde la aplicación del método científico” (Castro et al., 2023, pág. 147)

Se empleo investigación de campo y métodos de recolección de datos para analizar y optimizar la infraestructura tecnológica en el estudio actual sobre auditoría de seguridad informática en la Unidad Educativa Hortensia Vásquez Salvador, para esto se emplearon técnicas prácticas, por ejemplo, análisis de riesgos o pruebas de vulnerabilidad, las cuales fueron adaptada a las necesidades concretas del entorno educativo.

3.3 Métodos de Investigación

En cuanto a los métodos de investigación, son procedimientos y estrategias organizada que se usan para recolectar, analizar y mostrar información, por un lado, están los cualitativo como las observaciones y las entrevistas; por otro lado, los cuantitativos, como los experimentos y las entrevistas, ambos aportan a la construcción y validad del conocimiento en distintas áreas.

3.3.1 Método Analítico

El método analítico, en el ámbito de la investigación, es un proceso que se basa en descomponer un todo en sus componentes o elementos esenciales para analizarlos y entender el origen, la esencia y las relaciones internas del fenómeno que se investiga. Este proceso tiene como objetivo obtener explicaciones más detalladas acerca de cómo y por qué suceden ciertos hechos o fenómenos, mediante el análisis individual de cada elemento. (Zamora , 2023)

En el presente trabajo se utilizó el método analítico para descomponer la infraestructura tecnológica en componentes individuales que permitirán identificar, evaluar y determinar vulnerabilidades y riesgos, además los hallazgos encontrados servirán para formular recomendaciones que contribuyan al mejoramiento de los equipos tecnológicos.

3.3.2 Método Deductivo

El método deductivo es una técnica de investigación que, a través de un proceso lógico y sistemático, se basa en principios, teorías o leyes generales para alcanzar conclusiones específicas o particulares. Principalmente, este método se emplea para verificar hipótesis porque posibilita comparar supuestos teóricos con la realidad observada, a partir de un razonamiento que va de lo general a lo particular. (Hernández y Mendoza, 2022)

En la auditoría de seguridad informática de la Unidad Educativa Hortensia Vásquez Salvador se empleó el método deductivo identificando y observando los incidentes específicos de seguridad en el cual se pudo identificar los hechos de vulnerabilidad, además se aplicaron principios generales de seguridad de tal manera que permita diseñar soluciones y prevenir futuros incidentes.

3.4 Fuentes de Información de Datos

Para el desarrollo de la presente investigación se emplearán fuentes de información primarias, las cuales permiten obtener datos de primera mano directamente del objeto de estudio. La recolección de información se estructurará a través de dos técnicas complementarias: la encuesta y la entrevista. Por un lado, la encuesta se aplicará a los estudiantes con el propósito de recopilar datos cuantitativos sobre sobre fallas de seguridad recurrentes para ello se utilizará como instrumento un cuestionario estructurado con preguntas. Por otro lado, la entrevista estará dirigida a personal técnico, con el objetivo de profundizar en

aspectos cualitativos, criterios normativos y procesos operativos sobre seguridad, esta se llevará a cabo mediante una guía de entrevista semiestructurada con preguntas abiertas que permitan obtener un análisis del entorno.

Sin embargo, como fuente secundaria tenemos a los docentes o al encargado del laboratorio, que son quienes emplean tecnología actualizada y oportuna para el aprendizaje de los estudiantes, desarrollando un plan de estudio que contribuya al mejoramiento de sus habilidades y sus conocimientos, ya que la tecnología es la herramienta para fortalecer el proceso de aprendizaje no solamente en la materia de computación sino en todas las demás.

3.5 Estrategia Operacional para la Recolección de Datos

3.5.1 Población

La población se define como un conjunto de elementos, entidades u objetos que comparten características comunes y constituyen el universo de estudio sobre el cual el investigador pretende sacar conclusiones a través de la recolección y análisis de datos. (Bernal , 2020)

En el presente trabajo la investigación fue de 263 estudiantes de bachillerato que reciben clases en la Unidad Educativa Hortensia Vásquez Salvador de la provincia Santo Domingo.

Por otro lado, se consideró para la entrevista al docente encargado de computación, ya que tiene los conocimientos necesarios para brindar información relevante respecto al estado de la infraestructura tecnológica del laboratorio.

3.5.2 Segmentación o Muestra

Una muestra es un subconjunto de la población, seleccionado de forma intencionada o probabilística, cuyos elementos son plenamente representativos de todo el grupo y permiten al investigador analizar los datos y sacar conclusiones válidas para el estudio. (Creswell y Creswell, 2021)

En la investigación se tomó a 88 estudiantes correspondientes al tercero de bachillerato, dicha muestra fue de carácter discrecional, por lo cual se les aplico una encuesta ya que tienen más conocimientos respecto a equipos tecnológicos.

3.5.3 Técnica y Tamaño de la muestra

La técnica de muestreo es un procedimiento mediante el cual el investigador selecciona elementos específicos de la población según ciertas reglas con el objetivo de crear una muestra que permita obtener información representativa y relevante para el análisis de la investigación. (Sekaran y Bougie, 2021)

Con relación a la población estudiada en la Unidad Hortensia Vásquez Salvador se tomará en cuenta a los estudiantes de bachillerato ya que ellos son tienen los conocimientos necesarios para brindarnos información relevante en relación a la infraestructura tecnológica del laboratorio.

Con estos antecedentes se tomará en cuenta a 88 los estudiantes del tercero de bachillerado para realizarle una pequeña encuesta que nos ayude a determinar factores relevantes en relación con el proyecto de investigación,

3.5.4 Plan de recolección de datos

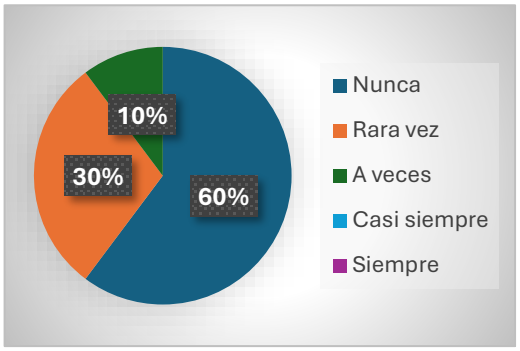
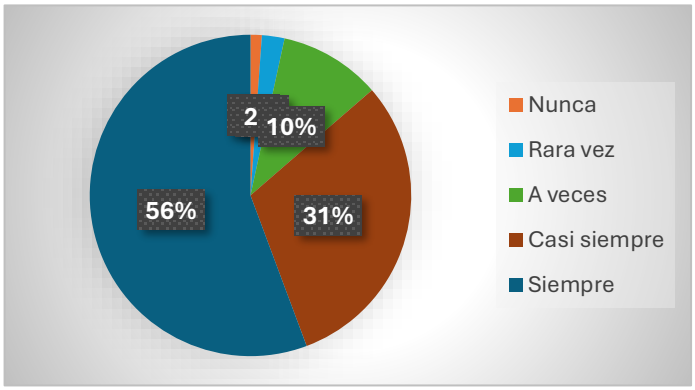
El plan de recolección de datos busca diagnosticar el estado actual de la infraestructura tecnológica y evaluar la eficacia de los controles de seguridad en el laboratorio de cómputo de la Unidad Educativa Hortensia Vázquez Salvador. Se recopilará información sobre riesgos físicos y lógicos, estado de las 33 computadoras, vulnerabilidades operativas y la presencia de amenazas como malware. Se utilizarán encuestas aplicadas a los estudiantes de tercero de bachillerato y entrevistas estructuradas dirigidas al encargado del área de computación como instrumentos principales. Este enfoque mixto cuantitativo y cualitativo, permitirá una evaluación integral del entorno tecnológico. Los datos se recolectarán en un periodo de dos semanas, garantizando la confidencialidad de la información y orientando los resultados hacia el diseño de estrategias efectivas de mitigación mediante la metodología MAGERIT y un SGSI.

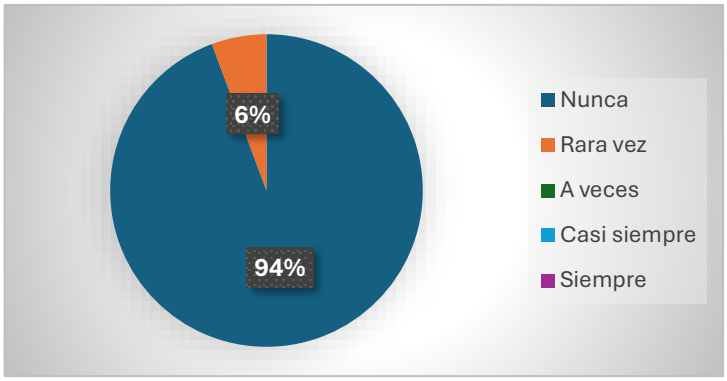
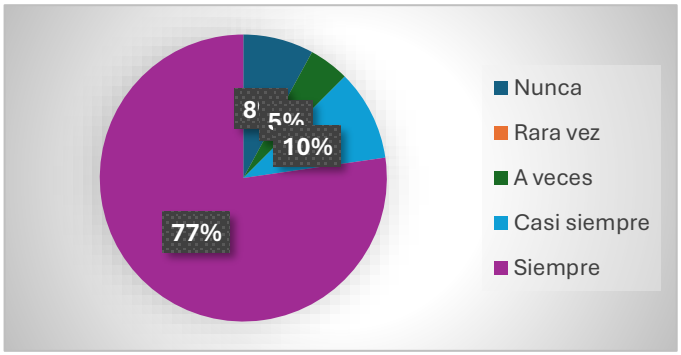
Individuos	Actividad	Fecha
88 estudiantes correspondientes a la muestra de tercero de bachillerato de la Unidad Educativa.	Se aplicaron encuestas estructuradas para identificar hábitos de uso de los equipos, hábitos de conexión de dispositivos USB, recepción de directrices de seguridad y percepción sobre la protección del laboratorio frente a amenazas informáticas.	20/04/2026 - 01/05/2026
1 docente / encargado del laboratorio de computación.	Se realizó una entrevista estructurada con una duración aproximada de 25 minutos. Con esta herramienta se obtuvo información técnica, detallada y basada en la experiencia operativa sobre la gestión de accesos, políticas de seguridad, mantenimiento preventivo y manejo de incidentes.	02/05/2026

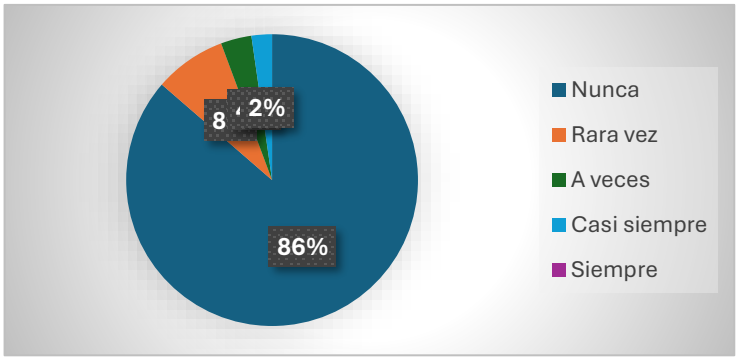
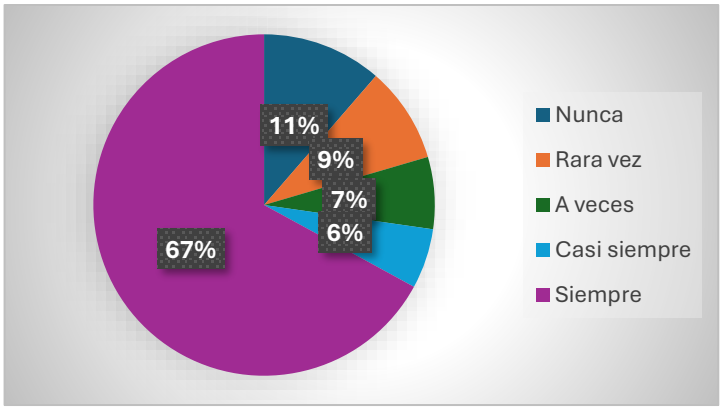
Tabla 1. *Plan de Recolección*

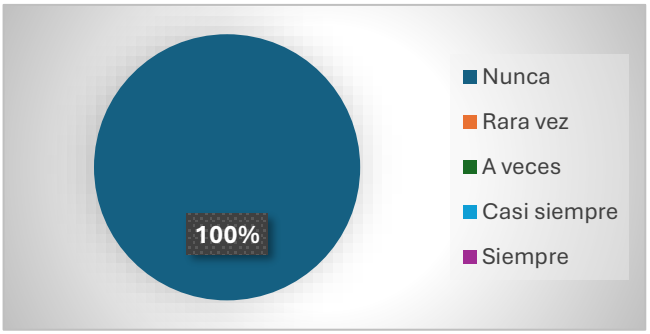
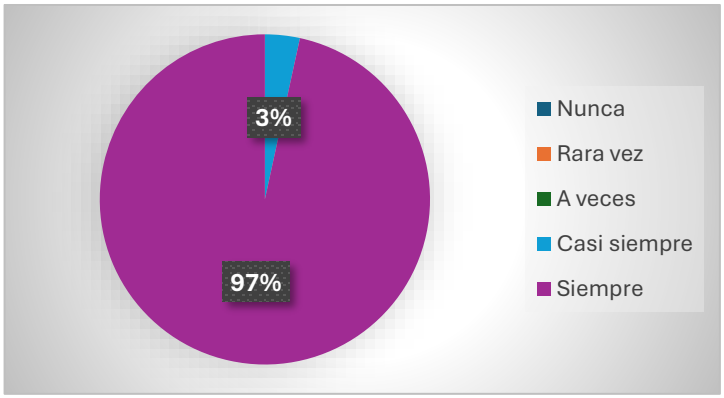
3.6 Análisis y Presentación de Resultados

3.6.1 Análisis de encuestas a estudiantes

<table>
<tr><th>Pregunta</th><th>Grafico</th></tr>
<tr><td>1. ¿Inicias sesión en los equipos del laboratorio usando un usuario o contraseña?</td><td> 
</td></tr>
<tr><td colspan="2">Análisis: Los resultados indican que la mayor parte de los usuarios emplean nombre de usuario y contraseña para entrar a las computadoras del laboratorio informático, lo cual constituye una medida básica para resguardar los datos. Pero un grupo pequeño todavía no la usa con frecuencia. Esta situación puede dar lugar a amenazas, ya que permite el acceso no autorizado a los dispositivos.</td></tr>
<tr><td>2. ¿Cierras sesión o apagas correctamente el equipo al terminar de usarlo?</td><td> 
</td></tr>
<tr><td colspan="2">Análisis: De acuerdo con los resultados, la mayor parte de los encuestados indica que apagan o cierran correctamente su sesión cuando terminan de usar las herramientas. Esta medida protege la información evita que personas sin autorización entren al sistema, sin embargo, existe un pequeño grupo que no realiza una buena práctica, por eso es fundamental recalcar esta norma entre los estudiantes.</td></tr>
</table>

Pregunta	Grafico
3. ¿Instala usted programas o aplicaciones sin autorización en los equipos de laboratorio?	
Análisis Según los datos recopilados la mayor parte respondió que no instala ningún programa sin previa autorización. Esto refleja un nivel apropiado de adherencia a las pautas definidas en el laboratorio. No obstante, existe un pequeño porcentaje que reconoce que realiza esta acción en determinadas ocasiones. La instalación de software no autorizado tiene el potencial de afectar la seguridad y el desempeño de los dispositivos. Por ende, es esencial optimizar los controles de instalación.	
4. ¿Conecta usted memoria USB u otros dispositivos externos los equipos del laboratorio?	
Análisis: De acuerdo con los resultados que se obtuvo muestra que muchos usuarios conectan estos dispositivos externos los equipos del laboratorio, si bien es algo habitual, esta práctica es la de mayor riesgo pues dichos dispositivos pueden introducir virus o programas maliciosos, por lo tanto, se sugiere definir pautas específicas para administrar el uso de estos dispositivos.	

Pregunta	Grafico
5. ¿Ha detectado virus, archivos sospechosos o mensajes extraños en los equipos?	
Análisis: La mayoría de los encuestado dice que rara vez o nunca ha encontrado virus u otros archivos, esto podría verse como una señal positiva del nivel de seguridad en el laboratorio, sin embargo, también podría significar que les falta conocimiento para identificar este tipo de problema, es decir que no se detecte no siempre quiere decir que los equipos están seguros.	
6. ¿Comparte archivos entre los equipos del laboratorio sin revisar si son seguros?	
Análisis: Los resultados muestran que el 67% de los usuarios siempre comparte archivos sin revisar si son seguros, estos datos confirman que los estos no aplican buenas prácticas de seguridad, así que es urgente capacitarlos y establecer controles, como los análisis obligatorios de los archivos.	

Pregunta	Grafico
7. ¿Modifica configuraciones del sistema (red, usuarios, permisos) sin autorización?	
Análisis: Todos los encuestados afirman no modificar la configuración del sistema sin previa autorización. El descubrimiento supone una alta adherencia a las normas establecidas en el laboratorio. También quiere decir que los usuarios no pueden entrar a configuraciones de mucha importancia. Esto ayuda a que los equipos sigan protegidos y estables. El laboratorio considera que este aspecto es una ventaja.	
8. ¿Recibe usted indicaciones de los docentes o responsables sobre el uso seguro de los equipos?	
Análisis: Los datos muestran que los estudiantes si reciben indicaciones sobre cómo usar los equipos del laboratorio de forma segura, esto quiere decir que existe cierto nivel de orientación por parte de los maestros, sin embargo, no todo reciben esta información de manera contante y esa falta de regularidad puede generar confusiones.	

