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 INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LABORATORIOS DE CÓMPUTOS DE LA CARRERA DE TI Y SOFTWARE "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN"

BASURTO MUÑOZ FERNANDA ELIZABETH

AUTORA

ING. CLARA GUADALUPE POZO HERNANDEZ, MGS

TUTORA

EL CARMEN, AGOSTO 2025

CERTIFICACIÓN

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

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante **BASURTO MUÑOZ FERNANDA ELIZABETH**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(2)-2025(1), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es "**Auditoría de seguridad informática a la infraestructura tecnológica de laboratorios de cómputos de la carrera de TI "Universidad Laica Eloy Alfaro de Manabí extensión El Carmen".** La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad del mismo, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

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

El Carmen, 18 de agosto del 2025

Lo certifico,

Ing. Clara Guadalupe Pozo Hernández, Mg.
Docente Tutor(a)
Área:

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 Laboratorios de Cómputos de la Carrera de TI "Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen".

Modalidad: Proyector Integrador

Autora: Basurto Muñoz Fernanda Elizabeth

Tutora: Ing. Pozo Hernandez Clara Guadalupe, Mg.

Tribunal de Sustentación:

Presidente:
Mg. Minaya Macias Renelmo Wladimir.

Miembro:
Ing. Mendoza Villamar Rocio Alexandra, Mg.

Miembro:
Ing. Reascos Pinchao Raul Saed, Mg.

Fecha de Sustentación: 10 de septiembre de 2025

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

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LABORATORIOS DE CÓMPUTOS DE LA CARRERA DE TI "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN", corresponde exclusivamente a: BASURTO MUÑOZ FERNANDA ELIZABETH con CI. 1351425176 y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Basurto Muñoz Fernanda Elizabeth
C.I. 1351425176

DEDICATORIA

A mi madre, por ser ese pilar fundamental en mi crecimiento profesional, por brindarme tu confianza y por tus consejos que me ayudaron a alcanzar mis metas. Eres mi mayor fuente de inspiración, la mujer que más amo y admiro. Gracias mi madre por tu apoyo incondicional, por creer en mí incluso en los momentos más difíciles cuando parecía imposible y por enseñarme que la perseverancia y el amor pueden con cualquier obstáculo. Has sido mi guía, mi fuerza y mi refugio en cada etapa de este camino ofreciéndome palabras de aliento y gestos de ternura cuando más los necesitaba. Este logro también es gracias a ti porque detrás de cada página y de cada meta que he alcanzado están tus palabras, tus consejos y tu cariño infinito.

Con cariño:

Fernanda Basurto

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, por abrirme las puertas y darme la oportunidad de desarrollarme profesionalmente. Quisiera agradecer a cada uno de los Ingenieros que compartieron sus conocimientos y experiencias, por sus enseñanzas y por el tiempo que dedicaron a nuestra formación.

En especial, extiendo mi gratitud a la Ing. Clara Pozo quien, con su carácter exigente y compromiso con la excelencia académica, me dejó valiosas lecciones que han impulsado mi trayectoria. Sus orientaciones, que en ocasiones me llevaron a enfrentar grandes desafíos y profundas reflexiones, me dejaron una valiosa lección: Que un buen maestro no es alguien que cede fácilmente ante el estudiante, sino alguien que se mantiene firme para sacar lo mejor de él y guiarlo hacia la excelencia.

Atentamente:

Fernanda Basurto Muñoz

ÍNDICE DE CONTENIDOS

ÍNDICE TABLAS

ÍNDICE GRÁFICOS E ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo tiene como objetivo realizar una auditoría de seguridad informática en la infraestructura tecnológica de los laboratorios de cómputo de las carreras de TI y Software de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, surgida ante la problemática del acceso no autorizado a los laboratorios que ha ocasionado anomalías y daños en los equipos tecnológicos. Para su desarrollo se emplearon enfoques cualitativos y cuantitativos recurriendo a fuentes académicas confiables entre ellas a una entrevista con el Ing. Bladimir Mora, coordinador de las carreras y una encuesta aplicada a una población finita de 149 estudiantes, con el fin de obtener resultados claros y precisos. La auditoría se efectuó en los laboratorios de cómputo 1 y 2, identificándose riesgos como robo, daño, incendio, inundación y malware de los cuales el robo y el malware fueron catalogados como muy graves, mientras que los demás representaron un nivel importante de riesgo lo que evidenció la necesidad de implementar medidas preventivas. Como propuesta final, se plantea un plan de mejora para el uso seguro de los laboratorios basado en un manual de políticas de seguridad y buenas prácticas complementado con la instalación de un sistema de cámaras de vigilancia que permita monitorear los accesos siendo esta una de las medidas más factibles y eficaces para reducir incidentes y garantizar un ambiente seguro en la infraestructura tecnológica de los laboratorios de la universidad.

