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 INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

## TEMA

Auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor

## AUTOR

Vélez Vélez Carolina Ibeth

## TUTOR

Minaya Macías Renelmo Wladimir

**El Carmen, Enero 2025**

# CERTIFICACIÓN

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

Haber dirigido y revisado el trabajo de investigación, bajo la autoría de la estudiante **VÉLEZ VÉLEZ CAROLINA IBETH**, legalmente matriculada en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(1)-2024(2), cumpliendo el total de 384 horas, bajo la opción de titulación de proyecto integrador, cuyo tema del proyecto es "Auditoría de Seguridad Informática a la Infraestructura Tecnológica de la Unidad Educativa Rumiñahui de la parroquia Wilfrido Loor".

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, 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, 20 de Diciembre del 2024.

Lo certifico,

Wladimir Minaya Macías, Mg.
**Docente Tutor**
**Área: Sistemas**

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

**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:**

Auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor.

**Modalidad:**

Proyector Integrador

**Autor:**

Carolina Ibeth Vélez Vélez.

**Tutor:**

Ing. Renelmo Wladimir Minaya Macías.

**Tribunal de Sustentación:**

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

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

- **Miembro:** Ing. Arturo Patricio Quiroz Valencia, Mg.

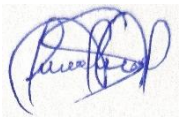
**Fecha de Sustentación:**

Jueves 23/01/2025

# DECLARACION DE AUTORÌA

UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ
EXTENSIÓN EN EL CARMEN

La responsabilidad del contenido de este Trabajo de titulación, con el tema: Auditoria de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor, corresponde exclusivamente a: Vélez Vélez Carolina Ibeth con cédula de ciudadanía No. 2300440951, y los derechos patrimoniales de la misma corresponden a la Universidad Laica “Eloy Alfaro” de Manabí.



Vélez Vélez Carolina Ibeth
C.C. 2300440951

## Dedicatoria

Para mis amados padres, mi pareja, a Diosito, la Virgen de Guadalupe, y el Divino Niño.

En este sendero de la vida, han sido mis faros, iluminando cada paso con amor y sabiduría. A través de sus enseñanzas y ejemplo, he encontrado fortaleza, comprensión y guía.

A ustedes, mis queridos padres y pareja, les dedico estas palabras con gratitud infinita. Su sacrificio, amor incondicional y apoyo constante son el cimiento sobre el cual construyo mis sueños y aspiraciones. En cada logro, veo reflejado su amor y dedicación, y en cada desafío, encuentro consuelo en su abrazo seguro.

Y a Diosito, la Virgen de Guadalupe, y el Divino Niño misericordioso, les elevo mi más profundo agradecimiento. En su infinita bondad, han tejido los hilos de mi existencia, guiándome con tu luz en los momentos de oscuridad y brindándome fuerzas cuando la carga parecía abrumadora. En cada paso de este viaje, siento su presencia amorosa, recordándome que nunca estoy sola.

Que estas palabras sirvan como tributo a la bendición que son en mi vida. Que el amor y la gracia de Dios continúen iluminando nuestro camino, y que la unión familiar siga siendo nuestro mayor tesoro.

Con amor y gratitud eterna,

Vélez Vélez Carolina Ibeth

## Agradecimiento

A mis queridos familiares, mi pareja y estimados docentes,

En el tapiz de mi vida, ustedes son los hilos que han tejido una red de apoyo, conocimiento y amor incondicional. A través de sus palabras alentadoras, gestos amables y dedicación incansable, han moldeado mi camino y han sido faros en mi travesía educativa.

A mi familia y pareja les agradezco por ser mi refugio en los momentos de adversidad y por celebrar conmigo cada logro y éxito. Su amor incondicional y constante apoyo han sido mi roca, brindándome fuerza y aliento en cada paso del camino.

A mis respetados docentes, les estoy profundamente agradecido por su dedicación, pasión y compromiso con mi aprendizaje. Han compartido su conocimiento con generosidad, han inspirado mi curiosidad y han sido guías sabios en mi búsqueda de conocimiento. Cada lección impartida, cada consejo ofrecido, ha dejado una huella indeleble en mi corazón y en mi mente.

En este momento de gratitud, les envío mis más sinceros agradecimientos por ser parte de mi viaje. Que sus enseñanzas y su afecto continúen inspirando y guiando mi camino hacia un futuro lleno de éxitos y realizaciones.

Con profunda apreciación,

Vélez Vélez Carolina Ibeth

## Índice General

## Índice de Tablas

**Índice de Ilustración**

# Resumen

El tema de la presente investigación fue “Auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor” y su objetivo es desarrollar una auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor. Se realizó la presentación del tema con su ubicación y la contextualización de la problemática junto con el objetivo general y los específicos, de igual manera se pudo conocer antecedentes históricos de investigaciones parecidas y se detalló el marco teórico con autores relevantes, así mismo se hizo una investigación bajo el enfoque cuanti-cualitativo con un tipo de investigación bbibliográfica, de campo y aplicada, los métodos fueron analítico-sintético y deductivo-inductivo, a la cual se hizo participar a una población perteneciente a la unidad educativa de los cuales nos pudieron dar datos. Las técnicas para la recolección de datos fueron la encuesta, entrevista y observación de campo. La auditoría se basó en la metodología MAGERIT, como conclusión, la auditoría de seguridad informática permitió identificar vulnerabilidades como falta de actualización de software, inseguridad en la red inalámbrica, falta de políticas de seguridad, entre otras. En la última parte se evidencia los resultados que es la conclusiones y recomendaciones, de estas recomendaciones se pudo proponer una guía de estudio que servirá para poder hacer que se mejoren ciertos procesos con respecto a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui”.



**Palabras claves:** Auditoria de seguridad informática, infraestructura tecnológica, equipos informáticos, seguridad informática.

## Summary

The topic of this research was “Computer security audit of the technological infrastructure of the “Rumiñahui” Educational Unit of the Wilfrido Loor parish” and its objective is to develop a computer security audit of the technological infrastructure of the “Rumiñahui” Educational Unit. from the Wilfrido Loor parish. The presentation of the topic was carried out with its location and the contextualization of the problem along with the general and specific objectives, in the same way it was possible to know historical background of similar investigations and the theoretical framework was detailed with relevant authors, likewise a research under the quantitative-qualitative approach with a type of bibliographic, field and applied research, the methods were analytical-synthetic and deductive-inductive, in which a population belonging to the educational unit participated, from which they could give us data. The techniques for data collection were survey, interview and field observation. The audit was based on the MAGERIT methodology; in conclusion, the computer security audit allowed us to identify vulnerabilities such as lack of software update, insecurity in the wireless network, lack of security policies, among others. In the last part, the results are evident, which are the conclusions and recommendations. From these recommendations, a study guide could be proposed that will serve to improve certain processes with respect to the technological infrastructure of the “Rumiñahui” Educational Unit.



**Keywords:** Computer security audit, technological infrastructure, computer equipment, computer security.

# CAPITULO I

## 1.1. Introducción.

Controlar el uso de infraestructura tecnológica a nivel mundial es crucial para salvaguardar la privacidad, seguridad y equidad. Con regulaciones efectivas, se promueve la innovación responsable, se previenen abusos y se garantiza un acceso justo, fortaleciendo así la base de una sociedad digital sostenible y justa.

La auditoría de seguridad informática es un proceso vital que evalúa la integridad, confidencialidad y disponibilidad de los sistemas y datos de una organización. Identifica vulnerabilidades, garantiza el cumplimiento normativo y recomienda medidas correctivas para proteger contra amenazas cibernéticas y asegurar la continuidad del negocio o institución.

En este contexto en América Latina como en Ecuador, los procesos de auditoría de seguridad informática en instituciones educativas son esenciales para salvaguardar datos sensibles de estudiantes y personal, evaluar la efectividad de los controles de seguridad, garantizar el cumplimiento normativo y prevenir incidentes cibernéticos que puedan afectar el proceso educativo y la reputación de la institución.

En este orden de ideas, la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor, al ser una unidad educativa, requiere llevar el control de su infraestructura tecnológica, es por ello, que se planteó como objetivo general, desarrollar auditoria de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor, y los objetivos específicos: fundamentar teóricamente sobre auditoria de seguridad informática e infraestructura tecnológica, realizar un estudio de campo sobre la infraestructura tecnológica existente en la Unidad Educativa “Rumiñahui”, evaluar controles de seguridad en los laboratorios de informática de la Unidad Educativa “Rumiñahui” aplicando la metodología MAGERIT y por último presentar un plan de auditoría de seguridad informática de la infraestructura tecnológica en la Unidad Educativa “Rumiñahui”.

En este contexto el desarrollo de la auditoria de seguridad informática estuvo conformada por los siguientes capítulos. En el capítulo 1 se realizó un análisis general

sobre la institución y la importancia de desarrollar una auditoria de seguridad informática, en el capítulo II se realizó una fundamentación teórica sobre lo que es auditoria de seguridad informática e infraestructura tecnológica, en el capítulo III, se obtuvo información sobre la realidad de la infraestructura tecnológica de la institución, en el capítulo IV se realizó el proceso de auditoría de seguridad informática con los datos obtenidos en el capítulo III, en el capítulo V, se hizo una evaluación de resultados y se planteó alternativas en la auditoria de seguridad informática, por último en el capítulo VI se plantearon las conclusiones y recomendaciones de la auditoría realizada.

Ahora bien, dentro de esta perspectiva, la auditoría de seguridad informática en la Unidad Educativa "Rumiñahui" es crucial para proteger datos sensibles de estudiantes y personal, prevenir ataques cibernéticos, garantizar la continuidad del servicio educativo, cumplir con regulaciones legales y promover mejoras continuas en la seguridad tecnológica. Este proceso asegura la integridad y confidencialidad de la información en un entorno educativo cada vez más digitalizado.

## 1.2. Presentación del tema.

La evaluación de riesgos está presente en la auditoria de seguridad informática, este proceso implica identificar, analizar y evaluar los riesgos potenciales para la seguridad de la información en un sistema informático. La auditoría de seguridad informática debe incluir una evaluación exhaustiva de los riesgos para determinar las posibles vulnerabilidades y amenazas a la seguridad de los datos y de la infraestructura tecnológica. Esta evaluación ayuda a priorizar las medidas de seguridad y a desarrollar estrategias efectivas para mitigar los riesgos identificados.

Esto se corrobora por lo manifestado por Montalbán et al. (2020) al decir: La evaluación de riesgos en tecnología de la información es crucial para identificar y mitigar posibles amenazas a la seguridad de datos, garantizando la integridad, confidencialidad y disponibilidad de la información. Ayuda a priorizar recursos y estrategias para proteger sistemas y salvaguardar la continuidad del negocio.

En este contexto es evidente desarrollar auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido

Loor.

### 1.3. Ubicación y contextualización de la problemática.

La parroquia Wilfrido Loor Moreira, conocida como “Maicito”, pertenece al cantón El Carmen, provincia de Manabí, sus bellos paisajes y el carisma de la gente hacen que propios y extraños se enamoren de este bello lugar de la patria. El crecimiento de la población en los últimos años ha sido exponencial, dando lugar a la construcción de nuevas infraestructuras y llegada de nuevos habitantes.

El Ministerio de Educación de Ecuador (MINEDUC), creo la Unidad Educativa “Rumiñahui” en el año 1959, cuenta con varios niveles de educación, entre ellos: inicial, básica elemental, básica media, básica superior y bachillerato con la especialidad ciencias generales. actualmente cuenta con 625 estudiantes, 27 docentes y el departamento del DECE. Fuente Ing. Manuel Solorzano, actual rector de la institución. Siendo las cosas así, entre las políticas públicas del MINEDUC, está la implementación de infraestructura tecnológica.

En este contexto las unidades educativas, a través de las autoridades de turno, deben velar por el cuidado de la infraestructura tecnológica, ya que es esencial para garantizar su rendimiento y seguridad. Incluye mantenimiento regular, actualizaciones de software y hardware, copias de seguridad frecuentes y medidas de seguridad cibernética para proteger contra amenazas externas, asegurando la continuidad y eficiencia operativa.

La Unidad Educativa “Rumiñahui” actualmente cuenta con dos laboratorios que se encuentran ubicados en el mismo espacio físico con un número de 40 computadoras. Los dos laboratorios se diferencias por la tecnología que permite el funcionamiento de los equipos, y características de estos.

Actualmente, la Unidad Educativa “Rumiñahui” no cuenta con políticas, manuales, ni normas de uso y cuidado de los laboratorios. Esto ocasiona que los equipos e infraestructura tecnológica se vaya destruyendo cada vez más y más. A esto se suma,

que no existe un técnico responsable de los laboratorios, ni una persona encargada de toda la infraestructura tecnológica de la institución.

Cuando se requiere de algún soporte técnico, las autoridades de turno deben acudir al Distrito de Educación 13D05, y solicitar el apoyo requerido, siendo en algunos casos, imposible contar con este respaldo de manera inmediata, dando lugar al deterioro de los equipos informáticos e infraestructura tecnológica.

Con estos antecedentes la presente investigación toma importancia para efectuar la Auditoria de seguridad informática a la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor Moreira.

## 1.4. Planteamiento del problema.

### 1.4.1. Problematización.

La auditoría de seguridad informática a nivel mundial es crucial para identificar vulnerabilidades y fortalecer la infraestructura tecnológica. Ayuda a prevenir ataques cibernéticos, proteger datos sensibles y garantizar el cumplimiento de regulaciones. Mejora la confianza en los sistemas, promueve la innovación segura y reduce los riesgos de ciberdelincuencia a escala global.

En este orden de ideas, Moya (2023) señala: La auditoría de seguridad informática es fundamental para evaluar y fortalecer la protección de los sistemas de información contra amenazas cibernéticas. Ayuda a identificar vulnerabilidades, garantizar el cumplimiento de regulaciones y salvaguardar la integridad, confidencialidad y disponibilidad de los datos.

La auditoría de seguridad informática es vital en América Latina y Ecuador para proteger la infraestructura digital contra amenazas cibernéticas en constante evolución. Ayuda a mitigar riesgos, cumplir con regulaciones y fortalecer la confianza en los sistemas, crucial para el desarrollo económico y la protección de datos sensibles en la región.

Con estos antecedentes cabe mencionar a Macias et al. (2023) al manifestar: La implementación de auditorías de seguridad informática es esencial para evaluar y fortalecer la protección de sistemas digitales. Identifica vulnerabilidades, garantiza el cumplimiento normativo y protege datos sensibles, asegurando la confianza en los sistemas y la continuidad operativa.

En este contexto, en El Carmen, provincia de Manabí, parroquia Wilfrido Loor, en la Unidad Educativa "Rumiñahui" es necesario desarrollar una auditoria de seguridad informática a la infraestructura tecnológica, para establecer políticas, manuales y normas para el uso y control de los laboratorios de informática.

### 1.4.2. Génesis del problema.

En la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor, al contar con dos laboratorios de computadoras, con un total de 40 computadoras, y no tener un técnico responsable, los equipos de computación como el resto de la infraestructura tecnológica se están deteriorando. Es por ello que surge la necesidad de desarrollar una auditoria de seguridad informática a la infraestructura tecnológica.

En este marco general, la falta de una auditoría de seguridad en la infraestructura tecnológica de una unidad educativa puede exponerla a riesgos significativos. Esto incluye posibles brechas de seguridad que podrían resultar en la pérdida o compromiso de datos confidenciales de estudiantes y personal, interrupciones en el funcionamiento de sistemas clave, y vulnerabilidades que podrían ser explotadas por ciberatacantes, poniendo en peligro la integridad y confidencialidad de la información, así como la reputación de la institución.

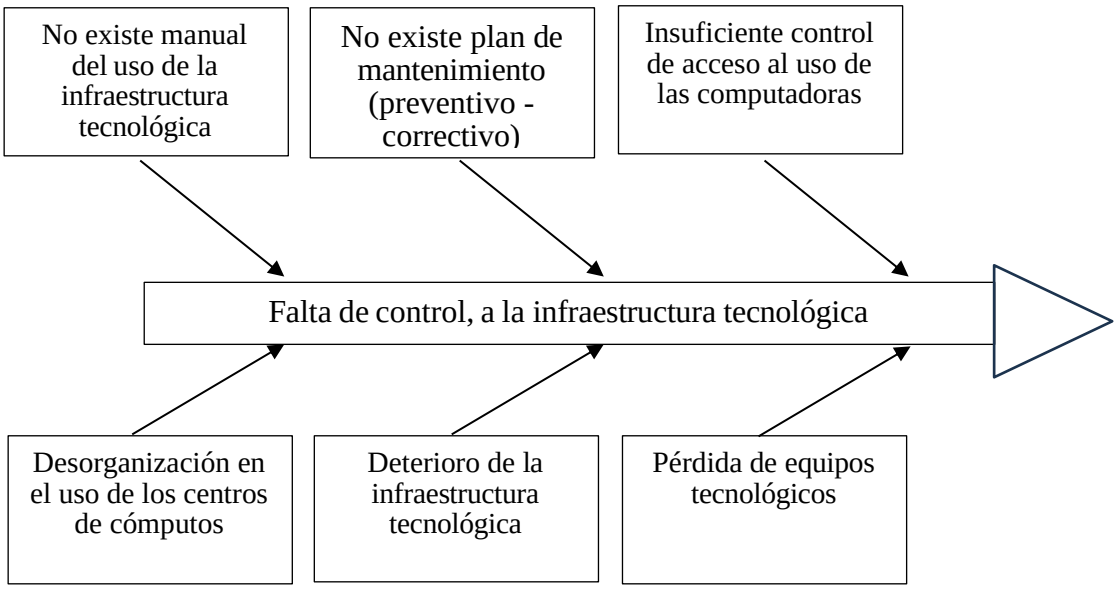
### 1.4.3. Estado actual del problema.

Al no contar con un técnico responsable, para que dé servicio de mantenimiento preventivo y correctivo, ni soporte a los usuarios y docentes que hacen uso de los laboratorios ni infraestructura tecnológica, de la Unidad Educativa "Rumiñahui", se corre

alto riesgo de que estos equipos se dañen, la información y datos de estudiantes, docentes y autoridades estén en peligro de caer en manos de ciberdelincuentes. Es por ello y siguiendo este orden de ideas, es acertado crear una auditoría de seguridad informática de la infraestructura tecnológica en la Unidad Educativa “Rumiñahui”.

## 1.5. Diagrama causa – efecto del problema.

Ilustración 1: Diagrama causa – efecto




Fuente: Carolina Vélez (2024)

## 1.6. Objetivos.

### 1.6.1. Objetivo general.

Desarrollar una auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor.

### 1.6.2. Objetivos específicos.

- Fundamentar teóricamente sobre auditoria de seguridad informática e infraestructura tecnológica.
- Realizar un estudio de campo sobre la infraestructura tecnológica existente en la Unidad Educativa "Rumiñahui"
- Presentar un plan de auditoría de seguridad informática de la infraestructura tecnológica en la Unidad Educativa "Rumiñahui"
- Evaluar controles de seguridad en los laboratorios de informática de la Unidad Educativa "Rumiñahui" aplicando la metodología MAGERIT.
- Construir una guía o manual de uso de centros de cómputo en la UE Rumiñahui, contribuyendo a la seguridad informática de los mismos.

## 1.7. Justificación.

Desarrollar una auditoría de seguridad informática en la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" es esencial para salvaguardar la integridad y confidencialidad de los datos sensibles de estudiantes, profesores y personal administrativo. La creciente dependencia de la tecnología en el entorno educativo ha aumentado la exposición a amenazas cibernéticas, como el robo de información personal, el malware y los ataques de ransomware. Por lo tanto, es imperativo evaluar regularmente la seguridad de los sistemas de información para identificar y mitigar posibles vulnerabilidades que podrían comprometer la privacidad y seguridad de los datos.

Además, una auditoría de seguridad informática proporciona una oportunidad para

evaluar el nivel de preparación de la unidad educativa ante posibles incidentes de seguridad cibernética. Al examinar los protocolos de respuesta ante emergencias, las políticas de gestión de contraseñas y las medidas de protección de la red, se pueden identificar áreas de mejora y fortalecer las defensas contra posibles ataques. Esta evaluación proactiva no solo reduce el riesgo de sufrir una violación de seguridad, sino que también prepara a la institución para responder de manera eficaz y rápida en caso de un incidente.

Por otra parte, además de proteger la información confidencial, una auditoría de seguridad informática también contribuye a garantizar la continuidad de las operaciones educativas. La interrupción de los sistemas informáticos podría afectar negativamente la enseñanza y el aprendizaje, así como la gestión administrativa de la unidad educativa. Al identificar y mitigar posibles riesgos de seguridad, se pueden prevenir fallos en los sistemas críticos y asegurar un entorno tecnológico estable y funcional para todos los usuarios.

Finalmente, una auditoría de seguridad informática ayuda a la Unidad Educativa "Rumiñahui" a cumplir con las regulaciones y estándares de seguridad de datos aplicables. En un entorno normativo cada vez más estricto, es fundamental demostrar el cumplimiento de las leyes de protección de datos y las mejores prácticas de seguridad cibernética. Al realizar auditorías periódicas, la institución puede documentar sus esfuerzos por proteger la privacidad de los datos y mantener la confianza de la comunidad educativa y los organismos reguladores.

## 1.8. Impactos esperados.

### 1.8.1. Impacto tecnológico.

El impacto tecnológico de desarrollar una auditoría de seguridad informática en la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" es significativo. Fortalece la protección de datos sensibles de estudiantes y personal, asegura la continuidad de las operaciones educativas al prevenir interrupciones tecnológicas y garantiza el cumplimiento de regulaciones de privacidad, promoviendo así un entorno

educativo seguro y confiable.

### 1.8.2. Impacto social.

La realización de una auditoría de seguridad informática en la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" tiene un impacto social significativo. Garantiza la protección de datos personales de estudiantes y personal, promueve la confianza en la institución al demostrar su compromiso con la seguridad digital y asegura un entorno educativo seguro y confiable para toda la comunidad.

### 1.8.3. Impacto ecológico.

El desarrollo de una auditoría de seguridad informática en la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" tiene un impacto ecológico positivo al promover prácticas de eficiencia energética y gestión sostenible de recursos. Reduce el consumo de energía y la generación de residuos electrónicos, contribuyendo así a la conservación del medio ambiente y fomentando una cultura de responsabilidad ambiental en la comunidad educativa.

# CAPÍTULO II

## 2. Marco teórico de la investigación.

### 2.1. Antecedentes históricos.

La auditoría de seguridad informática evalúa la robustez de la infraestructura tecnológica de una organización, identificando vulnerabilidades, riesgos y deficiencias en sistemas, redes y políticas de seguridad. Mediante análisis exhaustivos y pruebas de penetración, se busca fortalecer la protección de datos y sistemas contra amenazas cibernéticas, garantizando la integridad y confidencialidad de la información.

En este contexto, se menciona a Bailón (2019), que realizó una investigación titulada “Auditoria informática al control y mantenimiento de una infraestructura tecnológica” cuyo objetivo fue evaluar la auditoria informática al control y mantenimiento de una infraestructura tecnológica en la empresa SEVIMAR COOPERATIVA de la ciudad Portoviejo – Ecuador, la investigación fue de tipo evaluativa, mediante una auditoria informática.

En este orden de ideas, esta investigación nos hace ver la importancia de desarrollar una auditoría de seguridad informática en la Unidad Educativa "Rumiñahui" en la parroquia Wilfrido Loor. Al evaluar su infraestructura tecnológica, se identifican vulnerabilidades y riesgos que podrían comprometer la integridad de los datos y la privacidad de los estudiantes y personal.

Por otra parte, cabe mencionar a Narváez (2023), que realizó una investigación titulada “Análisis de Políticas de Seguridad Aplicables a Infraestructuras Tecnológicas del Gobierno Autónomo Descentralizado del Cantón Babahoyo”, cuyo objetivo fue analizar las políticas de seguridad aplicables al Gobierno Autónomo Descentralizado de Babahoyo para un mejor control y uso de la información.

La metodología de investigación fue, un estudio de casos, para examinar de

manera minuciosa uno o varios casos y comprender mejor los desafíos que conlleva implantar políticas de seguridad en las infraestructuras de las instituciones. Dentro de las técnicas de investigación aplicadas fue, la entrevista con expertos en seguridad informática para obtener información relevante sobre las necesidades y desafíos de implantar políticas adecuadas de seguridad.

En este contexto, también menciona que empleó una metodología de análisis de documentos para recopilar información relacionada con el uso de políticas aplicables a tecnologías y seguridad de infraestructuras tecnológicas en instituciones. Esta metodología se enfocó en documentos especializados en el tema, como informes, libros y artículos.

Dentro de esta investigación, una de las conclusiones fue, que para lograr tener mejores resultados de seguridad en toda la infraestructura tecnológica pueden combinarse políticas informáticas con controles provenientes de normas como las ISO 27001 y 27002, ya que estas ofrecen a las instituciones una guía detallada sobre cómo establecer sistemas de gestión de seguridad de la información efectivo y eficiente.

Como se puede observar esta investigación da pautas para crear políticas de seguridad informática, basadas en normas como la ISO 27001 y 27002, que ofrecen una guía detallada para establecer normas de seguridad informática en una infraestructura tecnológica. Siendo este caso en la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor, en el cantón El Carmen – provincia de Manabí.

## 2.2. Antecedentes de investigaciones.

La auditoría de seguridad informática es vital para identificar y mitigar vulnerabilidades en la infraestructura tecnológica, asegurando la protección de datos y sistemas contra amenazas cibernéticas, y garantizando la continuidad operativa de las organizaciones, siendo las cosas así, se menciona a Ibarra y Narváez (2023), quienes realizaron una investigación sobre “Sistema de Gestión de Seguridad de la Información con estándares ISO/IEC 27001 y MAGERIT en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto”, el objetivo fue “implementar un Sistema de Gestión de Seguridad de

la Información SGSI con estándares ISO/IEC 27001 y MAGERIT que permita garantizar la seguridad de la información en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto".

El paradigma de investigación que utilizaron fue cuantitativo, ya que busca recolectar, analizar, sintetizar mediante gráficos y estadísticas cada una de las áreas funcionales de la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto. La técnica utilizada en esta investigación fue la observación visual, donde se realizó una observación detallada del comportamiento del personal de la empresa. Durante el proceso se tomó nota de las actividades y procesos realizados por el personal, para posteriormente analizar y obtener conclusiones.

Como resultado final de la investigación implementaron un Sistema de Gestión de Seguridad de la Información SGSI con estándares ISO/IEC 27001 y MAGERIT que permita garantizar la seguridad de la información en la empresa SP Sistemas Palacios Ltda de la ciudad de Pasto.

En este orden de ideas, se puede evidenciar que se pueden crear políticas sobre seguridad informática de infraestructura tecnológica, basadas en los estándares ISO/IEC 27001 y la metodología MAGERIT.

Por otra parte, cabe mencionar a Vargas (2023), que realizó una investigación titulada "Diseño un plan de seguridad informática en la Alcaldía de la Jagua de Ibirico-Cesar", cuyo objetivo fue "Diseñar un plan de seguridad informática para la Alcaldía de la Jagua de Ibirico, Cesar", el tipo de investigación empleada, fue descriptiva, ya que, corresponde al análisis y desarrollo de una propuesta para diseñar un plan de seguridad informática para la Alcaldía de la Jagua de Ibirico, de acuerdo al alcance definido, las necesidades de la entidad y tomando para base para ello, el modelo de referencia de seguridad de la norma ISO/IEC 27001.

Así mismo, la investigación se trabajó con enfoque cuantitativo ya que, se utilizaron técnicas pertinentes para la recolección de datos, como la observación, las encuestas y la revisión de documentos generalizando los resultados encontrados en un

grupo (muestra).

Ahora bien, siguiendo este orden de ideas, se puede evidenciar que el tipo de investigación para realizar una auditoría de seguridad informática a la infraestructura tecnológica puede ser descriptiva, con un enfoque cuantitativo, y la metodología para desarrollar las políticas y estándares de uso, se puede basar en las normas ISO/ICE27001 y MAGERIT.

## 2.3. Definiciones conceptuales.

### 2.3.1. Auditoría de seguridad informática

#### 2.3.1.1. Auditoría informática.

Para Albarracín et al. (2021), la auditoría informática es un proceso sistemático que evalúa la integridad, confiabilidad y seguridad de los sistemas de información de una organización. Mediante pruebas y análisis exhaustivos, se identifican vulnerabilidades, se evalúan controles de seguridad y se recomiendan mejoras para garantizar el cumplimiento normativo, la eficiencia operativa y la protección de datos contra amenazas cibernéticas.

La auditoría informática es un examen crítico de los sistemas y procesos de información de una organización para garantizar su integridad, seguridad y cumplimiento normativo, identificando riesgos y proponiendo mejoras.

Cabe considerar, por otra parte, lo manifestado por Macías et al. (2023), al decir que "los resultados de evaluación de una auditoría informática se obtienen al constatar en qué medida las organizaciones cumplen con las normas, estándares y procedimientos vigentes" (p.586). Dentro de este marco, se puede evidenciar la importancia de implementar una auditoria informática en las empresas como instituciones.

Dicho de otro modo, implementar una auditoría informática es crucial para asegurar la integridad, seguridad y eficiencia de los sistemas de información. Ayuda a identificar vulnerabilidades, garantizar el cumplimiento de normativas y proteger datos sensibles.

Además, mejora la confianza de los usuarios y optimiza el rendimiento, reduciendo riesgos y costos asociados a fallos tecnológicos o brechas de seguridad.

#### 2.3.1.2. Características de una auditoría en informática.

Una auditoría informática es un proceso integral que evalúa la eficacia, seguridad y cumplimiento normativo de los sistemas de información de una organización. Caracterizada por su enfoque sistemático y objetivo, implica la revisión exhaustiva de la infraestructura tecnológica, políticas de seguridad, procedimientos operativos y controles de acceso. Utiliza herramientas especializadas y técnicas de análisis para identificar vulnerabilidades, riesgos y deficiencias en la gestión de datos. Las recomendaciones resultantes buscan fortalecer la protección contra amenazas cibernéticas, mejorar la eficiencia operativa y garantizar la conformidad con regulaciones vigentes, asegurando la integridad y confidencialidad de la información (Angamarca, 2022).

La auditoría informática es sistemática y objetiva, evaluando la seguridad y eficacia de los sistemas de información. Identifica riesgos, vulnerabilidades y deficiencias, proponiendo mejoras para garantizar la protección y cumplimiento normativo.