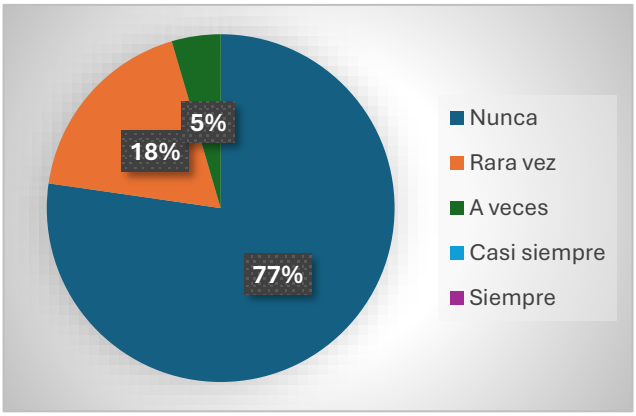
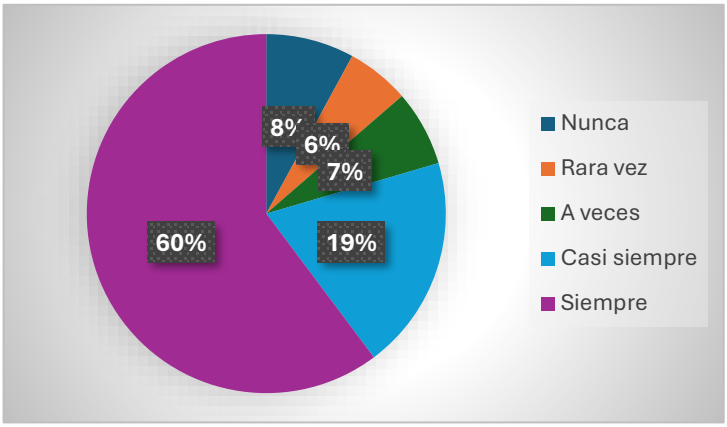
<table>
<tr><th>Pregunta</th><th>Grafico</th></tr>
<tr><td>9. ¿Has notado que otros estudiantes utilizan los equipos para actividades no académicas?</td><td> 
</td></tr>
<tr><td colspan="2">Análisis: Los hallazgos muestran que los estudiantes usan con frecuencia los equipos del laboratorio pata estas actividades que no tiene nada relacionado con lo académico, esta conducta es un peligro para la seguridad informática, dejando en evidencia que no existe control.</td></tr>
<tr><td>10. ¿Consideras que los equipos del laboratorio están protegidos contra amenazas informáticas?</td><td> 
</td></tr>
<tr><td colspan="2">Análisis: Según la mayoría de los encuestados, es comprensible que los equipos de laboratorio estén protegidos contra amenazas informáticas. Sin embargo, un porcentaje importante es expresión de incertidumbre sobre el nivel real de seguridad. Esta vista muestra que las acciones implementadas no son completamente obvias o comprensibles para los usuarios. La realización de una auditoría informática está justificada si existe confianza parcial en la seguridad del sistema. Esto le permitirá identificar lagunas y sugerir mejoras.</td></tr>
</table>

***Tabla 2**. Análisis de las encuestas aplicada a los estudiantes*

El análisis general de la encuesta evidencia que en el laboratorio de computación existen prácticas básicas de seguridad informática que son conocidas por la mayoría de los usuarios. Existen acciones que muestran que existe un nivel básico de conciencia sobre lo importante que es proteger los equipos, aunque no se aplican de manera pareja, lo que deja ver debilidades en el control y la supervisión del uso del laboratorio.

por otro lado, se identifica riesgos importantes con el uso frecuente de dispositivos externos, el compartir archivos de vez en cuando sin verificarlos y el uso equipos para actividades no académicas, estas prácticas aumentan la probabilidad que ocurran incidentes de seguridad y de quedar expuesto a amenazas informáticas.

Es más, como no hay políticas formales ni mecanismos de control más estrictos, estos comportamientos siguen aconteciendo, por eso los resultados justifican la necesidad de hacer una auditoria se seguridad informática que ayude a fortalecer la protección del laboratorio y a mejorar el uso de herramientas tecnológicas.

3.6.2 Análisis de Entrevista a Autoridades de la Institución

Tabla 3:Análisis de la entrevista aplicada al docente

Pregunta	Respuesta	Análisis
1. ¿Qué políticas o normas de seguridad informática existen en el laboratorio de computación y por qué se implementaron esas medidas?	En el laboratorio existen algunas normas básicas de seguridad informática, como la prohibición de instalar software sin autorización y el uso adecuado de los equipos. Estas normas se implementaron principalmente para evitar daños en los equipos y el uso indebido del sistema. Sin embargo, no todas las normas están documentadas formalmente ni se aplican de manera estricta, lo que hace que en algunos	Como se indicó en la entrevista, en el laboratorio sólo existen reglas básicas de seguridad informática. Estas reglas no están registradas oficialmente ni se aplican estrictamente. A los estudiantes se les

Pregunta	Respuesta	Análisis
	casos los estudiantes no las respeten completamente.	hace difícil cumplir con los requisitos.
2. ¿Cómo se gestiona el acceso de estudiantes y docentes a los equipos de laboratorio y qué criterios se usa para automatizar o restringir ese acceso?	Se gestiona principalmente mediante la supervisión del docente decir, no se cuenta con un sistema individualizado de usuarios para cada estudiante, debido a limitaciones técnicas y administrativas. Esto facilita el acceso, pero también representa un riesgo, ya que no siempre es posible identificar quién realizó determinadas acciones en los equipos.	El acceso al equipo está controlado principalmente por el profesor, sin el uso de cuentas personales. Esta modalidad permite el uso del laboratorio, pero limita el seguimiento realizado.
3. ¿Qué mecanismos se utilizan para prevenir virus, malware u otras amenazas informáticas en los equipos del laboratorio y por qué se eligieron esas herramientas o métodos?	Los equipos tienen antivirus instalado, el cual se actualiza cierto tiempo, sin embargo, las actualizaciones no siempre se realizan con la frecuencia que lo amerita.	El laboratorio si cuenta con antivirus pero gratis y además las actualizaciones no se realizan en el tiempo adecuado, lo que significa un riesgo grave, todo esto demuestra que las medidas actuales no alcanzan
4. ¿Cómo se controla la instalación de software y lo cambios	La instalación de software está restringida, pero algunos instalan programa cambian configuraciones	Aunque existen restricciones a la instalación de

Pregunta	Respuesta	Análisis
de configuración de equipos y que dificulta mantener ese control?	básicas, se hace difícil mantenerlos vigilado a todos	software, no se aplican de manera uniforme. Algunos estudiantes logran implementar cambios básicos en el equipo. Esto se debe a que no existe un seguimiento y una estandarización constantes.
5. ¿Con qué frecuencia se realizan mantenimientos y actualizaciones de hardware y software, del laboratorio?	Se realiza de forma ocasional no está establecido una fecha en específico, principalmente cuando se presentan fallas evidentes. No existe un cronograma formal de mantenimiento preventivo, lo que puede afectar el rendimiento y la seguridad de los equipos. A pesar de ello, se intenta mantener los sistemas operativos y programas principales actualizados dentro de las posibilidades del laboratorio.	El mantenimiento de los equipos se realiza sólo de forma ocasional y no de forma preventiva. La falta de cronograma afecta negativamente la seguridad y la producción del laboratorio. El dispositivo puede contener errores o defectos.
6. ¿Cuándo ocurre un incidente de seguridad (virus, pérdida de información, uso	Cuando pasa un incidente de seguridad, como la aparición de un virus o falla en el sistema se revisa el equipo afectado sin embargo no existe ningún protocolo a seguir.	El entrevistado cuenta que no existe un método formal para manejar los incidentes de

Pregunta	Respuesta	Análisis
indebido de equipos), ¿qué procedimientos se siguen y por qué se actúa de esa manera?		seguridad, por lo que las acciones dependen de la experiencia del equipo responsable.
7. ¿Cuáles son los principales riesgos de seguridad informática en el laboratorio y qué mejoras considera prioritarias para reducirlos?	Considero en base a mi experiencia que están relacionados con el uso de dispositivos externos, la falta de control de usuarios y la ausencia de políticas formales de seguridad creo que sería prioritario implementar cuentas de usuario individuales, establecer normas de seguridad más claras y realizar mantenimientos periódicos.	Los riesgos con mayor afectación son lo de dispositivos externos y falta de control También se hace referencia a la falta de políticas de seguridad informática establecidas.

A partir del análisis general de la entrevista, se puede identificar que la seguridad informática del laboratorio se gestiona de manera básica y de muchos casos de manera informal, si bien las normas existentes apuntan principalmente a evitar daños visibles de los equipos, estas no se encentran debidamente documentadas ni se complementan de forma constante.

Asimismo, queda en evidencia que no hay procedimientos claro para dar mantenimiento a los equipos ni para atender incidente de seguridad informática, las medidas correctivas se aplican únicamente cuando surge algún problema, es decir, se trabaja con un enfoque reactivo y no preventivo, a esto se suma que los riesgos detectados, como el uso de dispositivos externos y la falta de control de usuarios, se mantiene latentes por la ausencia de política formales. Esta situación demuestra la necesidad de fortalecer la gestión de la seguridad informática mediante una auditoría que permita establecer controles adecuados y mejorar la protección del laboratorio.

3.6.3 Descripción de los resultados obtenidos

El propósito de esta investigación fue identificar problemas, vulnerabilidades, amenazas que recaen en los equipos tecnológicos y seguridad del laboratorio de computación de la Unidad Educativa Hortensia Vásquez Salvador, y proponer una guía SGSI.

En la pregunta 3 y 7 de la encuesta y pregunta 4 de la entrevista se habla de la instalación de programas de terceros en los computadores del laboratorio dando a conocer que, aunque no es frecuente y muchos niegan hacerlo, la entrevista revela que si existen casos de cambios de la configuración para instalación de programas.

En la pregunta 4 y 6 de la encuesta y la pregunta 3 de la entrevista dan a conocer una falencia en cuanto a seguridad y virus ya que los resultados dicen que permite instalar cualquier USB, comparten archivos entre equipos y sumado eso los antivirus muchas veces se encuentran desactualizados. Lo que da puerta abierta a posibles infecciones.

En la pregunta 5 y 6 de la entrevista se evidencia que no existe un plan de mantenimiento ya que no hay fechas ni periodos para hacerlos, además que tampoco existen protocolos de acción ante un accidente o falla en el laboratorio, es decir no se sabe cómo actuar ante accidentes.

La pregunta 1 y 2 de la entrevista nos habla de que no existe un seguimiento en el control de las reglas del laboratorio, por lo que muchas veces son ignoradas. Y tampoco hay control sobre las actividades que se hacen en el laboratorio ya que a un solo docente se le complica vigilar a tanto estudiante.

3.6.4 Informe final del análisis de los datos

La situación crítica en el laboratorio de computación de la Unidad Educativa Hortensia Vásquez Salvador, es principalmente consecuencia de una gestión de seguridad informática de manera informal, la ausencia de mantenimientos periódicos y la falta de políticas claras. Los problemas existentes fueron confirmados a través de encuestas aplicadas a 88 estudiantes de tercero de bachillerato y la entrevista realizada al docente responsable, lo que hizo evidente la urgencia de aplicar la metodología MAGERIT y establecer una guía SGSI.

Los hallazgos destacan vulnerabilidades severas en el control de acceso, dado que la supervisión es únicamente visual por parte del docente y no existen cuentas de usuario individuales, dificultando el seguimiento de las acciones en los equipos. Hay una alta exposición a virus por el uso descontrolado de memorias USB, la carencia de análisis obligatorios de archivos compartidos y la dependencia de software antivirus desactualizado.

Aunque los estudiantes afirman conocer reglas básicas de uso y reportan no percibir infecciones masivas de virus, el análisis cruzado revela que estas prácticas son insuficientes y se realizan actividades no académicas con frecuencia dentro del laboratorio. Existe un consenso generalizado en la evaluación integral sobre la necesidad inminente de tomar medidas correctivas. Estas carencias operativas justifican la implementación de restricciones mediante perfiles de usuario, el diseño de normativas de seguridad documentadas y la programación de mantenimientos periódicos para garantizar la confidencialidad, integridad y disponibilidad del laboratorio.

CAPÍTULO IV

4 Marco Propositivo

4.1 Introducción

En capítulos anteriores evidenció la existencia de vulnerabilidades y riesgos en la seguridad informática de los equipos tecnológicos de la Unidad Educativa Hortensia Vázquez Salvador. Las mismas que representan una amenaza real para la confidencialidad, integridad y disponibilidad de la información en la institución. En respuesta a esta situación, el presente capítulo desarrolla el marco propositivo de la investigación, consiste en la aplicación de una auditoría de seguridad física, la cual se fundamenta en la aplicación de la metodología MAGERIT. La implementación de esta propuesta busca no solo mitigar los riesgos actuales, sino también implantar capacidades de respuesta en la Unidad Educativa Hortensia Vázquez Salvador para gestionar de mejor forma su seguridad informática a futuro, contribuyendo así a la mejora de la calidad educativa y protección de datos.

4.2 Descripción de la propuesta

La propuesta consiste en la realización de una auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa Hortensia Vázquez Salvador, con el propósito de identificar, analizar, evaluar y tratar los riesgos asociados a la seguridad de la información. Esta propuesta tiene un enfoque preventivo, que busca no solo diagnosticar el estado actual de seguridad, sino también a generar proponer un modelo de mejora continua que se mantenga a largo plazo. La auditoría abarcará los componentes tecnológicos como: hardware, software, redes, dispositivos y los procesos de gestión de información.

Se desarrollará mediante la aplicación de la metodología MAGERIT, organizada en seis fases claramente definidas:

- Planificación y Definición del Alcance
- Valoración de Activos
- Análisis de Riesgos
- Identificación de riesgos

- Evaluación de Riesgos
- Tratamiento y Gestión de Riesgos
- Monitoreo y Mejora Continua

Como resultado principal de esta auditoría se elaborará una guía del sistema de gestión de seguridad de la información, documento práctico y adaptado a las características y recursos de la Unidad Educativa. Esta guía servirá como herramienta de referencia para docentes o personal administrativo, la misma que contará con: políticas, procedimientos, roles y responsabilidades en materia de seguridad informática. De esta forma, se busca reducir significativamente la exposición a incidentes de seguridad, proteger la información, y promover una cultura de seguridad informática dentro de la institución.

4.3 Determinación de recursos

Para la ejecución exitosa de la auditoría de seguridad informática y la implementación de la guía SGSI en la Unidad Educativa Hortensia Vázquez Salvador, se requiere la asignación adecuada de recursos humanos, tecnológicos y económicos. A continuación, se detalla cada uno de ellos.

4.3.1 Humanos

Los recursos humanos hacen referencia a el personal que es fundamental para llevar a cabo la propuesta. Se contemplan los siguientes roles:

Cantidad	Roles	Tiempo estimado	Responsabilidades principales
1	Investigador: Wilson Campoverde	120h	• Investigación de campo • Documentación de resultados • Creación de la Guía

Cantidad	Roles	Tiempo estimado	Responsabilidades principales
1	Tutor: Ing. Vladimir Minaya	40h	• Tutorías • Correcciones
1	Rector: Msc, Ángel Benito Rodriguez	10h	• Permisos
1	Docente de computación: Msc, Ángel Benito Rodriguez	5h	• Concede información extra de los equipos

4.3.2 Tecnológicos

Los recursos de este tipo por su parte son todos aquellos instrumentos tecnológicos que se usaron y fueron de ayuda en el desarrollo de la propuesta. Se encuentran los siguientes:

Recurso Tecnológico	Cantidad	Uso principal	Disponibilidad
Laptop	1	Herramienta fundamental para documentar, almacenar y editar información.	Propia
Impresora	1	Herramienta vital para imprimir en papel documentos importantes.	Prestada
Celular	1	Dispositivo usado para comunicación y fácil acceso a	Propia

Recurso Tecnológico	Cantidad	Uso principal	Disponibilidad
		documentos y aplicación herramientas	
Internet / Megas	9 meses	Vital para investigación y consultas	Pagado
Herramientas de Microsoft (Office, Form, Excel)	1	Se uso para el desarrollo de la propuesta (tablas, formularios)	Licencia

4.3.3 Económicos

Por recursos económicos se describe a todos aquellos gastos involucrados durante el desarrollo de la propuesta. En este tipo se encuentran los siguientes:

Gasto	Cantidad	Costo unitario	Valor Total
Transporte y viáticos	40 días	$5	$200
Honorarios del auditor	120 horas	$20	$2400
Microsoft (Office, Form, Excel)	1 licencia, 1 año	$60	$60
Laptop	1	500$	500$
Celular	1	400$	400$
Impresora	1	250$	250$
Internet celular	6 meses	$10	60$

Gasto	Cantidad	Costo unitario	Valor Total
Materiales de impresión y documentación	-	-	200$
Internet casa	9 meses	25$	225$
TOTAL			4295$

4.4 Etapas de acción para el desarrollo de la propuesta

4.4.1 Planificación programa de auditoria

PLANIFICACIÓN PROGRAMA DE AUDITORÍA DE SEGURIDAD FÍSICA PARA LA ELABORACIÓN DE UNA GUÍA SGSI, EN EL LABORATORIO DE CÓMPUTO DE LA UNIDAD EDUCATIVA HORTENCIA VÁZQUEZ SALVADOR.		
Objetivo • Identificar los riesgos de seguridad física que afectan a los equipos informáticos del Laboratorio de cómputo de la Unidad Educativa Hortensia Vázquez Salvador. • Elaborar una guía, que garantice la continuidad operativa del laboratorio en caso de riesgos.		
Técnicas y Procedimientos	**Ref. a Papel**	**Fecha**

1- Planificación • Repaso de metodología MAGERIT	4.4.1 4.4.2	04/05/2026
2- Valoración de Activos • Identificar de los activos • Valorar activos	4.4.2.2 4.4.2.2.1 4.4.2.2.4	16/05/2026
3- Análisis de Riesgos • Diseño y aplicación de instrumentos de recolección. • Tabulación de datos • Valorar probabilidad • Valorar impacto • Cálculo del Riesgo Inherente • Construcción de la Matriz de Riesgo • Estimación del riesgo	4.4.2.3 4.4.2.3.1 4.4.2.3.2 4.4.2.3.3 4.4.2.3.4 4.4.2.3.5 4.4.2.3.6 4.4.2.3.7	01/06/2026
4- Identificación de riesgos • Identificación de amenazas • Identificación de vulnerabilidades. • Identificación de salvaguardas existentes	4.4.2.4 4.4.2.4.1 4.4.2.4.2 4.4.2.4.3	20/06/2026

5- Evaluación de Riesgos • Valoración del riesgo (aceptable/no aceptable). • Evaluar la eficacia de los controles existentes	4.4.2.5 4.4.2.5.1 4.4.2.5.2	28/06/2026
6- Tratamiento y Gestión de Riesgos • Selección de estrategias de tratamiento • Diseño e implementación de nuevas salvaguardas. • Definición de indicadores de seguimiento y revisión periódica. • Mecanismos de seguimiento	4.4.2.6 4.4.2.6.1 4.4.2.6.2 4.4.2.6.3 4.4.2.6.4	02/07/2026
7- Monitoreo y Mejora Continua • Implementación del ciclo PDCA para el SGSI. • Cronograma de Auditorías y actualización • Monitoreo Constante	4.4.2.7 4.4.2.7.1 4.4.2.7.2	05/07/2026

4.4.2 Repaso de la Metodología

4.4.2.1 Metodología MAGERIT

Ilustración 2: Estructura de la metodología. Elaboración propia

El modelo basado en MAGERIT que se propone en este trabajo de titulación de una auditoria, cuenta con 6 fases, que parte de la identificación de activos, analizar y gestionar los riesgos, evaluar y plantear salvaguardas actuales y plantar nuevos controles y establecer una mejora continua, asegurando que la institución sepa actuar ante las adversidades en su seguridad informática.

La metodología MAGERIT que significa metodología de análisis y gestión de riesgos de los sistemas de información, caracterizada por ser de uso público, orientada a el análisis y la gestión de riesgos creada por el consejo superior de administración electrónica en España. Proporciona una estructura clara para asistir en la toma decisiones, protegiendo los activos de información Y haciendo una valoración adecuada de amenazas, vulnerabilidades e impactos, con el fin de garantizar la confidencialidad, integridad, disponibilidad, autenticidad y

trazabilidad de la información. Además, de permitir gestionar riesgos alineándose a la norma ISO 31000. (Ministerio de Hacienda y Administraciones Públicas, 2012)

4.4.2.2 *Fase 1.- Valoración de Activos*

4.4.2.2.1 Identificar de los activos

Un activo se define como todo aquello que tiene valor para la institución y, por lo tanto, requiere de protección ante las amenazas que se puedan presentar. Para la identificación de los activos se toma en cuenta los activos lógicos y fiscos como se hace a continuación:

4.4.2.2.2 Activos físicos

ID	Cantidad	Nombre del activo	Procesador	Especificaciones	Periféricos asociados	Marca	Uso principal
PC-001	8	Estación de Trabajo 1	Intel Celeron N3050	4 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-002	5	Estación de Trabajo 2	Intel Celeron N4020	4 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-003	4	Estación de Trabajo 3	Intel Celeron J4105	4 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-004	4	Estación de Trabajo 4	Intel Core i3-6100U	8 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio

ID	Cantidad	Nombre del activo	Procesador	Especificaciones	Periféricos asociados	Marca	Uso principal
PC-005	3	Estación de Trabajo 5	Intel Core i3-10110U	8 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-006	3	Estación de Trabajo 6	Intel Core i5-7200U	8 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-007	2	Estación de Trabajo 7	Intel Core i5-8250U	8 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-008	2	Estación de Trabajo 8	Intel Pentium Silver N5000	4 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-009	1	Estación de Trabajo 9	Intel Core i3-1115G4	8 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio
PC-010	1	Estación de Trabajo 10	AMD Ryzen 3 3250U	8 GB/120 GB SSD-Windows 10 Home	Mouse, teclado	LG	Laboratorio

ID	Cantidad	Nombre del activo	Procesador	Especificaciones	Periféricos asociados	Marca	Uso principal
PC-011	33	Monitor	-	HD - 24” - 60hz	CPU	LG	Laboratorio
PC-012	1	Televisión	-	LCD- 43”	-	TCL	Laboratorio
PC-013	1	Bocina	-	500 watts	-	American Extreme	Laboratorio
PC-014	1	Aire Acondicionado	-	24K BTU	-	LG	Laboratorio
PC-015	1	Rack	-	Aluminio	-	-	Laboratorio
PC-016	1	Switch	-	16 puertos	-	Cisco	Laboratorio
PC-017	1	Router	-	2.4 GHz – wifi 5 – 300Mbps	-	TpLink	Laboratorio
PC-018	2	Proyector	-	3500 lúmenes – 3LCD – (1024 x 768 px)	-	Epson	Laboratorio

ID	Cantidad	Nombre del activo	Procesador	Especificaciones	Periféricos asociados	Marca	Uso principal
PC-019	1	Instalaciones eléctricas	-	Regletas, + 120 metros cable	-	-	Laboratorio

Tabla 4. Activos Físicos. Investigación de campo, Elaboración propia

4.4.2.2.3 Activos lógicos

Código	Nombre del Activo	Tipo	Versión/ Licencia	Cantidad	Uso Principal	Criticidad
SW-001	Microsoft Windows 10 home	Sistema Operativo	22H2	33	Sistema operativo principal	Alta
SW-002	Microsoft Office 2019	Paquete Ofimático	Licencia Educativa	25	Documentos, planillas y presentaciones	Alta
SW-003	Navegador Google Chrome	Navegador web	Última versión	33	Acceso a recursos educativos en línea	Alta
SW-004	Antivirus de Windows, FIREWALL	Seguridad	Licencia Educativa	33	Protección contra malware	Alta

Tabla 5. Activos Lógicos. Investigación de campo, Elaboración propia

4.4.2.2.4 Valorar activos (en las 3 dimensiones MAGERIT)

Se van a evaluar los activos que se identificaron mediante una visita de campo. Las dimensiones con las que se va a trabajar en este documento se obtuvieron de MAGERIT V3 son las siguientes:

Ilustración 3. PRINCIPIOS DE LA S.I,

Fuente: ***(infosegur, 2013)***

Dimensión	¿Qué evalúa?
Confidencialidad	El daño que causa si la información pasa a manos no autorizadas
Integridad	El daño que causa si la información es manipulada
Disponibilidad	El daño que causa que la información no esté disponible

Tabla 6. Dimensiones. Elaboración propia

La valoración se va a hacer en una escala cuantitativa donde se mide el valor del activo siendo 1 el más bajo y 4 el más alto. Mide los activos críticos basándose en su impacto en las actividades, estos criterios se muestran en el cuadro a continuación:

VA	Valor de Activo	Descripción
1	**Bajo**	Activo de poca importancia, su perdida no interrumpe actividades.
2	**Medio**	Activo más necesario. Su pérdida puede afectar poco tiempo los servicios.
3	**Alto**	Activo de carácter importante. Su falla interrumpe actividades.
4	**Muy Alto**	Activo fundamental su pérdida detiene las operaciones y compromete a la seguridad.

Tabla 7. Valor de activos, Elaboración propia

Finalmente, la tabla de la valoración queda de la siguiente manera, dando el valor global de cada activo:

Código	Nombre del Activo	Confidencialidad	Integridad	Disponibilidad	Valor Global
PC-001 PC-010	Equipos de trabajo	4	4	4	**4**
PC-011	Monitor	1	1	3	**1.6**
PC-012	Televisión	1	1	3	**1.6**
PC-013	Bocina	0	0	3	**1**

Código	Nombre del Activo	Confidencialidad	Integridad	Disponibilidad	Valor Global
PC-014	Aire Acondicionado	0	0	4	**1.3**
PC-015	Rack	0	0	2	**0.6**
PC-016	Switch	1	1	4	**2**
PC-017	Router	3	3	3	**3**
PC-018	Proyector	0	0	4	**1.3**
PC-019	Instalaciones eléctricas	1	2	4	**2.3**
SW-001 SW-004	Software – programas	4	3	3	**3.3**

Tabla 8. Valorización de activos, Elaboración propia.

La tabla de valoración de activos críticos muestra una evaluación de diferentes equipos y software según los criterios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, resultando en un valor promedio. Como activos críticos se detectaron: los equipos de trabajo con un valor global de 4. Entre los dispositivos individuales, el router es el activo más crítico con valor de 3, seguido del switch 2. La mayoría de los periféricos se ubican en un rango de entre 1 y 2, mientras que rack tiene el valor más bajo con un 0.6. El software registra un valor global de 3.3, siendo un valor muy alto también.

4.4.2.3 Fase 2.- Análisis de Riesgos

4.4.2.3.1 Diseño y aplicación de instrumentos de recolección.

Para identificar los riesgos se crearon formularios para identificar las mayores amenazas a la seguridad de la información en los equipos del laboratorio de cómputo de la

unidad educativa estudiada. Las encuestas realizadas se encuentran ancladas en los anexos, el siguiente es el formato utilizado:

CUESTIONARIO PARA IDENTIFICAR RIESGOS			**PT1 | Página 1 - 5**
Preguntas	**Si**	**No**	**Observaciones**
Robo: R-001			
1. ¿El laboratorio permanece sin supervisión durante el día?			
2. ¿Los equipos cuentan con anclajes de seguridad?			
3. ¿Las puertas tienen cerraduras reforzadas?			
4. ¿El laboratorio cuenta con cámaras de vigilancia?			
5. ¿Las cámaras instaladas funcionan correctamente?			
6. ¿Existe un registro de ingreso y salida de los estudiantes al laboratorio?			
7. ¿Personas ajenas a la institución pueden ingresar fácilmente al laboratorio?			
8. ¿El laboratorio cuenta con un responsable asignado permanentemente?			
9. ¿Se realizan controles periódicos de inventario de los equipos?			
10. ¿Se realizan mantenimiento preventivo a los equipos?			
11. ¿Las ventanas cuentan con protección?			

12. ¿Los equipos permanecen conectados al terminar la jornada?			
13. ¿El laboratorio se encuentra en una zona segura?			
14. ¿Existe iluminación adecuada en el área del laboratorio?			
15. ¿El personal conoce los protocolos ante un intento de robo?			
16. ¿Hay señalización de seguridad en el laboratorio?			
17. ¿El acceso está restringido mediante horarios definidos?			
18. ¿Se han reportado robos anteriormente?			
19. ¿Se controla el uso de mochilas o bolsos dentro del laboratorio?			
20. ¿Cuentan con alarmas de seguridad?			
21. ¿Los cables periféricos o accesorios están asegurados?			
22. ¿Existe políticas claras sobre el uso y cuidado de los equipos?			
23. ¿Las llaves están bajo resguardo?			
24. ¿Se realiza supervisión al finalizar las clases?			
25. ¿El laboratorio queda sin vigilancia durante los fines de semana o feriados?			
Elaborado por: Wilson Campoverde Revisado por: Ing. Minaya Wladimir			

Fecha: 20/06/2026	Fecha:

Tabla 9. Cuestionarios de identificación de riesgos. Elaboración propia

4.4.2.3.2 Tabulación de datos

Con la aplicación de los cuestionarios al encargado del laboratorio de cómputo para los riesgos, sigue analizar las respuestas de cada pregunta basándonos en la siguiente escala:

Valor	Detalle
0	Riesgo
1	Seguridad
2	No aplica

Tabla 10.Escala de seguridad. Elaboración propia.

La encuesta se realizó de manera presencial, un ejemplo de una encuesta aplicada es de la siguiente forma y donde se observa también la calificación dada a las respuestas:

CUESTIONARIO PARA IDENTIFICAR RIESGOS			PT1 Página 1 - 5	
PREGUNTAS	SI	NO	OBSERVACIONES	
Robo: R-001				
1. ¿El laboratorio permanece sin supervisión durante el día?	X			0
2. ¿Los equipos cuentan con anclajes de seguridad?		X		0
3. ¿Las puertas tienen cerraduras reforzadas?	X			1
4. ¿El laboratorio cuenta con cámaras de vigilancia?		X		0
5. ¿Las cámaras instaladas funcionan correctamente?		X	NA	2
6. ¿Existe un registro de ingreso y salida de los estudiantes al laboratorio?		X	Docentes que usan el laboratorio	2
7. ¿Personas ajenas a la institución pueden ingresar fácilmente al laboratorio?		X		1
8. ¿El laboratorio cuenta con un responsable asignado permanentemente?		X	Hay pero no es permanente	1
9. ¿Se realizan controles periódicos de inventario de los equipos?	X			1
10. ¿Se realizan mantenimiento preventivo a los equipos?	X			1
11. ¿Las ventanas cuentan con protección?	X			1
12. ¿Los equipos permanecen conectados al terminar la jornada?		X		1
13. ¿El laboratorio se encuentra en una zona segura?	X			1
14. ¿Existe iluminación adecuada en el área del laboratorio?		X		0
15. ¿El personal conoce los protocolos ante un intento de robo?	X			1
16. ¿Hay señalización de seguridad en el laboratorio?		X		0
17. ¿El acceso está restringido mediante horarios definidos?	X			1
18. ¿Se han reportado robos anteriormente?		X		1
19. ¿Se controla el uso de mochilas o bolsos dentro del laboratorio?		X	Entran sin mochila	2
20. ¿Cuentan con alarmas de seguridad?		X		0
21. ¿Los cables periféricos o accesorios están asegurados?		X		0
22. ¿Existe políticas claras sobre el uso y cuidado de los equipos?	X			1
23. ¿Las llaves están bajo resguardo?	X			1
24. ¿Se realiza supervisión al finalizar las clases?	X			1
25. ¿El laboratorio queda sin vigilancia durante los fines de semana o feriados?	X			0
Elaborado por: Campoverde Vásquez Wilson Andrés			**Revisado por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:			**Firma:**	

Ilustración 4. Ejemplo de cuestionario de riesgos. Elaboración propia

Ilustración 5. Toma de cuestionario imagen 1.

Ilustración 6. Toma de cuestionario imagen 2

Ilustración 7. Laboratorio

La evaluación de los riesgos del laboratorio evidenció que, aunque existen condiciones de seguridad aceptables en algunos aspectos, persisten vulnerabilidades significativas en áreas críticas. Se considera imprescindible fortalecer los controles de seguridad física e informática, implementar medidas preventivas y mejorar los protocolos existentes. Estas acciones permitirán reducir los niveles de riesgo identificados y garantizar un entorno tecnológico más seguro, estable y confiable.

Tipo	**Riesgo**	**Seguridad**	**N/A**	**Valor de Riesgo (%)**	**Seguridad (%)**	**Nivel de Riesgo**
Robo	8	14	3	32%	56%	Riesgo Apreciable
Daño de equipos	14	11	0	56%	44%	Riesgo Importante

Tipo	Riesgo	Seguridad	N/A	Valor de Riesgo (%)	Seguridad (%)	Nivel de Riesgo
Incendio	7	16	2	28%	64%	Riesgo Apreciable
Malware	15	9	1	60%	36%	Riesgo Importante
Inundación	13	11	1	52%	44%	Riesgo Importante
			Promedio	46%	49%	

Tabla 11. Nivel de Riesgo

Gráficamente se representaría de la siguiente manera:

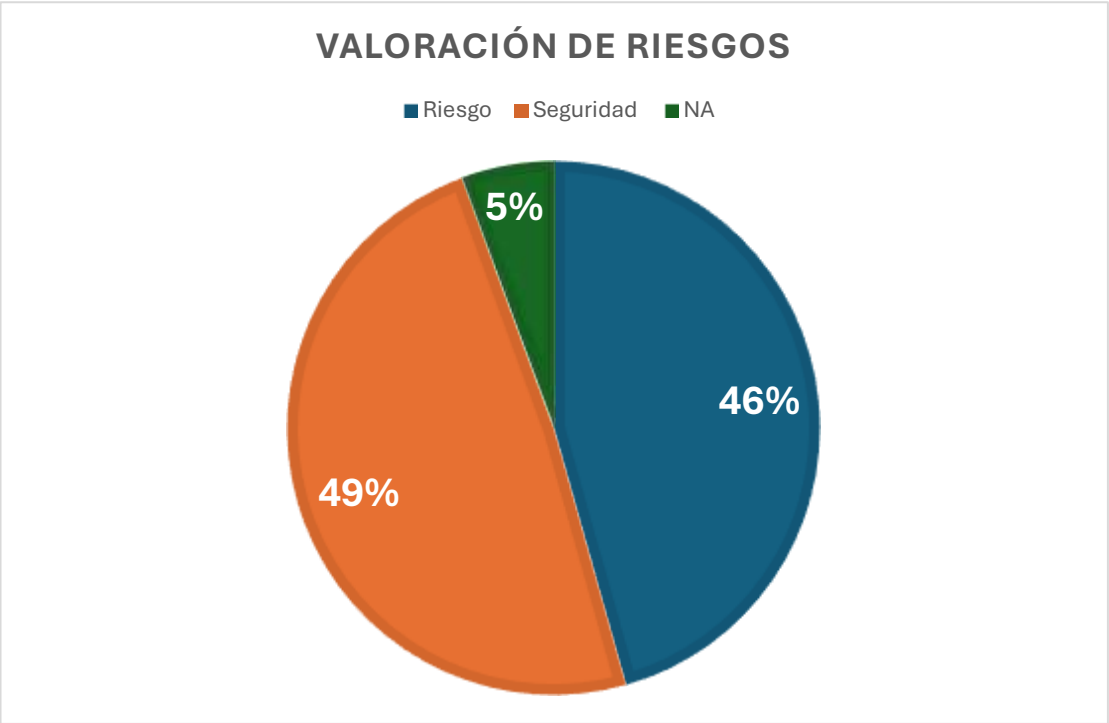


Ilustración 8. Valoración de riesgos

4.4.2.3.3 Valorar probabilidad

Con los resultados obtenidos en porcentaje de riesgo se puede medir el nivel de riesgo que genera el peligro identificado en cuestión ya a partir de aquí se puede calcular la probabilidad tomando en cuenta en la siguiente escala:

Valor de probabilidad	% de riesgo
1	1%-10%
2	10%-30%
3	30%-50%
4	50%-75%
5	75%-100%

Tabla 12. Escala de probabilidad. Elaboración Propia

4.4.2.3.4 Valorar impacto

La escala para obtener el impacto es la siguiente:

Valor De Impacto	Descripción
1	**Muy baja:** Las actividades no se ven interrumpidas
2	**Bajo:** Ocasiona un impacto menor en las actividades
3	**Moderado:** pausas momentáneas en las actividades
4	**Alto:** genera daños notables y causa pausas temporales en las actividades.
5	**Muy alta:** daños considerables, y una detención total de las actividades.