En este contexto cabe mencionar a López y Beneyto (2020), al señalar que existen cuatro características esenciales en una auditoria informática: 1. Evaluación de Seguridad, examina la protección contra amenazas y vulnerabilidades, 2. Revisión de Sistemas, verifica la integridad y eficiencia de los sistemas informáticos, 3. Cumplimiento Normativo, asegura que se cumplen leyes y regulaciones, 4. Análisis de Riesgos, identifica y evalúa riesgos potenciales en los sistemas y procesos informáticos.

En efecto, la auditoría informática se centra en la evaluación de seguridad para proteger contra amenazas, y la revisión de sistemas para asegurar su integridad y eficiencia. También garantiza el cumplimiento normativo verificando que las operaciones informáticas se ajusten a leyes y regulaciones. Además, realiza un análisis de riesgos para identificar y evaluar posibles vulnerabilidades y amenazas en los sistemas y procesos tecnológicos.

#### 2.3.1.3. Campos de la auditoría informática.

Según Menjívar et al. (2021), los campos de la auditoría informática abarcan la evaluación exhaustiva de la seguridad de sistemas, controles de acceso, integridad de datos, cumplimiento normativo, eficiencia operativa y continuidad del negocio. Esto implica revisar políticas, procedimientos y tecnologías para identificar riesgos, vulnerabilidades y deficiencias, con el objetivo de fortalecer la protección de datos y garantizar la conformidad con regulaciones.

La auditoría informática cubre la evaluación de la seguridad de sistemas, controles de acceso, integridad de datos, cumplimiento normativo y eficiencia operativa. Identifica riesgos y vulnerabilidades para fortalecer la protección de datos.

Por otra parte, Palomino y Villegas (2022)., señalan: "la auditoría informática, abarca no solo a la Dirección de Tecnologías de Información, sino también a todas las direcciones de una entidad, porque en ellas se desarrollan actividades con Sistemas y Tecnologías de la Información" (p.1).

En este sentido se comprende, que la auditoria informática se la debe ejecutar en áreas que representan los puntos críticos donde la tecnología y la información juegan un papel esencial en las operaciones diarias, y donde una auditoría informática puede asegurar la eficacia, seguridad y cumplimiento.

#### 2.3.1.4. Seguridad informática.

La seguridad informática se refiere a la protección de sistemas, redes y datos contra ataques cibernéticos. Implica la implementación de medidas técnicas y procedimientos para prevenir, detectar y responder a amenazas como virus, malware y ataques de hackers. Incluye la autenticación de usuarios, el cifrado de datos, la monitorización de la red y la educación sobre seguridad. La seguridad informática es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información en entornos digitales (Postigo, 2020).

La seguridad informática aborda la protección de sistemas y datos contra amenazas cibernéticas. Incluye medidas como la autenticación de usuarios, cifrado de datos y monitoreo de red para garantizar la confidencialidad e integridad de la información.

En relación con la problemática expuesta, Moya (2023), señala: “la seguridad informática es esencial en la educación digital para proteger la información y garantizar su integridad, confidencialidad y disponibilidad” (p.2).

La seguridad informática protege los sistemas y datos contra accesos no autorizados, ataques y daños. Incluye medidas como la ciberseguridad, para defenderse de amenazas externas, y controles de acceso, que limitan quién puede interactuar con información crítica. Además, garantiza la integridad y disponibilidad de los datos, y asegura el cumplimiento normativo para proteger la privacidad y evitar sanciones legales.

#### 2.3.1.5. Etapas de la seguridad informática.

Para Castillo (2021), las etapas de la seguridad informática comprenden la evaluación de riesgos, la planificación de seguridad, la implementación de medidas preventivas y correctivas, así como la respuesta ante incidentes y la mejora continua. Esto implica identificar vulnerabilidades, establecer políticas y controles, capacitar al personal, monitorear la red y mantenerse actualizado con las últimas amenazas y tecnologías para garantizar la protección de sistemas y datos contra ataques cibernéticos.

Las etapas de la seguridad informática comprenden la evaluación de riesgos, planificación, implementación de medidas preventivas y correctivas, respuesta a incidentes y mejora continua, asegurando la protección contra amenazas cibernéticas.

En este contexto, resulta claro, mencionar a Castillo (2021), al indicar que las etapas de la seguridad informática son: identificación, protección, detección, respuesta y recuperación.

Con los antecedentes antes expuestos, las etapas de la seguridad informática comprenden la identificación de activos y riesgos, la implementación de medidas de

protección, la vigilancia y detección de amenazas, la respuesta ágil ante incidentes y la posterior recuperación de sistemas y datos. Estas etapas son fundamentales para garantizar la integridad, confidencialidad y disponibilidad de la información, así como para mitigar los impactos de posibles ataques y vulnerabilidades.

#### 2.3.1.6. ISO/ICE 27001

ISO/IEC 27001 es un estándar internacional para la gestión de la seguridad de la información. Define requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). Este estándar ayuda a las organizaciones a identificar y gestionar los riesgos de seguridad, implementar controles adecuados y garantizar la confidencialidad, integridad y disponibilidad de la información crítica (Malatji, 2023).

ISO/IEC 27001 establece requisitos para la gestión de la seguridad de la información. Ayuda a las organizaciones a identificar y gestionar riesgos, implementar controles adecuados y garantizar la confidencialidad, integridad y disponibilidad de la información.

Según Martín (2021), “el Sistema de Gestión de Seguridad ISO 27001 busca proteger la información y de los sistemas de información del acceso, divulgación o destrucción no autorizada” (p.496). Además, ISO 27001 permite implementar un Sistema de Gestión de Seguridad de la Información y el desarrollo de una herramienta digital que permita medir el grado de madurez de seguridad con respecto a la norma ISO 27001.

Ahora bien, la norma ISO/IEC 27001 permite a las organizaciones establecer, implementar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) eficaz. Proporciona un marco estructurado para proteger la confidencialidad, integridad y disponibilidad de la información, mediante la identificación de riesgos, la implementación de controles de seguridad y la mejora continua.

#### 2.3.1.7. Metodología MAGERIT

Para Guamán et al. (2023), MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un marco desarrollado por el Gobierno español para evaluar riesgos en sistemas de información. Se centra en identificar activos, amenazas y vulnerabilidades, evaluar riesgos y establecer controles adecuados para mitigarlos. MAGERIT facilita la toma de decisiones informadas sobre seguridad de la información, garantizando la protección de activos críticos y la continuidad operativa de las organizaciones frente a amenazas cibernéticas.

MAGERIT es una metodología para evaluar riesgos en sistemas de información. Identifica activos, amenazas, y vulnerabilidades, estableciendo controles para mitigar riesgos y garantizar la seguridad de la información.

Siendo las cosas así, resulta claro, mencionar a Avila y Cuenca (2021), al decir que la metodología MAGERIT es un marco español que ayuda a identificar, analizar y gestionar los riesgos en los sistemas de información. Facilita la protección de los activos de información mediante la evaluación de amenazas y vulnerabilidades y la implementación de medidas de mitigación.

En resumen, MAGERIT es una metodología para la gestión de riesgos en sistemas de información. Ayuda a identificar y evaluar amenazas y vulnerabilidades, protegiendo los activos de información a través de la implementación de medidas preventivas y correctivas para mitigar los riesgos detectados.

### 2.3.2. Infraestructura tecnológica

#### 2.3.2.1. Hardware.

Para Blind et al. (2021), el hardware se refiere a todos los componentes físicos de un sistema informático, como la unidad central de procesamiento (CPU), memoria RAM, disco duro, tarjeta madre y dispositivos periféricos como teclados, ratones y monitores. Es la parte tangible de un sistema informático que permite el procesamiento, almacenamiento y

transmisión de datos. El hardware es fundamental para el funcionamiento de dispositivos electrónicos, desde computadoras personales hasta dispositivos móviles y servidores.

El hardware es la parte física y tangible de un sistema informático, que incluye componentes como la CPU, memoria, disco duro y dispositivos periféricos. Es fundamental para el procesamiento, almacenamiento y transmisión de datos.

A este respecto, Dally (2023), indica que hardware es el conjunto de componentes físicos de un sistema informático, como la CPU, memoria, discos duros, placas base, y periféricos como monitores y teclados. Estos elementos permiten la ejecución de software y el procesamiento de datos.

Como se puede evidenciar, el hardware es el conjunto de componentes físicos que conforman un sistema informático. Incluye dispositivos internos como la CPU, memoria RAM, discos duros y la placa base, así como periféricos externos como monitores, teclados e impresoras. Estos elementos permiten la ejecución y funcionamiento del software, posibilitando el procesamiento y almacenamiento de datos.

**2.3.2.2. Software.**

El software es un conjunto de instrucciones y datos que permiten a una computadora realizar tareas específicas. Incluye programas, aplicaciones, sistemas operativos y utilidades que controlan el funcionamiento del hardware. El software puede ser de sistema, que gestiona recursos y proporciona servicios básicos, o de aplicación, diseñado para realizar tareas específicas, como procesamiento de texto, diseño gráfico o navegación web. Es esencial para la funcionalidad y utilidad de los dispositivos informáticos (Xing, 2021).

El software es un conjunto de instrucciones y datos que permiten a los dispositivos informáticos realizar diversas tareas, desde procesamiento de datos hasta ejecución de programas y aplicaciones.

Siguiendo este orden de ideas, para Gauthier y Budán (2023), software es el conjunto de programas y aplicaciones que permiten a los dispositivos informáticos realizar tareas

específicas. Incluye sistemas operativos que gestionan el hardware, aplicaciones que ejecutan funciones específicas, y utilidades que optimizan el rendimiento. El software es esencial para la operación y funcionalidad de cualquier sistema computacional.

#### 2.3.2.3. Infraestructura tecnológica.

Para Riofrio et al. (2023), la infraestructura tecnológica comprende los elementos físicos y virtuales que soportan el funcionamiento de sistemas informáticos y de comunicación. Incluye hardware, como servidores, redes y dispositivos, así como software, sistemas operativos y aplicaciones. También abarca servicios en la nube, centros de datos y protocolos de seguridad. Una infraestructura tecnológica robusta y bien gestionada es crucial para facilitar operaciones eficientes, garantizar la disponibilidad y seguridad de los datos, y promover la innovación tecnológica en las organizaciones. La infraestructura tecnológica es el conjunto de hardware, software, redes y servicios que sostienen la operación de sistemas informáticos y de comunicación. Es fundamental para garantizar la eficiencia, disponibilidad y seguridad de los datos en las organizaciones.

Por otra parte, Chiquito (2023), señala que: es vital brindar seguridad a la infraestructura tecnológica y reducir riesgos en una organización con la implementación de sistemas de seguridad de la información SGSI alineado con el estándar ISO/IEC 27001.

En este contexto brindar seguridad a la infraestructura tecnológica es crucial para proteger los datos sensibles, asegurar la continuidad operativa y prevenir pérdidas financieras. Fortalece la confidencialidad**,** integridad **y** disponibilidad de la información, salvaguardando contra ataques cibernéticos y fallos de sistema. Además, cumple con regulaciones y mantiene la confianza de clientes y socios comerciales.

#### 2.3.2.4. Tipos de infraestructuras de TI

Existen varios tipos de infraestructuras de tecnología de la información (TI), como las físicas (hardware, servidores, dispositivos de red), virtuales (nube, máquinas virtuales), de redes (redes locales, redes inalámbricas), de almacenamiento (almacenamiento en disco, almacenamiento en la nube), de seguridad (firewalls, sistemas de detección de intrusos), y de

servicios (plataformas de software como servicio, infraestructura como servicio), todas fundamentales para el funcionamiento eficiente y seguro de los sistemas informáticos y de comunicación de una organización (Sánchez, 2023).

Los tipos de infraestructuras de TI incluyen hardware, como servidores y dispositivos de red, infraestructuras virtuales, como la nube, y servicios como plataformas de software como servicio, esenciales para el funcionamiento de sistemas informáticos.

En otras palabras, la infraestructura tecnológica abarca varios componentes clave: hardware, que incluye servidores, computadoras, redes y dispositivos de almacenamiento; software, como sistemas operativos, aplicaciones y bases de datos; y redes de comunicación, que proporcionan conectividad a través de cables, redes inalámbricas y protocolos. También comprende servicios en la nube, que permiten almacenamiento y procesamiento remoto, y seguridad de TI, que incorpora medidas como firewalls, sistemas de detección de intrusos y soluciones antivirus para proteger los sistemas y datos.

#### 2.3.2.5. Infraestructura tradicional de TI

Según Zamora (2023), la infraestructura tradicional de TI se refiere a sistemas físicos y locales, incluyendo servidores, redes y almacenamiento, gestionados en las instalaciones de una organización. Estos componentes requieren inversión inicial y mantenimiento continuo. Aunque ofrecen control directo y privacidad de datos, pueden ser costosos y difíciles de escalar. Sin embargo, siguen siendo utilizados por muchas empresas debido a requisitos de cumplimiento, necesidades de rendimiento específicas o preferencias de seguridad.

La infraestructura tradicional de TI abarca sistemas físicos y locales, como servidores y redes, gestionados en las instalaciones de una organización, ofreciendo control directo, pero con costos y escalabilidad limitados.

Ahora bien, para Chirinos (2023), la infraestructura tradicional de TI se compone principalmente de hardware físico ubicado en las instalaciones de la empresa, como servidores, computadoras, dispositivos de almacenamiento y redes. Estos componentes son

gestionados por un equipo de TI interno. El software en esta configuración incluye sistemas operativos y aplicaciones instalados localmente en el hardware.

La red de comunicación conecta los dispositivos a través de cables y redes locales (LAN). Esta infraestructura requiere una inversión significativa en mantenimiento y actualización de equipos. Además, incluye medidas de seguridad de TI para proteger los datos y sistemas contra amenazas y accesos no autorizados, como firewalls y sistemas de detección de intrusos (Chirinos, 2023).

#### 2.3.2.6. Infraestructura de nube de TI

La infraestructura de nube de TI es un entorno de computación basado en la nube que proporciona recursos de hardware, software y almacenamiento a través de Internet. Permite la escalabilidad bajo demanda, flexibilidad y acceso remoto a servicios, eliminando la necesidad de mantener hardware local. La infraestructura de nube puede ser pública, privada o híbrida, ofreciendo opciones para adaptarse a las necesidades y presupuestos de diferentes organizaciones (Zamora, 2023).

La infraestructura de nube de TI proporciona recursos de hardware, software y almacenamiento a través de Internet, permitiendo escalabilidad, flexibilidad y acceso remoto a servicios sin necesidad de mantener hardware local.

En este contexto para Bárcenas et al. (2023), la infraestructura de nube de TI proporciona recursos informáticos a través de internet, incluyendo servidores, almacenamiento y redes virtualizados, gestionados por proveedores de servicios en la nube, permitiendo escalabilidad y flexibilidad.

Siendo las cosas así, la infraestructura de nube de TI es fundamental ya que ofrece flexibilidad, escalabilidad y acceso remoto a recursos informáticos. Permite a las organizaciones reducir costos, mejorar la eficiencia operativa y adaptarse rápidamente a las demandas del negocio, facilitando la innovación y el crecimiento empresarial.

### 2.3.2.7. Infraestructura hiperconvergente de TI

Para Jiménez (2023), La infraestructura hiperconvergente de TI integra computación, almacenamiento, redes y virtualización en una única plataforma. Ofrece escalabilidad horizontal, administración centralizada y simplificada, y permite la implementación rápida de recursos. Al eliminar la necesidad de infraestructuras separadas y optimizar el uso de recursos, la infraestructura hiperconvergente mejora la eficiencia y agilidad operativa, reduciendo costos y complejidades en entornos de TI empresariales.

La infraestructura hiperconvergente de TI integra computación, almacenamiento, redes y virtualización en una plataforma única. Proporciona escalabilidad, administración simplificada y rápida implementación de recursos, reduciendo costos y complejidades operativas.

Según Zamora (2023), la infraestructura hiperconvergente de TI combina almacenamiento, cómputo y virtualización en un único sistema escalable y gestionado mediante software. Optimiza la gestión y reduce la complejidad al consolidar recursos en una plataforma integrada y modular.

La infraestructura hiperconvergente de TI es una arquitectura que combina cómputo, almacenamiento y redes en un único sistema integrado y gestionado de manera centralizada, proporcionando escalabilidad y simplificación operativa.

### 2.3.2.8. Gestión de la infraestructura de TI

La gestión de la infraestructura de TI implica planificar, implementar y mantener los componentes tecnológicos de una organización para garantizar su eficiencia y seguridad. Esto incluye la administración de servidores, redes, almacenamiento y sistemas operativos, así como la supervisión de la disponibilidad, rendimiento y cumplimiento normativo. Una gestión efectiva de la infraestructura de TI optimiza los recursos, minimiza los tiempos de inactividad y apoya los objetivos comerciales de la organización (Cruz, 2024).

La gestión de la infraestructura de TI implica planificar, implementar y mantener los componentes tecnológicos de una organización para garantizar su eficiencia, seguridad y alineación con los objetivos empresariales.

Atendiendo a estas consideraciones, Goicochea (2023), la gestión de la infraestructura de TI implica planificar, implementar y supervisar los componentes tecnológicos de una organización, incluyendo hardware, software, redes y servicios en la nube, garantizando su disponibilidad, rendimiento, seguridad y cumplimiento normativo, así como la alineación con los objetivos empresariales y la optimización de costos.

La gestión de la infraestructura de TI en una auditoría implica evaluar la eficacia de la planificación, implementación y supervisión de los recursos tecnológicos de una organización, garantizando su alineación con los objetivos empresariales y las mejores prácticas de seguridad y cumplimiento normativo (Goicochea, 2023).

# CAPITULO III

## 3. MARCO INVESTIGATIVO

### 3.1. Introducción

La investigación cuali-cuantitativa integra métodos cualitativos y cuantitativos para proporcionar una comprensión completa de un fenómeno. Combina la profundidad y contexto de los datos cualitativos con la objetividad y generalización de los cuantitativos, permitiendo explorar complejas relaciones y tendencias en un estudio más robusto y holístico (Padilla y Marroquín, 2021).

En este contexto, en la presente investigación se usó una investigación cualitativa al emplear la técnica de la entrevista y obtener resultados que luego se analizaron minuciosamente, así mismo, se empleó una investigación cuantitativa, al usar la técnica de la encuesta, cullos resultados fueron ordenados y tabulados para sacar gráficos estadísticos relacionados al fenómeno de estudio.

### 3.2. Tipos de investigación

#### 3.2.1. Investigación bibliográfica

La investigación bibliográfica o documental para Reyes y Carmona (2020), “es una de las técnicas de la investigación cualitativa que se encarga de recolectar, recopilar y seleccionar información de las lecturas de documentos, revistas, libros, grabaciones, filmaciones, periódicos, artículos resultados de investigaciones, memorias de eventos, entre otros” (p.1).

En esta investigación, se usó la investigación bibliográfica-documental para recolectar y analizar datos previos de fuentes confiables, proporcionando un marco teórico y contexto necesario para interpretar y validar los hallazgos del estudio.

#### 3.2.2. Investigación de campo

La investigación de campo recopila datos directamente del entorno donde ocurre el

fenómeno estudiado, mediante observación, entrevistas o encuestas. Permite obtener información precisa y contextualizada, reflejando la realidad de los participantes. Es esencial para estudios que requieren datos actuales y específicos sobre comportamientos y condiciones locales (Sandoval, 2020).

En la presente investigación sobre auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa "Rumiñahui", se utilizó la investigación de campo para evaluar directamente los sistemas y redes. Mediante inspección in situ, entrevistas al personal y análisis de la configuración de seguridad, se identificaron vulnerabilidades y se validaron las medidas de protección implementadas.

### 3.2.3. Investigación aplicada

Según Castro et al. (2023), la investigación aplicada, "concentra 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" (p.147).

En la presente investigación sobre auditoría de seguridad informática en la Unidad Educativa "Rumiñahui", se utilizaron técnicas específicas para evaluar y mejorar la infraestructura tecnológica. Se aplicaron métodos prácticos, como pruebas de vulnerabilidad y análisis de riesgos, adaptados a las necesidades específicas del entorno educativo.

## 3.3. Métodos de investigación

Los métodos de investigación son estrategias y técnicas sistemáticas para recolectar, analizar y presentar datos. Incluyen enfoques cualitativos, como entrevistas y observaciones, y cuantitativos, como encuestas y experimentos, que ayudan a generar y validar conocimientos en diversos campos.

### 3.3.1. Método Analítico – Sintético

Portilla y Honorio (2022), manifiestan que "El método analítico-sintético consiste en una ruta cognitiva que adopta el lector para descomponer y recomponer la estructura textual

siguiendo ciertas etapas a fin de comprender el significado del texto" (p.47).

En la auditoría de seguridad informática de la Unidad Educativa "Rumiñahui", el método analítico-sintético se utilizó para descomponer la infraestructura tecnológica en componentes individuales, identificar y analizar vulnerabilidades y riesgos específicos. Posteriormente, se integraron estos hallazgos para formular recomendaciones de mejora que abordan el sistema globalmente, optimizando su seguridad.

### 3.3.2. Método Deductivo – Inductivo

El método inductivo-deductivo integra dos enfoques: la inducción, que extrae conclusiones generales de observaciones específicas, y la deducción, que aplica principios generales a casos particulares para validar teorías o predecir resultados. Este método permite desarrollar hipótesis basadas en datos observados y verificarlas mediante razonamiento lógico, combinando lo específico y lo general (Sarguera et al., 2024).

En la auditoría de seguridad informática de la Unidad Educativa "Rumiñahui", el método inductivo-deductivo se empleó observando incidentes específicos de seguridad (inducción) para identificar patrones de vulnerabilidad. Luego, se aplicaron principios generales de seguridad informática (deducción) para diseñar soluciones que prevenían futuros incidentes, combinando datos concretos y normas generales de protección.

## 3.4. Fuentes de información de datos

### 3.4.1. Fuentes primarias y secundarias

En esta investigación, se identifican como principales fuentes de información a los estudiantes de la Unidad Educativa "Rumiñahui", ubicada en la parroquia Wilfrido Loor. Estos estudiantes asisten a clases y realizan sus prácticas en el laboratorio de informática, además de desplazarse por todas las áreas de la institución.

La infraestructura tecnológica juega un papel crucial en el fortalecimiento del proceso educativo. En este sentido, asegurar su integridad es vital para mejorar continuamente los

conocimientos adquiridos mediante el uso de diversas herramientas y aplicaciones tecnológicas disponibles hoy en día.

Como fuentes secundarias, se consideraron a los docentes, quienes emplean tecnologías en sus clases para enriquecer sus programas educativos. Cada profesor adapta y potencia su currículo mediante la integración de recursos tecnológicos, mejorando así sus métodos pedagógicos y didácticos en beneficio de los estudiantes de diferentes niveles. Estos docentes, familiarizados con las instalaciones tecnológicas de la Unidad Educativa "Rumiñahui", también se mueven por todas las áreas, asegurándose de que la tecnología apoya efectivamente el proceso de enseñanza-aprendizaje.

## 3.5. Estrategia operacional para la recolección de datos

### 3.5.1 Población - Segmentación - Técnica de muestreo - Tamaño de la muestra

#### 3.5.1.1 Población

Piedra y Manqueros (2021), señalan que la población "es un conjunto definido, limitado y accesible del universo que forma el referente para la elección de la muestra. Es el grupo al que se intenta generalizar los resultados" (p.84). La población se refiere al conjunto completo de elementos (personas, objetos, eventos) que poseen características específicas y sobre los cuales se desea obtener conclusiones.

En la presente investigación la población fue de 625 estudiantes de los diferentes niveles de educación, que reciben clases en el laboratorio de informática y tienen acceso a internet dentro de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor.

Siguiendo este orden de ideas, se consideró a tres docentes que trabajan dando clases y a su vez desempeñan las funciones de directivos de la Unidad Educativa "Rumiñahui". Estos docentes tienen bastos conocimientos en el uso de aplicaciones informáticas e infraestructura tecnológica.

### 3.5.1.2. Segmentación o muestra

Mucha et al. (2021), señalan que la segmentación o muestra "es el subconjunto seleccionado de la población, que se utiliza para recopilar datos y obtener conclusiones. La muestra debe ser representativa y suficiente para generalizar los resultados a la población total."

En la presente investigación se trabajó con 239 estudiantes a los grados más superiores que reciben clases en el laboratorio de informática, dicha muestra fue de carácter discrecional a ellos se les aplicó porque tienen más conocimientos en el uso de equipos informáticos y dispositivos móviles.

Por otra parte, se consideró a tres docentes que imparten clases y cumplen el papel de directivos dentro de la institución. Además, son docentes que tienen conocimientos en el uso de infraestructura tecnológica.

### 3.5.1.3 Técnica del muestreo

La técnica del muestreo para Chacón et al. (2022), es considerado como:

La parte de la práctica estadística mediante la cual se seleccionan elementos de una población, utilizando una determinada técnica, con la intención de arribar a conclusiones de alcance limitado (muestral) o de obtener conocimientos sobre la población que se va a observar para realizar una inferencia estadística generalizadora (p. 681).

En este mismo contexto, para Hernández (2021), la selección de los participantes se realiza mediante expertos que establecen criterios a seguir. El muestreo intencional selecciona participantes basados en características específicas o criterios determinados, con el objetivo de obtener información relevante y representativa de la población en estudio.

### 3.5.1.4 Tamaño de la muestra

Una vez definida la población a ser estudiada y la técnica del muestreo, se procede a realizar un muestreo discrecional o intensional, donde se tomó en cuenta a los estudiantes que

son de básica superior y bachillerato, y tienen conocimientos básicos en el uso de infraestructura tecnológica.

Con estos antecedentes, la encuesta se debe aplicar a 239 estudiantes de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor.

Siguiendo este contexto, se menciona que la entrevista se aplicará a 3 docentes, que tienen cargo administrativo y tienen conocimientos en el uso de aplicaciones informáticas e infraestructura tecnológica.

### 3.5.2 Análisis de las herramientas de recolección de datos a utilizar

#### 3.5.2.1 Encuesta

Para Romero (2021), la encuesta es un método de investigación que recopila datos de un grupo de personas mediante preguntas estructuradas. Se utiliza para obtener información sobre opiniones, comportamientos o características, facilitando el análisis de tendencias y patrones en una población específica.

En la presente investigación se aplicó la encuesta a los 239 estudiantes de los diferentes niveles de la Unidad Educativa “Rumiñahui”, donde reconocieron su experiencia sobre el uso de las aplicaciones informáticas, laboratorio y dieron su punto de vista sobre la infraestructura tecnológica existente en la unidad educativa.

#### 3.5.2.2 Entrevista

Según Lopezosa (2020), la entrevista es:

> Un instrumento de gran eficacia para desarrollar investigaciones cualitativas y tiene como función principal recabar datos que después podremos aplicar a nuestros estudios. Se trata de una técnica que se caracteriza por tratarse de una conversación más o menos dirigida (dependiente del tipo de entrevista) entre el investigador (emisor) y el sujeto de estudio (receptor) con un fin siempre bien determinado y enfocado a la resolución de los objetivos y preguntas de investigación de trabajos. Para alcanzar este fin el investigador plantea interrogantes al receptor para que éste le dé su opinión, los

responda o los resuelva, según el caso (p. 89).

La entrevista es una técnica de recolección de información basada en una conversación estructurada o semiestructurada entre un entrevistador y un entrevistado, destinada a profundizar en temas específicos y obtener respuestas detalladas. En esta investigación se aplicó la entrevista a tres docentes con cargos administrativos, que tienen más de tres años trabajando en la unidad educativa, y tienen vastos conocimientos en el uso de aplicaciones informáticas como infraestructura tecnológica.

#### 3.5.2.3. Estructura de lo(s) instrumento(s) de recolección de datos aplicados

##### 3.5.2.3.1. Estructura de la encuesta

La encuesta fue aplicada a estudiantes de los diferentes niveles de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Vera.

Los datos logrados fueron solamente para fines investigativos y desarrollo de la presente investigación, la información personal de los participantes no fue divulgada.

La encuesta se compuso de preguntas de respuesta breve diseñadas para evaluar varios aspectos relacionados con el uso del laboratorio de informática y la infraestructura tecnológica en la unidad educativa. Específicamente, se buscó medir: el nivel de satisfacción de los estudiantes, la importancia que le otorgan, la frecuencia con la que utilizan estos recursos, las dificultades que enfrentan y el grado de desacuerdo respecto a las condiciones y disponibilidad de la tecnología en el entorno educativo.

##### 3.5.2.3.2. Estructura de la entrevista

La entrevista se realizó con tres docentes, seleccionados por su amplia experiencia en la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor, su conocimiento en procesos administrativos y su competencia en el uso de herramientas tecnológicas.

Los resultados obtenidos se utilizaron exclusivamente con fines investigativos y para el desarrollo de este estudio, garantizando la confidencialidad de los datos personales de los

entrevistados.

Se empleó una guía de entrevista semiestructurada con preguntas abiertas, diseñada para recopilar información y opiniones sobre el laboratorio de informática y la infraestructura tecnológica en la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor.

#### 3.5.2.3.3. Plan de recolección de datos

Para recopilar información de los estudiantes de diversos niveles educativos de la Unidad Educativa “Rumiñahui” en la parroquia Wilfrido Loor, se utilizó un cuestionario administrado a través de Google Forms.

Este cuestionario fue enviado a los estudiantes a través de sus correos electrónicos institucionales y por WhatsApp. La validación de las respuestas se realizó mediante la base de datos proporcionada por Gmail. Posteriormente, los datos verificados se analizaron y se generaron gráficos estadísticos en Excel.

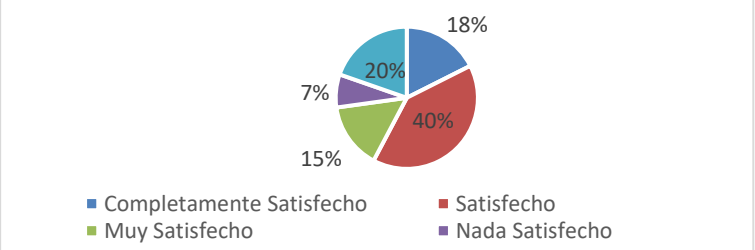
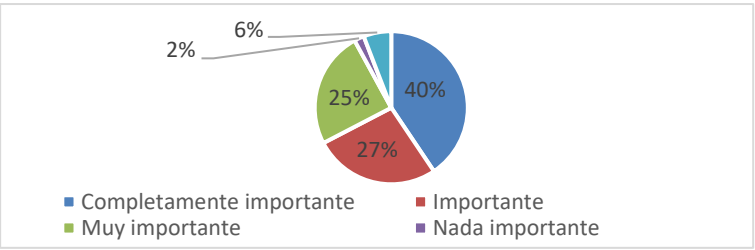
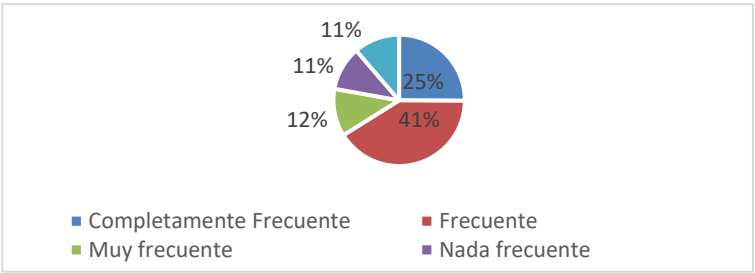
En cuanto a las entrevistas con los docentes, estas se llevaron a cabo tanto a través de Zoom como de manera presencial, y se grabaron para su análisis posterior.