Tabla 13. Nivel de impacto. Elaboración propia

Teniendo la noción de la escala de nivel de impacto establecido era momento de medirlo en los riesgos que se identificaron. Para lo cual se tomó en cuenta 3 dimensiones que son confidencialidad, disponibilidad, integridad a evaluar como son:

Riesgos	Confidencialidad	Disponibilidad	Integridad	promedio
Robo	4	5	3	**4**
Daño de equipo	3	3	2	**2.6**
Incendio	2	5	2	**3**
Malware	4	3	5	**4**
Inundación	2	4	2	**2.6**

Tabla 14. Gravedad (Impacto). Elaboración propia

4.4.2.3.5 Cálculo del Riesgo Inherente (Probabilidad × Impacto)

Una vez que tenemos el valor de la probabilidad y el del impacto, los multiplicamos para obtener el valor de la matriz de riesgo y riesgo inherente. Con esto se conoce que riesgos debe ser tomados con mayor urgencia. A continuación, las tablas de escala de nivel de gravedad:

leyenda		PROBABILIDAD				
		1 MUY BAJA	**2 BAJA**	**3 MEDIA**	**4 ALTA**	**5 MUY ALTO**
IMPAC	**5 MUY ALTO**	5	10	15	20	25
	4 ALTA	4	8	12	16	20
	3 MEDIA	3	6	9	12	15

TO	**2 BAJA**	2	4	6	8	10
	1 MUY BAJA	1	2	3	4	5

Tabla 15. Impacto x probabilidad. Elaboración propia

MUY GRAVE	**Riesgo Muy grave:** Riesgo crítico, requiere medidas preventivas urgentes; no iniciar proyecto sin reducir y controlar el riesgo.
IMPORTANTE	**Riesgo Importante:** Riesgo moderado, evaluar económicamente medidas preventivas; si no es viable, controlar variables.
APRECIABLE	**Riesgo Apreciable:** Riesgo reducido, se monitorea sin necesidad de medidas preventivas de inicio.
MARGINAL	**Riesgo Marginal:** Riesgo mínimo, solo requiere vigilancia sin medidas preventivas iniciales.

Tabla 16. Nivel de Gravedad. Elaboración propia

4.4.2.3.6 Construcción de la Matriz de Riesgo (con Riesgo Inherente)

Finalmente uniendo los datos obtenidos de las tablas anteriores (probabilidad e impacto) y sumado a el cálculo del nivel de riesgos, se completa la matriz de riesgos. Y permite observar y concluir que el riesgo que necesita medidas preventivas urgentes es: malware. Sin dejar a un lado los otros que tienen cifras bastantes altas.

MATRIZ DE RIESGOS				
RIESGO	**Aparición (probabilidad)**	**Gravedad (Impacto)**	**Valor de Riesgo**	**Nivel de riesgo**
Robo	3	4	12	**Importante**
Daño de equipo	4	2.6	10.4	**Importante**
Incendio	2	3	6	**Apreciable**
Malware	4	4	16	**Muy grave**
Inundación	4	2.6	10.4	**Importante**

Tabla 17. Matriz de Riesgos. Elaboración propia

4.4.2.3.7 Estimación del riesgo

Según lo evaluado podemos concluir que el riesgo más grande en el laboratorio es el malware con un nivel de riesgo muy grave, mientras que otros riesgos como robo, daño de equipo, inundación se identificaron como riesgos importantes y el que presenta un menos riego según las encuestas es el incendio con un riesgo apreciable. Tras todo lo apreciado se define la existencia de problemas de seguridad informática serios en el laboratorio de la unidad educativa Hortensia Vásquez Salvador que pone en riesgo a todos los equipos e infraestructura de la institución.

4.4.2.4 Fase 3.- Identificación de riesgos

4.4.2.4.1 Identificación de amenazas (usando catálogo MAGERIT).

Se identificaron amenazas que haciéndose uso del catálogo oficial de amenazas de MAGERIT. El catálogo contiene más de 100 amenazas agrupadas en categorías, del mismo se obtuvieron:

Código	Amenaza	Categoría MAGERIT	Activos afectados	Dimensión afectada
R-001	Robo	Origen humano deliberado	Equipos de trabajo, monitores	Disponibilidad, Confidencialidad
R-002	Daño de equipos	Técnico/Ambiental	Todos los equipos	Disponibilidad, Integridad
R-003	Incendio	Técnico	Todo el laboratorio	Disponibilidad
R-004	Malware	Cibernético	Software y datos	Integridad, Disponibilidad
R-005	Inundación	Natural/Ambiental	Equipos y rack	Disponibilidad

Tabla 18. Amenazas según el catálogo de MAGERIT, elaboración propia.

4.4.2.4.2 Identificación de vulnerabilidades.

El análisis de seguridad informática realizado en el laboratorio mediante investigación de campo y encuestas ha revelado vulnerabilidades que comprometen a la institución, sus equipos y sus actividades. Se analizaron por cada riesgo identificado anteriormente: robos, daños en los equipos, incendios, malware e inundaciones. La falta de salvaguardas pone en peligro la continuidad de las actividades académicas y técnicas. Además, ayuda a la preservación del equipamiento informático.

Vulnerabilidades ante Robo:

- No cuentan con anclajes de seguridad
- No cuentan con cámaras de seguridad
- En los alrededores no cuentan con iluminación adecuada
- No cuentan con alarmas de seguridad

- No cuenta con supervisión durante desuso y fines de semana
- No se realiza supervisión al finalizar la clase

Vulnerabilidades ante Daño de equipo:

- No cuentan con instalaciones eléctricas en buen estado
- La ventilación del laboratorio no es adecuada
- Se ha detectado uso inadecuado de los equipos
- Los equipos no se apagan correctamente
- Los equipos no están protegidos contra polvo y humedad
- Manipulación incorrecta de puertos y cables

Vulnerabilidades ante Incendio:

- No cuentan con extintores
- No cuenta con señalización visible de rutas de evacuación
- Los cables eléctricos no están en buen estado
- No cuenta con un plan de emergencia ante incendio
- No cuenta con iluminación de emergencia

Vulnerabilidades ante Malware:

- No cuenta con antivirus de terceros instalado, solo cuenta con el instalado por defecto en Windows, que tiene un nivel bajo de protección.
- No se realiza revisión de virus a los equipos
- Los estudiantes tienen acceso a las configuraciones avanzadas
- No cuenta con control sobre la instalación de programas

- No se controla memorias USB
- Lentitud y fallas presentes frecuentemente
- El responsable no atiende a tiempo los incidentes de virus
- No se controla el acceso a páginas web

Vulnerabilidades ante Inundación:

- Existe filtraciones de agua en techos y paredes
- El sistema de drenaje se obstruye frecuentemente
- Las puertas no impiden el ingreso de agua
- No cuentan con bombas de drenaje

No dispone con sensores de humedad o agua

- Las áreas cercanas acumulan agua con facilidad

4.4.2.4.3 Identificación de salvaguardas existentes

Riesgo	Salvaguardas existentes	Detalles
Robo	• Cerraduras en puerta • Buena ubicación • Ventanas aseguradas • No se permite acceso fuera de horarios • Estudiantes entran sin mochila	Las cerraduras no son blindadas, no existe vigilancia continua.
Daño de equipos	• Mantenimiento preventivo • Protectores de voltaje	Se hace mantenimientos, pero no existe un protocolo, ni lapsos de tiempo para

Riesgo	Salvaguardas existentes	Detalles
	• Supervisión del uso de equipos	hacerlo. Protectores de voltaje, algunos en muy mal estado.
Incendio	• Salida de emergencia • Interruptor general • Revisión de conexiones • Buena ventilación • Simulacros y procedimientos • Detector de humo	Se revisan las conexiones cuando empiezan a fallar, ya que si están en mal estado.
Malware	• Antivirus de Windows • Firewall	La protección ante virus es muy limitada.
Inundación	• Elevación de equipos • Ventanas selladas • Sistema de drenaje	Se encuentra bien ubicado el laboratorio, pero no esta excepto de inundaciones y los equipos si están elevados en su mayoría.

Tabla 19. Salvaguardas existentes

4.4.2.5 Fase 4. Evaluación de Riesgos

4.4.2.5.1 Valoración del riesgo (aceptable/no aceptable).

Se valora cada riesgo justificando el problema que genera y tomando en cuenta su nivel de riesgo obtenido de la matriz de riesgo, para tomar una decisión que puede ir desde aceptable o no aceptable, pero también condicionalmente aceptable si despende de un factor externo.

Riesgo	Nivel de riesgo	Justificación	Decisión
Robo	Importante	Pérdida de activos tecnológicos representa un costo elevado para la institución.	No aceptable
Daño de equipo	Importante	Afecta directamente la disponibilidad y confidencialidad de los equipos para clases prácticas. Y puede causar retrasos en las actividades	No aceptable
Incendio	Apreciable	Existen algunos controles físicos, pero falta un plan formal de emergencia.	No aceptable
Malware	Muy grave	Alto impacto en la confidencialidad y disponibilidad de la información académica. Además de una gran amenaza por el uso de memorias USB	No aceptable

		por parte de estudiantes y falta de antivirus más potente.	
Inundación	Importante	Aunque la probabilidad es baja, el impacto es significativo.	Condicionalmente Aceptable

Tabla 20. Valoración de activos. Elaboración propia

4.4.2.5.2 Evaluar la eficacia de los controles existentes

Para poder calificar las salvaguardas se toma de inspiración COBIT que evalúa los controles informáticos basándose en su diseño y su operación. De ahí se extrae la lógica para calificar un control:

- **Ineficaz:** El control está instalado, pero no funciona en absoluto.
- **Baja:** El control funciona a veces, pero depende otros factores para activarse.
- **Moderada:** El control protege moderadamente, pero se ve superado en crisis.
- **Alta:** El control protege bien, está automatizado, documentado y se actualiza solo.

Riesgo	Salvaguardas existentes	Análisis	Tipo de control	Eficacia
Controles existentes para la amenaza de Robo de Activos (R-001)	Cerraduras en puerta	Cerraduras en mal estado	Físico	Baja
	Buena ubicación	Un segundo piso, muy visible al publico	Físico	Ineficaz

Riesgo	Salvaguardas existentes	Análisis	Tipo de control	Eficacia
	Ventanas aseguradas	Sin refuerzos de metal en las ventanas	Físico	Ineficaz
	No se permite acceso fuera de horarios	No existe un control para ello, aunque la puerta está asegurada	Política de control	Baja
	Estudiantes entran sin mochila	Una acción que no siempre se cumple	Política de control	Ineficaz
Controles existentes para la amenaza de Daño Físico (R-002)	Mantenimiento preventivo	No se hacen a tiempo, pasa a veces mucho tiempo para hacerlos	Técnico	Baja
	Protectores de voltaje	No todos los dispositivos funcionan correctamente	Técnico	Ineficaz
	Supervisión del uso de equipos	Son muchos estudiantes para la supervisión de un solo docente	Política de control	Ineficaz
Controles existentes para la	Salida de emergencia	La misma salida de emergencia es	Físico	Baja

Riesgo	Salvaguardas existentes	Análisis	Tipo de control	Eficacia
amenaza de Incendio (R-003)		la entrada, una sola puerta		
	Interruptor general	Buena opción para emergencias	Técnico	Moderada
	Revisión de conexiones	No es frecuente y por lo general se revisan cuando sucede un problema eléctrico	Técnico	Baja
	Buena ventilación	Por estar en un segundo piso, pero depende de abrir las ventanas	Físico	Baja
	Simulacros y procedimientos	No existe un documento para eso, se hacen por prevención y no seguido	Política de control	Baja
	Detector de humo	Herramienta eficiente ante alguna emergencia, se queda mucho sin batería	Físico	Baja

Riesgo	Salvaguardas existentes	Análisis	Tipo de control	Eficacia
Controles existentes para la amenaza de Malware (R-004)	Antivirus de Windows	Es el antivirus por defecto y muy poco eficiente	Lógico	Ineficaz
	Firewall	Pocas configuraciones y prohibiciones	Lógico	Ineficaz
Controles existentes para la amenaza de Inundación (R-005)	Elevación de equipos	La altura al piso beneficia en caso de inundación	Físico	Alta
	Ventanas selladas	Selladas, pero tienen pequeñas filtraciones por el pasar del tiempo	Físico	Moderada
	Sistema de drenaje	Sistema con fallas fáciles de solucionar, busca evitar acumulación de agua en caso de filtraciones	Físico	Moderada

Tabla 21. Evaluación de Salvaguardas. Elaboración propia.

Para resumir la tabla anterior se obtiene el promedio de nivel de eficacia por cada riesgo identificado.

Riesgo	Salvaguardas Principales	Promedio de eficacia
R-001: Robo	Cerraduras Ubicación	Ineficaz
R-002: Daño de equipos	Mantenimiento Protectores voltaje	Ineficaz
R-003: Incendio	Detector humo Interruptor general	Baja
R-004: Malware	Antivirus Windows Firewall	Ineficaz
R-005: Inundación	Elevación Drenaje Ventanas	Moderada

Tabla 22. Resumen Nivel de Eficacia. Elaboración propia.

4.4.2.6 Fase 5. Tratamiento y Gestión de Riesgos

4.4.2.6.1 Selección de estrategias de tratamiento (evitar, asumir, mitigar, transferir).

Para tratar los riesgos toca identificar que estrategia tomar ante cada uno por sus salvaguardas actuales.

Estrategia	Descripción	Cuando aplicarlo
Evitar	Eliminar la actividad que genera el riesgo.	Cuando el riesgo es demasiado alto y no hay salvaguardas efectivas.

Mitigar	Reducir el impacto del riesgo mediante nuevas salvaguardas.	Cuando el riesgo es inaceptable, pero se puede reducir.
Transferir	Trasladar el riesgo a un tercero.	Cuando mitigar el riesgo es muy costoso o imposible.
Asumir	Aceptar el riesgo tal como está.	Cuando el riesgo ya se encuentra en un nivel apreciable o marginal.

Tabla 23. Tipos de tratamiento. Elaboración propia.

Ya con las estrategias definidas en la tabla anterior, se plasma el riesgo y su nivel de riesgo calculado anteriormente, a las cuales se le va a asignar una estrategia y finalmente justificar la acción a tomar.

Riesgo	**Nivel de Riesgo**	**Estrategias seleccionadas**	**Justificación**
Robo	Importante	Mitigar	Es un riesgo importante. No es posible evitarlo ni transferirlo, por lo que se debe reducir su probabilidad e impacto.
Daño de equipos	Importante	Mitigar	Se puede reducir notablemente con mantenimiento y buenas prácticas.
Incendio	Apreciable	Mitigar - Asumir	Se mitiga con controles físicos o se

			asume aceptando las consecuencias.
Malware	Muy grave	Mitigar	No se puede evitar, ni asumir. Se debe reducir con medidas de bajo costo.
Inundación	Importante	Mitigar - Asumir	Se mitigan algunas causas y se asume el riesgo por limitaciones presupuestarias.

Tabla 24. Tabla de estrategias a tomar. Elaboración personal.

4.4.2.6.2 Diseño e implementación de nuevas salvaguardas.

En el siguiente enunciado se busca plantear nuevos controles para proponer a la unidad educativa, haciendo una comparativa con las salvaguardas ya existentes y con niveles de eficiencia actuales con los que se espera tener de aplicar los cambios y finalmente un promedio de presupuesto para dar una idea a la institución del costo de los cambios propuestos.

Riesgo	**Salvaguardas existentes**	**Salvaguardas recomendadas**	**Nivel de eficacia actual**	**Nivel de eficacia esperado**	**Acción Requerida**	**Costo Promedio**
Controles existentes para la amenaza de Robo de Activos	Cerraduras en puerta	Instalación de cerraduras blindadas o biométricas	Ineficaz	Alta	Cotizar e instalar cerraduras y adquirir al menos una cámara de seguridad,	60$ - 200$
	Buena ubicación	Ubicar cámaras de vídeo				50$ -

Riesgo	Salvaguardas existentes	Salvaguardas recomendadas	Nivel de eficacia actual	Nivel de eficacia esperado	Acción Requerida	Costo Promedio
(R-001)		vigilancia en el laboratorio.			puede ser IP por la economía.	250$
	Ventanas aseguradas	Mejorar la seguridad de las ventanas con marcos de metal				200$ - 300$
	No se permite acceso fuera de horarios	-				-
	Estudiantes entran sin mochila	-				-
Controles existentes para la amenaza de Daño Físico (R-002)	Mantenimiento preventivo	Plan de mantenimientos con cronograma en la guía SGSI	Ineficaz	Moderada	Adquirir protectores de voltaje para estabilizar la corriente y documentar una guía SGSI una política estricta de	0$
	Protectores de voltaje	Recuperar los protectores de voltaje que están en mal estado				500$ - 1500$

Riesgo	Salvaguardas existentes	Salvaguardas recomendadas	Nivel de eficacia actual	Nivel de eficacia esperado	Acción Requerida	Costo Promedio
	Supervisión del uso de equipos	-			mantenimiento semestral.	
Controles existentes para la amenaza de Incendio (R-003)	Salida de emergencia	Extintores de CO2 para aparatos electrónicos	Baja	Moderada	Adquirir unidades de CO2 e instalar señalética normativa.	30$ - 150$
	Interruptor general	Señalética para rutas de evacuación				40$ - 80$
	Revisión de conexiones	-				-
	Buena ventilación	-				-
	Simulacros y procedimientos	-				-
	Detector de humo	-				-
Controles existentes	Antivirus de Windows	Antivirus corporativo	Ineficaz	Moderada	Buscar antivirus que	0$

Riesgo	Salvaguardas existentes	Salvaguardas recomendadas	Nivel de eficacia actual	Nivel de eficacia esperado	Acción Requerida	Costo Promedio
para la amenaza de Malware (R-004)		con licencia educativa.			tengan licencias estudiantiles para las estaciones de trabajo y reconfigurar los permisos del sistema operativo.	
	Firewall	Configuración de perfiles de usuario sin privilegios de administrador.				0$
Controles existentes para la amenaza de Inundación (R-005)	Elevación de equipos	Instalación de canaletas porta cables elevadas para proteger el cableado	Moderada	Alta	Comprar e instalar canaletas y reubicar el cableado que esté a nivel del suelo.	25$
	Ventanas selladas	Revisar sellos de las ventanas y tapar filtraciones				0$ - 50$
	Sistema de drenaje	-				-
Total:						905$ -

Riesgo	Salvaguardas existentes	Salvaguardas recomendadas	Nivel de eficacia actual	Nivel de eficacia esperado	Acción Requerida	Costo Promedio
						2555$

Tabla 25. Propuesta de Salvaguardas. Elaboración propia.