Es importante señalar que toda la información obtenida a través de las encuestas y entrevistas es estrictamente confidencial y se utilizará únicamente para esta investigación, manteniendo la privacidad de las fuentes.

### 3.6 Análisis y presentación de resultados

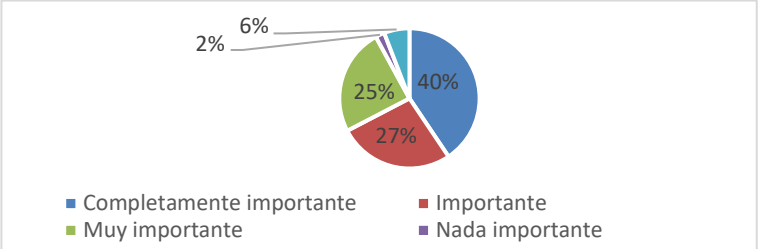
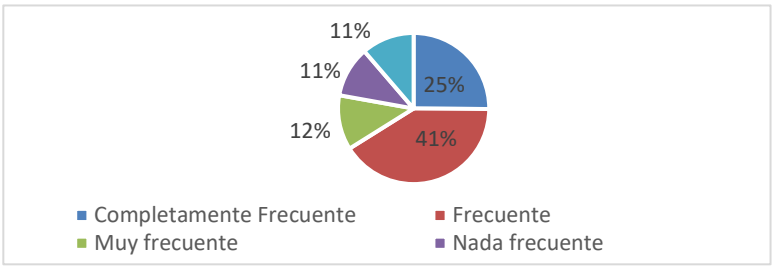
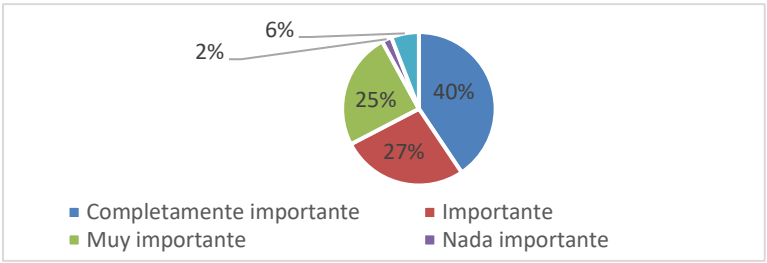
#### 3.6.1 Análisis de encuestas a estudiantes

**Tabla 1: Análisis de las encuestas aplicadas a estudiantes**

| Pregunta | Gráfico |
|---|---|
| 1. ¿Qué tan satisfecho está con la experiencia del uso del laboratorio de informática de la Unidad educativa "Rumiñahui"? |  |
| **Análisis:**<br>Se puede evidenciar que el 40% de los estudiantes están satisfechos con la experiencia en el laboratorio de informática, un 20% están pocos satisfechos, un 18% manifiestan que están completamente satisfechos, un 15% están muy satisfechos y un 7% nada satisfechos. | |
| **Pregunta** | **Gráfico** |
| 2. ¿Qué tan importante considera que es el laboratorio de informática para los estudiantes? |  |
| **Análisis:**<br>Se puede evidenciar que el 39% de los estudiantes manifiesta que es importante el laboratorio de informática, el 36% señala que es muy importante, el 23% que es completamente importante, un 2% que es nada importante, y un 0% señala que es poco importante. | |
| **Pregunta** | **Gráfico** |
| 3. ¿Con que frecuencia le gustaría recibir clases en el laboratorio de informática? |  |
| **Análisis:**<br>Se puede evidenciar que el 60% de los estudiantes señalan que frecuentemente les gustaría recibir clases en el laboratorio de informática, el 20% señala que debería ser completamente frecuente, un 18% señala que debe ser muy frecuente, un 2% debe ser poco frecuente, y un 0% que nada frecuente. | |

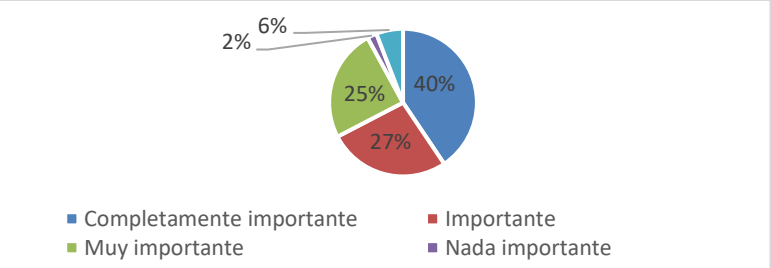
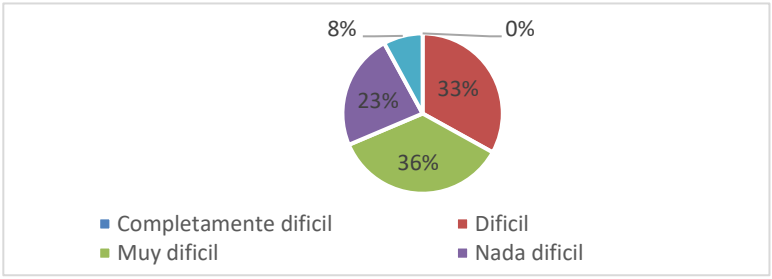
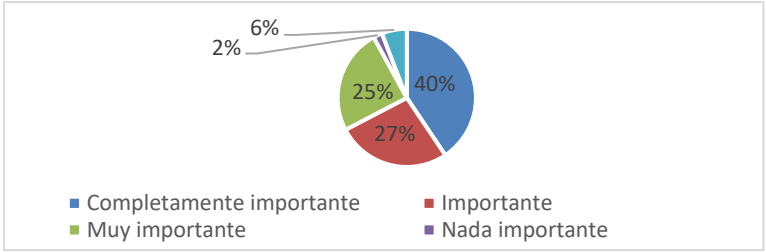
Fuente: Carolina Vélez (2024)

**Tabla 2: Análisis de las encuestas aplicadas a estudiantes**

| Pregunta | Gráfico |
|---|---|
| 4. ¿Cómo considera el uso de las aplicaciones informáticas para realizar tus investigaciones o trabajos? |  |
| **Análisis:**<br>Se puede evidenciar que el 37% de los estudiantes señalan que el uso de aplicaciones informáticas es muy importante para realizar trabajos e investigaciones, el 33% señala que son completamente importantes, el 20% indica que son importantes, el 10% que son poco importantes y un 0% que no son nada importante. | |
| **Pregunta** | **Gráfico** |
| 5. ¿Las autoridades cuidan el buen funcionamiento del laboratorio de informática de la Unidad educativa “Rumiñahui”? |  |
| **Análisis:**<br>Se puede evidenciar que el 41% de los estudiantes señalan que frecuentemente las autoridades cuidan el buen funcionamiento del laboratorio de informática, un 25% señala que completamente frecuente lo hacen, un 12% señala que muy frecuentemente lo hacen, un 11% manifiesta que nada frecuente hacen esta actividad, y otro 11% señala que con poca frecuencia lo hacen. | |
| **Pregunta** | **Gráfico** |
| 6. ¿Qué tan importante consideras el uso de cámaras de seguridad en todas las áreas de la Unidad educativa “Rumiñahui”? |  |
| **Análisis:**<br>Se puede evidenciar que el 35% de los estudiantes señalan es importante el uso de cámaras de seguridad en la unidad educativa, un 24% señala que es muy importante, un 20% señala que es completamente importante, un 12% manifiesta que es nada importante y un 9% señala que es poco importante el uso de cámaras de seguridad. | |

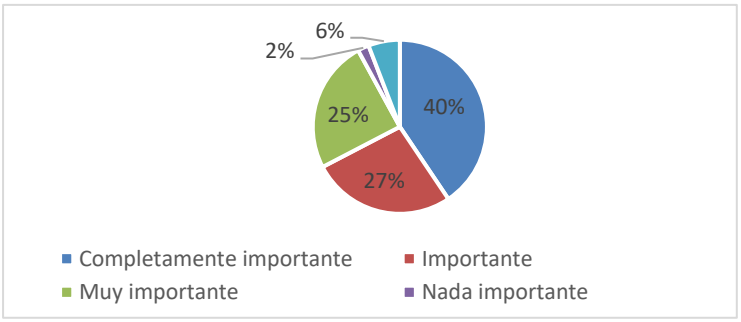
Fuente: Carolina Vélez (2024)

**Tabla 3: Análisis de las encuestas aplicadas a estudiantes**

| Pregunta | Gráfico |
|---|---|
| 7. ¿Qué tan importante consideras el uso de sirenas de auxilio en todas las áreas de la Unidad educativa "Rumiñahui"? |  |
| **Análisis:**<br>Se puede evidenciar que el 40% de los estudiantes señalan que es completamente importante el uso de sirenas de auxilio en la unidad educativa, un 27% señala que es importante, un 25% señala que es muy importante, un 6% señala que es poco importante, y un 2% señala que es nada importante el uso de sirenas de auxilio. | |
| **Pregunta** | **Gráfico** |
| 8. ¿Qué tan difícil se te hace conectarte a una red wifi en la Unidad educativa "Rumiñahui"? |  |
| **Análisis:**<br>Se puede evidenciar que el 36% de los estudiantes señala que es muy difícil conectarse a la red wifi, un 33% señala que es difícil, un 23% señala que no es nada difícil, un 8% señala que es poco difícil y un 0% señala que es nada difícil, conectarse a la red wifi. | |
| **Pregunta** | **Gráfico** |
| 9. ¿Qué tan importante considera la implementación de puntos wifi en todas las áreas de la Unidad educativa "Rumiñahui"? |  |
| **Análisis:**<br>Se puede evidenciar que el 40% de los estudiantes señalan que es completamente importante instalar puntos wifi en todas las áreas de la unidad educativa, un 27% señala que es importante, un 25% señala que es muy importante, un 6% señala que es poco importante, y un 2% señala que no es nada importante instalar más puntos wifi en la unidad educativa. | |

Fuente: Carolina Vélez (2024)

**Tabla 4: Análisis de las encuestas aplicadas a estudiantes**

| Pregunta | Gráfico |
|---|---|
| 10. ¿Consideras importante implementar otro laboratorio de informática en la Unidad Educativa "Rumiñahui"? |  |
| **Análisis:**<br>Se puede evidenciar que el 40% de los estudiantes señalan que es completamente importante implementar otro laboratorio en la unidad educativa, un 27% señala que es importante, un 25% señala que es muy importante, un 6% señala que es poco importante y un 2% señala que es nada importante implementar otro laboratorio en la unidad educativa. | |



Fuente: Carolina Vélez (2024)

**Análisis de las encuestas.**

El estudio revela diversas percepciones de los estudiantes sobre el uso de las instalaciones y recursos tecnológicos en su unidad educativa. En cuanto a la experiencia en el laboratorio de informática, el 40% de los estudiantes se siente satisfecho, mientras que un 18% está completamente satisfecho. Sin embargo, existe un 7% que no se muestra conforme. Respecto a la frecuencia deseada para recibir clases en el laboratorio, un 60% preferiría que estas fueran frecuentes, y un 20% las considera completamente necesarias.

En cuanto a la importancia de los recursos tecnológicos, como las aplicaciones informáticas y las cámaras de seguridad, se destaca que un 37% de los estudiantes cree que las aplicaciones son muy importantes para sus trabajos, y un 35% señala la relevancia del uso de cámaras de seguridad en la institución. Además, se observa una percepción positiva sobre la necesidad de implementar más puntos wifis, siendo el 40% el que lo considera completamente importante.

Finalmente, en relación con el cuidado de las instalaciones, el 41% de los estudiantes considera que las autoridades frecuentemente supervisan el funcionamiento del laboratorio, aunque un 11% cree que esta actividad se realiza de manera insuficiente. También se evidencia la necesidad de un segundo laboratorio de informática, con un 40% de los encuestados a favor de su implementación completa.

### 3.6.2 Análisis de entrevista a autoridades de la institución

**Tabla 5: Análisis de las entrevistas aplicadas a las autoridades**

| Pregunta | Respuesta | Análisis |
|---|---|---|
| 1. ¿Qué tan satisfecho está con la experiencia en el laboratorio de informática de la Unidad educativa "Rumiñahui"? | E1. Moderada, debido a que existe el equipo necesario, pero lamentablemente por falta de mantenimiento y reparación no están habilitadas en un 100%.<br>E2. Tomando en consideración el servicio que se está dando en el Laboratorio de Informática, considero que muy satisfecho de poder ser parte del proceso en la Unidad Educativa Fiscal "Rumiñahui"<br>E3. Normal, hace falta equipos. | Se puede evidenciar que la experiencia en el laboratorio de informática es aceptable, sin embargo, es necesario dar mantenimiento a toda la infraestructura tecnológica. |
| 2. ¿Qué tan importante considera que es el laboratorio de informática para los estudiantes y docentes? | E1. Sumamente importante, el laboratorio de informática es indispensable para el desarrollo en cada una de las asignaturas (ejes transversales).<br>E2. Considero que es muy importante, porque los estudiantes tienen acceso al servicio que brindamos en el proceso educativo a través de las diferentes áreas de estudio.<br>E3. Muy importante es parte del proceso de estudios. | El uso del laboratorio es importante para estudiantes como para docentes y autoridades, el uso del laboratorio forma parte del proceso educativo. |
| 3. ¿Con que frecuencia le gustaría dar clases en el laboratorio de informática? | E1. Siempre (una vez a la semana por cada asignatura)<br>E2. En mi caso (Lengua y Literatura), me gustaría impartir 2 horas clases por semana.<br>E3. Varias veces a la semana. | Cada docente debería tener varias horas de clases en el laboratorio. |
| 4. ¿Qué tan difícil se le hace utilizar las aplicaciones informáticas para dar clases? | E1. Por ahora no hay dificultad en las aplicaciones informáticas.<br>E2. Realmente no manejo de manera perfecta la tecnología, pero es importante la auto preparación en el tema y sí lo hago.<br>E3. Fácil. | Por parte de los docentes no se presenta dificultad al momento de usar las aplicaciones informáticas. |
| 5. ¿Las autoridades cuidan el buen funcionamiento del laboratorio de informática de la Unidad educativa "Rumiñahui"? | E1. Si<br>E2. Siempre ha habido el cuidado necesario por parte de las autoridades y de la persona que se ha designado para su mantenimiento permanente.<br>E3. Siempre las autoridades se preocupan por el buen funcionamiento. | Se evidencia que las autoridades se preocupan por el mantenimiento y cuidado de la infraestructura tecnológica. |
| 6. ¿Existe cobertura wifi, en todas las áreas de la Unidad educativa "Rumiñahui"? | E1. Solo existe en el bloque principal el servicio de internet.<br>E2. Hasta los actuales momentos, sí tenemos cobertura wifi.<br>E3. Falta implementar en algunas áreas. | Actualmente existe cobertura wifi en la unidad educativa, pero si es necesario instalar mas puntos wifi. |
| 7. ¿Considera necesario la implementación de sirenas de auxilio en las áreas de la Unidad educativa "Rumiñahui"? | E1. Si<br>E2. Muy necesario e indispensable.<br>E3. Si | El uso de sirenas de auxilio es muy importante en la unidad educativa. |
| 8. ¿Se debería implementar cámaras de seguridad en las áreas de la Unidad educativa "Rumiñahui"? | E1. Si, en el bloque 2 principalmente.<br>E2. La implementación de cámaras es otro servicio que requiere nuestra Unidad Educativa.<br>E3. Claro que si. | El uso de cámaras de seguridad es muy importante en la unidad educativa. Hace falta instalar más cámaras. |

Fuente: Carolina Vélez (2024)

**Tabla 6: Análisis de las entrevistas aplicadas a las autoridades**

| Pregunta | Respuesta | Análisis |
|---|---|---|
| 9. ¿La clave wifi debe ser la misma para docentes y estudiantes? | E1. No. Los estudiantes no tienen acceso al internet, a excepción que sea desde el laboratorio de computación.<br>E2. Considero y desde mi punto de vista, debería ser una para estudiantes, otra para el personal docente.<br>E3. Debe ser diferente. | Las claves wifi deben ser segmentadas, para un buen funcionamiento del internet. |
| 10. ¿Se debería instalar un computador con internet y proyector en cada una de las aulas de clases? | E1. Claro que si<br>E2. Sería uno de los objetivos cristalizados para quienes tenemos la responsabilidad de llevar el proceso educativo con eficacia.<br>E3. Seria muy necesario. | Es necesario que en cada aula de clases, exista un computador, proyector y conexión a internet. |
| 11. ¿Con que frecuencia se realizan mantenimiento preventivo y correctivo de la infraestructura tecnológica? | E1. Cada año o al finalizar el año escolar.<br>E2. Cada año.<br>E3. Cuando es necesario. | Se realiza mantenimiento a la infraestructura tecnológica, pero este mantenimiento se lo debe realizar dos veces al año. |
| 12. ¿ Unidad educativa "Rumiñahui" cuenta con políticas y normas estandarizadas de control sobre el uso de la infraestructura tecnológica? | E1. Si, a través del manual para el uso del laboratorio.<br>E2. Si<br>E3. Desconozco. | Se debe socializar a la comunidad educativa las políticas y normas para el uso de la infraestructura tecnológica. |

Fuente: Carolina Vélez (2024)

### 3.6.3. Informe final del análisis de los datos

Primero, con relación a la pregunta 1, sobre la satisfacción con el laboratorio de informática, se evidencia que mientras el 40% de los estudiantes está satisfecho y un 18% completamente satisfecho, las autoridades consideran que hay equipos necesarios pero que falta mantenimiento, lo que afecta la experiencia general. La combinación de estas respuestas sugiere que, aunque hay una aceptación moderada del laboratorio, hay margen de mejora en términos de mantenimiento y actualización del equipo.

En cuanto a la pregunta 2, sobre la importancia del laboratorio de informática, un 39% de los estudiantes lo considera importante y un 23% completamente importante. Las autoridades coinciden, indicando que el laboratorio es indispensable para el desarrollo de asignaturas. Esta concordancia subraya la relevancia del laboratorio tanto para estudiantes como para docentes, y la necesidad de seguir invirtiendo en su mejora.

Sobre la pregunta 3, con relación a la frecuencia de uso del laboratorio, el 60% de los

estudiantes desean clases frecuentes en el laboratorio. Los docentes también expresan el deseo de impartir clases regularmente en el laboratorio, con algunos sugiriendo clases semanales. Esta alineación destaca una demanda común por un mayor uso del laboratorio en el proceso educativo diario.

En cuanto a la pregunta 4, sobre la dificultad en el uso de aplicaciones informáticas, un 37% de los estudiantes considera su uso muy importante para investigaciones y trabajos, mientras que las autoridades no reportan grandes dificultades en su uso, aunque algunos docentes mencionan la necesidad de auto-prepararse. Esto sugiere que, si bien las aplicaciones son valoradas, es crucial ofrecer más formación y soporte técnico para optimizar su utilización.

Respecto a la pregunta sobre el mantenimiento del laboratorio, el 41% de los estudiantes perciben un cuidado frecuente por parte de las autoridades. Las entrevistas confirman esta percepción, señalando que se realiza mantenimiento, aunque debería ser más frecuente. Esta coherencia resalta la necesidad de implementar un mantenimiento más regular y eficiente para asegurar el buen funcionamiento del laboratorio.

En la pregunta 6, en el tema de la cobertura wifi, un 36% de los estudiantes encuentra difícil conectarse a la red, mientras que las autoridades reconocen que la cobertura actual es limitada y sugieren la instalación de más puntos wifi. Esto indica una necesidad urgente de mejorar la infraestructura de red para facilitar el acceso a internet en toda la unidad educativa.

Por último, en la pregunta 7 y 8, en cuanto a la seguridad, tanto estudiantes como autoridades consideran importante la implementación de cámaras de seguridad y sirenas de auxilio en todas las áreas de la institución. Esto refleja una preocupación compartida por la seguridad y la necesidad de medidas adicionales para garantizar un ambiente seguro.

En resumen, el análisis del documento revela que hay una percepción general positiva respecto al laboratorio de informática, pero también subraya la necesidad de mejoras en mantenimiento, formación en el uso de aplicaciones, y la ampliación de la infraestructura de red y seguridad. Las opiniones de estudiantes y autoridades están alineadas en muchos aspectos, lo que proporciona una base sólida para planificar y ejecutar mejoras efectivas en la Unidad Educativa “Rumiñahui”.

# CAPITULO IV

## 4. MARCO PROPOSITIVO

### 4.1. Introducción

La parroquia Wilfrido Loor Moreira, conocida como “Maicito”, está ubicada en el cantón El Carmen, en la provincia de Manabí. Sus paisajes naturales y la calidez de su gente cautivan a todos los que la visitan, generando un ambiente acogedor. La belleza del lugar y la hospitalidad de los habitantes hacen que tanto turistas como residentes se sientan como en casa.

En los últimos años, la parroquia ha experimentado un crecimiento poblacional notable, lo que ha impulsado la construcción de nuevas infraestructuras. Este desarrollo ha atraído a nuevos habitantes, favoreciendo el dinamismo y progreso de la comunidad.

El Ministerio de Educación de Ecuador (MINEDUC) fundó la Unidad Educativa “Rumiñahui” en 1959 con el objetivo de proporcionar educación de calidad a los estudiantes de la zona. Desde su creación, la institución ha ampliado su oferta educativa, ofreciendo diversos niveles que incluyen inicial, básica elemental, básica media, básica superior y bachillerato con la especialidad en ciencias generales. En la actualidad, la unidad educativa cuenta con una matrícula de 625 estudiantes, quienes reciben formación académica integral para su desarrollo personal y profesional. Además, la institución cuenta con un equipo de 27 docentes y un departamento del DECE, encargado de brindar apoyo psicológico y orientaciones a los estudiantes.

Dentro de las políticas públicas impulsadas por el Ministerio de Educación de Ecuador, se destaca la implementación de infraestructura tecnológica en las instituciones educativas,

incluida la Unidad Educativa “Rumiñahui”. Esta iniciativa busca modernizar los procesos educativos y facilitar el acceso a herramientas digitales que enriquezcan la enseñanza y el aprendizaje. Gracias a estos avances, los estudiantes tienen la oportunidad de interactuar con recursos tecnológicos, desarrollando habilidades esenciales para su futura inserción en un mundo cada vez más digitalizado. La integración de tecnología también ha permitido mejorar la calidad educativa y optimizar los procesos administrativos de la institución.

En este contexto, las unidades educativas tienen la responsabilidad de gestionar de manera eficiente el cuidado y mantenimiento de la infraestructura tecnológica. Las autoridades de turno deben asegurarse de que se realicen intervenciones periódicas para garantizar el buen funcionamiento de los equipos, tanto de software como de hardware. Esto incluye la actualización constante de los sistemas operativos y programas utilizados, así como la reparación o reemplazo de cualquier componente dañado. Además, es crucial realizar copias de seguridad de toda la información almacenada en los dispositivos para prevenir pérdidas de datos en caso de fallos inesperados.

Las medidas de seguridad cibernética también juegan un papel fundamental en la protección de la infraestructura tecnológica. Las unidades educativas deben implementar protocolos para proteger los sistemas contra amenazas externas, como ataques cibernéticos o accesos no autorizados, lo que garantiza la privacidad y seguridad de la información de estudiantes, docentes y personal administrativo. Asegurando la continuidad y eficiencia operativa, estas acciones contribuyen al mantenimiento de un ambiente educativo seguro y actualizado, favoreciendo el uso adecuado de la tecnología como herramienta de aprendizaje y gestión dentro de la institución.

La Unidad Educativa “Rumiñahui” actualmente cuenta con dos laboratorios que se encuentran ubicados en el mismo espacio físico con un número de 40 computadoras. Los dos laboratorios se diferencias por la tecnología que permite el funcionamiento de los equipos, y características de estos.

Actualmente, la Unidad Educativa “Rumiñahui” enfrenta una seria deficiencia en la gestión y cuidado de sus laboratorios, ya que no cuenta con políticas, manuales ni normas

claras para el uso adecuado de los equipos y la infraestructura tecnológica. Esta falta de regulaciones específicas ha generado que los equipos se deterioren progresivamente, lo que afecta directamente el rendimiento y la calidad de los recursos educativos disponibles para los estudiantes. Sin una guía que oriente a los usuarios sobre el manejo adecuado de los laboratorios, es más probable que los equipos sufran daños irreparables, lo que limita las posibilidades de aprendizaje y el aprovechamiento de la tecnología disponible.

Además, la ausencia de un técnico especializado en la gestión y mantenimiento de los laboratorios agrava aún más la situación. No contar con una persona encargada de supervisar el buen funcionamiento de la infraestructura tecnológica de la institución dificulta la resolución de problemas técnicos y el mantenimiento preventivo de los equipos. Esto genera una dependencia de recursos externos cuando surgen inconvenientes, lo que retrasa las soluciones y provoca que la infraestructura quede obsoleta rápidamente. Es fundamental implementar una estructura de gestión tecnológica adecuada, con responsables específicos para cada área, con el fin de asegurar la continuidad y efectividad de los procesos educativos y tecnológicos en la institución.

Cuando surge la necesidad de soporte técnico en la Unidad Educativa "Rumiñahui", las autoridades de turno deben dirigirse al Distrito de Educación 13D05 para solicitar el apoyo necesario. Sin embargo, este proceso de solicitud puede resultar lento y, en ocasiones, el respaldo solicitado no es proporcionado de manera inmediata. Debido a la falta de personal técnico especializado dentro de la institución, la dependencia del apoyo externo se convierte en una barrera para abordar los problemas de manera eficiente. Como resultado, los equipos informáticos y la infraestructura tecnológica se deterioran aún más, afectando tanto a la calidad educativa como a la operatividad general de la institución.

Este retraso en la atención de las necesidades tecnológicas tiene repercusiones significativas en el funcionamiento del establecimiento. El tiempo que se tarda en recibir la ayuda técnica necesaria no solo impide que los estudiantes y docentes utilicen las herramientas tecnológicas en su totalidad, sino que también contribuye a la obsolescencia de los equipos. A medida que los problemas técnicos no se resuelven de forma oportuna, los recursos educativos se ven comprometidos, lo que afecta el ambiente de aprendizaje y limita las

oportunidades de formación para los estudiantes. Es crucial que la institución cuente con un sistema más ágil y eficiente de atención de soporte técnico, o bien con personal capacitado internamente que pueda garantizar el mantenimiento preventivo y la reparación de los equipos cuando sea necesario.

Con los antecedentes mencionados, la presente investigación adquiere relevancia al enfocarse en la necesidad urgente de realizar una Auditoría de Seguridad Informática a la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor Moreira. La falta de políticas y normas claras para el uso y cuidado de los laboratorios, sumado a la ausencia de soporte técnico adecuado y la dependencia de recursos externos, hace evidente la vulnerabilidad de los equipos y sistemas tecnológicos. Una auditoría exhaustiva permitirá identificar las debilidades y riesgos existentes en la infraestructura tecnológica, así como las áreas que requieren intervención para mejorar la seguridad y operatividad de los recursos.

La realización de esta auditoría es crucial no solo para evaluar el estado actual de la infraestructura, sino también para establecer estrategias de mejora y asegurar que los equipos sean gestionados de manera eficiente y segura. Además, el análisis permitirá detectar posibles amenazas cibernéticas y brechas de seguridad que podrían comprometer la protección de la información y el funcionamiento de los sistemas. A través de la auditoría, se podrán definir recomendaciones específicas para fortalecer la infraestructura tecnológica, desarrollar políticas y manuales de uso, y capacitar a los responsables en la gestión adecuada de los recursos, garantizando así un entorno seguro y funcional para el aprendizaje y la administración escolar.

### 4.2. Descripción de la propuesta

El propósito de este proyecto es desarrollar una auditoría detallada y efectiva que permita evaluar de manera integral la infraestructura tecnológica de la Unidad Educativa "Rumiñahui", ubicada en la parroquia Wilfrido Loor Moreira. Este análisis busca identificar fortalezas, debilidades y oportunidades de mejora en los recursos tecnológicos existentes, asegurando que estén alineados con las necesidades educativas y objetivos institucionales. Además, se pretende ofrecer recomendaciones prácticas para optimizar su uso y garantizar un entorno de aprendizaje más eficiente y moderno.

## 4.3. Determinación de recursos

### 4.3.1. Recursos Humanos

El uso eficiente y estratégico del recurso humano, combinado con el apoyo técnico y logístico adecuado, permitirá a la investigación agilizar significativamente los procesos necesarios para la mejora de la infraestructura, asegurando resultados más efectivos y alineados con los objetivos planteados.

Tabla 7: Recursos Humanos

| Cantidad | Recurso | Función | Actividad |
|---|---|---|---|
| 1 | Vélez Vélez Carolina Ibeth | Investigadora | Realizar el proyecto integrador |
| 1 | Mg. Manuel Solórzano | Rector | Entrevista sobre infraestructura tecnológica |
| 1 | Mg. Elita Vargas | Vice-Rector | Entrevista sobre infraestructura tecnológica |
| 1 | Lic. Holger Roger Zambrano Loor | Inspector | Entrevista sobre infraestructura tecnológica |
| 239 | Estudiantes | Uso de la infraestructura tecnológica | Realizar la encuesta |

Fuente: Elaboración propia 2024

### 4.3.2. Recursos tecnológicos

El uso eficiente del recurso tecnológico facilitará la identificación, gestión y recaudación de los equipos necesarios para llevar a cabo de manera efectiva la actividad propuesta dentro del proyecto, garantizando así el cumplimiento de los objetivos establecidos de forma óptima.

Tabla 8: Recursos Tecnológicos

| Cantidad | Recurso | Actividad |
|---|---|---|
| 1 | Computador portátil | Desarrolla el proyecto integrador |
| 1 | Impresora | Imprimir informes y proyecto |
| 1 | Celular | Comunicación |
| 1 | Microsoft Office | Realizar informes |
| 239 | Internet | Obtener información y comunicación |

Fuente: Elaboración propia 2024

### 4.3.3. Recursos Económicos

El uso adecuado de los recursos económicos permitirá adquirir los materiales necesarios para la realización del proyecto, satisfaciendo plenamente las necesidades de la institución y garantizando la impartición de las clases sin contratiempos ni interrupciones.