4.4.2.7 Elaboración del Plan de Tratamiento de los riesgos.

4.4.2.7.1 Diseñar la Guía Rápida del SGSI.

El sistema de gestión de seguridad de la información se define como un marco de trabajo sistemático y documentado que permite a las instituciones gestionar la seguridad de la información, tal como lo establece la norma ISO/IEC 27001. Además, busca preservar la confidencialidad, integridad y disponibilidad de la información. Más que lograr una protección absoluta que en teoría es imposible, el SGSI tiene como propósito identificar, evaluar, asumir y minimizar los riesgos de seguridad de forma continua y adaptándose a los cambios. (ISO27000, 2020)

La guía rápida del SGSI es una herramienta práctica que se piensa para que sea de fácil aplicación y además permite a la Unidad Educativa Hortensia Vásquez Salvador implementar y mantener la seguridad de informática con mayor control sobre posibles accidentes. Su diseño se hizo pensando en la realidad económica de la institución, destacando especialmente el cronograma de mantenimientos y la revisión periódica de cableados, aspectos críticos para prevenir daños físicos e incendios, por otro lado, ayuda también a garantizar la continuidad de actividades.

4.4.2.8 Definición de indicadores, seguimiento y revisión periódica.

4.4.2.8.1 Indicadores Clave de Desempeño (KPI)

Los siguientes indicadores permiten medir la efectividad de los controles y el cumplimiento del SGSI, va ser la meta que tiene el laboratorio, es decir el margen a mantenerse después de cada mantenimiento:

Indicador	Descripción	Frecuencia	Meta
Cobertura de Antivirus	Porcentaje de equipos con antivirus instalado y actualizado	Mensual	≥ 95%
Incidentes de Malware	Número de incidentes de virus o malware reportados	Mensual	≤ 2 por mes
Cumplimiento de Mantenimiento	Porcentaje de mantenimientos realizados según cronograma	Trimestral	100%
Revisión de Cableados	Porcentaje de revisiones de cableado eléctrico realizadas	Bimestral	100%
Cierre de Sesión Correcto	Porcentaje de estudiantes que cierran sesión al finalizar	Trimestral	≥ 85%
Inventario Actualizado	Porcentaje de equipos inventariados correctamente	Mensual	100%
Capacitación	Porcentaje de estudiantes y docentes capacitados en buenas prácticas	Semestral	≥ 90%
Tiempo de Respuesta a Incidentes	Tiempo promedio para atender un incidente	Por incidente	≤ 48 horas

Tabla 26. Indicadores KPI. Elaboración propia

4.4.2.8.2 Mecanismos de Seguimiento

- **Registro mensual de actividades**: El docente de computación llenará un formulario de control mensual, donde se explica las actividades realizadas en el control de la seguridad del laboratorio.

- **Reportes trimestrales**: Se presentará al rector un informe resumido del estado de seguridad del laboratorio, junto la cotización de componentes necesarios para el mantenimiento de los equipos, además de sugerencias de mejoras de tenerlas.

- **Auditoría interna semestral**: Revisión corta realizada por el docente de computación, donde se listen los activos, daños y porcentaje de riesgo.

- **Formularios de incidentes**: Todos los eventos de seguridad tanto prevención como accidentes serán registrados y analizados para identificar sus causas. Como por ejemplo los mantenimientos y revisión de cableado.

4.4.2.9 Fase 6 Monitoreo y Mejora Continua

4.4.2.9.1 Implementación del ciclo PDCA para el SGSI.

La implementación del ciclo PDCA que se resume a planificar, hacer, verificar y actuar, en este contexto es el pilar fundamental para garantizar la mejora continua del SGSI en el laboratorio de computación de la Unidad Educativa Hortensia Vásquez Salvador. Este es un enfoque iterativo que a su vez permite asegurar que las medidas de seguridad no permanezcan estáticas, sino que vayan evolucionando a las nuevas amenazas que aparecen. Su aplicación se divide en las siguientes cuatro fases operativas:

Ilustración 9. Ciclo PDCA. ***(Mitti, 2020)***

- **Planificar:** En esta fase se establecen las políticas, objetivos, procesos y procedimientos necesarios para gestionar los riesgos de seguridad informática. En el contexto de este proyecto, esta fase ya incluye la evaluación de riesgos realizada mediante la metodología MAGERIT, la priorización de vulnerabilidades y el diseño de la Guía Rápida del SGSI adaptada a la realidad económica de la institución.

- **Hacer:** Hace referencia a la ejecución operativa del plan. Involucra la implementación práctica de las salvaguardas propuestas y de la Guía SGSI. Entre las acciones específicas se encuentran: la instalación de cámaras IP, extintores de CO2, instalación de antivirus, y la aplicación de las políticas de uso del laboratorio por parte de docentes y estudiantes.

- **Consultar:** Se centra en el monitoreo y evaluación constante del rendimiento de los controles implementados frente a los objetivos establecidos. Esto se logra mediante el seguimiento riguroso de los indicadores clave de desempeño KPI definidos, la recolección de reportes de incidentes y la ejecución de las auditorías internas pautadas.

- **Actuar:** A partir de los resultados obtenidos en la fase de verificación, se toman decisiones y acciones correctivas o de mejora. Si un control demuestra ser ineficaz en la práctica, en esta etapa se redefinen los protocolos, se actualizan las herramientas tecnológicas y se ajusta la Guía SGSI, reiniciando así el ciclo hacia una nueva planificación.

4.4.2.10 Cronograma de Auditorías, revisiones y actualización del análisis.

4.4.2.10.1 Cronograma de revisión y actualización

Para asegurar la vigencia, viabilidad y efectividad a largo plazo de los controles establecidos, es indispensable contar con una programación estructurada de monitoreo. A continuación, se detalla el cronograma de revisión y actualización, el cual define las actividades de auditoría, supervisión técnica y capacitación continua, asignando responsabilidades claras para su ejecución:

Actividad	Frecuencia	Responsable	Detalles
Revisión mensual de KPI	Mensual	Docente de computación	Última semana de cada mes
Revisión del cronograma de Mantenimiento y cableado	Trimestral	Docente de computación, Rector	Por lo general fines de semana
Auditoría interna del SGSI	Semestral	Docente de computación	Dos veces durante el periodo electivo
Revisión y actualización de la guía SGSI	Semestral	Docente de computación, Rector	Dos veces durante el periodo electivo
Capacitación general a estudiantes	Semestral	Docente de computación	Dos veces durante el periodo electivo
Simulacro de evacuación	Anual	Rector	Una vez cada año electivo

Tabla 27. Plan de actualización. Elaboración propia.

4.4.2.10.2 Monitoreo constante

Para llevar un correcto monitoreo toca tomar en cuenta que los riesgos no son estáticos. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar de un día a otro sin dar aviso. Por eso es necesario el monitoreo constante y se estableció actualización de la guía cada semestre para detectar cambios. La unidad educativa debe enfocarse en el monitoreo de los siguientes aspectos:

1. Activos nuevos que se han incluido.
2. Modificaciones necesarias de los valores de los activos.
3. Nuevas amenazas que podrían estar activas y que no se han valorado.
4. Probabilidad de nuevas vulnerabilidades.
5. El incremento en el impacto o las consecuencias de las amenazas evaluadas, lo que puede resultar en un nivel inaceptable de riesgo.
6. Incidentes de la seguridad de la información.

Los cambios importantes que afectan a la institución deberían ser la razón para una revisión más específica. Por lo tanto, las actividades de monitoreo del riesgo se deberían repetir seguido y las acciones de tratamiento del riesgo se deberían revisar periódicamente. (Ministerio de telecomunicaciones y de la sociedad de la informacion, 2020)

CAPÍTULO V

5 Auditoria

5.1 Informe de Auditoría

Tipo de Auditoría: Auditoría de Seguridad Informática

Dirigido a: Msc, Ángel Benito Rodriguez, Rector de la Unidad Educativa Hortensia Vásquez Salvador

5.1.1 Objetivo

El objetivo principal de esta auditoría es realizar una evaluación de la seguridad informática de los equipos tecnológicos del laboratorio de cómputo de la Unidad Educativa Hortensia Vásquez Salvador, aplicando la metodología MAGERIT, con el fin de identificar, analizar, evaluar y tratar los riesgos que afectan a los activos.

5.1.1.1 Los objetivos específicos son:

- Identificar los riesgos de seguridad física que afectan a los equipos informáticos del Laboratorio el laboratorio de cómputo de la unidad educativa Hortensia Vázquez Salvador.
- Elaborar una guía, que garantice la continuidad operativa del laboratorio en caso de riesgos.

5.1.2 Personal Involucrado

- **Investigador:** responsable del levantamiento de información, aplicación de la metodología de evaluación de riesgos y diseño de los planes de contingencia.
- **Rector**: Aprobar políticas y asignar recursos.
- **Docente de Computación**: Ejecutar controles diarios y reportar incidentes.
- **Estudiantes y Personal**: Cumplir las normas de uso.

5.1.3 Alcance

La auditoría de sistemas informáticos abarcó:

Planificación

- Repaso de metodología MAGERIT

Valoración de Activos

- Identificar de los activos
- Valorar activos

Análisis de Riesgos

- Diseño y aplicación de instrumentos de recolección.
- Tabulación de datos
- Valorar probabilidad
- Valorar impacto
- Cálculo del Riesgo Inherente
- Construcción de la Matriz de Riesgo
- Estimación del riesgo

Identificación de riesgos

- Identificación de amenazas
- Identificación de vulnerabilidades.
- Identificación de salvaguardas existentes

Evaluación de Riesgos

- Valoración del riesgo (aceptable/no aceptable).
- Evaluar la eficacia de los controles existentes.

Tratamiento y Gestión de Riesgos

- Selección de estrategias de tratamiento
- Diseño e implementación de nuevas salvaguardas.
- Definición de indicadores de seguimiento y revisión periódica.
- Mecanismos de seguimiento

Monitoreo y Mejora Continua

- Implementación del ciclo PDCA para el SGSI.
- Cronograma de Auditorías y actualización
- Monitoreo Constante

5.1.4 Análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas)

Con el fin de evaluar la viabilidad e impacto de implementar el SGSI en el laboratorio de computación de la Unidad Educativa Hortensia Vásquez Salvador, se realizó el siguiente análisis FODA:

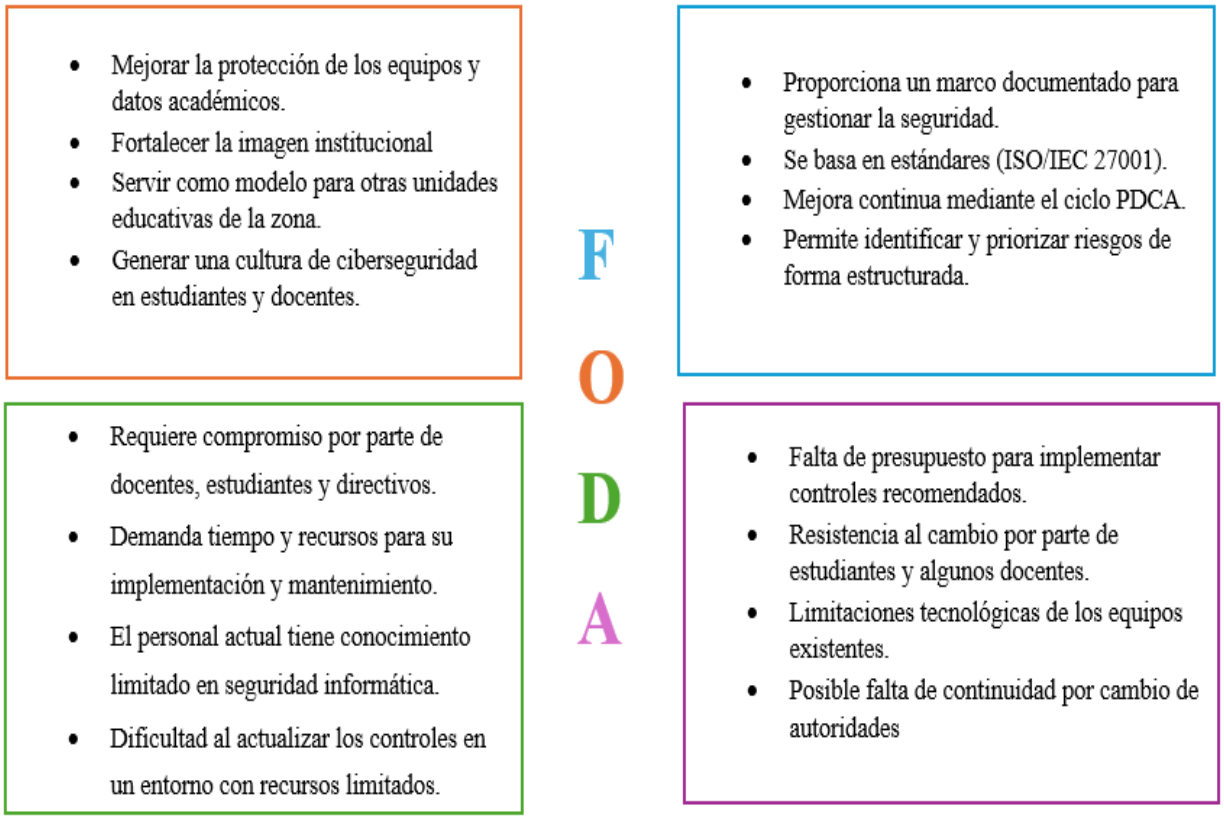


Ilustración 10. Análisis FODA. Elaboración propia

5.1.5 Hallazgos

El gráfico general evidencia que el laboratorio presenta niveles de riesgo entre importante y muy grave frente a amenazas como daños, inundación, incendio, robo y malware lo que revela vulnerabilidades y falta de controles. Los resultados destacan la urgente necesidad de reforzar la seguridad física y aplicar medidas correctivas alineadas con la metodología MAGERIT.

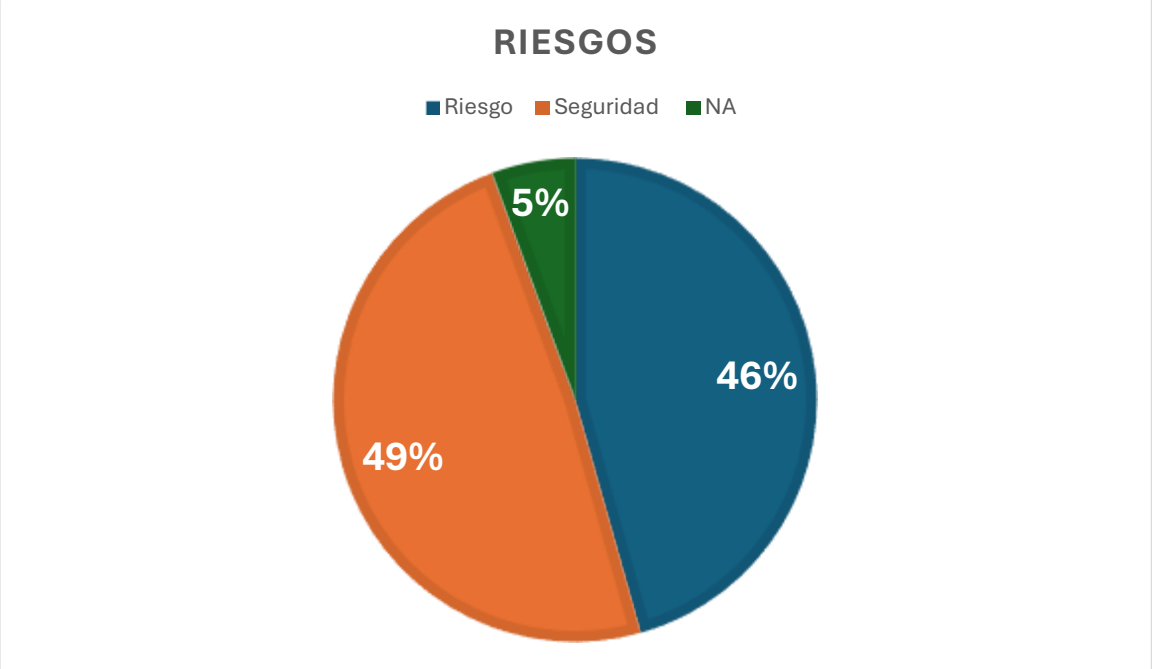
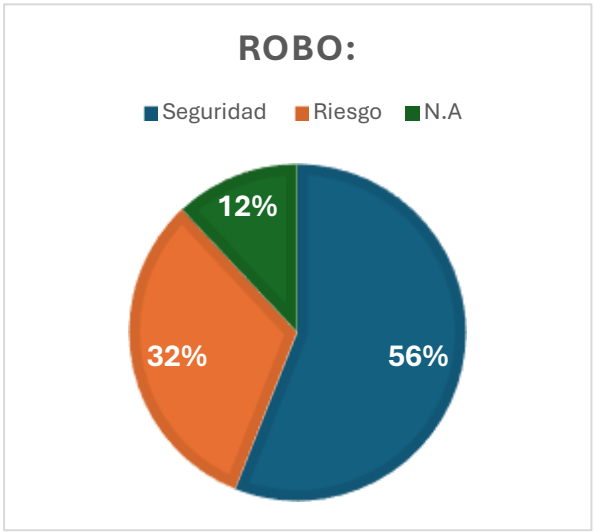
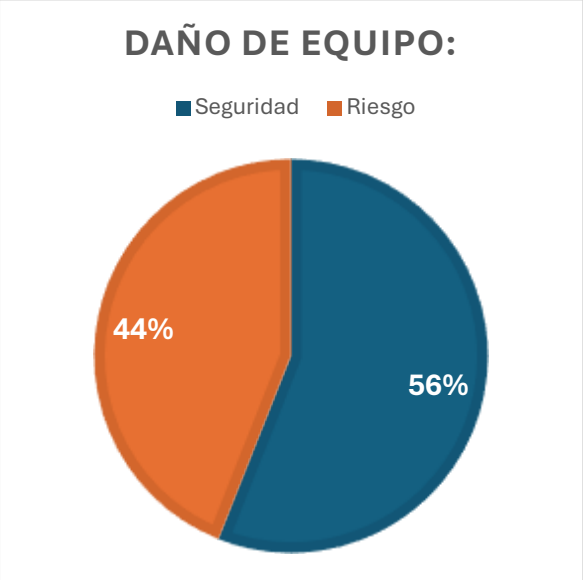


Ilustración 11. Resumen de Riesgos. Elaboración propia.