Tabla 9: Recursos Económicos

| Cantidad | Descripción | SubTotal | Total |
|---|---|---|---|
| 1 | Computador portatil | $800 | $800 |
| 1 | Impresora | $250 | $250 |
| 1 | Comunicación Datos | $22 | $88 |
| 1 | Resma de papel | $4 | $4 |
| 1 | Movilidad | $30 | $30 |
| TOTAL | | | **1.172** |

Fuente: Elaboración propia 2024

### 4.4. Etapas del desarrollo de la propuesta

La supervisión y gestión de la infraestructura tecnológica resultan esenciales para el progreso de la Unidad Educativa “Rumiñahui”, ubicada en la parroquia Wilfrido Loor Vera, constituyendo un pilar clave para su desarrollo sostenible. Este proceso requiere la colaboración activa de autoridades, docentes y estudiantes, quienes desempeñan un papel fundamental al facilitar la evaluación y cumplimiento de los objetivos establecidos dentro de lo planificado, garantizando así un entorno educativo óptimo y alineado con las necesidades actuales.

#### 4.4.1. Datos Informativos

##### 4.4.1.1. Datos Generales

| | |
|---|---|
| Institución | UNIDAD EDUCATIVA “RUMIÑAHUI” |
| Código AMIE | 13H01422 |
| Zona: | 4 |
| Distrito: | 13D01 |
| Provincia: | Manabí |
| Lugar: | Parroquia Wilfrido Loor |
| Niveles de educación: | Básica elemental, media y superior, bachillerato |
| Número de autoridades: | 3 |
| Número de estudiantes: | 625 |

##### 4.4.1.2. Misión

La Unidad Educativa "Rumiñahui" tiene como misión brindar una educación de calidad, inclusiva y equitativa que fomente el desarrollo integral de los estudiantes. A través de una enseñanza innovadora y centrada en valores, buscamos formar personas con competencias académicas sólidas, conciencia ambiental y compromiso social, preparadas para

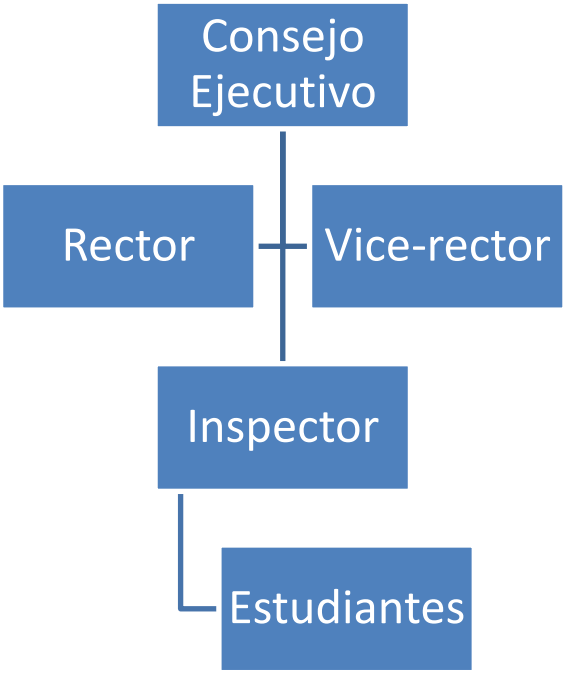
enfrentar los retos del mundo actual y contribuir activamente al bienestar de su comunidad.

#### 4.4.1.3. Visión

La Unidad Educativa "Rumiñahui" se proyecta como una institución líder en la formación integral de estudiantes, comprometida con el desarrollo de competencias académicas, tecnológicas y humanas. Buscamos formar ciudadanos críticos, responsables y comprometidos con el progreso de su comunidad y del país, promoviendo valores de equidad, respeto y sostenibilidad en un ambiente inclusivo y participativo.

#### 4.4.1.4. Organigrama

Ilustración 2: Organigrama Unidad Educativa “Rumiñahui”




Fuente: Elaboración propia 2024

### 4.4.2. Programa de Auditoría Informática

#### 4.4.2.1. Planificación

Tabla 10: Programa de auditoria

| **PROGRAMA DE: AUDITORIA DE SEGURIDAD INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LA UNIDAD EDUCATIVA "RUMIÑAHUI" DE LA PARROQUIA WILFRIDO LOOR** | | |
|---|---|---|
| **Objetivo General:** Realizar una auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor.<br>**Objetivos Específicos:**<br>• Evaluar la infraestructura tecnológica de la Unidad Educativa "Rumiñahui".<br>• Analizar las amenazas, riesgos y vulnerabilidades de la infraestructura tecnológica de la Unidad Educativa "Rumiñahui". | | |
| **TECNICAS Y PROCEDIMIENTOS** | **DESCRIPCIÒN** | **FECHAS** |
| 1.Fundamentar teóricamente sobre auditoria de seguridad informática, y metodología MAGERIT. | PDT1 | 10/07/2024 |
| 2.Analizar las técnicas de recolección de datos: encuesta y entrevista. | PDT2 | 10/08/2024 |
| VALOR ACTIVOS<br>3.Analizar la ficha de observación, sobre la infraestructura tecnológica. | PDT3 | 20/08/2024 |
| DEFINIR Y VALOR DE ACTIVOS<br>4.Analizar los riesgos, amenazas y vulnerabilidades de la infraestructura tecnológica. | PDT4 | 02/09/2024 |
| ELABORACIÓN DE INSTRUMENTOS PARA ANALIZAR RIESGOS<br>5.Elaborar informe de los resultados obtenidos. | PDT5 | 15/09/2024 |
| APLICACIÓN DE LA AUDITORIA<br>6.Elaborar guía para el adecuado uso de la infraestructura tecnológica. | PDT6 | 25/09/2024 |
| 7.Presentar conclusiones y recomendaciones de la auditoria de seguridad informática. | PDT7 | 05/10/2024 |
| Realizado por: Carolina Vélez<br>Fecha: Octubre del 2024 | | |

Fuente: elaboración propia 2024

**PDT1 = Auditoría de seguridad informática y metodología MAGERIT:** La auditoría de seguridad informática evalúa los sistemas, redes y recursos tecnológicos para identificar posibles riesgos y vulnerabilidades. La metodología MAGERIT se enfoca en la gestión de riesgos, proporcionando un marco estructurado para evaluar y proteger los activos de información a través de un análisis detallado de sus recursos.

**PDT2 = Técnicas de recolección de datos:** encuesta y entrevista: Las encuestas son herramientas estructuradas que recopilan información cuantitativa de una amplia muestra de personas, mientras que las entrevistas son más cualitativas y personalizadas, permitiendo obtener datos más profundos y detallados. Ambas son esenciales para la recolección de datos en investigaciones o auditorías.

**PDT3 = Ficha de observación sobre la infraestructura tecnológica:** La ficha de observación es una herramienta utilizada para registrar detalladamente las condiciones y características de la infraestructura tecnológica. Permite evaluar equipos, redes y sistemas, proporcionando información clave sobre el estado físico y operativo de los recursos tecnológicos, ayudando en la identificación de posibles áreas de mejora.

**PDT4 =** n Los riesgos son posibles eventos que pueden afectar negativamente la infraestructura tecnológica, mientras que las amenazas son factores que pueden explotar esas debilidades. Las vulnerabilidades son fallos o debilidades en los sistemas que pueden ser aprovechados por las amenazas. Identificar estos elementos es crucial para la protección de los activos.

**PDT5 = Elaboración del informe de resultados obtenidos:** El informe de resultados resume los hallazgos obtenidos a través de una auditoría o investigación, proporcionando una visión clara de los problemas, soluciones y áreas de mejora. Debe ser preciso, estructurado y ofrecer recomendaciones basadas en los datos y análisis previos.

**PDT6 = Guía para el adecuado uso de la infraestructura tecnológica:** Una guía para el uso adecuado de la infraestructura tecnológica proporciona recomendaciones y normas

que los usuarios deben seguir para optimizar el uso de los recursos tecnológicos. Abarca desde la correcta manipulación de equipos hasta el cumplimiento de protocolos de seguridad, promoviendo eficiencia y protección.

**PDT7 = Conclusiones y recomendaciones de la auditoría de seguridad informática**: Las conclusiones de una auditoría de seguridad informática sintetizan los hallazgos clave sobre el estado de los sistemas, identificando riesgos y debilidades. Las recomendaciones están orientadas a mitigar estos riesgos, mejorar la seguridad y optimizar los procesos tecnológicos, con el fin de fortalecer la infraestructura tecnológica.

#### 4.4.2.2. Normas de Seguridad

##### 4.4.2.2.1. ISO 27001

La ISO 27001 es un estándar internacional que proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger la información asegurando su confidencialidad, integridad y disponibilidad, minimizando riesgos y gestionando amenazas. Este estándar es útil para organizaciones que buscan garantizar la seguridad de sus datos, cumplir con regulaciones y generar confianza en clientes y socios (ISO. 2022).

### 4.4.3. Metodología MAGERIT

Para la realización de la auditoría de seguridad informática, se utilizó la metodología MAGERIT. Esta metodología, ampliamente reconocida en el ámbito de la gestión de riesgos de sistemas de información, ofrece un enfoque estructurado para identificar, analizar y gestionar los riesgos que pueden afectar a los activos de una organización. En este orden de ideas, se menciona a Guamán et al. (2023), donde se señala que la metodología MAGERIT sirve para identificar y categorizar las amenazas, vulnerabilidades y riesgos. Esto implica un proceso detallado de evaluación en el que se clasifican los activos críticos en las diferentes áreas de la organización, permitiendo priorizar aquellos elementos que requieren mayor protección. La categorización de amenazas se realiza considerando su origen, lo que incluye errores de usuarios, fallos técnicos, ataques deliberados, desastres naturales, entre otros factores.

La implementación de MAGERIT en una auditoría de seguridad informática permite establecer un marco sólido para la toma de decisiones relacionadas con la gestión de riesgos. Esta metodología no solo identifica los riesgos existentes, sino que también facilita el diseño de controles y medidas preventivas para mitigar dichos riesgos. Según Guamán et al. (2023), uno de los aspectos más relevantes de MAGERIT es su capacidad para proporcionar una visión integral de los riesgos al considerar tanto los aspectos técnicos como los organizativos. Esto asegura que la organización no solo se enfoque en soluciones tecnológicas, sino también en mejorar sus procesos y procedimientos internos.

Además, MAGERIT promueve la documentación y el análisis continuo de los riesgos, lo que permite a las organizaciones adaptarse a nuevos desafíos y amenazas emergentes. La flexibilidad de esta metodología la hace aplicable a diversos entornos empresariales, independientemente de su tamaño o sector. Por ejemplo, en organizaciones grandes, MAGERIT puede ayudar a coordinar esfuerzos entre diferentes departamentos, mientras que en empresas más pequeñas puede guiar la implementación de medidas básicas de seguridad. Esto demuestra la versatilidad y efectividad de MAGERIT como herramienta clave en la gestión de riesgos de seguridad informática.

Otro aspecto relevante es que MAGERIT facilita la comunicación de los riesgos identificados a todos los niveles de la organización. Esto es fundamental para crear una cultura organizacional orientada a la seguridad y la prevención. Al involucrar a diferentes actores en el proceso de gestión de riesgos, se logra un compromiso colectivo que fortalece la protección de los activos críticos. De acuerdo con Guamán et al. (2023), esta participación activa es esencial para el éxito de cualquier estrategia de seguridad, ya que la seguridad informática no solo depende de los sistemas tecnológicos, sino también del comportamiento y la conciencia del personal.

En conclusión, la aplicación de la metodología MAGERIT en la auditoría de seguridad informática proporciona un enfoque integral y sistemático para identificar, evaluar y gestionar los riesgos. Su capacidad para clasificar amenazas según su origen y priorizar activos críticos contribuye a una gestión de riesgos más efectiva. Además, al fomentar la participación organizacional y la mejora continua, MAGERIT se consolida como una herramienta

indispensable para fortalecer la seguridad informática en cualquier tipo de organización.

### 4.4.4. Aplicación de la metodología MAGERIT

#### 4.4.4.1. Valor Activos

La ficha proporcionada permite evaluar y estimar los valores de impacto sobre los recursos establecidos, facilitando así la identificación de áreas críticas y la priorización de acciones. Para esto, se utiliza un sistema de semaforización que asigna un valor de impacto a cada recurso según un esquema de colores. El valor más bajo se representa con el color verde (1), lo que indica un impacto mínimo, mientras que el color rojo (3) señala el mayor impacto. El color amarillo (2) se utiliza para representar un impacto medio, indicando que se deben considerar medidas de mitigación.

Este sistema de semaforización es útil para gestionar los recursos de manera eficiente, ya que permite visualizar rápidamente las áreas que requieren atención urgente y aquellas que no presentan problemas inmediatos. Además, facilita la toma de decisiones estratégicas al proporcionar un marco visual claro para evaluar el impacto de diferentes factores sobre los recursos, optimizando así el tiempo y los recursos disponibles para implementar soluciones y acciones correctivas.

**Tabla 11: Valor de activos**

| No | IDENTIFICADOR DE RIESGO | IMPACTO | COLOR |
|---|---|---|---|
| 1 | 1 | Bajo | |
| 2 | 2 | Medio | |
| 3 | 3 | Alto | |

Fuente: elaboración propia 2024

### 4.4.4.2. Definir y valor de activos

**Tabla 12: Evaluación de riesgo**

| Infraestructura tecnológica de la Unidad Educativa "Rumiñahui" | | | | | | |
|---|---|---|---|---|---|---|
| **No** | **Nombre** | **Disponibilidad** | **Integridad** | **Seguridad** | **Autenticidad** | **Riesgo** |
| | | **Se puede usar el recurso** | **Correcto funcionamiento** | **Normas de seguridad** | **Información real** | **MAGERIT Riesgo Amenaza vulnerabilidad** |
| R1 | CPU Normal | 1 | 1 | 2 | 1 | 2 |
| | Monitor | 1 | 1 | 2 | 1 | 2 |
| | Teclado | 1 | 2 | 2 | 1 | 2 |
| | Mouse | 1 | 1 | 2 | 1 | 2 |
| R1(2) | CPU Concentrado | 2 | 2 | 2 | 2 | 3 |
| | Monitor | 1 | 1 | 2 | 1 | 2 |
| | Teclado | 1 | 2 | 2 | 2 | 2 |
| | Mouse | 2 | 2 | 2 | 2 | 2 |
| R2 | Impresora | 1 | 2 | 2 | 2 | 2 |
| | Escáner | 3 | 3 | 3 | 3 | 3 |
| | Proyector | 1 | 1 | 3 | 1 | 2 |
| R3 | Memorias USB | 1 | 1 | 1 | 1 | 1 |
| R4 | Router | 1 | 1 | 2 | 1 | 2 |
| | Switch | 1 | 1 | 2 | 2 | 2 |
| | Estructura de red | 1 | 2 | 2 | 2 | 2 |
| R5 | Sistemas Operativos | 1 | 2 | 2 | 2 | 2 |
| R6 | Programas de Office | 1 | 1 | 2 | 1 | 2 |
| | Utilitarios | 1 | 1 | 2 | 1 | 2 |
| | Aplicaciones informáticas | 1 | 1 | 2 | 1 | 2 |
| | Antivirus | 3 | 3 | 3 | 3 | 3 |
| | Navegadores | 1 | 1 | 2 | 1 | 2 |
| | Buscadores | 1 | 1 | 2 | 1 | 2 |

Fuente: elaboración propia 2024

**Tabla 13: Evaluación de riesgo**

| Infraestructura tecnológica de la Unidad Educativa "Rumiñahui" | | | | | | |
|---|---|---|---|---|---|---|
| **No** | **Nombre** | **Disponibilidad** | **Integridad** | **Seguridad** | **Autenticidad** | **Riesgo** |
| | | **Se puede usar el recurso** | **Correcto funcionamiento** | **Normas de seguridad** | **Información real** | **MAGERIT Riesgo Amenaza vulnerabilidad** |
| R7 | Mesas | 1 | 1 | 1 | 1 | 1 |
| | Sillas | 1 | 1 | 1 | 1 | 1 |
| R8 | Instalaciones físicas | 1 | 2 | 2 | 2 | 2 |
| R9 | Cableado | 1 | 1 | 2 | 1 | 2 |
| | Tomacorrientes | 1 | 1 | 2 | 1 | 2 |
| | Ups | 2 | 2 | 2 | 2 | 2 |
| | Breaker | 1 | 1 | 2 | 1 | 2 |
| | Interruptores | 1 | 1 | 2 | 1 | 2 |
| R10 | Aire acondicionado | 3 | 3 | 3 | 3 | 3 |
| | Ventiladores | 2 | 2 | 2 | 2 | 2 |
| R11 | Cámaras de Videovigilancia | 1 | 1 | 2 | 1 | 2 |
| R12 | Sirenas de auxilio | 1 | 1 | 2 | 1 | 2 |

Fuente: elaboración propia 2024

#### 4.4.4.3. Elaboración de instrumentos para analizar riesgos

Para llevar a cabo la presente auditoría de seguridad informática, se utilizó un enfoque de investigación cualitativo y cuantitativo. Se emplearon técnicas como entrevistas y encuestas para recopilar datos sobre el uso de la infraestructura tecnológica en la Unidad Educativa "Rumiñahui". Al aplicar estas técnicas y sus respectivos instrumentos, se pudo determinar que, aunque la institución cuenta con infraestructura tecnológica, es necesario implementar un plan de mejora para optimizar su rendimiento y seguridad, garantizando así un entorno educativo más seguro y eficiente.

En este sentido, se señala que la infraestructura tecnológica de la institución incluye un laboratorio de informática, oficinas administrativas, aulas equipadas con computadoras, proyectores y conexión a internet. Además, se dispone de antenas wifi en diversas áreas. Sin embargo, se destaca la necesidad de implementar un plan de mejora que optimice todos estos recursos, asegurando un funcionamiento más eficiente y acorde con las necesidades actuales de la Unidad Educativa "Rumiñahui".

A través de las entrevistas y encuestas realizadas, se recopilaron opiniones y percepciones tanto de los docentes como de los estudiantes sobre el uso de la infraestructura tecnológica, lo que permitió obtener una visión clara de las fortalezas y debilidades de los sistemas actuales. Los resultados de estos instrumentos revelaron que, aunque la infraestructura está en uso frecuente, existen varios aspectos que requieren atención, tales como la seguridad de los equipos, la capacitación del personal en el manejo adecuado de la tecnología y la actualización de algunos dispositivos.

Además de los aspectos técnicos, la investigación también permitió identificar que la formación en seguridad informática es una necesidad urgente dentro de la institución. La mayoría de los usuarios no están completamente informados sobre las mejores prácticas de seguridad, lo que aumenta el riesgo de incidentes cibernéticos. Por lo tanto, se recomienda desarrollar un programa de concientización y capacitación en seguridad informática para docentes y estudiantes, con el fin de garantizar que todos los miembros de la comunidad educativa comprendan la importancia de proteger los recursos tecnológicos y la información.

#### 4.4.4.3.1. Formato entrevista aplicada a las autoridades

**Tabla 14: Formato Entrevista aplicada a las autoridades**

| **Preguntas** |
|---|
| 1. ¿Qué tan satisfecho está con la experiencia en el laboratorio de informática de la Unidad educativa “Rumiñahui”? |
| 2. ¿Qué tan importante considera que es el laboratorio de informática para los estudiantes y docentes? |
| 3. ¿Con que frecuencia le gustaría dar clases en el laboratorio de informática? |
| 4. ¿Qué tan difícil se le hace utilizar las aplicaciones informáticas para dar clases? |
| 5. ¿Las autoridades cuidan el buen funcionamiento del laboratorio de informática de la Unidad educativa “Rumiñahui”? |
| 6. ¿Existe cobertura wifi, en todas las áreas de la Unidad educativa “Rumiñahui”? |
| 7. ¿Considera necesario la implementación de sirenas de auxilio en las áreas de la Unidad educativa “Rumiñahui”? |
| 8. ¿Se debería implementar cámaras de seguridad en las áreas de la Unidad educativa “Rumiñahui”? |
| 9. ¿La clave wifi debe ser la misma para docentes y estudiantes? |
| 10. ¿Se debería instalar un computador con internet y proyector en cada una de las aulas de clases? |
| 11: ¿Con que frecuencia se realizan mantenimiento preventivo y correctivo de la infraestructura tecnológica? |
| 12.¿ Unidad educativa “Rumiñahui” cuenta con políticas y normas estandarizadas de control sobre el uso de la infraestructura tecnológica? |

Fuente: Elaboración propia 2024

#### 4.4.4.3.2. Formato encuesta aplicada a los estudiantes

Tabla 15: Formato encuesta aplicada a estudiantes

| Pregunta | Respuesta |
|---|---|
| 1. ¿Qué tan satisfecho está con la experiencia en el laboratorio de informática de la Unidad educativa “Rumiñahui”? | Completamente satisfecho<br>Muy satisfecho<br>Satisfecho<br>Poco satisfecho<br>Nada satisfecho |
| 2. ¿Qué tan importante considera que es el laboratorio de informática para los estudiantes? | Completamente importante<br>Muy importante<br>Importante, Poco importante<br>Nada importante |
| 3. ¿Con que frecuencia le gustaría recibir clases en el laboratorio de informática? | Completamente frecuente<br>Muy frecuente<br>frecuente<br>Poco frecuente<br>Nada frecuente |
| 4. ¿Cómo considera el uso de las aplicaciones informáticas para realizar tus investigaciones o trabajos? | Completamente importante<br>Muy importante<br>Importante<br>Poco importante<br>Nada importante |
| 5. ¿Las autoridades cuidan el buen funcionamiento del laboratorio de informática de la Unidad educativa “Rumiñahui”? | Completamente frecuente<br>Muy frecuente<br>frecuente<br>Poco frecuente<br>Nada frecuente |
| 6. ¿Qué tan importante consideras el uso de cámaras de seguridad en todas las áreas de la Unidad educativa “Rumiñahui”? | Completamente importante<br>Muy importante<br>Importante<br>Poco importante<br>Nada importante |
| 7. ¿Qué tan difícil se te hace conectarte a una red wifi en la Unidad educativa “Rumiñahui”? | Completamente difícil<br>Muy difícil<br>Difícil<br>Poco difícil<br>Nada difícil |
| 8. ¿Qué tan importante considera la implementación de puntos wifi en todas las áreas de la Unidad educativa “Rumiñahui”? | Completamente importante<br>Muy importante<br>Importante<br>Poco importante<br>Nada importante |
| 9. ¿Qué tan importante consideras la implementación de sirenas de auxilio en todas las áreas de la Unidad educativa “Rumiñahui”? | Completamente importante<br>Muy importante<br>Importante<br>Poco importante<br>Nada importante |

Fuente: Elaboración propia 2024

### 4.4.4.3.3. Formato ficha de observación 1

Ilustración 3: Formato 1 - ficha de levantamiento de información in situ

| NOMBRE DEL DOCUMENTO | IDENTIFICACIÓN: | |
|---|---|---|
| FICHA DE LEVANTAMIENTO DE INFORMACION IN SITU | CV-001-2024 | |
| **PROCEDIMIENTO:** | ESTUDIO DE CAMPO | |
| AREA INFORMÁTICA | AUDITORIA INFORMÁTICA | |

| **PERIODO ACADÉMICO 2024(2)** | | | |
|---|---|---|---|
| **ENTIDAD:** | | **HORA:** | |
| **AUDITOR:** | | **FECHA:** | |

**FICHA DE LEVANTAMIENTO DE INFORMACIÓN HARDWARE Y SOFTWARE IN SITU**

**INFORMACIÓN VISUAL**

| **IDENTIFICACIÓN DEL EQUIPO:** | **USUARIO:** | **FECHA:** |
|---|---|---|

**ELEMENTOS HARDWARE:**

| | | | |
|---|---|---|---|
| Periférico 1: | Serial: | Marca: | Observación: |
| Periférico 2: | Serial: | Marca: | Observación: |
| Periférico 3: | Serial: | Marca: | Observación: |
| Periférico 4: | Serial: | Marca: | Observación: |
| Periférico 5: | Serial: | Marca: | Observación: |

**ELEMENTOS SOFTWARE:**

| | | | |
|---|---|---|---|
| Sistema Operativo: | Versión: | Estado: | Clave: |
| Programa/Paquete: | Versión: | Estado: | Clave: |
| Utilitarios: | Versión: | Estado: | Clave: |
| Software 1: | Versión: | Estado: | Clave: |
| Software 2: | Versión: | Estado: | Clave: |
| Software 3: | Versión: | Estado: | Clave: |
| Software 4: | Versión: | Estado: | Clave: |

Vulnerabilidad: _____

**CONECTIVIDAD:**

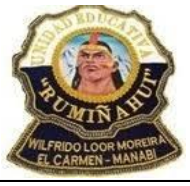
| | | | | | |
|---|---|---|---|---|---|
| Tipo de Conexión Internet: | Cable: | | Switch | Velocidad de Conexión: | Subida: |
| | Inalambrica: | | Router | | Bajada: |
| | Mixta: | | | | |
| | | | | | Subida: |
| Distancia del punto de acceso inalambrico: | | | | | Bajada: |

**OBSERVACIONES:**

Fuente: Elaboración propia 2024

### 4.4.4.3.4. Formato ficha de observación 2

Ilustración 4: Formato 2 - ficha de levantamiento de información in situ

| NOMBRE DEL DOCUMENTO | IDENTIFICACIÓN: |  |
|---|---|---|
| FICHA DE LEVANTAMIENTO DE INFORMACION IN SITU | CV-002-2024 | |
| **PROCEDIMIENTO:** | ESTUDIO DE CAMPO | |
| AREA INFORMÁTICA | AUDITORIA INFORMÁTICA | |

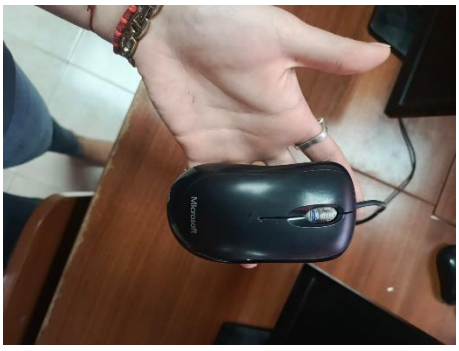
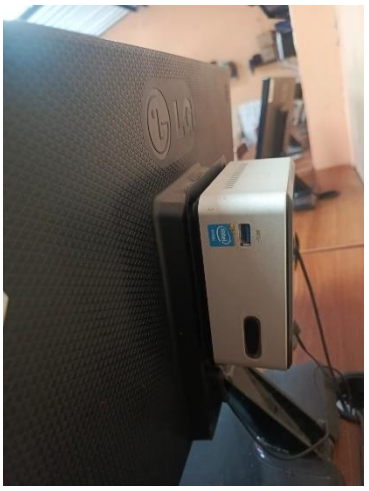


| **PERIODO ACADÉMICO 2024(2)** | | | |
|---|---|---|---|
| **ENTIDAD:** | | **HORA:** | |
| **AUDITOR:** | | **FECHA:** | |

| **FICHA DE LEVANTAMIENTO DE INFORMACIÓN DE INSTALACIONES IN SITU** |
|---|
| **INFORMACIÓN VISUAL** |
| **LUGAR:** |
| **INSTALACIONES**<br>1. Los muebles y enseres se encuentran: |
| 2. La distribución de los PC se encuentran: |
| 3. Las instalaciones de Red Eléctrica se encuentran: |
| 4. Las instalaciones de Red de Datos se encuentran: |
| 5. La ventilación e iluminación se encuentra: |
| 6. La seguridad se encuentra: |
| **HARDWARE**<br>1. Los equipos PC están bien identificados (Sellos, etiquetas, entre otros):<br><br>2. El estado físico de los (PC) se encuentran: |
| CRITERIO PREVIO AL INFORME DE AUDITORIA: |

Fuente: Elaboración propia 2024

### 4.4.4.4. Aplicación de la Auditoria

<table>
<tr>
<td>  </td>
<td>  </td>
</tr>
<tr>
<td>  </td>
<td>  </td>
</tr>
<tr>
<td>  </td>
<td>  </td>
</tr>
</table>

| NOMBRE DEL DOCUMENTO | IDENTIFICACIÓN: |
|---|---|
| FICHA DE LEVANTAMIENTO DE INFORMACION IN SITU | CV-001-2024 |
| PROCEDIMIENTO: | ESTUDIO DE CAMPO |
| AREA INFORMÁTICA | AUDITORIA INFORMÁTICA |

PERIODO ACADÉMICO 2024(2)

| ENTIDAD: | | HORA: | |
|---|---|---|---|
| AUDITOR: | | FECHA: | |

**FICHA DE LEVANTAMIENTO DE INFORMACIÓN HARDWARE Y SOFTWARE IN SITU**

**INFORMACIÓN VISUAL**

**IDENTIFICACIÓN DEL EQUIPO:** CPUUER01 **USUARIO:** CV **FECHA:** 30 OCTUBRE

**ELEMENTOS HARDWARE:**

| | | | |
|---|---|---|---|
| Periférico 1: CPU | Serial: CPU17833 | Marca: | Observación: REGULAR |
| Periférico 2: | Serial: | Marca: | Observación: |
| Periférico 3: | Serial: | Marca: HP | Observación: |
| Periférico 4: | Serial: | Marca: | Observación: |
| Periférico 5: | Serial: | Marca: | Observación: |

**ELEMENTOS SOFTWARE:**

| | | | | | |
|---|---|---|---|---|---|
| Sistema Operativo: WINDOWS | Versión: 10 | Estado: REGULAR | Clave: |
| Programa/Paquete: OFFICCE | Versión: 2016 | Estado: REGULAR | Clave: |
| Utilitarios: | Versión: | Estado: | Clave: |
| Software 1: ANTIVIRUS | Versión: NORTHON | Estado: | Clave: |
| Software 2: | Versión: | Estado: | Clave: |
| Software 3: | Versión: | Estado: | Clave: |
| Software 4: | Versión: | Estado: | Clave: |

Vulnerabilidad: _____

**CONECTIVIDAD:**

| | | | | | | |
|---|---|---|---|---|---|---|
| Tipo de Conexión Internet: | Cable: | X | Switch | Velocidad de Conexión: | Subida: | |
| | Inalambrica: | | Router | | Bajada: | |
| | Mixta: | | | | | |
| | | | | | Subida: | |
| Distancia del punto de acceso inalambrico: | | 0 | | | Bajada: | |

**OBSERVACIONES:** 2010

COMPUTADOR EN MAL ESTADO, SIN LICENCIA EN EL SISTEMA OPERATIVO Y OFFICE

| Elemento Hardware | Valoración de riesgo | Identificador de riesgo | Impacto | Color |
|---|---|---|---|---|
| CPU-UER01 | | 1 | Bajo | |
| | X | 2 | Medio | |
| | | 3 | Alto | |

| NOMBRE DEL DOCUMENTO | IDENTIFICACIÓN: |
|---|---|
| FICHA DE LEVANTAMIENTO DE INFORMACION IN SITU | CV-001-2024 |
| PROCEDIMIENTO: | ESTUDIO DE CAMPO |
| AREA INFORMÁTICA | AUDITORIA INFORMÁTICA |

**PERIODO ACADÉMICO 2024(2)**

| | | | |
|---|---|---|---|
| **ENTIDAD:** | | **HORA:** | |
| **AUDITOR:** | | **FECHA:** | |

**FICHA DE LEVANTAMIENTO DE INFORMACIÓN HARDWARE Y SOFTWARE IN SITU**

**INFORMACIÓN VISUAL**

| | | |
|---|---|---|
| **IDENTIFICACIÓN DEL EQUIPO:** CPUUER02 | **USUARIO:** CV | **FECHA:** 30 OCTUBRE |

**ELEMENTOS HARDWARE:**

| | | | |
|---|---|---|---|
| Periférico 1: CPU | Serial: CPU17833 | Marca: | Observación: REGULAR |
| Periférico 2: | Serial: | Marca: | Observación: |
| Periférico 3: | Serial: | Marca: HP | Observación: |
| Periférico 4: | Serial: | Marca: | Observación: |
| Periférico 5: | Serial: | Marca: | Observación: |

**ELEMENTOS SOFTWARE:**

| | | | | | |
|---|---|---|---|---|---|
| Sistema Operativo: WINDOWS | Versión: 10 | Estado: REGULAR | Clave: |
| Programa/Paquete: OFFICCE | Versión: 2016 | Estado: REGULAR | Clave: |
| Utilitarios: | Versión: | Estado: | Clave: |
| Software 1: ANTIVIRUS | Versión: NORTHON | Estado: | Clave: |
| Software 2: | Versión: | Estado: | Clave: |
| Software 3: | Versión: | Estado: | Clave: |
| Software 4: | Versión: | Estado: | Clave: |

Vulnerabilidad: _____

**CONECTIVIDAD:**

| | | | | | | |
|---|---|---|---|---|---|---|
| Tipo de Conexión Internet: | Cable: | X | Switch | Velocidad de Conexión: | Subida: | |
| | Inalambrica: | | Router | | Bajada: | |
| | Mixta: | | | | | |
| | | | | | Subida: | |
| Distancia del punto de acceso inalambrico: | | 0 | | | Bajada: | |

**OBSERVACIONES:** 2010

COMPUTADOR EN MAL ESTADO, SIN LICENCIA EN EL SISTEMA OPERATIVO Y OFFICE

| Elemento Hardware | Valoración de riesgo | Identificador de riesgo | Impacto | Color |
|---|---|---|---|---|
| **CPU-UER02** | | 1 | Bajo | |
| | **X** | 2 | Medio | |
| | | 3 | Alto | |

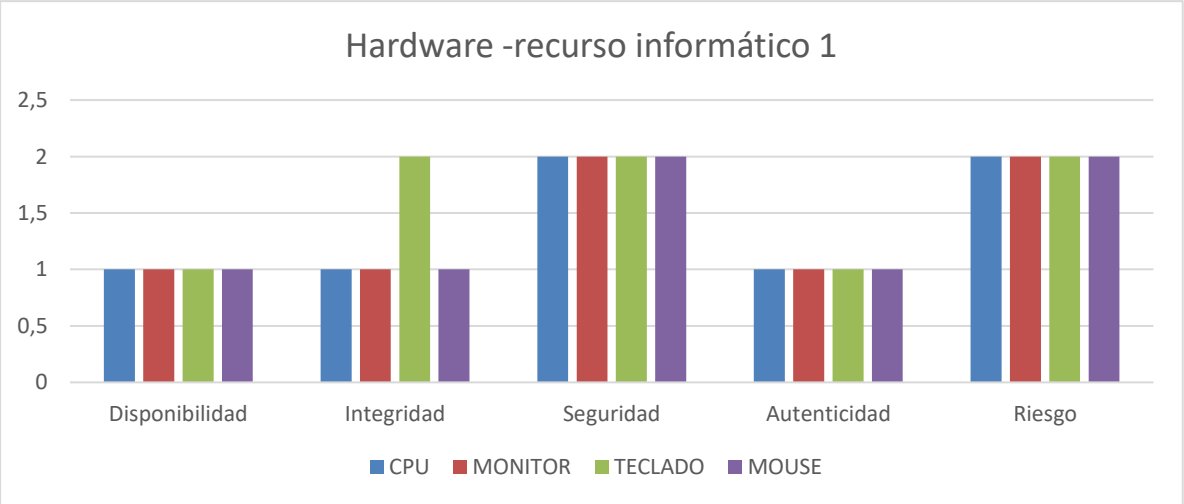
#### 4.4.4.4.1. Análisis de riesgos, amenazas y vulnerabilidades que está expuesta la infraestructura tecnológica de la Unidad Educativa "Rumiñahui"

Mediante la ejecución de la metodología MAGERIT, se identificó los riesgos, amenazas y vulnerabilidades, que están presentes en la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" de la parroquia Wilfrido Loor. En este contexto, se muestran los resultados conseguidos mediante la observación in sitio, de los recursos hardware, software del laboratorio, instrumentos tecnológicos de las aulas, sistema de video vigilancia y alarmas de auxilio, implementadas en diferentes espacios de la Unidad Educativa.

A continuación, se presentan los resultados por cada uno de los recursos valorados según la metodología MAGERIT.

**RECURSO 1 (Computadoras de escritorio – normales)**

Ilustración 5: Gráfico, valoración del recurso 1, equipamiento informático 1




Elaborado: Fuente propia de información 2024

Análisis del RECURSO 1: Hardware – Equipamiento tecnológico

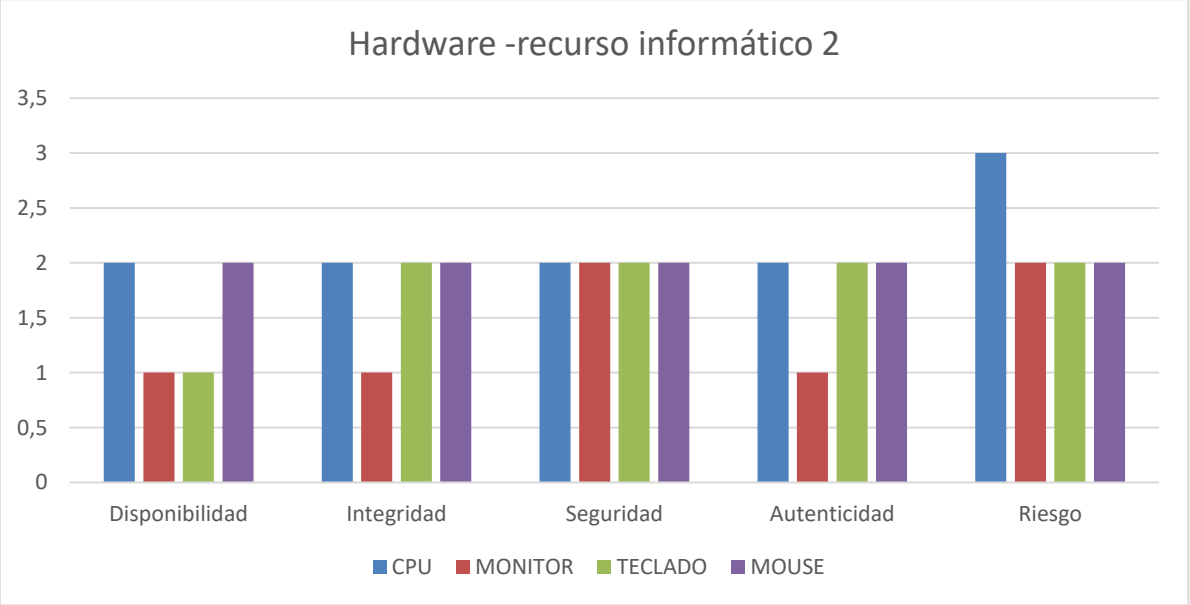
El equipamiento tecnológico, compuesto por CPU, monitores, teclados y mouse, es fundamental para el funcionamiento de cualquier organización. Según la metodología

MAGERIT, estos activos tienen una valoración de 2, lo que indica que están expuestos a posibles daños que pueden afectar su operatividad. Esta clasificación resalta la importancia de implementar medidas de seguridad que protejan estos dispositivos ante riesgos físicos o fallos técnicos.

Para mitigar estos riesgos, se recomienda realizar mantenimiento preventivo al menos dos veces al año. Esta práctica permite detectar fallas a tiempo, prolongar la vida útil de los equipos y garantizar un rendimiento óptimo. Además, es esencial establecer protocolos de seguridad física y digital que protejan el hardware frente a posibles amenazas externas, contribuyendo así a la continuidad operativa de la organización.

**RECURSO 1 (Computadoras de escritorio – CPU concentrados)**

Ilustración 6: Gráfico, valoración del recurso 1, equipamiento informático 2




Elaborado: Fuente propia de información 2024

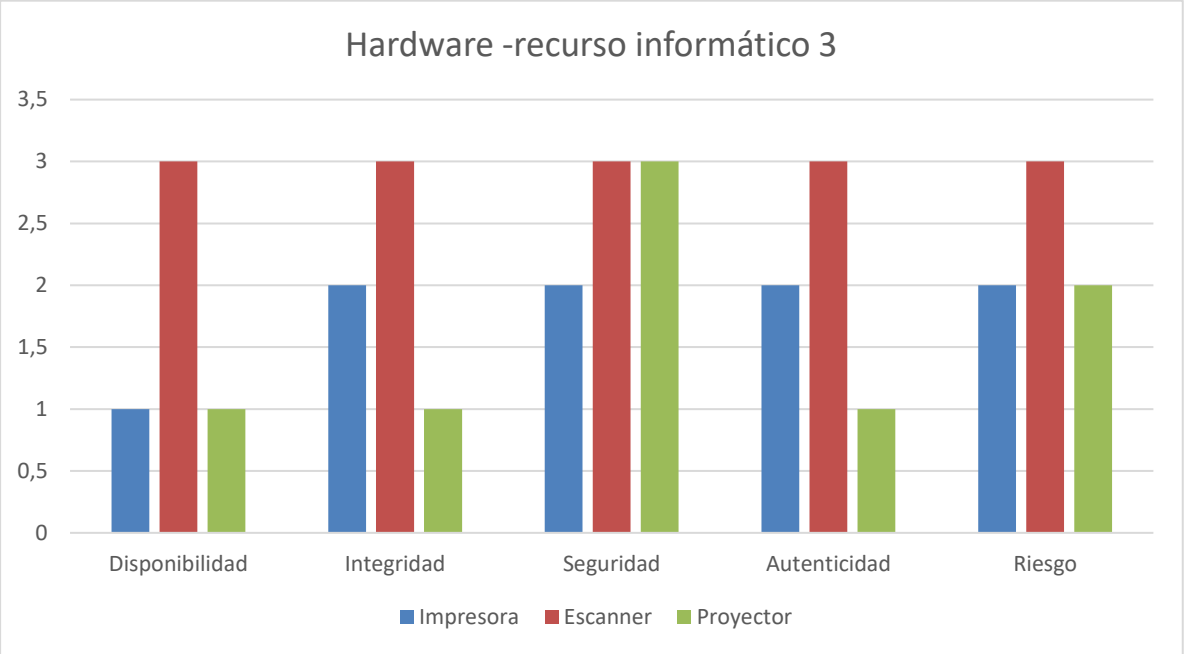
Análisis del RECURSO 1: Hardware – Equipamiento tecnológico 2, como se puede evidenciar dentro de este grupo de recursos, los CPU, monitores, teclados y mouse requieren de atención prioritaria en el tema de seguridad, estos activos se encuentran con una valoración de 2 según la metodología de MAGERIT. Pero cabe resaltar de los CPU en la categoría de riesgo tienen una valoración de 3, donde indica que este activo puede sufrir daños irreversibles. En este sentido, se recomienda dar mantenimiento preventivo por lo menos dos veces al año, y tratar de reemplazar a los CPU.

Ante este panorama, se recomienda implementar un programa de mantenimiento

preventivo al menos dos veces al año, con el objetivo de prolongar la vida útil de los dispositivos y reducir el riesgo de fallos. Además, es fundamental evaluar la posibilidad de reemplazar los CPU de forma gradual, priorizando aquellos que presenten signos de desgaste o problemas recurrentes. Estas acciones contribuirán a minimizar el impacto de posibles daños y garantizarán la continuidad operativa de los sistemas tecnológicos.

**RECURSO 1 (Impresora, escáner, proyector)**

Ilustración 7: Gráfico, valoración del recurso 1, equipamiento informático 3




Elaborado: Fuente propia de información 2024

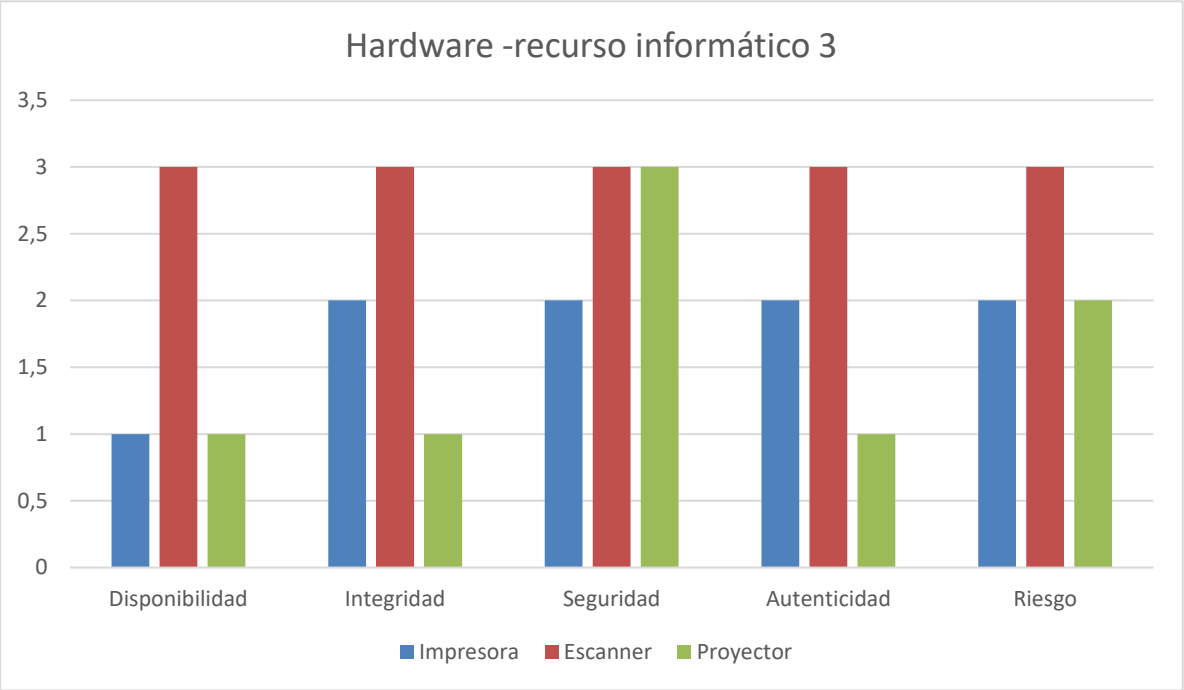
Análisis del RECURSO 1: Hardware – Equipamiento tecnológico 3, como se puede evidenciar dentro de este grupo de recursos, el escáner requiere ser reemplazado, la impresora y el proyector requieren de atención prioritaria en el tema de seguridad, estos recursos se encuentran con una valoración de 2 según la metodología de MAGERIT, donde indica que este recurso puede sufrir daños irreversibles. En este sentido, se recomienda dar mantenimiento preventivo por lo menos dos veces al año.

Ante este escenario, se recomienda implementar un plan de mantenimiento preventivo para estos dispositivos, realizándolo al menos dos veces al año. Esta acción permitirá extender la vida útil de los equipos, minimizar fallas críticas y garantizar un funcionamiento seguro y

eficiente. Además, atender oportunamente las necesidades de seguridad de la impresora y el proyector contribuirá a prevenir posibles incidentes que puedan afectar la infraestructura tecnológica.

**RECURSO 2 (Impresora, escáner, proyector)**

Ilustración 8: Gráfico, valoración del recurso 2, equipamiento informático 3



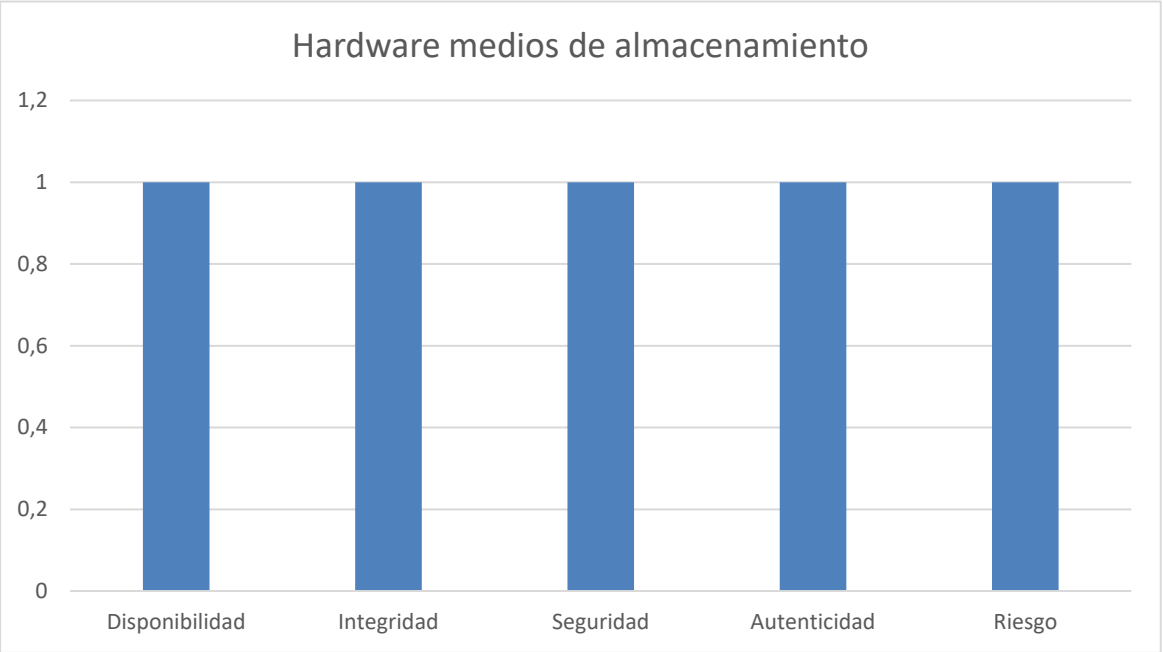

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 2: Hardware – Equipamiento tecnológico 3 revela que dentro de este grupo de recursos, el escáner presenta la necesidad de ser reemplazado debido a su deterioro o falta de funcionamiento adecuado. Asimismo, la impresora y el proyector requieren atención prioritaria en términos de seguridad, ya que ambos dispositivos presentan vulnerabilidades que podrían poner en riesgo su rendimiento o integridad.

Según la metodología MAGERIT, estos recursos obtienen una valoración de 2, lo que indica que podrían sufrir daños irreversibles si no se toman las medidas adecuadas. Como recomendación, es crucial realizar mantenimiento preventivo por lo menos dos veces al año, con el fin de evitar que los dispositivos lleguen a un estado de inoperatividad o vulnerabilidad.

**RECURSO 3 (medios de almacenamiento)**

Ilustración 9: Gráfico, valoración del recurso 3, medios de almacenamiento



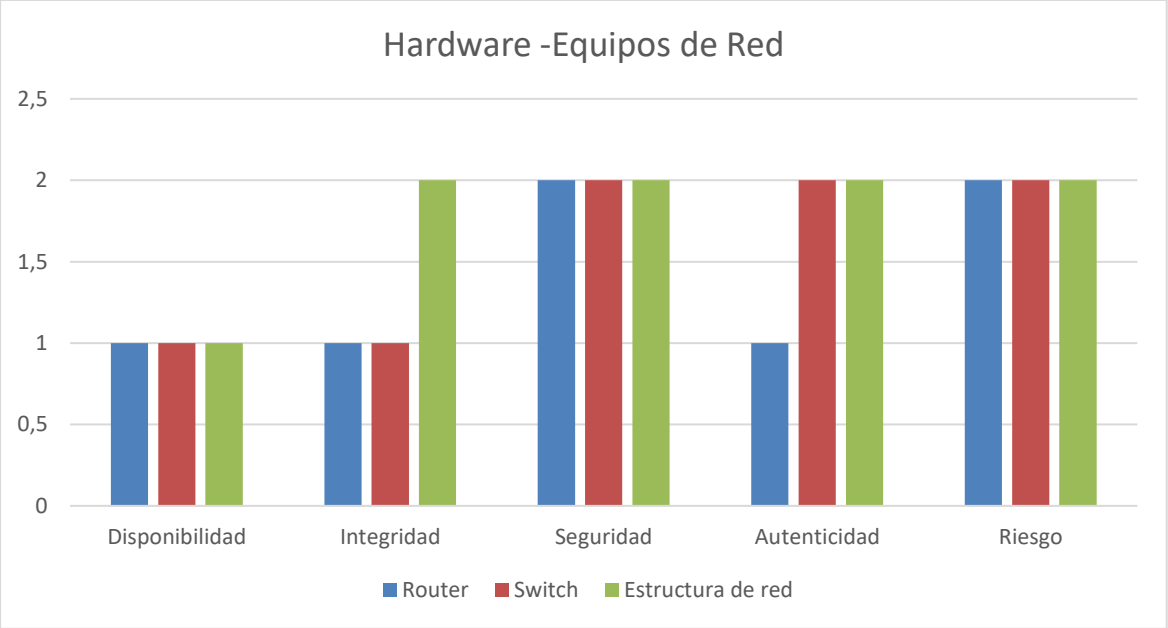

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 3: medios de almacenamiento muestra que las memorias de almacenamiento dentro de este grupo no presentan problemas significativos. Según la metodología MAGERIT, estas memorias obtienen una valoración de 1, lo que sugiere que no están en riesgo de sufrir daños o deterioro. Esto refleja un nivel de estabilidad y confiabilidad en su funcionamiento, lo que las convierte en recursos adecuados para su uso continuo.

A pesar de su buena valoración, se recomienda seguir utilizando estos recursos bajo las mismas normas de seguridad ya establecidas. Es fundamental mantener los protocolos de protección y gestión de datos para asegurar que las memorias continúen operando de manera eficiente y sin exponer la información a riesgos innecesarios.

**RECURSO 4 (Equipos de red)**

Ilustración 10: Gráfico, valoración del recurso 4, equipos de red



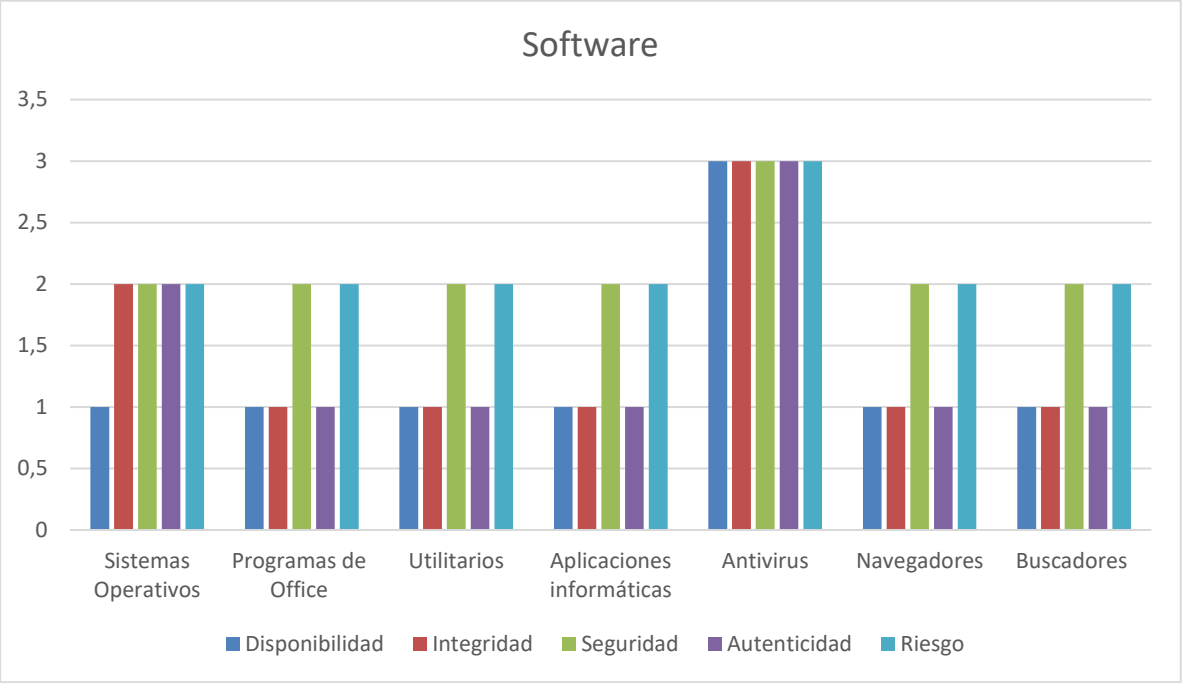

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 4: equipos de red indica que toda la infraestructura de red requiere un mantenimiento urgente para garantizar su funcionamiento adecuado. Según la metodología MAGERIT, tanto los routers como los switches necesitan ser reconfigurados, lo que implica la necesidad de un mantenimiento correctivo para resolver problemas técnicos que podrían afectar la conectividad y el rendimiento de la red. Esta situación señala una prioridad en la atención de estos equipos.

Ante esta situación, se recomienda realizar una revisión exhaustiva de toda la infraestructura de red existente. Verificar el estado de los equipos, su configuración y el correcto funcionamiento de todos los componentes es esencial para evitar posibles fallas en la red, asegurando su operatividad y protegiendo el flujo de información dentro de la organización.

**RECURSO 5 (Software)**

Ilustración 11: Gráfico, valoración del recurso 5, software



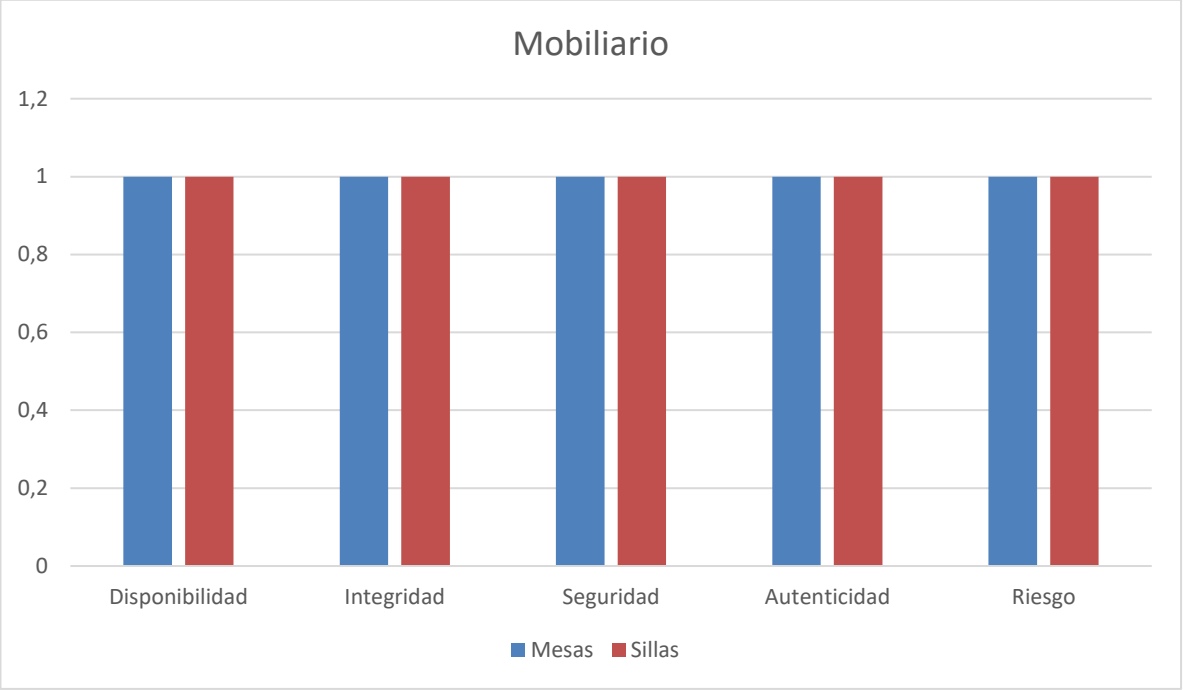

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 5: software revela que los antivirus instalados en las computadoras requieren atención urgente debido a su valoración de 3 según la metodología de MAGERIT. Este recurso presenta una grave vulnerabilidad, ya que no cuenta con una licencia válida para su uso, lo que podría comprometer la seguridad de los sistemas y exponerlos a posibles amenazas. Además, el resto de las aplicaciones, incluido el sistema operativo, también utilizan licencias craqueadas, lo que aumenta los riesgos de vulnerabilidad y no cumple con los estándares legales y de seguridad.

De acuerdo con la metodología MAGERIT, el software instalado en las computadoras necesita una revisión urgente para asegurar que todos los programas estén correctamente licenciados y funcionando de manera segura. Se recomienda llevar a cabo una actualización y verificación de todas las licencias, así como garantizar que los antivirus cuenten con una versión licenciada y actualizada, para proteger los sistemas contra posibles ciberataques y mejorar la eficiencia general del entorno informático.