Riesgo de robo:	**Debido a:**
	• No cuentan con anclajes de seguridad • No cuentan con cámaras de seguridad • En los alrededores no cuentan con iluminación adecuada • No cuentan con alarmas de seguridad • No cuenta con supervisión durante desuso y fines de semana • No se realiza supervisión al finalizar la clase
Interpretación:	

Riesgo apreciable: El análisis del riesgo de robo (**Riesgo Importante**) evidencia un nivel de riesgo del 32%, frente a un 56% de condiciones de seguridad, lo que indica que, aunque existen medidas de protección implementadas, aún persisten vulnerabilidades que podrían facilitar la ocurrencia de incidentes. Este porcentaje de riesgo se relaciona principalmente con la ausencia de anclajes de seguridad, la falta de cámaras y alarmas, la insuficiente iluminación en los alrededores y la inexistencia de supervisión durante los periodos de desuso, fines de semana y al finalizar las clases.

Por lo que se recomienda fortalecer los controles existentes y aplicar medidas preventivas adicionales para reducir la probabilidad de ocurrencia.

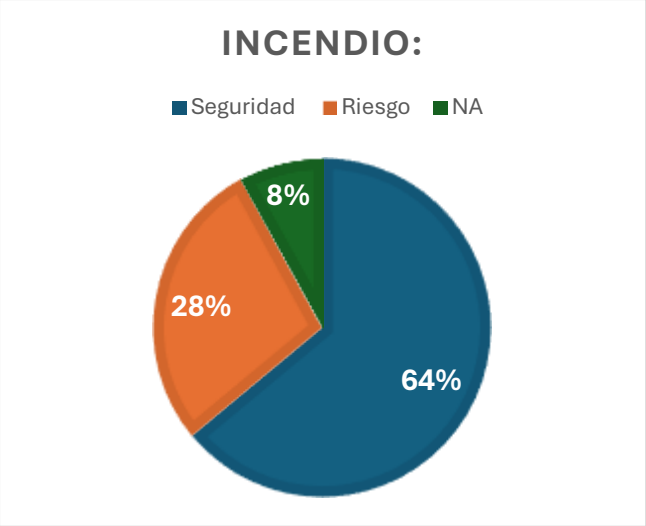
Riesgo de daño de equipo:	**Debido a:**
	• No cuentan con instalaciones eléctricas en buen estado • La ventilación del laboratorio no es adecuada • Se ha detectado uso inadecuado de los equipos • Los equipos no se apagan correctamente • Los equipos no están protegidos contra polvo y humedad • Manipulación incorrecta de puertos y cables

Interpretación:

Riesgo importante: El riesgo de daño de equipos (**Riesgo Importante**) presenta un 56% de riesgo y un 44% de seguridad, lo que evidencia un predominio del riesgo sobre las condiciones de protección.

Este nivel de riesgo se explica principalmente por diversas deficiencias en las condiciones del laboratorio, entre las cuales destacan el mal estado de las instalaciones eléctricas, la inadecuada ventilación del ambiente, el uso incorrecto de los equipos y la falta de procedimientos adecuados para su apagado.

Por lo que implica la necesidad de implementar acciones correctivas inmediatas, tales como el mantenimiento preventivo de los equipos, el uso adecuado de los mismos y el fortalecimiento de las normas de operación.

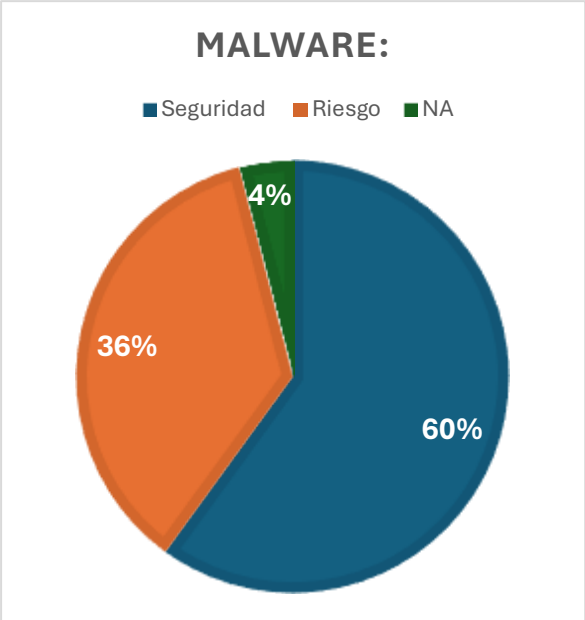
Riesgo de incendio:	**Debido a:**
	• No cuentan con extintores • No cuenta con señalización visible de rutas de evacuación • Los cables eléctricos no están en buen estado • No cuenta con un plan de emergencia ante incendio • No cuenta con iluminación de emergencia

Interpretación:

Riesgo apreciable: El riesgo de incendio (**Riesgo Apreciable**) muestra un 28% de riesgo y un 64% de seguridad, lo que refleja un nivel de protección mayoritario.

El porcentaje de riesgo identificado se debe principalmente a la ausencia de extintores, la falta de señalización visible de las rutas de evacuación, el deterioro de los cables eléctricos, la inexistencia de un plan de emergencia ante incendios y la falta de iluminación de emergencia.

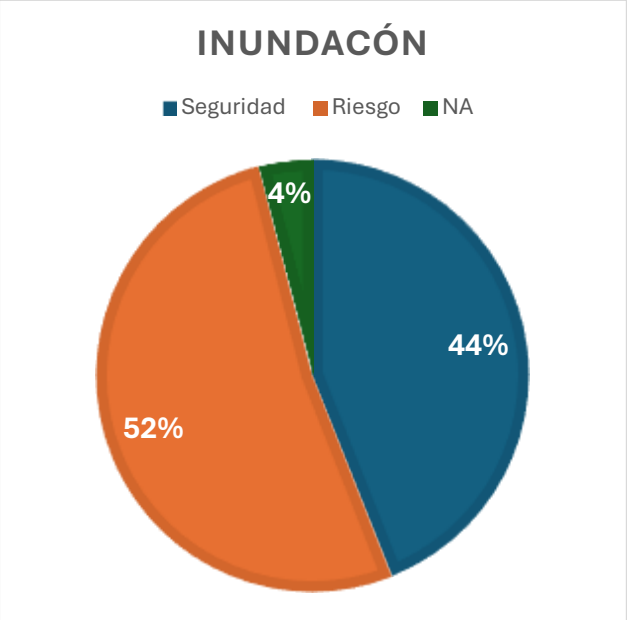
Por lo que resulta necesario mantener y mejorar las medidas de prevención, tales como la señalización, los extintores y los planes de emergencia.

Riesgo de malware:	**Debido a:**
	• No cuenta con antivirus instalado • No se realiza revisión de virus a los equipos • Los estudiantes tienen acceso a las configuraciones avanzadas • No cuenta con control sobre la instalación de programas • No se controla memorias USB • Lentitud y fallas presentes frecuentemente • El responsable no atiende a tiempo los incidentes de virus • No se controla el acceso a página

Interpretación:

Riesgo importante: El riesgo de malware (**Riesgo Muy Grave**) presenta un 60% de riesgo frente a un 36% de seguridad, lo que evidencia un nivel elevado de vulnerabilidad en los sistemas informáticos. Este nivel de riesgo se debe principalmente a la ausencia de antivirus en los equipos, la falta de revisiones periódicas de virus y la inexistencia de controles sobre la instalación de programas. Asimismo, el acceso de los estudiantes a configuraciones avanzadas, la falta de control sobre el uso de memorias USB.

Se requiere la implementación urgente de medidas de seguridad informática, como antivirus, controles de acceso, políticas de uso y monitoreo de sistemas.

Riesgo de inundación:	**Debido a:**
	• Existe filtraciones de agua en techos y paredes • El sistema de drenaje se obstruye frecuentemente • Las puertas no impiden el ingreso de agua • No cuentan con bombas de drenaje • No dispone con sensores de humedad o agua • Las áreas cercanas acumulan agua con facilidad
Interpretación: **Riesgo importante:** El riesgo de inundación (**Riesgo Inundación**) presenta un 52% de riesgo y un 44% de seguridad, lo que indica casi un equilibrio entre factores de vulnerabilidad y medidas de protección. Este nivel de riesgo se debe principalmente a la presencia de filtraciones de agua en techos y paredes, la obstrucción frecuente del sistema de drenaje y la falta de barreras adecuadas en las puertas para impedir el ingreso de agua. Asimismo, la ausencia de bombas de drenaje, sensores de humedad o agua, y la acumulación de agua en áreas cercanas. Este escenario se clasifica como un riesgo a tomar en cuenta, por lo que se recomienda implementar medidas preventivas y correctivas para reducir la probabilidad de ocurrencia.	

5.1.5.1 *Opinión*

La evaluación en el laboratorio reveló un nivel de riesgo preocupante, donde el malware destaca como la vulnerabilidad más alta. Tras considerar las salvaguardas que ya posee el laboratorio, la reducción de los índices fue mínima. Dado que tres de los riesgos siguen siendo preocupantes, se procedió a plantear controles adicionales para fortalecer la seguridad.

RIESGO	Nivel de riesgo
Robo	Importante
Daño de equipo	Importante
Incendio	Apreciable
Malware	Muy grave
Inundación	Importante

Tabla 28. Riesgo auditoría. Elaboración Propia.

5.1.6 Conclusión

- La auditoría demuestra la necesidad urgente de implementar controles técnicos para elevar el nivel de la seguridad informática del laboratorio.
- El riesgo más crítico identificado es el malware, que aun con el análisis inherente permanece en nivel importante incluso después de considerar las salvaguardas existentes. Esto se debe principalmente a la ausencia de un antivirus robusto, falta de control en el uso de dispositivos USB y ausencia de políticas claras.

5.1.7 Recomendaciones

- Se recomienda actualizar la auditoria cada seis meses, ya que las amenazas cambian constantemente y aparecen nuevas, muchas veces por el cambio de equipos, componentes o instalación de nuevos programas generaría más vulnerabilidades.
- Implementar la guía rápida del SGSI que se puede ver en anexo G, que incluye políticas claras de uso del laboratorio, roles y responsabilidades, y el cronograma de mantenimiento preventivo.
- De aplicar los cronogramas de mantenimiento o el de revisión de cableados, lo mismos están dispuestos a tomar cambios en las frecuencias adaptándose a los tiempos del encargado del laboratorio de cómputo.

5.1.8 PLAN DE RECUPERACIÓN

Se creo una guía SGSI ante desastres del laboratorio de la unidad educativa Hortensia Vásquez Salvador, que cuenta con el propósito, objetivo, resumen de los riesgos y salvaguardas a plantear, identificación de escenarios, roles y documentos de respaldo en caso de emergencias.

Unidad Educativa Hortensia Vásquez Salvador	
Guía Rápida del Sistema de Gestión de Seguridad de la Información (SGSI)	
Elaborado por: Wilson Campoverde	
La institución se compromete a proteger la confidencialidad, integridad y disponibilidad de la información y los equipos tecnológicos mediante el cumplimiento de salvaguardas y mejora continua.	
Laboratorio de Computación **Fecha:** Julio 2026	**Versión:** 1.0

Anexo A: Guía SGSI

Propósito y Alcance
Esta guía rápida tiene como objetivo establecer políticas, procedimientos y cronogramas para proteger la confidencialidad, integridad y disponibilidad de los equipos tecnológicos en el laboratorio de cómputo de la Unidad Educativa Hortensia Vásquez Salvador. Es de cumplimiento obligatorio para docentes, estudiantes y otro personal. Todo esto basándose en la auditoria de seguridad informática realizada.

Roles

Rector	Aprobar políticas, asignar presupuesto y supervisar el SGSI
Docente de computación	Ejecutar controles diarios, mantenimientos y capacitaciones
Estudiantes	Cumplir las normas de uso del laboratorio
Personal Administrativo	Reportar incidentes y respetar las políticas

Políticas básicas de seguridad para usuarios

Para mitigar los riesgos de origen humano y cibernético, se establecen las siguientes reglas:

- **Gestión de sesiones:** Todos los usuarios deben iniciar sesión al utilizar los equipos y asegurarse de cerrarla o apagar correctamente la computadora al finalizar la clase, según como lo estipule el docente.
- **Control de dispositivos externos:** Queda estrictamente prohibido conectar memorias USB, discos externos o teléfonos celulares sin permiso del docente encargado y se recomienda hacer un escaneo con el antivirus o antimalware instalado.
- **Restricción de software:** Ningún estudiante está autorizado para instalar programas, juegos, extensiones de navegador o modificar las configuraciones del sistema. Además, está prohibido ingresar a páginas no permitidas.
- **Uso exclusivo:** Los equipos del laboratorio están destinados única y exclusivamente para actividades académicas y de investigación.

Soluciones realistas adaptadas a la institución propuestas ante los riesgos encontrados

Riesgo	Salvaguarda	Precio Estimado	Referencia	Objetivo
Robo	Instalación de cámara IP tplink c240 tipo domo/4mp	47$		Mejorar la seguridad, reducir el riesgo de robos y resguardar equipos
Daño de equipos	Kit con mochila anti desastres	620$		Actuar rápido ante una emergencia.
	Diseño de una guía SGSI	0$	Documento actual	Prevenir accidentes, y tener un documento de respaldo.
Incendio	Extintor de CO2-10 lb TRITON	61.45$		Evitar catástrofes, o disminuir las perdidas.
	Señales adhesivas y letreros de emergencia	65$		Guía de acción ante emergencias

Malware	Instalación de un antimalware, recomendado: Bit defender	0$		Evitar el daño de los equipos por ataques de virus.
	Instalación de antivirus gratuitos. Recomendado: MalwareBytes	0$		Evitar el daño de los equipos por ataques de virus.
Inundación	Silicón sellador 100% silicón de curado acético	6$		Evitar filtraciones con revisiones periódicas
	Canaletas	25$		Para elevar la altura al piso de los cables y protegerlos de daños.

Cronograma de Mantenimiento de Equipos Tecnológicos y Revisión de Cableados			
Con el fin de evitar el deterioro de los equipos y ya que ese riesgo es de nivel importante y demás mitigar los ataques de malware con un nivel de riesgo muy grave, se establece el siguiente cronograma de mantenimiento preventivo:			
Frecuencia	**Actividad de mantenimientos**	**Responsable**	**Documento de Registro**

Mensual	Escaneo completo con antivirus	Docente de computación	Reporte de Antivirus
Mensual	Actualización de drivers	Docente de computación	Registro de Actualizaciones
Mensual	Actualización de Windows y software	Docente de computación	Registro de Actualizaciones
Trimestral	Limpieza interna de polvo (teclados, ventiladores)	Docente de computación	Checklist de Limpieza
Trimestral	Revisión y prueba de protectores de voltaje	Docente de computación	Checklist Eléctrico
Bimestral	Revisión de cableados y conexiones	Docente de computación	Reporte de Cableado
Semestral	Revisión de canaletas y cableado elevado	Docente de computación	Reporte de Infraestructura
Semestral	Mantenimiento general profundo (formateo si es necesario)	Docente de computación	Acta de Mantenimiento
Mensual	Inventario físico de equipos	Docente de computación	Hoja de inventario
Anual	Simulacro de evacuación e incendio	Docente de computación	Acta de simulacros

Protocolo Básico de Respuesta a Incidentes
• **Ante infección de Malware:** 1. Desconectar inmediatamente el cable de red del equipo afectado para evitar la propagación. 2. Notificar al área técnica 3. Ejecutar una limpieza profunda con el antivirus corporativo. 4. Aplicar solución y documentar acciones correctivas. 5. Analizar causa raíz 6. actualizar controles.
1. **Ante daño eléctrico o conato de incendio:** 2. Bajar inmediatamente el interruptor general de energía del laboratorio, 3. Evacuar a los estudiantes ordenadamente 4. Utilizar el extintor de CO2 para equipos electrónicos. 5. Aplicar solución y documentar acciones correctivas. 6. Analizar causa raíz 7. Actualizar controles.
1. **Ante una inundación:** 2. Bajar el interruptor general para dejar sin energía al laboratorio, 3. Precautelar revisar que los cableados no se vean afectador por filtraciones, 4. Revisar que las salidas de agua no estén obstruidas. 5. Aplicar solución y documentar acciones correctivas. 6. Analizar causa raíz 7. Actualizar controles.

1. **Ante un daño de equipo:**
2. Reportar a rectoría el daño
3. Valorar los daños del equipo
4. Cotizar los daños y ver si necesita inversión o solo mantenimiento
5. Aplicar solución y documentar acciones correctivas.
6. Analizar causa raíz
7. Actualizar controles.

1. **Ante robo:**
2. Reportar a rectoría el robo
3. Valorar las pérdidas y estimar el costo de la perdida
4. Llamar a la policía
5. Entregar un reporte de lo sucedido
6. En caso de implementar las cámaras se debe obtener las evidencias y entregarlas
7. documentar acciones correctivas.
8. Analizar causa raíz
9. Actualizar controles.

Kit de recuperación recomendado ante una emergencia
Herramientas que se debe tener a la mano para una acción rápida de el encargado

ítem	**Descripción**	**Cantidad**	**Precio**	**Total**
Mochila	• 40 litros • Impermeable • Color naranja o rojo	1	50$	50$

Extintor	• Co2 • 2.5 lb	1	25$	25$
Kit de emergencia	• Linterna • Botiquín	1	15$	15$
Kit de herramientas de mantenimiento	• Destornilladores • Pinzas • Pulsera antiestática • Guantes • Voltímetro • Pasta térmica • Borrador • Soplador • Tornillos • Quita seguros • RAM • Disco	1	150$	150$
Disco duro externo	• Programas • Llaves de recuperación • Sistemas operativos • Copias de seguridad	1	50$	50$
USB de respaldo de sistema	• Para instalar sistemas operativos • Pasar información	2	10$	20$
Bridas	• Para asegurar mobiliario, cables, dispositivos.	20	0.10$	2$

cinta aislante	• reparar cableados	2	4$	8$
Cables	• reparar cableados • Cable Ethernet Categoría 5 • Cable de cobre	5 metro	3$	30$
Conectores	• JR45	10	20$	200
Periféricos	• Mouse • Teclado • Audífonos • Parlante	1 cada uno	5$	20$
Total				620$

CAPÍTULO VI

6 Conclusiones y recomendaciones

6.1 Conclusiones

Se realizó una auditoría de seguridad informática a los 33 equipos del laboratorio, router, software entre otros, aplicando la metodología MAGERIT. Esta evaluación permitió identificar, analizar, evaluar y tratar los riesgos que afectan la confidencialidad, integridad y disponibilidad de los equipos.

Se analizaron varias fuentes bibliográficas sobre auditoría de seguridad informática, incluyendo el estudio de las normas ISO 27001 y ISO 27002. Seguidamente se analizó la metodología elegida para llevar a cabo este proyecto, sus fases y herramientas de obtención de datos. Con todo esto se estableció un marco teórico sólido que sirvió de base para el desarrollo.

Por otro lado, se diagnosticó el estado actual del laboratorio mediante investigación de campo en conjunto de la observación directa. Además, de apoyarme con instrumentos como encuestas a estudiantes de tercero de bachillerato, entrevista al docente encargado y cuestionarios para la identificación de riesgos basados en MAGERIT. Los resultados de las herramientas aplicadas revelaron un nivel de seguridad preocupante.

Se eligió una metodología adaptada al contexto del laboratorio. En la cual se definieron claramente las fases de la auditoría según MAGERIT, donde sus puntos principales son: planificación, valoración de activos, identificación, análisis, evaluación, tratamiento y monitoreo.

Se propuso un plan de mejora que incluye la elaboración de la guía rápida del sistema de gestión de seguridad de la información, la cual va a contar con planteamiento de nuevas salvaguardas, un cronograma de mantenimiento, un cronograma de revisión de cableados, indicadores KPI y protocolo de respuesta a incidentes. El mismo está vinculado al ciclo PDCA para la mejora continua.

6.2 Recomendaciones

Se recomienda aplicar tiempos de recuperación RPO y RTO por medio de cuestionarios más técnicos. Para tener resultados más cuantificables y poder llevar así un monitoreo mejor, con ello los resultados y los niveles de eficacia se disparan. Además, se podría cambiar la guía rápida SGSI por un plan estructurado anti desastres.

Otro punto importante es tomar en cuenta las posibilidades económicas de la institución y la disponibilidad de tiempo del encargado del laboratorio de cómputo, y adaptar la guía a nuevas frecuencias que se verán en la implementación de las salvaguardas recomendadas en el documento SGSI.

Implementar de manera continua las etapas del ciclo PDCA con el objetivo de evaluar la efectividad del SGSI a largo plazo y no dejarlo estático. Se sugiere realizar reuniones mensuales para examinar el cumplimiento de los KPI establecidos con los reportes y verificar la correcta ejecución de los cronogramas planteados, garantizando salvaguardas actualizadas.

Bibliografía

Aicad Business School. (17 de Julio de 2021). *https://www.aicad.es/*. https://www.aicad.es/: https://www.aicad.es/herramientas-tecnologicas

Alegre, R. M. (2023). *Sistemas Informáticos.* Madrid: Carmen Lara Carmona.

BenQ. (2021). *Trends in digital projection for corporate environments.* enQ Technical Report.

Bernal , C. (2020). *Metodología de la investigación (4.ª ed.).* Pearson Educación.

Bocanegra, L. (2021). *Infraestructura tecnológica y gestión empresarial.* Alfaomega.

Campos , E. M., Campos, M., & López , J. (2022). *Hardware y sistemas operativos.* Madrid: RA-MA.

Carmona , A., & Reyes, L. (2020). *La investigación documental para la comprensión ontológica del objeto de estudio.*

Castro , J., Gómez , L., & Camargo , E. (2023). *La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI.* Tecnura.

Chicano Tejada, E. (2023). *Auditoria de seguridad informatica IFCT0109.* Málaga : IC Editorial.

CISA. (2023). *Guía de estudio para el examen CISA de Auditor Certificado de Sistemas de Información.* Packt Publishing.

Cisco Press. (2021). *Networking fundamentals.* Cisco Press.

Conrado García , B. (2024). *Auditoría de seguridad informática MF0487.* San Millán : Tutor Formación.

Creswell, J., & Creswell, D. (2021). *Diseño de investigación: enfoques cualitativos, cuantitativos y de métodos mixtos.* SAGE Publications.

Epson. (2022). *Advances in document scanning and OCR technology.* Epson Technical Report.

Fuentea, O. (2 de Mayo de 2025). *https://www.iebschool.com/*. https://www.iebschool.com/: https://www.iebschool.com/hub/ventajas-desventajas-tecnologia/

Furht, B., & Escalante, A. (2021). *Handbook of data intensive computing.* Springer.

González, M. (2021). *Gestión de infraestructura tecnológica.* Alfaomega.

Health. (2023). *Definición de equipos tecnológicos.* Universidad Estatal del Sur de Manabí.

Hernández , F., & Klimenko. (2025). *Metodología de la investigación, enfoque cualitativo, cuantitativo y mixto.* Nexus: Multidisciplinary Research Journal.

Hernández, R., & Mendoza, C. (2022). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill Education.

HP Inc. (2023). *Security and management of enterprise printing environments.* HP Whitepaper.

International Organization for Standardization 27002. (2022). *Information security controls.* ISO.

Intriago , J., Quimis , J., Choez , C., & Marcillo, M. (2023). *Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información.*

Iquiquealdia. (20 de Febrero de 2025). *https://iquiquealdia.cl/*. https://iquiquealdia.cl/: https://iquiquealdia.cl/2025/02/20/que-son-los-dispositivos-tecnologicos-y-para-que-sirven/

Laudon, K., & Laudon, J. (2020). *Sistemas de información gerencial (16.ª ed.).* Pearson.

Laudon, K., & Laudon, J. (2021). *Management Information Systems: Managing the Digital Firm (16th ed.).* Pearson.

Laudon, K., & Laudon, J. (2022). *Management Information Systems (17th ed.).* Pearson.

Loor , A., & Espinoza, V. (2014). *Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la ESPAM MFL.*

Marinescu, D. (2023). *Cloud computing: Theory and practice (3rd ed.).* Morgan Kaufmann.

Mata, A. (2024). *Seguridad de Equipos Informaticos* . RA-MA.

Menéndez Arantes , S. C. (2022). *Auditoria de Seguridad Informatica* . RA-MA.

Menéndez Arantes, S. C. (2023). *Auditoría de Seguridad Informática.* Editorial Ra-ma. https://doi.org/https://efaidnbmnnnibpcajpcglclefindmkaj/https://pocketbook.de/de_de/downloadable/download/sample/sample_id/8140464/?srsltid=AfmBOoqzbAegTw2Zl2b6npd2pSrMFixRrmnaj1XP1yzuD5tsFT2sCJbN

Ministerio de Hacienda y Administraciones Públicas. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid, España: Ministerio de Hacienda y Administraciones Públicas. https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=magerit

Montoya , C. (2023). *Reparacion y ampliacion de equipos y componentes hardware microinformáticos* . Málaga: IC Editorial .

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations. U.S.* Department of Commerce.

Oltsik, J. (2021). *The state of data protection and cyber recovery.* Enterprise Strategy Group.

Otero, A. R. (2019). *Information Technology Control and Audit.* Fifth Edition. https://doi.org/https://es.scribd.com/document/899648899/Information-technology-control-and-audit-Fifth-Edition-Otero-download

Paladines, L. (2023). *Auditoría de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre en el periodo 2022.*

Reyes , G. (2018). *Auditoria de seguridad informática en los laboratorios de la Unidad Académica de Ciencias Empresariales de la UTMACH.*

Romero , M., & González, D. (2018). *Diseño de un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes.*

Romero, J. (2022). *Gestión de activos tecnológicos en organizaciones modernas.* Alfaomega.

Rountree, D., & Castrillo, I. (2021). *The Basics of Cloud Computing.* Syngress.

Sandoval, E. (2022). *El trabajo de campo en la investigación social en tiempos de pandemia* . Cuaderno Venezolano de Sociología.

Sekaran, U., & Bougie, R. (2021). *Research methods for business: A skill-building approach (9th ed.).* John Wiley & Sons.

SentinelOne. (7 de Septiembre de 2025). *https://www.sentinelone.com/es*. https://www.sentinelone.com/es: https://www.sentinelone.com/es/cybersecurity-101/cybersecurity/benefits-of-security-audits/

Stallings, W. (2022). *Computer Organization and Architecture (12th ed.).* Pearson.

Tanenbaum, A., & Wetherall, D. (2021). *Computer networks (6th ed.).* Pearson.

Torecilla, J. (15 de Febrero de 2025). *https://www.astraps.com/*. https://www.astraps.com/: https://www.astraps.com/articulo/1389/tipos-de-herramientas-tecnologicas/

Turban, E., Pollard, C., & Wood, G. (2021). *Information Technology for Management: Driving Digital Transformation (12th ed.).* Wiley.

Yanza Chávez, W. G., & Montoya Lunavictoria, J. K. (2022). *Auditoria Informática* . Universidad Nacional de Chimborazo (UNACH).

Zamora , E. (2023). *Metodología de la investigación: Enfoques y aplicaciones.* Editorial Académica.

Zapata, D. (2025). *https://sites.google.com/*. https://sites.google.com/: https://sites.google.com/site/inftecdelia/Inicio/club-de-interes-robotica/ventajas-y-desventajas-aparatos-electronicos

Anexos

Anexo B: Asignación de tutor

Universidad Laica Eloy Alfaro de Manabí

Periodo 2025-2 - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Estimad@
Docente y Estudiante
Uleam

En cumplimiento de lo establecido en la Ley, el Reglamento de Régimen Académico y las disposiciones estatutarias de la Uleam, por medio de la presente se oficializa la dirección y tutoría en el desarrollo del Trabajo de Integración curricular / Trabajo de Titulación del siguiente estudiante:

Tema: AUDITORIA DE SEGURIDAD INFORMATICA A LOS EQUIPOS TECNOLOGICOS DE LA UNIDAD EDUCATIVA HORTENSIA VASQUEZ SALVADOR

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

Tipo de proyecto: Trabajo de Integración Curricular / Trabajo de titulación se articula con proyectos y programas de investigación

Apellidos y nombres del tutor asignado: MINAYA MACIAS RENELMO WLADIMIR

Apellidos y nombres del estudiante: CAMPOVERDE VASQUEZ WILSON ANDRES

Carrera: TECNOLOGIAS DE LA INFORMACION 2022 (EL CARMEN)

Periodo de Inducción: Periodo 2025-2

Sírvase cumplir con lo dispuesto en el Manual de Procedimientos de TITULACION DE ESTUDIANTES DE GRADO: TRABAJO DE INTEGRACION CURRICULAR Y UNIDAD DE TITULACION https://departamentos.uleam.edu.ec/gestion_aseguramiento_calidad/files/2020/06/PAT_04_Titulacion_de_Estudiantes_de_grado_UIC_y_UT.pdf

Particular que se informa para los fines consiguientes.

Atentamente,

Comisión Académica y Responsable de Titulación

Anexo C: Cuestionarios para identificar riesgos y requisitos

CUESTIONARIO PARA IDENTIFICAR RIESGOS			PT1 Página 1 - 5	
PREGUNTAS	SI	NO	OBSERVACIONES	
Robo: R-001				
1. ¿El laboratorio permanece sin supervisión durante el día?	X			0
2. ¿Los equipos cuentan con anclajes de seguridad?		X		0
3. ¿Las puertas tienen cerraduras reforzadas?	X			1
4. ¿El laboratorio cuenta con cámaras de vigilancia?		X		0
5. ¿Las cámaras instaladas funcionan correctamente?		X	NA	2
6. ¿Existe un registro de ingreso y salida de los estudiantes al laboratorio?		X	Docentes que usan el laboratorio	2
7. ¿Personas ajenas a la institución pueden ingresar fácilmente al laboratorio?		X		1
8. ¿El laboratorio cuenta con un responsable asignado permanentemente?		X	Hay pero no es permanente	1
9. ¿Se realizan controles periódicos de inventario de los equipos?	X			1
10. ¿Se realizan mantenimiento preventivo a los equipos?	X			1
11. ¿Las ventanas cuentan con protección?	X			1
12. ¿Los equipos permanecen conectados al terminar la jornada?		X		1
13. ¿El laboratorio se encuentra en una zona segura?	X			1
14. ¿Existe iluminación adecuada en el área del laboratorio?		X		0
15. ¿El personal conoce los protocolos ante un intento de robo?	X			1
16. ¿Hay señalización de seguridad en el laboratorio?		X		0
17. ¿El acceso está restringido mediante horarios definidos?	X			1
18. ¿Se han reportado robos anteriormente?		X		1
19. ¿Se controla el uso de mochilas o bolsos dentro del laboratorio?		X	Entran sin mochila	2
20. ¿Cuentan con alarmas de seguridad?		X		0
21. ¿Los cables periféricos o accesorios están asegurados?		X		0
22. ¿Existe políticas claras sobre el uso y cuidado de los equipos?	X			1
23. ¿Las llaves están bajo resguardo?	X			1
24. ¿Se realiza supervisión al finalizar las clases?	X			1
25. ¿El laboratorio queda sin vigilancia durante los fines de semana o feriados?	X			0
Elaborado por: Campoverde Vásquez Wilson Andrés			**Revisado por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:			**Firma:**	

CUESTIONARIO PARA IDENTIFICAR RIESGOS			PT1 Página 2 - 5	
PREGUNTAS	SI	NO	OBSERVACIONES	
Daño de Equipo: R-002				
1. ¿El laboratorio cuenta con instalaciones eléctricas en buen estado?		X		0
2. ¿Los equipos están protegidos con reguladores de voltaje?	X			1
3. ¿Se presentan con frecuencia cortes de energía?		X		1
4. ¿La ventilación del laboratorio es adecuada?		X		0
5. ¿Las mesas y mobiliario donde se ubican los equipos son seguros?	X			1
6. ¿Los estudiantes reciben instrucciones de cómo usar correctamente el laboratorio?	X			1
7. ¿Existe supervisión durante el uso de los equipos?	X			1
8. ¿Se ha detectado uso inadecuado por los usuarios?	X			0
9. ¿Está prohibido el consumo de alimento y bebida?	X			1
10. ¿Los equipos son apagados correctamente después de su uso?		X	Se encontro equipos encendidos	0
11. ¿El laboratorio cuenta con un plan de mantenimiento preventivo?	X			1
12. ¿Se realiza limpieza periódica de los equipos?	X			1
13. ¿Los equipos presentan fallas técnicas de manera recurrente?		X		1
14. ¿Se lleva un registro de daños de los equipos?		X		0
15. ¿Existe personal responsable del mantenimiento del laboratorio?		X		0
16. ¿Se revisa el estado de los equipos antes de las clases?	X			1
17. ¿Se han presentado daños por mal uso?	X			0
18. ¿Están protegidos contra polvo o humedad?		X		0
19. ¿Se ha producido daño por sobrecalentamiento?		X		0
20. ¿Se ha presentado daños periféricos por mal uso?	X			0
21. ¿Se ha presentado daños por falta de capacitación a usuarios?	X			0
22. ¿Se realizan apagones forzados a los equipos?	X			0
23. ¿Los equipos presentan señales de desgaste físico?	X			0
24. ¿Se han presentado daños por manipulación incorrecta de cables o puertos?	X			0
25. ¿Se han producido fallas por instalación de software no autorizado?		X		1
Elaborado por: Campoverde Vásquez Wilson Andrés **Fecha:**			**Revisado por:** Ing. Minaya Macias Wladimir Renelmo **Firma:**	