**RECURSO 6 (mobiliario)**

Ilustración 12: Gráfico, valoración del recurso 6, mobiliario



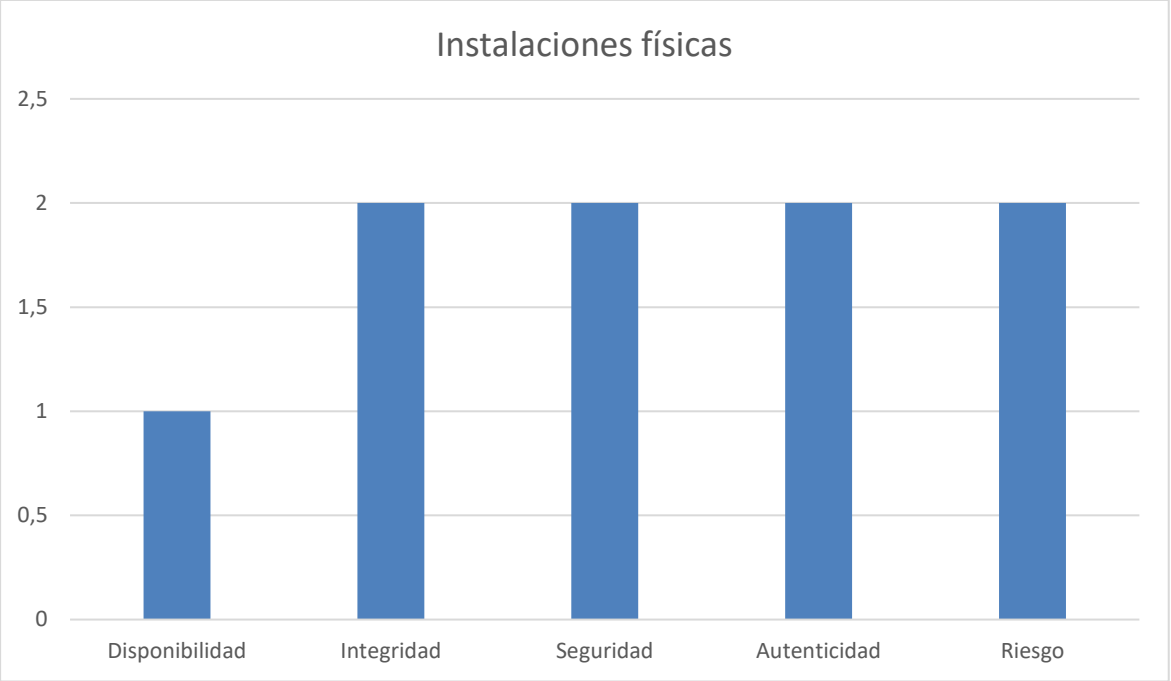

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 6: mobiliario indica que este grupo de recursos tiene una valoración de 1 según la metodología MAGERIT, lo que significa que no presenta una necesidad urgente de intervención. Esto refleja que el mobiliario se encuentra en un estado funcional y no muestra signos de deterioro inminente que afecten su uso.

A pesar de no requerir atención inmediata, se recomienda realizar mantenimiento preventivo al menos dos veces al año. Este enfoque ayudará a mantener el mobiliario en condiciones óptimas, prevenir posibles daños a largo plazo y asegurar un ambiente de trabajo cómodo y seguro para los usuarios.

**RECURSO 7 (Instalaciones físicas)**

Ilustración 13: Gráfico, valoración del recurso 7, instalaciones físicas



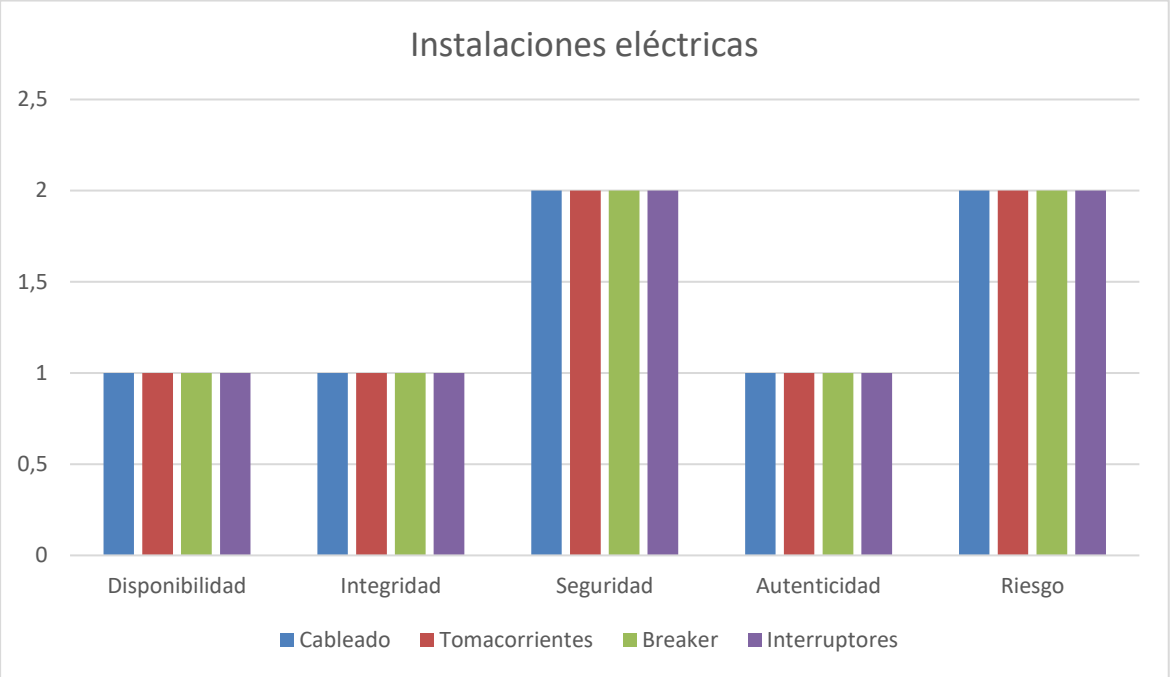

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 7: instalaciones físicas muestra que estas tienen una valoración de 2 según la metodología MAGERIT. Esto indica que las instalaciones requieren atención, ya que podrían sufrir daños irreversibles si no se toman medidas correctivas. Es necesario realizar mantenimiento correctivo para reparar cualquier defecto o fallo que pueda comprometer el funcionamiento adecuado de las instalaciones.

A pesar de la necesidad de corrección, también se recomienda implementar mantenimiento preventivo por lo menos dos veces al año. Esto ayudará a prevenir problemas futuros, garantizar el buen estado de las instalaciones físicas y asegurar un entorno de trabajo seguro y eficiente para los usuarios.

**RECURSO 8 (Instalaciones eléctricas)**

Ilustración 14: Gráfico, valoración del recurso 8, instalaciones eléctricas



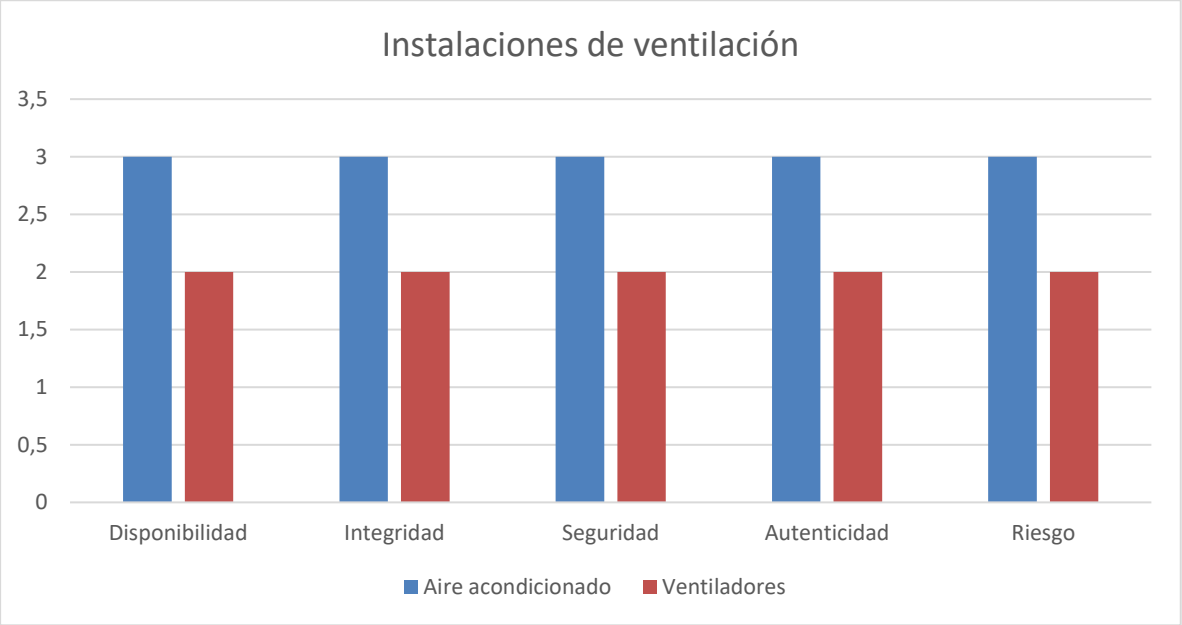

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 8: instalaciones eléctricas revela que este grupo de recursos tiene una valoración de 2 en términos de seguridad, según la metodología MAGERIT. Esto significa que las instalaciones eléctricas enfrentan un alto riesgo de fallas que podrían comprometer la integridad de los equipos. Un factor crítico es el mal funcionamiento de los UPS (sistemas de alimentación ininterrumpida), ya que si no operan correctamente, podrían provocar daños irreversibles a los equipos informáticos durante apagones eléctricos.

Ante este panorama, se recomienda realizar mantenimiento correctivo para reparar los UPS y otras posibles fallas en las instalaciones eléctricas. Además, es crucial implementar un mantenimiento preventivo al menos dos veces al año. Esto no solo garantizará la protección de los equipos informáticos, sino que también mejorará la seguridad general de las instalaciones eléctricas, reduciendo los riesgos asociados a posibles fallos o cortocircuitos.

**RECURSO 9 (Instalaciones de ventilación)**

Ilustración 15: Gráfico, valoración del recurso 9, instalaciones de ventilación



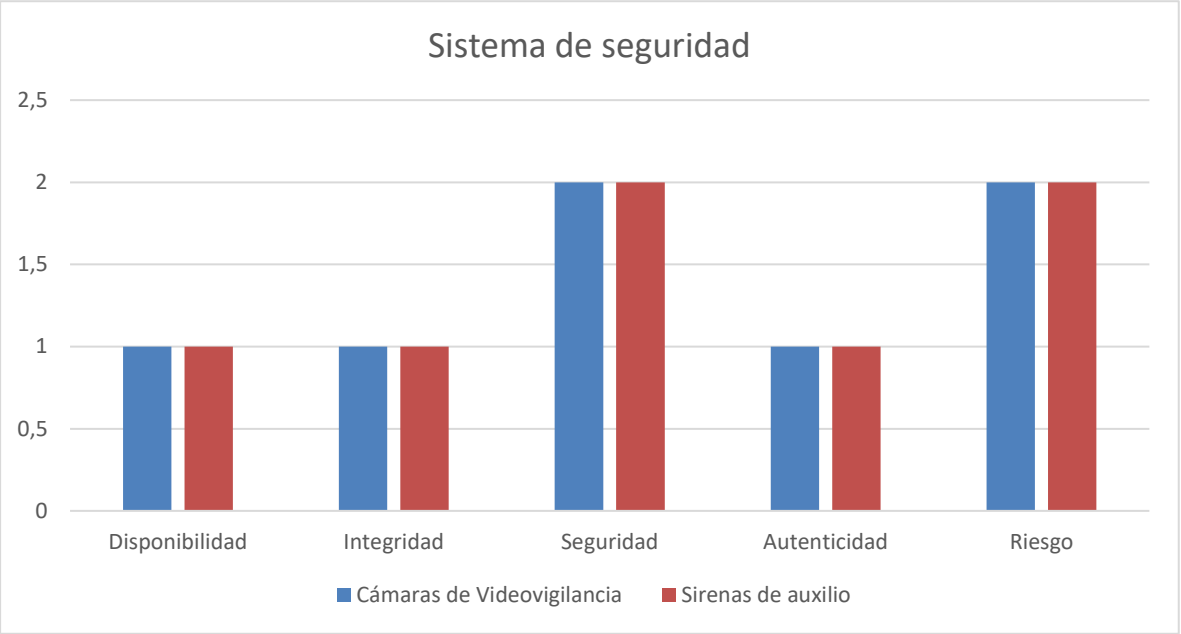

Elaborado: Fuente propia de información 2024

El análisis del RECURSO 9: instalaciones de ventilación señala que los aires acondicionados tienen una valoración de 3, lo que indica que ya cumplieron su vida útil y no ofrecen el rendimiento esperado. Además, los ventiladores requieren de mantenimiento correctivo para garantizar su funcionamiento adecuado. Según la metodología MAGERIT, estas instalaciones no están en óptimas condiciones y presentan riesgos de no cumplir su función correctamente, lo que podría afectar el ambiente de trabajo.

Dado el estado actual de los equipos, se recomienda reemplazar tanto los aires acondicionados como los ventiladores para evitar fallas que afecten la ventilación y climatización del espacio. Este reemplazo contribuiría a mejorar la eficiencia energética y a mantener un ambiente de trabajo confortable. Además, sería adecuado implementar un mantenimiento preventivo para asegurar el buen funcionamiento de los nuevos sistemas de ventilación y prolongar su vida útil.

**RECURSO 10 (Instalaciones de seguridad)**

Ilustración 16: Gráfico, valoración del recurso 10, instalaciones de seguridad




Elaborado: Fuente propia de información 2024

El análisis del RECURSO 10: instalaciones de seguridad indica que las cámaras de seguridad y las alarmas de auxilio tienen una valoración de 2, lo que sugiere que requieren atención para evitar posibles fallos. Según la metodología MAGERIT, estos recursos no están en condiciones óptimas y podrían comprometer la seguridad del entorno si no se corrigen a tiempo. Por lo tanto, es necesario realizar un mantenimiento correctivo para asegurar su funcionamiento adecuado.

Para garantizar su efectividad a largo plazo, se recomienda realizar mantenimiento preventivo al menos dos veces al año. Este mantenimiento ayudará a identificar problemas potenciales antes de que ocurran y mejorará la confiabilidad de los sistemas de seguridad, garantizando una protección continua y eficiente. Mantener estos equipos en buen estado es crucial para la seguridad general del entorno y la protección de los recursos e instalaciones.

#### 4.4.4.4.2. Análisis general.

El análisis de los recursos tecnológicos y físicos en función de la metodología MAGERIT revela diversas necesidades de mantenimiento y riesgos de daño en los activos de la organización. En el caso de los recursos de hardware como CPU, monitores, teclados y mouse, se destaca una valoración de riesgo de 2, indicando que podrían sufrir daños, por lo que se sugiere mantenimiento preventivo bianual. Sin embargo, los CPU específicamente se valoran con un riesgo de 3, sugiriendo una posible vulnerabilidad a daños irreparables que podría justificar su reemplazo. Del mismo modo, otros equipos tecnológicos, como escáneres y proyectores, también requieren atención prioritaria para evitar un deterioro irreparable.

Los medios de almacenamiento y mobiliario, con una valoración de riesgo de 1, no presentan necesidades de intervención urgente, pero se recomienda continuar con el mantenimiento preventivo regular. Por otro lado, la infraestructura de red y el software instalado exigen una revisión urgente. Los equipos de red, como routers y switches, deben ser reconfigurados y recibir mantenimiento correctivo; mientras que el software instalado presenta licencias inadecuadas y antivirus desactualizados, lo que representa un riesgo alto para la seguridad de la información y la funcionalidad operativa de la red.

Finalmente, se observan riesgos relevantes en las instalaciones físicas, eléctricas y de ventilación. Estas tienen valoraciones de 2 y 3, señalando riesgos altos que requieren intervenciones correctivas. Las instalaciones de seguridad, como cámaras y alarmas, también necesitan mantenimiento correctivo y preventivo para garantizar su efectividad. Estas recomendaciones reflejan la importancia de implementar políticas de mantenimiento que mitiguen los riesgos y optimicen la durabilidad de los recursos de la organización, de acuerdo con las pautas de seguridad establecidas.

A continuación, se presente un informe de resultados.

#### 4.4.4.4.3. Informe de Análisis de Recursos Tecnológicos y Físicos según la Metodología MAGERIT

**Introducción**

El análisis de los recursos tecnológicos y físicos de la organización, realizado bajo la metodología MAGERIT, ha permitido identificar diversas necesidades de mantenimiento y riesgos potenciales en los activos clave. Este informe presenta una valoración detallada de cada tipo de recurso, así como las recomendaciones necesarias para mitigar los riesgos y asegurar el correcto funcionamiento y la durabilidad de los equipos y las instalaciones.

**Análisis de los Recursos Tecnológicos**

**Hardware (CPU, monitores, teclados y mouse)**

Los recursos de hardware, incluyendo CPU, monitores, teclados y mouse, presentan una valoración de riesgo de 2, lo que indica la posibilidad de sufrir daños, aunque estos no sean irreparables. Para mitigar estos riesgos, se recomienda realizar un mantenimiento preventivo bianual. En particular, los CPU, con una valoración de 3, presentan un riesgo mayor de daños irreparables, lo que justifica considerar su reemplazo a corto plazo.

**Equipos tecnológicos adicionales (escáneres, proyectores)**

Los escáneres y proyectores requieren atención prioritaria. Estos dispositivos, al estar en una etapa crítica de su ciclo de vida, deben ser monitoreados y mantenidos adecuadamente para evitar un deterioro irreparable que impacte en la operatividad.

**Medios de almacenamiento y mobiliario**

Con una valoración de riesgo de 1, los medios de almacenamiento y el mobiliario no requieren intervención urgente. Sin embargo, se recomienda continuar con el mantenimiento preventivo regular para garantizar su óptimo estado y prolongar su vida útil.

## Análisis de Infraestructura de Red y Software

### Equipos de red (routers y switches)

Los equipos de red, como routers y switches, presentan una necesidad urgente de mantenimiento correctivo. Estos deben ser reconfigurados y sometidos a una revisión técnica para evitar fallas que puedan afectar la conectividad y funcionalidad de la red.

### Software instalado

Se ha identificado que el software instalado presenta licencias inadecuadas y antivirus desactualizados, lo que constituye un riesgo alto para la seguridad de la información. Se recomienda una actualización inmediata de las licencias y la instalación de antivirus actualizados, así como una revisión periódica de las soluciones de seguridad.

## Análisis de Infraestructura Física y de Seguridad

### Instalaciones físicas, eléctricas y de ventilación

Las instalaciones físicas, incluyendo las infraestructuras eléctricas y de ventilación, han sido valoradas con riesgos de 2 y 3, lo que indica la necesidad de intervenciones correctivas urgentes. Se recomienda revisar y reparar las instalaciones eléctricas para prevenir riesgos de sobrecarga o fallos que puedan afectar la operatividad de los sistemas.

### Instalaciones de seguridad (cámaras y alarmas)

Las cámaras y alarmas de seguridad requieren mantenimiento correctivo y preventivo para garantizar su efectividad. Es crucial asegurar que estos sistemas operen sin fallos para proteger las instalaciones de la organización frente a posibles amenazas externas o internas.

## Conclusión

El análisis realizado ha permitido identificar riesgos significativos en los recursos

tecnológicos y físicos de la organización, que pueden comprometer la operatividad y seguridad. Las recomendaciones de mantenimiento preventivo y correctivo son esenciales para mitigar estos riesgos y optimizar el rendimiento de los activos. La implementación de políticas de mantenimiento regulares, junto con una actualización adecuada de los sistemas tecnológicos, garantizará la durabilidad de los recursos y la continuidad de las operaciones, en línea con las mejores prácticas de seguridad y gestión de activos.

# CAPITULO V

## 5. Evaluación de resultados

### 5.1. Introducción

Realizar una auditoría informática en la Unidad Educativa "Rumiñahui" garantiza la seguridad, eficiencia y buen funcionamiento de su infraestructura tecnológica. Permite identificar vulnerabilidades, mejorar el rendimiento de los sistemas, asegurar el cumplimiento de normativas, optimizar recursos y proteger la información crítica de estudiantes y personal ante posibles riesgos o ataques cibernéticos.

En este sentido, se puede señalar que la Unidad Educativa "Rumiñahui", al no aplicar un adecuado control ni realizar los mantenimientos preventivos o correctivos requeridos en su infraestructura tecnológica, podría enfrentar un rápido deterioro. Además, la falta de políticas y normas estandarizadas para el uso de los recursos informáticos complica su gestión y protección, lo que aumenta el riesgo de daño o mal uso de estos activos, afectando su durabilidad y funcionalidad en el corto y largo plazo.

### 5.2. Informe de auditoría

#### Tipo de auditoría

Auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor.

**Dirigido a:** Lic. Manuel Solorzano, Rector de la Unidad Educativa “Rumiñahui”

**Motivo:** Trabajo de titulación

**Objetivos**

• Analizar los riesgos de seguridad actual de la Unidad Educativa “Rumiñahui”.

• Identificar el nivel de seguridad de la infraestructura tecnológica de la Unidad Educativa “Rumiñahui”.

**Personal relacionado**

- Personal administrativo
- Docentes
- Estudiantes

**Alcance**

Para el desarrollo de la Auditoría se aplicaron los siguientes técnicas y procedimientos.

- Revisión bibliográfica de seguridad, normas y políticas.
- Investigar la metodología MAGERIT, sus fases ejecutarlas.
- Identificar o Definir activos y valorarlos.
- Identificar o Definir amenazas.
- Realizar el diseño de Instrumentos.
- Ejecución de Auditoría, entrevistar a las autoridades y estudiantes de bachillerato de la Unidad Educativa “Rumiñahui”
- Tabulación y análisis de datos.
- Valoración de riesgo (Matriz de riesgo).
- Políticas de seguridad.
- Elaborar Informe.

## 5.3. Hallazgos

### 5.3.1. Hardware - Recurso informático

En cuanto al equipamiento informático, se observa que la ausencia de políticas de uso y normas de control puede acelerar el desgaste de los equipos, reduciendo su vida útil. Los mantenimientos preventivos son esenciales y deben llevarse a cabo al menos dos veces al año, o cuando sea necesario.

En este contexto, la Unidad Educativa “Rumiñahui” debería contar con un técnico de planta dentro de su personal administrativo, responsable del cuidado y mantenimiento de la infraestructura tecnológica.

La auditoría realizada evidencia que tanto docentes como estudiantes utilizan los equipos sin preocuparse por su mantenimiento, lo que incrementa el riesgo de fallos y deterioro prematuro de la infraestructura. En este sentido, es imprescindible contar con un técnico especializado que no solo garantice el adecuado cuidado de los recursos tecnológicos, sino también supervise su correcto uso, implemente medidas preventivas y capacite a los usuarios sobre las mejores prácticas. De este modo, se asegura un funcionamiento óptimo y prolonga la vida útil de los equipos, optimizando el rendimiento de la infraestructura tecnológica en la Unidad Educativa.

### 5.3.2. Hardware – Medios de almacenamiento

Es importante señalar que la Unidad Educativa “Rumiñahui” utiliza dispositivos de almacenamiento físico, como memorias USB, para guardar información. Sin embargo, en la actualidad, es preferible adoptar soluciones más modernas y seguras, como el uso de almacenamiento en la nube. En este sentido, se recomienda emplear herramientas como OneDrive o Google Drive, que ofrecen mayor seguridad y accesibilidad.

Además, dado el creciente volumen de información que manejan los docentes y estudiantes, sería ideal que cada docente disponga de un hosting personal en la web, donde puedan almacenar sus datos de manera organizada y segura. Esto no solo mejoraría la gestión de la información, sino que también reduciría el riesgo de pérdida o daño a los archivos, al contar con copias respaldadas en servidores confiables. Implementar estas medidas optimizaría el almacenamiento de datos y facilitaría el acceso a la información desde cualquier lugar y dispositivo.

### 5.3.3. Hardware – Dispositivos de red

Una vez concluida la auditoría de la infraestructura tecnológica de la Unidad Educativa "Rumiñahui", es fundamental centrarse en los recursos de la red de datos. En este aspecto, es crucial realizar tanto mantenimientos preventivos como correctivos para asegurar su correcto funcionamiento. Con el tiempo, el uso constante de los recursos de red provoca desgaste y deterioro. En algunos casos, es necesario reemplazarlos, mientras que en otros se requiere una

reconfiguración adecuada, donde se implementen criterios de calidad de servicio (QoS) para optimizar el rendimiento.

La evolución constante de la tecnología hace indispensable la actualización de equipos como routers y switches, que deben contar con funcionalidades avanzadas para configurar la calidad de servicio (Q&Q). Esto garantiza que la red pueda manejar de manera eficiente el tráfico de datos y asegurar que los servicios críticos reciban prioridad, mejorando la experiencia del usuario. Además, estos dispositivos más modernos permiten una gestión más flexible y segura de la red, adaptándose a las crecientes demandas tecnológicas. La implementación de equipos con capacidad de calidad de servicio también contribuye a una mayor estabilidad y rendimiento en el uso de aplicaciones multimedia, videoconferencias y plataformas educativas en línea, que cada vez requieren mayor ancho de banda y confiabilidad. La inversión en estos dispositivos no solo optimiza el rendimiento inmediato de la red, sino que también asegura una infraestructura robusta para enfrentar futuros desafíos tecnológicos, manteniendo a la institución actualizada.

Además, el sistema de cableado, tanto de datos como de energía, debe estar debidamente identificado, etiquetado y protegido para garantizar la seguridad. También es importante mantener una correcta organización estética en la instalación, lo que implica una disposición ordenada y eficiente de los cables. Esto no solo mejora la apariencia del espacio, sino que también facilita el mantenimiento y reduce el riesgo de problemas futuros en la red.

### 5.3.4. Software

La Unidad Educativa "Rumiñahui" no cuenta con las licencias correspondientes para el uso de aplicaciones y herramientas de Office, ya que se han instalado sin autorización oficial. En la auditoría realizada a su infraestructura tecnológica, se constató la falta de licencias tanto para las aplicaciones de Office como para el sistema operativo Windows, que también se encuentra instalado sin una licencia original.

El uso de licencias originales es un componente esencial para garantizar el correcto funcionamiento de los equipos informáticos. Las licencias originales no solo aseguran la estabilidad del sistema operativo y las aplicaciones, sino que también permiten recibir

actualizaciones de seguridad que protegen los equipos de posibles vulnerabilidades. Además del sistema operativo Windows, se encontraron otras aplicaciones y utilitarios instalados sin licencias válidas, lo que incrementa el riesgo de fallos técnicos y problemas legales.

Por tanto, es imprescindible que la Unidad Educativa "Rumiñahui" adquiera las licencias necesarias, especialmente para el sistema operativo, software antivirus, y las herramientas y aplicaciones utilizadas por los docentes en el proceso de enseñanza-aprendizaje. Esto no solo garantizaría un entorno tecnológico seguro, sino que también mejoraría la eficiencia y protección de la infraestructura educativa.

### 5.3.5. Mobiliario

En cuanto al mobiliario, se observa que la Unidad Educativa “Rumiñahui” dispone de equipamiento adecuado para sus equipos informáticos y el resto de su infraestructura tecnológica. No obstante, se sugiere que, en el futuro, se adquieran más muebles para mejorar el confort de docentes y estudiantes, y optimizar los espacios de trabajo. Esto no solo aumentaría la comodidad, sino también la eficiencia en el uso de la tecnología, favoreciendo un ambiente más adecuado para el aprendizaje y el desarrollo de las actividades académicas dentro de la institución.

Además, es importante considerar que el mobiliario debe estar alineado con las necesidades ergonómicas de los usuarios, especialmente en un entorno educativo donde tanto docentes como estudiantes pasan varias horas utilizando equipos tecnológicos. Contar con sillas y mesas ajustables, espacios de almacenamiento adecuados, y una correcta disposición del mobiliario puede mejorar significativamente la postura y reducir el riesgo de problemas físicos a largo plazo. Invertir en mobiliario ergonómico y funcional no solo contribuye al bienestar y confort de los usuarios, sino que también fomenta un ambiente más productivo y dinámico, esencial para un entorno de aprendizaje eficiente y moderno.

### 5.3.6. Infraestructura (medios físicos)

En relación con la infraestructura física de la Unidad Educativa "Rumiñahui", que incluye el laboratorio, aulas y otros espacios destinados a la infraestructura tecnológica, se observa que actualmente se encuentra en condiciones normales. Sin embargo, es esencial

realizar un mantenimiento preventivo al menos una vez al año para garantizar la seguridad de docentes y estudiantes.

Este mantenimiento preventivo debe incluir la pintura de paredes, la revisión y reparación de verjas de protección, puertas y el mantenimiento del techo. Un cuidado adecuado de estos elementos es crucial para preservar la integridad y funcionalidad del espacio. Es importante destacar que el buen estado de la infraestructura física depende en gran medida del compromiso y cuidado que la comunidad educativa tenga con sus instalaciones, lo que asegura un entorno seguro y óptimo para el aprendizaje y el uso de la tecnología.

Además, es fundamental que el mantenimiento preventivo no solo se limite a aspectos visibles como la pintura y las reparaciones, sino que también incluya una revisión detallada de las instalaciones eléctricas y de seguridad. Asegurarse de que los sistemas eléctricos estén en buen estado y que los equipos de seguridad, como alarmas y detectores de humo, funcionen correctamente es esencial para prevenir incidentes y garantizar un entorno seguro. La implementación de un programa de mantenimiento regular y bien estructurado, que contemple inspecciones periódicas y acciones correctivas, contribuye a prolongar la vida útil de la infraestructura y minimizar posibles riesgos. Asimismo, fomentar la participación activa de la comunidad educativa en el cuidado de las instalaciones ayudará a crear un ambiente de responsabilidad compartida, promoviendo un mejor uso y conservación de los espacios destinados a la tecnología y el aprendizaje.

### 5.3.7. Instalaciones eléctricas

Se resume a continuación lo relacionado con las instalaciones eléctricas en el laboratorio de informática, aulas y otros espacios de la infraestructura tecnológica en la Unidad Educativa “Rumiñahui”. Estas instalaciones requieren tanto mantenimiento preventivo como correctivo.

Un mantenimiento adecuado asegura que las instalaciones eléctricas sean seguras y eficientes. Contar con cajas de breakers y reguladores de voltaje (UPS) es crucial para proteger los equipos informáticos y la infraestructura tecnológica de sobrecargas y fallos eléctricos.

La presencia de breakers y reguladores de voltaje ayuda a prevenir daños a los equipos.

Por lo tanto, se recomienda que la Unidad Educativa “Rumiñahui” lleve a cabo mantenimientos regulares, instale más breakers y adquiera reguladores de voltaje adicionales.