CUESTIONARIO PARA IDENTIFICAR RIESGOS			PT1 Página 3 - 5	
PREGUNTAS	SI	NO	OBSERVACIONES	
Incendio: R-003				
1. ¿El laboratorio cuenta con extintores operativos?		X		0
2. ¿Los extintores son del tipo adecuado para incendios eléctricos?		X	NA	2
3. ¿Los extintores se encuentran dentro de la fecha vigente?		X		2
4. ¿Existe señalización visible de rutas de evacuación dentro del laboratorio?		X		0
5. ¿Las salidas de emergencia están libres de obstáculos?	X			1
6. ¿El laboratorio cuenta con interruptor general de energía eléctrica?	X			1
7. ¿Las instalaciones eléctricas han sido revisadas técnicamente?	X			1
8. ¿Se evita el uso excesivo de extensiones eléctricas?	X			1
9. ¿Los cables eléctricos están en buen estado?		X		0
10. ¿Los tomacorrientes presentan sobrecargas?		X		0
11. ¿Los equipos cuentan con ventilación adecuada?	X			1
12. ¿El laboratorio está libre de materiales inflamables?		X		0
13. ¿Está prohibido el uso de fuego o llamas?	X			1
14. ¿Existe un plan de emergencia contra incendios?		X		0
15. ¿El personal conoce el procedimiento ante un incendio?	X			1
16. ¿Los estudiantes reciben indicaciones de seguridad?	X			1
17. ¿Se realizan simulacros de evacuación?	X			1
18. ¿Existen detectores de humo operativos?	X			1
19. ¿Los equipos se apagan al finalizar la jornada?	X			1
20. ¿Está prohibido beber o comer dentro del laboratorio?	X			1
21. ¿Se controla el uso de equipos eléctricos no autorizados?	X			1
22. ¿Existe iluminación de emergencia?		X		0
23. ¿Hay ventilación para la salida de humo?	X			1
24. ¿El laboratorio cumple con normas internas de seguridad?	X			1
25. ¿Se registra el mantenimiento eléctrico y de equipos?	X			1

Elaborado por:
Campoverde Vásquez Wilson Andrés

Revisado por:
Ing. Minaya Macias Wladimir Renelmo

Fecha:

Firma:

CUESTIONARIO PARA IDENTIFICAR RIESGOS			PT1 Página 4 - 5	
PREGUNTAS	SI	NO	OBSERVACIONES	
Malware: R-004				
1. ¿Los equipos del laboratorio cuentan con un antivirus instalado y en funcionamiento?		X		0
2. ¿El antivirus instalado en los equipos se mantiene actualizado de forma regular?		X		2
3. ¿Se realiza una revisión de virus en los equipos del laboratorio de manera periódica por el responsable?		X		0
4. ¿Los estudiantes tienen restringido el acceso a configuraciones avanzadas del sistema operativo?		X		0
5. ¿La instalación de programas está controlada?		X		0
6. ¿Se controlan memorias USB?		X		0
7. ¿Los USB se escanean?		X		0
8. ¿Se permite la instalación de juegos u otro software?	X			0
9. ¿Se autoriza el uso de memorias USB personales de los estudiantes en los equipos?	X			0
10. ¿Se han registrado casos de virus o malware en los equipos del laboratorio?		X		1
11. ¿los equipos presentan lentitud o fallas frecuentes?	X		Algunos	0
12. ¿Se han observado ventanas emergentes o mensajes sospechosos durante el uso de los equipos?		X		1
13. ¿Los sistemas operativos de los equipos cuentan con actualizaciones de seguridad vigentes?		X		0
14. ¿Los programas instalados en los equipos son originales o cuentan con licencias educativas?	X			1
15. ¿Se realiza mantenimiento preventivo a los equipos para evitar problemas de malware?	X			1
16. ¿La institución cuenta con un responsable asignado para el laboratorio de computación?	X			1
17. ¿El responsable del laboratorio atiende oportunamente los incidentes relacionados con virus?		X	no, depende del responsable	0
18. ¿Se formatea el equipo cuando hay infección?	X			1
19. ¿Los equipos del laboratorio se restauran periódicamente a un estado limpio o inicial?	X		solo cuando presenta problemas	1
20. ¿Se controla el acceso a páginas web no relacionadas con actividades educativas?		X		0
21. ¿Los equipos del laboratorio se revisan después de ser utilizados para detectar problemas o virus?	X			1
22. ¿Se aplican normas claras sobre el uso correcto de los equipos del laboratorio?	X			1
23. ¿Los equipos se apagan correctamente?		X		0
24. ¿Los docentes reciben capacitación básica sobre riesgos de virus informáticos?		X		0
25. ¿Se recibe orientación sobre los riesgos del malware?		X		0

Elaborado por:
Campoverde Vásquez Wilson Andrés
Fecha:

Revisado por:
Ing. Minaya Macias Wladimir Renelmo
Firma:

CUESTIONARIO PARA IDENTIFICAR RIESGOS			PT1 Página 5 - 5	
PREGUNTAS	SI	NO	OBSERVACIONES	
Inundación: R-005				
1. ¿El laboratorio está ubicado en planta baja o en un nivel propenso a inundación?		X		1
2. ¿La Institución se encuentra en una zona con antecedentes de inundaciones?		X		1
3. ¿Existen filtraciones de agua en techo o paredes?	X			0
4. ¿El sistema de drenaje del edificio presenta obstrucciones frecuentes?	X			0
5. ¿Se realiza mantenimiento a los desagües?	X			1
6. ¿Las ventanas cuentan con sellos impermeables?	X			1
7. ¿Las puertas impiden el ingreso de agua en caso de lluvias fuertes?		X		0
8. ¿Cuenta de un sistema de evacuación de aguas pluviales?	X			1
9. ¿Los equipos de computación están colocados directamente sobre el piso?		X		1
10. ¿Los cables se encuentran a nivel del suelo?		X		1
11. ¿Existen protecciones para equipos ante derrames o filtraciones?		X		0
12. ¿Cuenta con bombas de drenaje o sistemas de emergencia?		X		0
13. ¿Se han presentado inundaciones previas?	X		En el laboratorio NO.	2
14. ¿Hay plan de emergencia ante inundación?	X			1
15. ¿El personal está capacitado para actuar en caso de inundación?	X			1
16. ¿Existe señalización de rutas de evacuación por riesgo de inundación?		X		0
17. ¿Los tomacorrientes están en una altura segura?	X			1
18. ¿El sistema eléctrico cuenta con protección contra la humedad?		X		0
19. ¿Se examina el estado del techo antes de la temporada de lluvias?	X			1
20. ¿Dispone de sensores de humedad o agua?		X		0
21. ¿Los equipos están protegidos contra el agua?		X		0
22. ¿Existe un seguro institucional que cubra daños por inundación?		X		0
23. ¿Las áreas cercanas acumulan agua con facilidad?	X			0
24. ¿Se realizan simulacros por inundación?	X			1
25. ¿Cuenta con procedimientos de desconexión eléctrica ante inundaciones?		X		0
Elaborado por: Campoverde Vásquez Wilson Andrés **Fecha:**			**Revisado por:** Ing. Minaya Macias Wladimir Renelmo **Firma:**	

Anexo D: Fotografías de la institución

Anexo E Fotografía del laboratorio

Anexo F Evidencia de entrevista

Anexo G: Evidencia de encuesta

Anexo H. Formato de entrevista

INSTRUMENTO DE RECOLECCIÓN DE DATOS

ENTREVISTA

La presente entrevista tiene como objetivo recopilar información sobre las prácticas, políticas y procedimientos relacionados con la seguridad informática en el laboratorio de computación. A través de las respuestas del personal responsable, se busca identificar las fortalezas, debilidades y riesgos existentes en la gestión de los equipos tecnológicos, con el fin de obtener información relevante que contribuya al desarrollo de la auditoría informática y a la formulación de propuestas de mejora.

Autor del proyecto integrador: Wilson Andrés Campoverde Vásquez

1 ¿Qué políticas o normas de seguridad informática existen en el laboratorio de computación y por qué se implementaron esas medidas?

_____

_____

2 ¿Cómo se gestiona el acceso de estudiantes y docentes a los equipos del laboratorio y qué criterios se utilizan para autorizar o restringir dicho acceso?

_____

_____

3 ¿Qué mecanismos se utilizan para prevenir virus, malware u otras amenazas informáticas en los equipos del laboratorio y por qué se eligieron esas herramientas o métodos?

_____

_____

4 ¿Cómo se controla la instalación de software y la modificación de configuraciones en los equipos del laboratorio, y cuáles son las principales dificultades para mantener ese control?

5 ¿Con qué frecuencia se realizan mantenimientos y actualizaciones de hardware y software, y qué impacto considera que tiene esto en la seguridad informática del laboratorio?

6 cuando ocurre un incidente de seguridad (virus, pérdida de información, uso indebido de equipos), ¿qué procedimientos se siguen y por qué se actúa de esa manera?

7 desde su experiencia, ¿cuáles son los principales riesgos de seguridad informática en el laboratorio y qué mejoras considera prioritarias para reducirlos? Explique por qué.

Anexo I: Formato de la encuesta

INSTRUMENTO DE RECOLECCIÓN DE DATOS

ENCUESTA

Esta encuesta tiene como objetivo conocer la opinión y experiencia de los estudiantes respecto al uso, funcionamiento y condiciones del laboratorio de computación, con el fin de identificar necesidades y oportunidades de mejora.

1. ¿Inicias sesion en los equipos del laboratorio usando un usuario o contraseña?

Nunca

Rara vez

A veces

Casi siempre

Siempre

2. ¿Cierras sesion o apagas correctamente el equipo al terminar de usarlo?

Nunca

Rara vez

A veces

Casi siempre

Siempre

3. ¿Instala usted programas o aplicaciones si autorizacion en los equipos de laboratorio?

Nunca

Rara vez

A veces

Casi siempre

Siempre

4. ¿Conecta usted USB u otros dispositivos externos a los equipos del laboratoio?

Nunca

Rara vez

A veces

Casi siempre

Siempre

5. ¿Ha detectado virus, archivos sospechosos o mensaje extraños en los equipos?

Nunca

Rara vez

A veces

Casi siempre

Siempre

6. ¿Comparte archivos entre equipos del laboratorio sin revisar si son seguros?

Nunca

Rara vez

A veces

Casi siempre

Siempre

7. ¿Modifica configuraciones del sistema (red, usuarios, permisos sin autorizacion)?

Nunca

Rara vez

A veces

Casi siempre

Siempre

8. ¿Recibe usted indicasiones de los docntes o responsable sobre uso seguro de los equipos?

Nunca

Rara vez

A veces

Casi siempre

Siempre

9. ¿Has notado que otros estudiantes utilizan los equipos para actividades no academicas?

Nunca

Rara vez

A veces

Casi siempre

Siempre

10. ¿Consideras que los equipos del laboratorio están protegidos contra amenazas informaticas?

Nunca

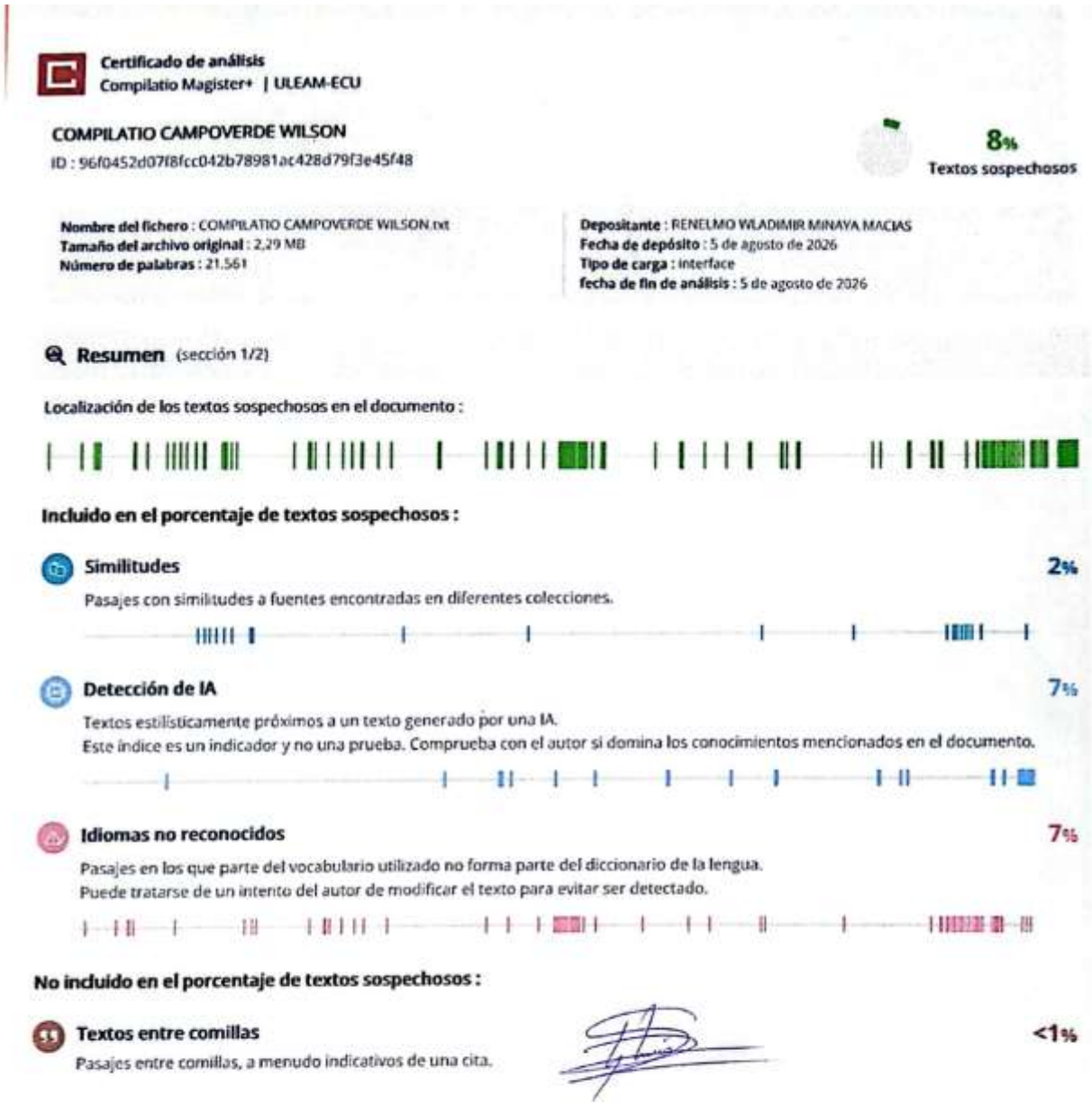
Rara vez

A veces

Casi siempre

Siempre

Anexo J: Certificado de coincidencia académica (emitido por tutor del sistema anti-plagio)



Certificado de análisis
Compilatio Magister+ | ULEAM-ECU

COMPILATIO CAMPOVERDE WILSON
ID : 96f0452d07f8fcc042b78981ac428d79f3e45f48

8%
Textos sospechosos

Nombre del fichero : COMPILATIO CAMPOVERDE WILSON.txt
Tamaño del archivo original : 2,29 MB
Número de palabras : 21.561

Depositante : RENELMO WLADIMIR MINAYA MACIAS
Fecha de depósito : 5 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 5 de agosto de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes **2%**
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 **7%**
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.

Glosario

Activo: todo recurso que tiene valor para la institución y que debe protegerse, ya sea un equipo, un programa o la información que se maneja en él.

Amenaza: cualquier evento que puede aprovechar una debilidad y causar daño a un activo.

Antivirus: programa encargado de detectar, bloquear y eliminar software malicioso antes de que afecte al equipo o a la información.

Auditoría de seguridad informática: revisión ordenada y documentada del estado de los equipos, los programas y los procesos, con el fin de detectar vulnerabilidades, medir riesgos y proponer mejoras.

Confidencialidad: garantía de que la información solo puede ser consultada por las personas autorizadas.

Disponibilidad: garantía de que la información y los equipos estén accesibles y funcionando cuando se los necesita.

Hallazgo: situación detectada durante la auditoría que evidencia una debilidad, un incumplimiento o una oportunidad de mejora.

Impacto: nivel de daño que sufriría la institución si una amenaza llegara a materializarse.

Integridad: garantía de que la información se mantiene completa y sin modificaciones no autorizadas.

ISO/IEC 27001 e ISO/IEC 27002: normas internacionales de seguridad de la información; la primera establece los requisitos para implementar un SGSI y la segunda reúne las buenas prácticas y los controles recomendados.

KPI (Indicador Clave de Desempeño): medida que permite verificar si un control o una actividad de seguridad está dando los resultados esperados.

MAGERIT: metodología de análisis y gestión de riesgos de los sistemas de información que ordena el trabajo en fases: alcance, gestión de activos, identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.

Malware: software creado con fines dañinos, como virus, gusanos o troyanos, que busca alterar, robar o bloquear la información.

Mantenimiento preventivo: revisión y limpieza programada de los equipos para evitar que las fallas ocurran.

Nivel de riesgo: clasificación que se asigna a un riesgo según su valor calculado; en este proyecto se usaron las categorías apreciable, importante y muy grave.

PDCA (Planificar, Hacer, Verificar, Actuar): ciclo de mejora continua que permite revisar y ajustar de forma periódica las medidas de seguridad implementadas.

Probabilidad: posibilidad de que una amenaza llegue a ocurrir en un periodo determinado.

Riesgo: combinación de la probabilidad de que ocurra una amenaza y del impacto que causaría sobre el activo.

Salvaguarda: medida, control o procedimiento que se aplica para reducir la probabilidad o el impacto de un riesgo.

SGSI (Sistema de Gestión de Seguridad de la Información): conjunto de políticas, roles, procedimientos y controles que permiten gestionar la seguridad de la información de manera organizada y continua.

Vulnerabilidad: debilidad de un equipo, programa o procedimiento que puede ser aprovechada por una amenaza.