Implementar estas medidas mejorará la seguridad eléctrica y la estabilidad del sistema. Un buen mantenimiento y la instalación de equipos de protección adecuados son esenciales para asegurar el funcionamiento continuo y seguro de la infraestructura tecnológica.

### 5.3.8. Instalaciones de ventilación

Es importante destacar que ciertos equipos tecnológicos necesitan un ambiente fresco para su óptimo funcionamiento y conservación. De igual manera, docentes y estudiantes se benefician de un clima agradable para mejorar su desempeño en el proceso de enseñanza-aprendizaje.

En este contexto, el sistema de ventilación, que incluye aires acondicionados y ventiladores, juega un papel crucial. Estos equipos deben estar en buenas condiciones para asegurar un ambiente adecuado tanto para la tecnología como para los usuarios.

Por lo tanto, es esencial realizar un mantenimiento preventivo regular y, cuando sea necesario, correcciones para el sistema de ventilación. Esto garantizará que tanto los equipos tecnológicos como los espacios de trabajo se mantengan en condiciones óptimas.

Se recomienda reemplazar el sistema de ventilación en la Unidad Educativa "Rumiñahui" debido a su insuficiente rendimiento y el impacto negativo en la conservación de equipos tecnológicos y el confort de docentes y estudiantes. Un sistema de ventilación nuevo y eficiente mejorará el ambiente y garantizará un funcionamiento óptimo de la infraestructura.

### 5.3.9. Sistema de seguridad

En términos de seguridad, es fundamental proteger tanto a las personas como a los bienes inmuebles y muebles dentro de una institución. En este contexto, la Unidad Educativa "Rumiñahui" ha implementado cámaras de videovigilancia y sirenas de auxilio en sus

instalaciones para mejorar la seguridad.

Sin embargo, se observa que, aunque ya existen cámaras y sirenas, es necesario ampliar la cobertura instalando más equipos. Esto garantizará que toda la superficie de la unidad educativa esté adecuadamente vigilada y protegida.

Para asegurar la eficacia continua de las cámaras y sirenas, se recomienda llevar a cabo un mantenimiento preventivo trimestral. Este enfoque ayudará a mantener los sistemas en óptimas condiciones y a prevenir fallos en su funcionamiento. Además, es crucial que la información capturada por las cámaras se almacene en un repositorio digital seguro en la web. La adopción de almacenamiento en la nube garantiza que los datos sean accesibles y estén protegidos, facilitando su gestión y recuperación en caso de necesidad. Implementar estas medidas mejorará significativamente la seguridad y la capacidad de respuesta ante cualquier incidente.

### 5.3.10 Guía para el uso de la infraestructura tecnológica

Tomando en consideración las amenazas, riesgos y vulnerabilidades identificadas en la auditoría de seguridad informática realizada a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui”, se ha elaborado una guía integral. Esta guía incluye políticas y normas estandarizadas diseñadas para garantizar el correcto funcionamiento, control y protección de toda la infraestructura tecnológica, abordando así las debilidades detectadas y fortaleciendo las medidas de seguridad necesarias para proteger tanto los datos como los equipos.

En cuanto al desarrollo y organización del código de las políticas y normas de control, estas serán detalladas en la guía mencionada. Se establecerá un sistema de codificación específico para cada política, por ejemplo, UER-BL-P1 para las políticas generales y UER-BL-R1-N1 para las normas correspondientes. Este esquema de codificación permitirá una fácil identificación y referencia de cada directriz, asegurando que los procedimientos y normas sean claros, accesibles y efectivos en la implementación y mantenimiento de las medidas de seguridad establecidas.

Tabla 16: Normalización de código para políticas

| No | NOMBRE | DESCRIPCIÓN |
|---|---|---|
| 1 | UER | Nombre de la Unidad Educativa |
| 2 | BL | Bloque de la Unidad Educativa |
| 3 | P1… | Número de política |

Elaborado: Fuente propia de información 2024

Tabla 17: Normalización de código para normas de control

| No | NOMBRE | DESCRIPCIÓN |
|---|---|---|
| 1 | UER | Nombre de la Unidad Educativa |
| 2 | BL | Bloque de la Unidad Educativa |
| 3 | R1 | Nombre del Recurso |
| 4 | N1… | Número de norma |

Elaborado: Fuente propia de información 2024

Con los antecedentes descritos anteriormente, se puede observar la Guía para el correcto uso de la infraestructura tecnológica, en el anexo 1.

## 5.4. Conclusiones y recomendaciones de la auditoria

### 5.4.1. Conclusiones

- Seguridad Mejorada**:** La evaluación de la infraestructura tecnológica de la Unidad Educativa "Rumiñahui" mediante la metodología MAGERIT reveló diversas amenazas, riesgos y vulnerabilidades. Las recomendaciones formuladas en el informe de auditoría son cruciales para mitigar estos problemas y mejorar la seguridad de los activos informáticos, lo que contribuirá a un entorno tecnológico más seguro y eficiente.
- Guía de Uso Efectiva: Con base en el análisis de las vulnerabilidades y riesgos identificados, se ha desarrollado una guía exhaustiva para el uso adecuado de la infraestructura tecnológica. Esta guía incluye políticas y normas que deben ser adoptadas por las autoridades, docentes y estudiantes, garantizando un manejo correcto y seguro de los recursos tecnológicos en la Unidad Educativa.

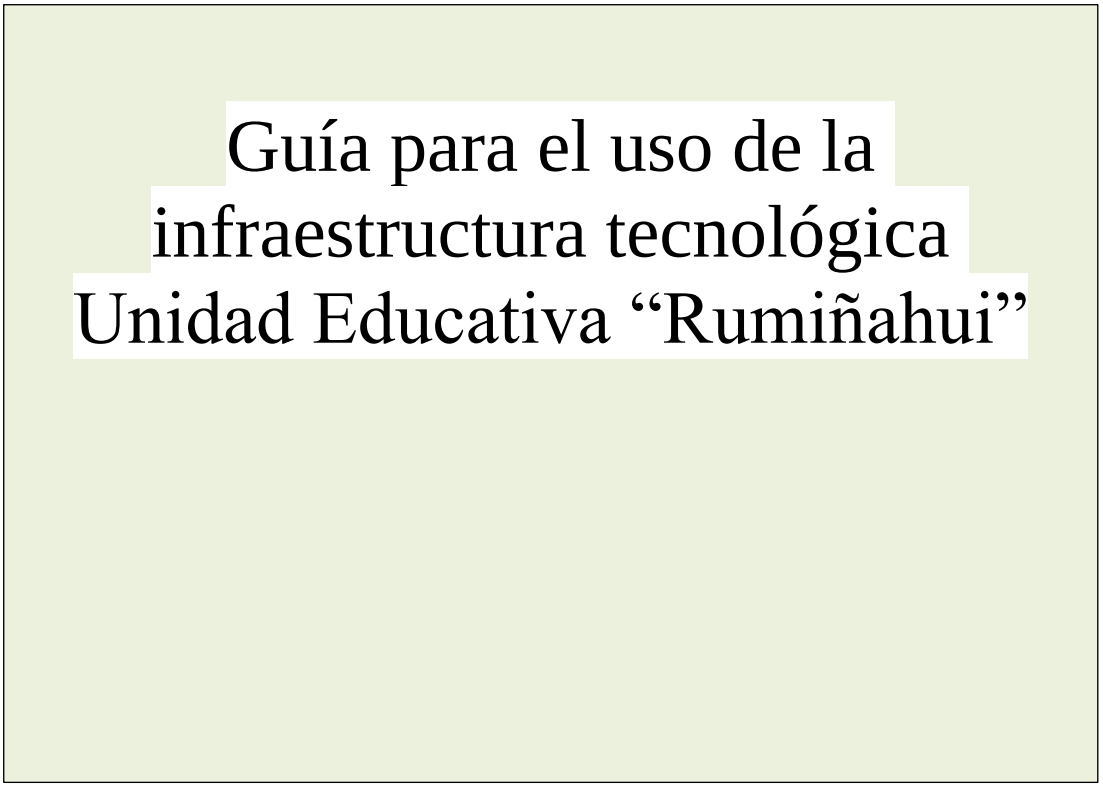
- Cumplimiento y Control: La implementación de las políticas y normas establecidas en la guía es fundamental para asegurar la protección y el buen funcionamiento de la infraestructura tecnológica. La adhesión a estas directrices por parte de toda la comunidad educativa ayudará a mantener la integridad, disponibilidad y confidencialidad de los sistemas y datos, reduciendo los riesgos asociados.

### 5.4.2. Recomendaciones

- A las autoridades de la Unidad Educativa "Rumiñahui": Se recomienda que supervisen la correcta aplicación y cumplimiento de las políticas y normas establecidas en la auditoría de seguridad informática. Esta supervisión debe ser continua y exhaustiva para asegurar que se mantenga un entorno tecnológico seguro y que todas las recomendaciones se implementen eficazmente.
- A las autoridades y docentes de la Unidad Educativa "Rumiñahui": Se sugiere que, además de hacer cumplir las políticas y normas de la guía de auditoría, supervisen de manera constante el comportamiento de los estudiantes al utilizar la infraestructura tecnológica. Esta vigilancia ayudará a garantizar que las normas se sigan adecuadamente y que los estudiantes empleen los recursos de manera segura y responsable.
- A los docentes: Se les aconseja que, además de hacer cumplir las normas establecidas en la guía de auditoría de seguridad informática, trabajen en fortalecer el proceso de enseñanza-aprendizaje mediante el uso efectivo de la tecnología. Fomentar el uso responsable y educativo de los recursos tecnológicos contribuirá a una mejor formación y preparación de los estudiantes.
- A los estudiantes: Se les recomienda que utilicen toda la infraestructura tecnológica disponible, siempre con un cuidado especial hacia los bienes. La responsabilidad en el uso y mantenimiento de estos recursos es crucial para asegurar su longevidad y funcionalidad, evitando daños y garantizando que todos puedan beneficiarse de ellos.

A continuación, se presente la guía de auditoría.

**Guía para el uso de la infraestructura tecnológica de la Unidad Educativa "Rumiñahui"**




**INDICE**

**1.- Políticas**

**UER-PG-P1:** Los equipos tecnológicos serán codificados sin excepción. Este código incluirá la fecha de adquisición, su nombre y serie. Por ejemplo: 20250106CPU. Además, se deberá registrar el estado inicial del equipo en un inventario detallado, que se actualizará de manera periódica para garantizar que toda la información esté al día y facilitar el seguimiento de cada equipo dentro de la institución.

**UER-PG-P2:** Para movilizar cualquier equipo tecnológico a otra área de la Unidad Educativa "Rumiñahui", se deberá realizar un pedido por escrito al rector. Este pedido debe realizarse con al menos dos horas de anticipación. Se sugiere también incluir una descripción detallada del motivo de la movilización y asegurar la entrega del equipo en condiciones óptimas.

**UER-PG-P3:** Si algún equipo tecnológico es dañado por un docente, estudiante o invitado, será responsabilidad de la persona responsable pagar por el arreglo o reponer el equipo en su totalidad. Además, se debe realizar un informe detallado del incidente y establecer medidas preventivas para evitar que situaciones similares vuelvan a ocurrir en el futuro.

**UER-PG-P4:** Si un docente requiere usar el laboratorio de informática, debe realizar la solicitud con la debida anticipación. Además, deberá presentar un plan de clase o actividad a realizar que justifique el uso del laboratorio. Se sugiere que el pedido se haga con un mínimo de 24 horas de anticipación para garantizar la disponibilidad de los recursos.

**UER-PG-P5:** Si se requiere facilitar el uso del laboratorio de informática a una institución externa o grupo de personas ajenas a la Unidad Educativa, se deberá realizar la solicitud directamente a la máxima autoridad de la institución. Además, es necesario incluir una justificación detallada del uso del espacio y cumplir con los reglamentos establecidos para su correcta utilización.

**UER-PG-P6:** Si no se cumple con cualquiera de las normas establecidas en esta guía, las personas involucradas, ya sean docentes o estudiantes, serán llamadas ante las autoridades de la Unidad Educativa. Se les aplicará una sanción según el Código de Convivencia de la institución. En casos graves, se podrían aplicar medidas disciplinarias adicionales o notificar a los representantes legales si fuese necesario.

**UER-PG-P7:** La máxima autoridad de la Unidad Educativa "Rumiñahui", junto con el técnico informático, debe presentar un plan de contingencia para casos de desastre natural o eventos que pongan en riesgo la infraestructura. Este plan debe actualizarse anualmente al

inicio de cada año lectivo y debe ser revisado para asegurar su eficacia y relevancia ante posibles riesgos.

**UER-PG-P8:** En caso de robo o daño a la infraestructura tecnológica de la institución, la máxima autoridad de la Unidad Educativa "Rumiñahui" debe presentar un informe completo y realizar la denuncia respectiva a las autoridades competentes. Es importante que esta denuncia se acompañe de toda la documentación y pruebas necesarias para facilitar el proceso legal.

**UER-PG-P9:** La máxima autoridad de la Unidad Educativa "Rumiñahui", con la colaboración del técnico informático, debe presentar los requerimientos de infraestructura tecnológica al distrito de educación al inicio de cada periodo académico. Estos requerimientos serán gestionados ante las autoridades correspondientes para su adquisición y deben basarse en una evaluación detallada de las necesidades de la institución.

**UER-PG-P10:** La máxima autoridad de la Unidad Educativa "Rumiñahui", en colaboración con el técnico informático, debe presentar un proyecto de innovación tecnológica al distrito de educación al inicio de cada periodo académico. Este proyecto será evaluado para analizar su viabilidad, y se sugiere también incluir propuestas que promuevan el uso eficiente de los recursos actuales.

**2.- Normas**

**UER-NG-R1-N1:** Está prohibido ubicar cualquier tipo de alimento, líquido o peso sobre cualquier equipo tecnológico. Esta medida se toma para prevenir daños por derrames o caídas accidentales que puedan comprometer el funcionamiento de los equipos y causar averías costosas que afecten a la comunidad educativa.

**UER-NG-R1-N2:** Está prohibido mover o separar cualquier equipo tecnológico dentro de la misma área sin autorización del docente a cargo de la clase o actividad. Mover el equipo sin supervisión puede provocar desconexiones, daños o alteraciones en la configuración del sistema, afectando su funcionamiento correcto.

**UER-NG-R1-N3:** Está prohibido destacar o retirar cualquier equipo tecnológico sin la autorización del técnico informático de la granja. El técnico debe garantizar que el equipo se manipule adecuadamente para evitar daños y asegurar que se mantenga en funcionamiento óptimo para las actividades educativas.

**UER-NG-R1-N4:** Está prohibido golpear, forzar o dañar cualquier equipo tecnológico. Este

tipo de comportamiento puede ocasionar daños irreversibles, lo que no solo afecta al equipo sino también al desarrollo de las actividades tecnológicas de la institución.

**UER-NG-R1-N5:** Está prohibido rayar o escribir con cualquier tipo de tinta o punta en los equipos tecnológicos. Marcar los dispositivos de esta manera no solo compromete su estética, sino que también podría interferir en su funcionalidad, afectando el uso futuro por parte de otros usuarios.

**UER-NG-R2-N6:** Para movilizar una impresora, proyector o escáner a otra área, se debe solicitar autorización al rector o al técnico informático con suficiente antelación. Además, es necesario contar con una autorización firmada, lo cual permite mantener un control sobre el uso y desplazamiento de los equipos tecnológicos.

**UER-NG-R3-N7:** Para utilizar un dispositivo de almacenamiento perteneciente a la Unidad Educativa "Rumiñahui", se debe solicitar con una hora de anticipación. Este dispositivo será devuelto durante el mismo día, y el pedido debe realizarse por escrito con la debida autorización. Este proceso garantiza la correcta gestión de los recursos compartidos.

**UER-NG-R4-N8:** Está prohibido cambiar la configuración de los dispositivos de red. Solo el técnico informático está autorizado para realizar este proceso, garantizando que la red se mantenga estable y segura, evitando alteraciones que puedan comprometer el acceso o la conectividad.

**UER-NG-R4-N8:** Está prohibido realizar cualquier tipo de adaptación en los dispositivos de red, como agregar routers o antenas sin autorización. Esto podría causar conflictos en la red y comprometer la seguridad y el rendimiento de la infraestructura tecnológica.

**UER-NG-R5-N9:** Está prohibido formatear o instalar cualquier software, aplicación o herramienta en los computadores sin la debida autorización del técnico informático. Esta norma busca prevenir la instalación de programas maliciosos o software no autorizado que pueda comprometer la seguridad de los sistemas.

**UER-NG-R6-N10:** Está prohibido realizar cualquier tipo de copia del software instalado en los computadores. Esta acción puede infringir leyes de propiedad intelectual y licencias de software, además de poner en riesgo la integridad de los sistemas al instalar copias no autorizadas.

**UER-NG-R6-N11:** Está prohibido desinstalar o actualizar cualquier tipo de software, aplicación o herramienta en los computadores sin autorización. Solo el técnico informático tiene permiso para gestionar este tipo de cambios, asegurando la compatibilidad y el funcionamiento óptimo del sistema.

**UER-NG-R7-N12:** Está prohibido rayar o escribir, con cualquier tipo de tinta o punta, sobre las mesas, sillas o paredes de las aulas o laboratorios. Estas acciones dañan el mobiliario y afectan la imagen y el ambiente de estudio, por lo que deben evitarse en todo momento.

**UER-NG-R8-N13:** Está prohibido dañar, sustraer o perjudicar la infraestructura física de cualquier área de la Unidad Educativa "Rumiñahui". El respeto por las instalaciones es esencial para garantizar su durabilidad y funcionalidad, manteniendo un entorno adecuado para el aprendizaje.

**UER-NG-R9-N14:** Está prohibido dañar, sustraer o perjudicar las instalaciones eléctricas, cableado, breaker o interruptores de cualquier área de la institución. Alterar el sistema eléctrico puede causar fallas, accidentes o poner en riesgo la seguridad de las personas dentro del plantel educativo.

**UER-NG-R9-N15:** Está prohibido conectar cualquier dispositivo electrónico que no pertenezca a la Unidad Educativa "Rumiñahui" sin previa autorización del técnico informático, del responsable de la actividad, o del rector. Esto ayuda a prevenir sobrecargas eléctricas, fallas en los sistemas o la instalación de dispositivos no seguros.

**UER-NG-R10-N16:** Está prohibido dañar, sustraer o perjudicar cualquier equipo del sistema de ventilación de la Unidad Educativa "Rumiñahui". Mantener estos equipos en buen estado es esencial para garantizar un ambiente cómodo y seguro en las instalaciones.

**UER-NG-R10-N17:** Está prohibido cambiar la configuración o programar los aires acondicionados, permitiéndose únicamente el uso de funciones comunes para la ambientación de las áreas. Cualquier ajuste incorrecto puede comprometer el rendimiento del equipo y afectar el confort en los espacios.

**UER-NG-R11-N18:** Está prohibido dañar, sustraer o perjudicar las cámaras de videovigilancia. Las cámaras son esenciales para garantizar la seguridad de las instalaciones, y cualquier manipulación o daño comprometería la vigilancia.

**UER-NG-R11-N19:** Está prohibido dañar o tapar el lente de las cámaras de videovigilancia de la Unidad Educativa "Rumiñahui". Obstruir la visión de las cámaras podría poner en riesgo la seguridad de las personas y los bienes dentro de la institución.

**UER-NG-R11-N20:** Está prohibido desconectar las cámaras de videovigilancia. Estas cámaras son una herramienta fundamental para el monitoreo continuo de las instalaciones y su desconexión puede afectar la seguridad.

**UER-NG-R12-N21:** Está prohibido dañar, sustraer o perjudicar las sirenas de auxilio de la Unidad Educativa "Rumiñahui". Estas sirenas son vitales para la seguridad y su correcto

funcionamiento es crucial en situaciones de emergencia.

**UER-NG-R12-N22:** Está prohibido desconectar las sirenas de auxilio. Estas deben permanecer siempre en funcionamiento para alertar de posibles emergencias, ya que su desconexión comprometería la capacidad de respuesta de la institución ante una crisis.

**UER-NG-R12-N23:** Está prohibido activar de cualquier modo las sirenas de auxilio si no existe alguna emergencia. El uso indebido de las sirenas puede causar confusión y afectar la preparación de la institución para enfrentar una verdadera emergencia.

## 3.- Conclusiones

a.) El cumplimiento de las políticas ayudará a preservar la infraestructura tecnológica de la Unidad Educativa "Rumiñahui". Además, garantizará un uso adecuado de los recursos tecnológicos, permitiendo una gestión eficiente y evitando posibles daños o pérdidas. La implementación constante de estas políticas también contribuirá a mantener actualizados los equipos y asegurar un ambiente óptimo para el desarrollo académico y administrativo.

b.) La correcta aplicación de las normas ayudará a preservar la infraestructura tecnológica de la Unidad Educativa "Rumiñahui". Esto no solo protege los equipos, sino que también fomenta una cultura de responsabilidad entre docentes, estudiantes y personal administrativo. Mantener el cumplimiento de estas normas asegura un uso adecuado de los recursos tecnológicos y minimiza riesgos de mal uso o deterioro prematuro, mejorando la calidad educativa.

c.) La realización de una auditoría informática ayuda a identificar las debilidades y amenazas que puede enfrentar la infraestructura tecnológica de una institución, permitiendo así la creación de un plan de mejora. Este proceso es fundamental para asegurar que los sistemas se mantengan actualizados, seguros y eficientes. Además, la auditoría permite tomar decisiones informadas que pueden prevenir problemas futuros y mejorar el rendimiento general de los recursos tecnológicos disponibles.

## 4.- Recomendaciones

a.) A las autoridades de las instituciones educativas que tienen infraestructura tecnológica, que realicen auditorías informáticas de forma periódica. Esto permitirá identificar posibles vulnerabilidades y asegurar el correcto funcionamiento de los equipos y sistemas. Además,

ayudará a garantizar que los recursos tecnológicos se utilicen de manera eficiente, mejorando el rendimiento institucional y asegurando la protección de la información crítica de la institución.

b.) A los docentes, que usen la infraestructura tecnológica de manera adecuada y le saquen el mayor provecho. Esto implica no solo utilizarla en sus clases, sino también mantenerse actualizados en su manejo y conocer las herramientas más avanzadas que pueden enriquecer el proceso de enseñanza-aprendizaje. El uso eficiente de estos recursos también contribuye al desarrollo de competencias digitales en los estudiantes.

c.) A los estudiantes, que usen la infraestructura tecnológica para ampliar sus conocimientos. El aprovechamiento adecuado de estos recursos no solo facilita el aprendizaje, sino que también fomenta habilidades tecnológicas que serán cruciales para su desarrollo académico y profesional. Además, es importante que los estudiantes sean responsables en el uso de la tecnología, cuidando los equipos y respetando las normas establecidas por la institución.

# CAPITULO VI

## 6. Conclusiones y recomendaciones

### 6.1. Conclusiones

• Una vez realizada la fundamentación teórica sobre auditoría de seguridad informática e infraestructura tecnológica, ayudó a tener una mejor comprensión de lo que implica una auditoría de seguridad informática. Además, permitió identificar claramente el proceso que se debe seguir para ejecutar una auditoría de manera eficiente y efectiva, asegurando que todos los elementos relevantes sean evaluados. Esta base teórica proporciona una perspectiva completa de los principios de seguridad en el ámbito informático.

• Una vez realizado el estudio de campo sobre la infraestructura tecnológica existente en la Unidad Educativa "Rumiñahui", se pudo identificar las amenazas, riesgos y vulnerabilidades más relevantes en el entorno. Esta información sirvió como insumo esencial para la auditoría informática, proporcionando datos precisos y necesarios para realizar un análisis detallado. Al mismo tiempo, permitió a los tomar decisiones informadas sobre las áreas que requieren una mayor atención y posibles mejoras.

• Una vez efectuada la auditoría de seguridad informática de la infraestructura tecnológica en la Unidad Educativa "Rumiñahui", se elaboró el informe final de auditoría, en el cual se incluyeron políticas y normas de control claras sobre el uso de los recursos tecnológicos. Este informe proporcionó recomendaciones específicas para mejorar la seguridad tecnológica, abordando las áreas de mayor vulnerabilidad. Además, incluyó una serie de sugerencias prácticas para fortalecer el control interno en la institución.

• Al finalizar la auditoría de seguridad informática de la infraestructura tecnológica en la Unidad Educativa "Rumiñahui", se creó una guía exhaustiva para el correcto uso de la infraestructura tecnológica. Esta guía incluye procedimientos detallados y buenas prácticas que garantizan la protección de los sistemas y la continuidad de las operaciones

tecnológicas. Además, se presentó un plan de capacitación dirigido a los usuarios para asegurar que comprendan la importancia del uso seguro de los recursos tecnológicos.

## 6.2. Recomendaciones

• A las autoridades de las instituciones educativas, sin importar el nivel de educación, se les recomienda realizar un proceso de auditoría interna para evaluar el estado de sus bienes o recursos. De esta manera, podrán crear un plan de contingencia efectivo, tomando las acciones correctivas necesarias. Este proceso debe incluir una revisión periódica de los sistemas de seguridad, asegurando que se mantengan al día con los avances tecnológicos y las nuevas amenazas.

• A las autoridades de las instituciones educativas, se les recomienda adquirir una librería digital o recursos relacionados con la ejecución de una auditoría informática, lo que les permitirá realizar este proceso de manera eficiente. Este proceso debería realizarse de forma periódica para identificar debilidades y fortalecer el uso, así como el cuidado de los recursos informáticos. Además, es importante que se contemple la actualización de estos recursos de manera continua para mantenerse alineados con las innovaciones tecnológicas.

• A los docentes, se les recomienda usar la tecnología de manera activa e innovadora en el proceso de enseñanza-aprendizaje. Hoy en día, la educación avanza con mayor rapidez cuando se emplean herramientas tecnológicas que potencien el aprendizaje. Asimismo, es esencial que los docentes reciban capacitación constante sobre nuevas plataformas y metodologías tecnológicas que les permitan mejorar la calidad educativa que ofrecen.

• A los estudiantes, se les recomienda aprovechar al máximo los recursos tecnológicos que tienen a su disposición en las instituciones educativas. Además, deben ser conscientes de la importancia de cuidar estos recursos, ya que son bienes que benefician a toda la comunidad. Al mantener en buen estado estos equipos, no solo aseguran su propia formación, sino también el acceso continuo para futuras generaciones de estudiantes.

• A los investigadores, se les recomienda utilizar la información obtenida en esta investigación, ya que es útil para seguir desarrollando nuevos estudios relacionados con auditorías informáticas. Esta investigación puede servir de base para análisis comparativos o para desarrollar propuestas más avanzadas en el campo de la seguridad

tecnológica. Además, su aplicación en diversos contextos educativos podría abrir nuevas líneas de investigación en el área.

**Bibliografía**


Angamarca, L. (2022). Estrategias de auditoría informática en la era de la transformación digital. *Technology Rain Journal*, *1*(1), e1-e1.

Albarracín Zambrano, L. O., Marín Vilela, C. M., Lozada Calle, J. C., & Martínez Matute,

Avila-Torres, R. A., & Cuenca-Tapia, J. P. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. *Domino de las Ciencias*, *7*(4), 363-376.

Bárcenas Cruz, V. A., Baños López, D. A., & Ponce Martínez, N. S. (2023). *Prototipo de infraestructura de nube comunitaria multi-región orientada a proporcionar servicios fundamentales* (Doctoral dissertation, Universidad de El Salvador).

Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., & Schubert, T. (2021). El impacto del software y el hardware de código abierto en la independencia tecnológica, la competitividad y la innovación en la economía de la UE. *Informe final del estudio. Comisión Europea, Bruselas, doi*, *10*, 430161.

Castillo Vera, O. (2021). Evaluación de metodologías de hacking ético para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa de servicios logísticos.

Castro Maldonado, J. J., Gómez Macho, L. K., & Camargo Casallas, E. (2023). La investigación aplicada y el desarrollo experimental en el fortalecimiento de las competencias de la sociedad del siglo XXI. *Tecnura*, *27*(75), 140-174.

CRUZ ROMERO, I. S. R. A. E. L. (2024). *Optimización de la Gestión del Alcance en Proyectos de Infraestructura TI con la integración efectiva de la metodología PMI* (Doctoral dissertation).

Chacón, L. J. R., Morales, G. E. R., Luna, A. C. P., Medina, J. H. C., & Cantuña-Vallejo, P. F. (2022). El Muestreo Intencional No Probabilístico como herramienta de la investigación científica en carreras de Ciencias de la Salud. *Universidad y Sociedad*, *14*(S5), 681-691.

Chiquito Manrique, C. D. (2023). *IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL HOSPITAL BÁSICO JIPIJAPA MEDIANTE UN APPLIANCE FORTINET 80E* (Bachelor's thesis, Jipijapa-Unesum).

Chirinos Chirinos, R. C. (2023). Diseño de un de plan de recuperación ante desastres (DRP) para salvaguardar la infraestructura de tecnologías de la información TI en la empresa Miranda y Amado.

Dally, B. (2023, agosto). Hardware para Deep Learning. En *2023 IEEE Hot Chips 35 Symposium (HCS)* (pp. 1-58). Sociedad de Computación IEEE.

Gauthier, M., & Budán, P. D. (2023). SETIC: un Software Educativo sobre el Funcionamiento de las Partes de un Computador. In *XXVIII Congreso Argentino de Ciencias de la Computación (CACIC)(La Rioja, 3 al 6 de octubre de 2022)*.

Goicochea Pozo, J. L. (2023). Integración de plataformas de monitoreo de infraestructura de redes para mejorar la gestión de TI en la empresa SEDALIB SA.

Guamán, M., Zenteno, J. A. C., Urgilés, C. F., Urgilés, C. F., & Egas, M. R. (2023). Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *7*(49), 139-165.

Hernández González, O. (2021). Aproximación a los distintos tipos de muestreo no probabilístico que existen. *Revista cubana de medicina general integral*, *37*(3).

Ibarra Bolaños, A. A., & Navaez Hernandez, C. A. (2023). Sistema de gestión de seguridad de la información con estándares ISO/IEC 27001 y Magerit en la empresa SP SISTEMAS PALACIOS LTDA de la ciudad de Pasto.

Jiménez Tello, C. E. (2023). *Propuesta de implementación de infraestructura de software en una red hiperconvergente dentro del sector de las PYMES de servicios* (Bachelor's thesis, Universidad del Azuay).

J. P. (2021). Auditoría informática dentro de la empresa "Promaelec" de la ciudad de Quevedo, en tiempo de COVID-19. *Revista Universidad y Sociedad, 13*(5), 345-354.

Lopezosa, C. (2020). Entrevistas semiestructuradas con NVivo: pasos para un análisis cualitativo eficaz. *Lopezosa C, Díaz-Noci J, Codina L, editores Methodos Anuario de Métodos de Investigación en Comunicación Social, 1. Barcelona: Universitat Pompeu Fabra; 2020. p. 88-97.*

López, M. A. A., & Beneyto, G. P. (2020). Los sistemas de información y la auditoría informática aplicados a una institución fiscalizadora subestatal: la Sindicatura de Comptes de la Comunidad Valenciana (España). Revista de Gestão e Secretariado, 11(2), 120-138.

Lourido, W. A. B. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. CIENCIAMATRIA, 5(1), 73-87.

Macias, M. M. M., Macias, R. W. M., Navarrete, M. L. I., & Navarrete, J. A. I. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *5*(4), 584-599.

Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In *2023 International conference on cyber management and engineering (CyMaEn)* (pp. 117-122). IEEE.

Martín, T. D. L. R. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, *13*(5), 495-506.

Menjívar Pino, G. A., Hernández Lemus, V. H., Alvarado Cáceres, D. A., & Tejada Contreras, E. O. (2021). *Modelo de Procesos de Auditoría Informática, basado en un estudio de las normas, técnicas y buenas prácticas relacionadas* (Doctoral dissertation, Universidad de El Salvador).

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

Montalbán, E. A. R., Gómez, R. J. M., & Borré, D. A. F. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Aglala*, *11*(1), 227-245.

Mucha-Hospinal, L. F., Chamorro-Mejía, R., Oseda-Lazo, M. E., & Alania-Contreras, R. D. (2021). Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado. *Desafíos*, *12*(1), 50-57.

Narváez Cerezo, A. D. (2023). *Análisis de políticas de seguridad aplicables a infraestructuras tecnológicas del Gobierno Autónomo Descentralizado del cantón Babahoyo* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).

Padilla-Avalos, C. A., & Marroquín-Soto, C. (2021). Enfoques de investigación en odontología: cuantitativa, cualitativa y mixta. *Revista estomatologica herediana*, *31*(4), 338-340.

Palomino Sysoeva, D. A., & Villegas Rojas, C. A. (2022). Propuesta de una metodología de auditoría informática para la oficina de Auditoría Interna de la Universidad Andina del Cusco.

Piedra, J. A. M., & Manqueros, J. M. C. (2021). El muestreo y su relación con el diseño metodológico de la investigación. *Manual de temas nodales de la investigación cuantitativa. un abordaje didáctico*, *81*.

Polanía Reyes, C. L., Cardona Olaya, F. A., Castañeda Gamboa, G. I., Vargas, I. A., Calvache Salazar, O. A., & Abanto Vélez, W. I. (2020). Metodología de investigación Cuantitativa & Cualitativa.

Portilla Menacho, G. E., & Honorio Valverde, C. F. (2022). Aplicación del método analítico-sintético para mejorar la comprensión de textos argumentativos en los estudiantes del cuarto grado de educación secundaria de la IEP “Buena Esperanza” del Distrito de Nuevo Chimbote,

2021.
Postigo Palacios, A. (2020). *Seguridad informática (Edición 2020)*. Ediciones Paraninfo, SA.
Riofrio, M. T., Singo, C. P., Baque, C. G., Espinosa, J. R., & Gaona, B. M. (2023). Modernización de Infraestructura tecnológica: Diseño de un software de gestión de información y mejora del sistema de cableado estructurado. *Domino de las Ciencias*, *9*(3), 1266-1283.

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

Romero-Martínez, M., Barrientos-Gutiérrez, T., Cuevas-Nasu, L., Bautista-Arredondo, S., Colchero, M. A., Gaona-Pineda, E. B., ... & Shamah-Levy, T. (2021). Metodología de la Encuesta Nacional de Salud y Nutrición 2021. *salud pública de méxico*, *63*(6), 813-818.

Sánchez Contreras, J. A. (2023). *Estudio comparativo de las infraestructuras de las TI y herramientas informáticas para mitigar ataques distribuidos de denegación de servicio* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).
Sandoval Forero, E. A. (2022). El trabajo de campo en la investigación social en tiempos de pandemia. *Espacio Abierto. Cuaderno Venezolano de Sociología*, *31*(3), 10-22.

Sarguera, R. B., Montero, A. R. C., & Quinter, A. P. (2024). El método inductivo-deductivo es solo una entelequia filosófica. *Revista Cubana de Educación Superior*, *43*(2 may-ago), 261-279.

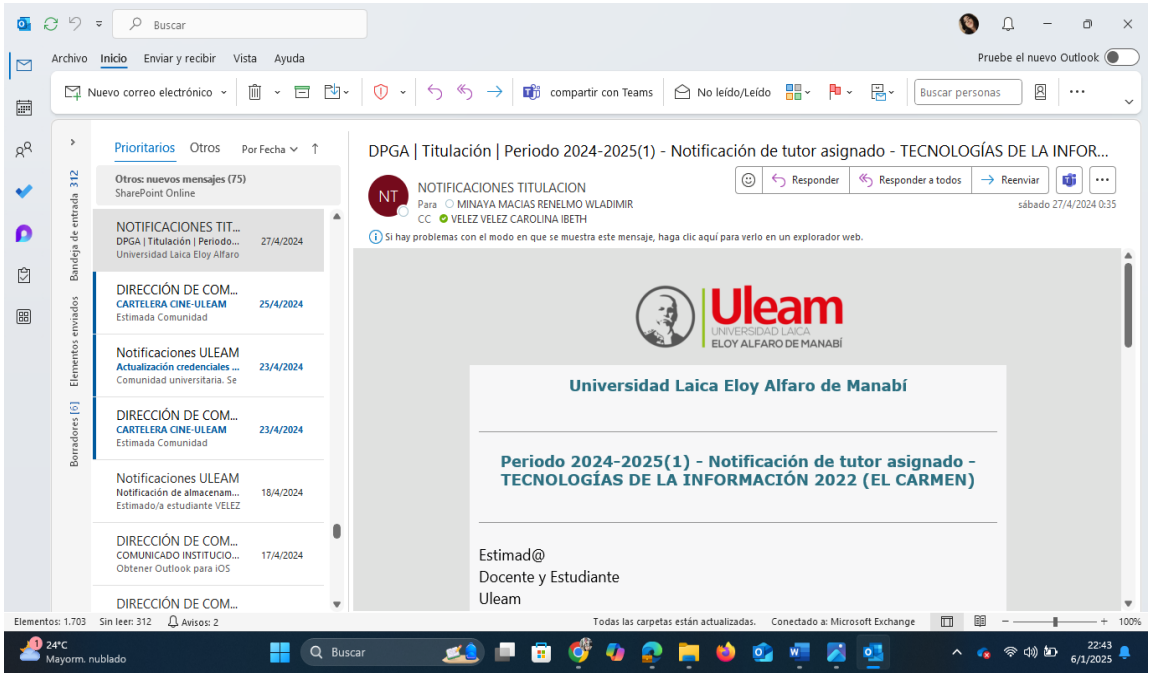
Vargas Diaz, M. M. (2023). Diseño de un plan de seguridad informática en la Alcaldía de la Jagua de Ibirico-Cesar.

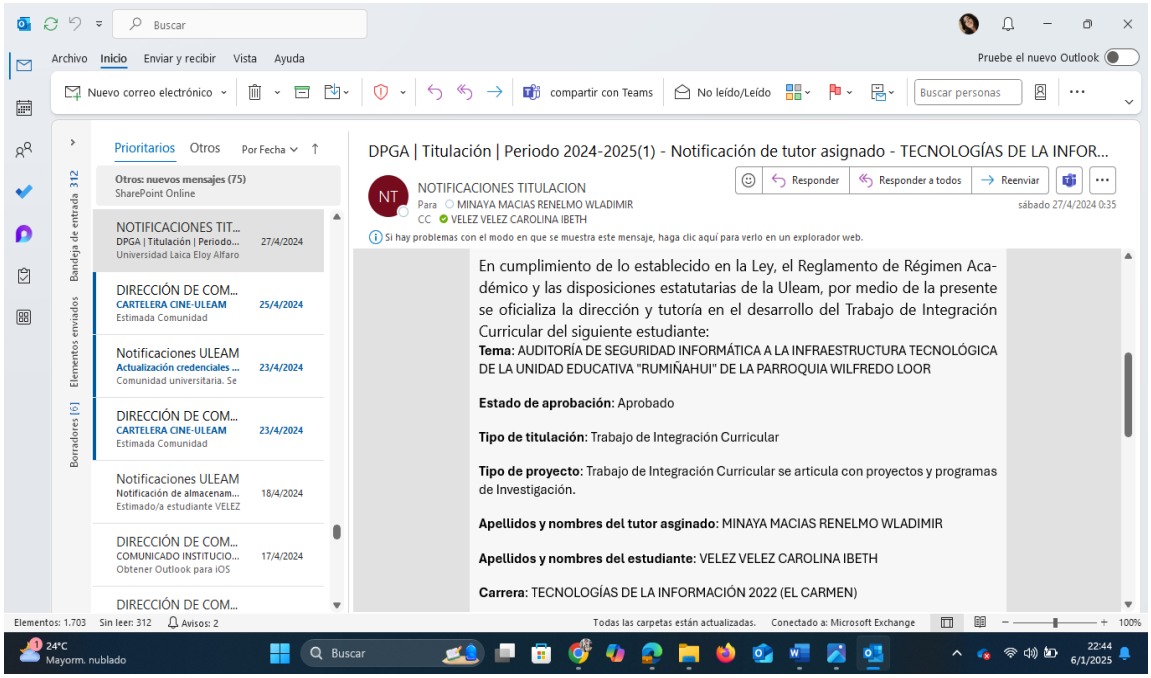
Xing, Y., & Li, S. (2021). Una implementación de hardware compacta del mecanismo de intercambio de claves seguro CCA CRYSTALS-KYBER en FPGA. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 328-356.

Zamora Naranjo, A. P. (2023). Propuesta de mejora para el área de TI basada en la implementación de una plataforma de software defined data center con infraestructura hiperconvergente en Banco Bolivariano Guayaquil-Ecuador, 2021.

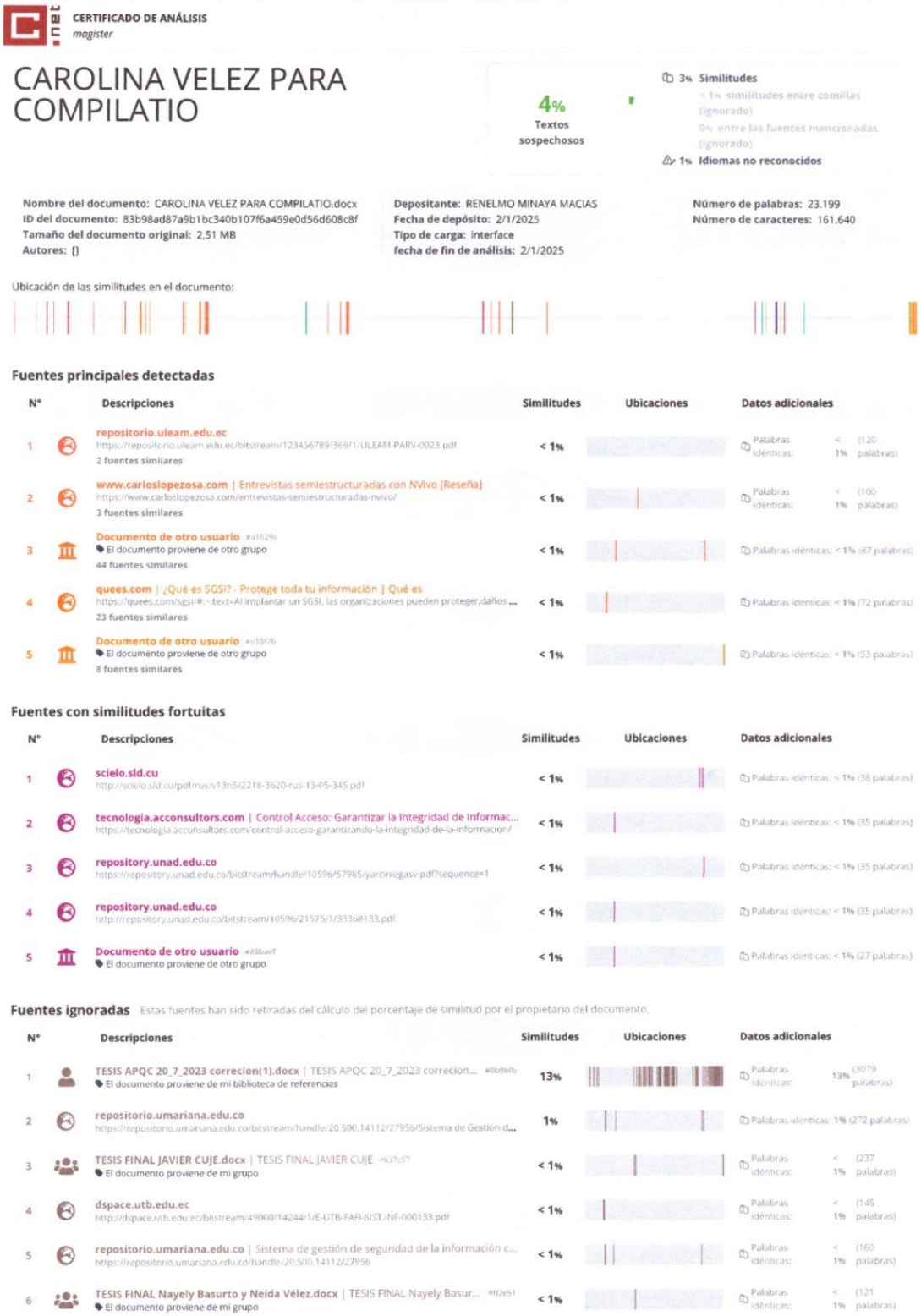
## Anexos.

## Anexo 1: Aprobación del tema (revisar en correo Notificación Titulación)



## Anexo 2: Certificado de análisis Compilatio con firma de tutor (digital o física)



CERTIFICADO DE ANÁLISIS
*magister*

# CAROLINA VELEZ PARA COMPILATIO

**4%** Textos sospechosos

3% Similitudes
< 1% similitudes entre comillas (ignorado)
0% entre las fuentes mencionadas (ignorado)
1% Idiomas no reconocidos

**Nombre del documento:** CAROLINA VELEZ PARA COMPILATIO.docx
**ID del documento:** 83b98ad87a9b1bc340b107f6a459e0d56d608c8f
**Tamaño del documento original:** 2,51 MB
**Autores:** []

**Depositante:** RENELMO MINAYA MACIAS
**Fecha de depósito:** 2/1/2025
**Tipo de carga:** interface
**fecha de fin de análisis:** 2/1/2025

**Número de palabras:** 23.199
**Número de caracteres:** 161.640

Ubicación de las similitudes en el documento:

### Fuentes principales detectadas

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | repositorio.uleam.edu.ec<br>https://repositorio.uleam.edu.ec/bitstream/123456789/369/1/ULEAM-PARV-0023.pdf<br>2 fuentes similares | < 1% | | Palabras idénticas: < 1% (120 palabras) |
| 2 | www.carloslopezosa.com \| Entrevistas semiestructuradas con NVivo [Reseña]<br>https://www.carloslopezosa.com/entrevistas-semiestructuradas-nvivo/<br>3 fuentes similares | < 1% | | Palabras idénticas: < 1% (100 palabras) |
| 3 | Documento de otro usuario #a162fa<br>El documento proviene de otro grupo<br>44 fuentes similares | < 1% | | Palabras idénticas: < 1% (87 palabras) |
| 4 | quees.com \| ¿Qué es SGSI? - Protege toda tu información \| Qué es<br>https://quees.com/sgsi/#:~:text=Al implantar un SGSI, las organizaciones pueden proteger,daños ...<br>23 fuentes similares | < 1% | | Palabras idénticas: < 1% (72 palabras) |
| 5 | Documento de otro usuario #e15f7b<br>El documento proviene de otro grupo<br>8 fuentes similares | < 1% | | Palabras idénticas: < 1% (53 palabras) |

### Fuentes con similitudes fortuitas

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | scielo.sld.cu<br>http://scielo.sld.cu/pdf/rus/v13n5/2218-3620-rus-13-05-345.pdf | < 1% | | Palabras idénticas: < 1% (38 palabras) |
| 2 | tecnologia.acconsultors.com \| Control Acceso: Garantizar la Integridad de Informac...<br>https://tecnologia.acconsultors.com/control-acceso-garantizando-la-integridad-de-la-informacion/ | < 1% | | Palabras idénticas: < 1% (35 palabras) |
| 3 | repository.unad.edu.co<br>https://repository.unad.edu.co/bitstream/handle/10596/57985/yarciniegasv.pdf?sequence=1 | < 1% | | Palabras idénticas: < 1% (35 palabras) |
| 4 | repository.unad.edu.co<br>http://repository.unad.edu.co/bitstream/10596/21575/1/33368133.pdf | < 1% | | Palabras idénticas: < 1% (35 palabras) |
| 5 | Documento de otro usuario #d8baef<br>El documento proviene de otro grupo | < 1% | | Palabras idénticas: < 1% (27 palabras) |

### Fuentes ignoradas

Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | TESIS APQC 20_7_2023 correcion(1).docx \| TESIS APQC 20_7_2023 correcion... #0b9bfb<br>El documento proviene de mi biblioteca de referencias | 13% | | Palabras idénticas: 13% (3079 palabras) |
| 2 | repositorio.umariana.edu.co<br>https://repositorio.umariana.edu.co/bitstream/handle/20.500.14112/27956/Sistema de Gestión d... | 1% | | Palabras idénticas: 1% (272 palabras) |
| 3 | TESIS FINAL JAVIER CUJE.docx \| TESIS FINAL JAVIER CUJE #637c57<br>El documento proviene de mi grupo | < 1% | | Palabras idénticas: < 1% (237 palabras) |
| 4 | dspace.utb.edu.ec<br>http://dspace.utb.edu.ec/bitstream/49000/14244/1/E-UTB-FAFI-SIST.INF-000133.pdf | < 1% | | Palabras idénticas: < 1% (145 palabras) |
| 5 | repositorio.umariana.edu.co \| Sistema de gestión de seguridad de la información c...<br>https://repositorio.umariana.edu.co/handle/20.500.14112/27956 | < 1% | | Palabras idénticas: < 1% (160 palabras) |
| 6 | TESIS FINAL Nayely Basurto y Neida Vélez.docx \| TESIS FINAL Nayely Basur... #f2e51<br>El documento proviene de mi grupo | < 1% | | Palabras idénticas: < 1% (121 palabras) |

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 7 | repositorioinstitucional.ufpso.edu.co<br>https://repositorioinstitucional.ufpso.edu.co/bitstream/handle/20.500.14167/3343/Diseño de un ... | < 1% | | Palabras idénticas: < 1% (107 palabras) |
| 8 | Tesis final Andy Cruz.docx \| Tesis final Andy Cruz #cac433<br>El documento proviene de mi grupo | < 1% | | Palabras idénticas: < 1% (82 palabras) |
| 9 | repository.unad.edu.co<br>http://repository.unad.edu.co/bitstream/10596/14253/1/1003165759.pdf | < 1% | | Palabras idénticas: < 1% (91 palabras) |
| 10 | www.doi.org<br>https://www.doi.org/10.23919/CISTI.2018.8399252 | < 1% | | Palabras idénticas: < 1% (53 palabras) |
| 11 | Documento de otro usuario #eecfd9<br>El documento proviene de otro grupo | < 1% | | Palabras idénticas: < 1% (30 palabras) |
| 12 | Documento de otro usuario #5ide15<br>El documento proviene de otro grupo | < 1% | | Palabras idénticas: < 1% (32 palabras) |
| 13 | repository.unad.edu.co<br>http://repository.unad.edu.co/bitstream/10596/6340/1/98396710.pdf | < 1% | | Palabras idénticas: < 1% (20 palabras) |
| 14 | repositorio.umariana.edu.co<br>https://repositorio.umariana.edu.co/bitstream/handle/20.500.14112/27956/RAI.pdf?sequence=2 | < 1% | | Palabras idénticas: < 1% (19 palabras) |
| 15 | dialnet.unirioja.es<br>https://dialnet.unirioja.es/descarga/articulo/8977055.pdf | < 1% | | Palabras idénticas: < 1% (16 palabras) |

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

## Anexo 3: Cuestionario de la encuesta

Estimado estudiante:
**UNIDAD EDUCATIVA "RUMIÑAHUI"**
Presente.-
Los resultados obtenidos en el presente cuestionario serán exclusivamente para fines investigativos y desarrollo de la presente tesis, los datos personales de los participantes no serán divulgados.
La encuesta está formada por preguntas de respuesta corta para medir: el nivel de satisfacción, el grado de importancia, la frecuencia de ocurrencia, el grado de dificultad y el nivel de desacuerdo que tienen los estudiantes con respecto al laboratorio de informática e infraestructura tecnológica.
(seleccione una de las respuesta)

**PREGUNTAS DE ENCUESTAS**
**(Estudiantes)**

**1. ¿Qué tan satisfecho está con la experiencia en el laboratorio de informática de la Unidad educativa "Rumiñahui"?**
Completamente satisfecho
Muy satisfecho
Satisfecho
Poco satisfecho
Nada satisfecho

**2. ¿Qué tan importante considera que es el laboratorio de informática para los estudiantes?**
Completamente importante
Muy importante
Importante
Poco importante
Nada importante

**3. ¿Con que frecuencia le gustaría recibir clases en el laboratorio de informática?**
Completamente frecuente
Muy frecuente
frecuente
Poco frecuente
Nada frecuente

**4. ¿Cómo considera el uso de las aplicaciones informáticas para realizar tus investigaciones o trabajos?**
Completamente importante
Muy importante
Importante
Poco importante
Nada importante

**5. ¿Las autoridades cuidan el buen funcionamiento del laboratorio de informática de la Unidad educativa "Rumiñahui"?**
Completamente frecuente
Muy frecuente
frecuente
Poco frecuente
Nada frecuente

**6. ¿Qué tan importante consideras el uso de cámaras de seguridad en todas las áreas de la Unidad educativa "Rumiñahui"?**
Completamente importante
Muy importante
Importante
Poco importante
Nada importante

**7. ¿Qué tan difícil se te hace conectarte a una red wifi en la Unidad educativa "Rumiñahui"?**
Completamente difícil
Muy difícil
Difícil
Poco difícil
Nada difícil

**8. ¿Qué tan importante considera la implementación de puntos wifi en todas las áreas de la Unidad educativa "Rumiñahui"?**
Completamente importante
Muy importante
Importante
Poco importante
Nada importante

**9. ¿Qué tan importante consideras la implementación de sirenas de auxilio en todas las áreas de la Unidad educativa "Rumiñahui"?**
Completamente importante
Muy importante
Importante
Poco importante
Nada importante

## Anexo 4: Guía de la entrevista.

Estimada autoridad:
(rector – vicerector – inspector)
**UNIDAD EDUCATIVA "RUMIÑAHUI"**
Presente. -

Los resultados obtenidos en la presente entrevista serán exclusivamente para fines investigativos y desarrollo de la presente tesis, los datos personales de los participantes no serán divulgados.
La encuesta está formada por preguntas de respuesta corta para medir: el nivel de satisfacción, el grado de importancia, la frecuencia de ocurrencia, el grado de dificultad y el nivel de desacuerdo que tienen los estudiantes con respecto al laboratorio de informática. (seleccione una de las respuestas)

**PREGUNTAS DE ENTREVISTAS**
**(Docentes con funciones de autoridad)**

1. ¿Qué tan satisfecho está con la experiencia en el laboratorio de informática de la Unidad educativa "Rumiñahui"?
2. ¿Qué tan importante considera que es el laboratorio de informática para los estudiantes y docentes?
3. ¿Con que frecuencia le gustaría dar clases en el laboratorio de informática?
4. ¿Qué tan difícil se le hace utilizar las aplicaciones informáticas para dar clases?
5. ¿Las autoridades cuidan el buen funcionamiento del laboratorio de informática de la Unidad educativa "Rumiñahui"?
6. ¿Existe cobertura wifi, en todas las áreas de la Unidad educativa "Rumiñahui"?
7. ¿Considera necesario la implementación de sirenas de auxilio en todas las áreas de la Unidad educativa "Rumiñahui"?
8. ¿Se debería implementar más cámaras de seguridad en todas las áreas de la Unidad educativa "Rumiñahui"?
9. ¿El clave wifi debe ser la misma para docentes y estudiantes?
10. ¿Se debería instalar un computador con internet y proyector en cada una de las aulas de clases?
11: ¿Con que frecuencia se realizan mantenimiento preventivo y correctivo de la infraestructura tecnológica?
12. ¿Unidad educativa "Rumiñahui" cuenta con políticas y normas estandarizadas de control sobre el uso de la infraestructura tecnológica?

## Anexo 5: Fichas de Observación

| NOMBRE DEL DOCUMENTO | IDENTIFICACIÓN: | |
|---|---|---|
| FICHA DE LEVANTAMIENTO DE INFORMACION IN SITU | CV-001-2024 | |
| **PROCEDIMIENTO:** | ESTUDIO DE CAMPO | |
| AREA INFORMÁTICA | AUDITORIA INFORMÁTICA | |

**PERIODO ACADÉMICO 2024(2)**

| | | | |
|---|---|---|---|
| **ENTIDAD:** | | **HORA:** | |
| **AUDITOR:** | | **FECHA:** | |

**FICHA DE LEVANTAMIENTO DE INFORMACIÓN HARDWARE Y SOFTWARE IN SITU**

**INFORMACIÓN VISUAL**

| **IDENTIFICACIÓN DEL EQUIPO:** | **USUARIO:** | **FECHA:** |
|---|---|---|

**ELEMENTOS HARDWARE:**

| | | | |
|---|---|---|---|
| Periférico 1: | Serial: | Marca: | Observación: |
| Periférico 2: | Serial: | Marca: | Observación: |
| Periférico 3: | Serial: | Marca: | Observación: |
| Periférico 4: | Serial: | Marca: | Observación: |
| Periférico 5: | Serial: | Marca: | Observación: |

**ELEMENTOS SOFTWARE:**

| | | | |
|---|---|---|---|
| Sistema Operativo: | Versión: | Estado: | Clave: |
| Programa/Paquete: | Versión: | Estado: | Clave: |
| Utilitarios: | Versión: | Estado: | Clave: |
| Software 1: | Versión: | Estado: | Clave: |
| Software 2: | Versión: | Estado: | Clave: |
| Software 3: | Versión: | Estado: | Clave: |
| Software 4: | Versión: | Estado: | Clave: |

Vulnerabilidad: _____

**CONECTIVIDAD:**

| | | | | | |
|---|---|---|---|---|---|
| Tipo de Conexión Internet: | Cable: | | Switch | Velocidad de Conexión: | Subida: |
| | Inalambrica: | | Router | | Bajada: |
| | Mixta: | | | | |
| | | | | | Subida: |
| Distancia del punto de acceso inalambrico: | | | | | Bajada: |

**OBSERVACIONES:**

## Anexo 6: Ficha de evaluación de activos

| NOMBRE DEL DOCUMENTO | IDENTIFICACIÓN: | |
|---|---|---|
| FICHA DE LEVANTAMIENTO DE INFORMACION IN SITU | CV-002-2024 | |
| **PROCEDIMIENTO:** | ESTUDIO DE CAMPO | |
| AREA INFORMÁTICA | AUDITORIA INFORMÁTICA | |

| **PERIODO ACADÉMICO 2024(2)** | | | |
|---|---|---|---|
| **ENTIDAD:** | | **HORA:** | |
| **AUDITOR:** | | **FECHA:** | |

| **FICHA DE LEVANTAMIENTO DE INFORMACIÓN DE INSTALACIONES IN SITU** |
|---|
| **INFORMACIÓN VISUAL** |
| **LUGAR:** |
| **INSTALACIONES**<br>1. Los muebles y enseres se encuentran: |
| 2. La distribución de los PC se encuentran: |
| 3. Las instalaciones de Red Eléctrica se encuentran: |
| 4. Las instalaciones de Red de Datos se encuentran: |
| 5. La ventilación e iluminación se encuentra: |
| 6. La seguridad se encuentra: |
| **HARDWARE**<br>1. Los equipos PC están bien identificados (Sellos, etiquetas, entre otros):<br><br>2. El estado físico de los (PC) se encuentran: |
| CRITERIO PREVIO AL INFORME DE AUDITORIA: |

**Glosario**

1. **Auditoría de Seguridad Informática:** Proceso de evaluación sistemática de los sistemas informáticos para identificar vulnerabilidades y verificar el cumplimiento de políticas de seguridad.

2. **Infraestructura Tecnológica:** Conjunto de hardware, software, redes y servicios que sustentan el funcionamiento de sistemas informáticos en una organización.

3. **Riesgo Informático:** Posibilidad de que una amenaza explote una vulnerabilidad, causando daño a los sistemas o la información.

4. **Vulnerabilidad:** Debilidad en un sistema que puede ser explotada por amenazas para comprometer la seguridad.

5. **Amenaza:** Cualquier evento o acción que pueda causar daño a la infraestructura tecnológica.

6. **Firewall:** Dispositivo o software que controla el tráfico de red para bloquear accesos no autorizados.

7. **Antivirus:** Programa diseñado para detectar, prevenir y eliminar software malicioso.

8. **Política de Seguridad:** Conjunto de normas y procedimientos que establecen cómo proteger los activos informáticos.

9. **Gestión de Riesgos:** Proceso de identificación, evaluación y mitigación de riesgos de seguridad.

10. **Penetration Testing (Pentesting):** Simulación de ataques para evaluar la seguridad de sistemas y redes.

11. **Backup:** Copia de seguridad de datos para garantizar su recuperación en caso de pérdida.

12. **Seguridad Perimetral:** Medidas de protección implementadas en los límites de la red para prevenir accesos no autorizados.

13. **Normas ISO 27001:** Estándar internacional para gestionar la seguridad de la información.

14. **Control de Acceso:** Mecanismos que regulan quién puede acceder a sistemas y recursos.

15. **Logs:** Registros de actividades de sistemas que permiten monitorear y auditar eventos.

16. **Phishing:** Técnica de engaño para obtener información confidencial mediante correos o sitios falsos.

17. **Malware:** Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos.

18. **Criptografía:** Técnica de codificación de información para protegerla de accesos no autorizados.

19. **Normativa Legal:** Leyes y regulaciones que rigen la protección de datos y la seguridad informática.

20. **Mitigación:** Conjunto de acciones para reducir el impacto de posibles amenazas o ataques.