ABSTRACT

The purpose of this paper is to conduct a computer security audit of the technological infrastructure of the computer labs of the IT and Software programs at the Universidad Laica Eloy Alfaro de Manabí, El Carmen Extension. This audit arose from the problem of unauthorized access to the labs, which has caused anomalies and damage to the technological equipment. Qualitative and quantitative approaches were used for its development, using reliable academic sources, including an interview with Eng. Bladimir Mora, coordinator of the programs, and a survey applied to a finite population of 149 students, in order to obtain clear and precise results. The audit was carried out in computer labs 1 and 2, identifying risks such as theft, damage, fire, flooding, and malware. Theft and malware were classified as very serious, while the others represented a significant level of risk, highlighting the need to implement preventive measures. As a final proposal, an improvement plan for the safe use of laboratories is proposed, based on a manual of security policies and best practices, complemented by the installation of a surveillance camera system to monitor access. This is one of the most feasible and effective measures to reduce incidents and ensure a safe environment in the technological infrastructure of the university's laboratories.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

La auditoría de seguridad informática física fue un proceso clave para identificar los riesgos y vulnerabilidades de la seguridad a los que están expuestos los activos tecnológicos de los laboratorios de cómputo, ya que esta área es fundamental para que las actividades y la institución mantengan un entorno eficiente y seguro.

Luego de llevar a cabo la implementación de la auditoría se analizaron detalladamente los resultados y los análisis exhaustivos con los cuales se identificaron necesidades específicas para fortalecer la seguridad de los activos tecnológicos dentro de los laboratorios. Enfocarse en estas áreas destaca la importancia de las medidas de seguridad para controlar el acceso de usuarios no autorizados y el uso indebido de equipos tecnológicos los cuales han sido factores que han provocado incidentes en esta área tecnológica.

La implementación de este mecanismo de evaluación contribuye a garantizar un entorno más seguro al proteger la infraestructura tecnológica y reducir los riesgos en los componentes tecnológicos. En este caso, la auditoría se realizó en los laboratorios de informática 1 y 2 de las carreras de TI y Software de la Universidad Laica Eloy Alfaro en Manabí, Extensión El Carmen, y se evaluaron cinco niveles de riesgo relacionados con la falta de medidas de seguridad. Estas medidas son básicas y es fundamental implementarlas.

Fue examinado para conocer a qué están expuestos y evaluar las medidas de seguridad lo que motivó a diseñar un manual de buenas prácticas el cual incluye políticas diseñadas para reducir riesgos. La infraestructura tecnológica de estos laboratorios requiere medidas preventivas de manera inmediata para garantizar el correcto funcionamiento y la protección de los equipos informáticos de los laboratorios

1.2 Presentación del tema

Auditoría de Seguridad Informática a la Infraestructura Tecnológica de Laboratorios de Cómputos de la carrera de TI & Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen.

1.3 Ubicación y contextualización de la problemática

La Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, se encuentra ubicada en la avenida 3 de Julio y Carlos Alberto Aray en el cantón El Carmen. Es considerada una de las mejores universidades dentro de la localidad; cuenta con un sistema de educación superior y una amplia oferta de carreras de tercer nivel. Cuenta con dos campos principales, como son el bloque central y el bloque de la granja; ambos ofrecen diversas carreras universitarias.

Tabla 1 Ubicación de la Universidad ULEAM, Extensión El Carmen

El presente proyecto de titulación se llevará a cabo una Auditoría de Seguridad Informática en la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, específicamente en el bloque central. El enfoque del proyecto será en los laboratorios de cómputos 1 y 2 de la planta alta en la carrera de Tecnología de la Información y Software. Los laboratorios están equipados de la siguiente manera.

El laboratorio 1 se encuentra en el aula 201, el cual está conformado por 24 estaciones mientras que en el laboratorio 2 se encuentra en el aula 207, con un total de 18 estaciones. Tanto las estaciones del laboratorio 1 como el 2 se encuentran equipadas con el mismo sistema operativos como es Windows y actualizada con la última versión.

1.4 Planteamiento del problema

Falta de controles para el uso de los equipos de los laboratorios de la carrera de Tecnología de la Información.

1.4.1 Problematización

En los laboratorios de cómputo de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, de las carreras de TI & Software, en las cuales se ha identificado falta de control sobre el uso de los equipos tecnológicos. Esta situación se vincula con uno de los principales factores: como son los accesos no autorizados, los cuales pueden causar pérdidas y fallos en los equipos. Estos hechos afectan de forma negativa el funcionamiento de los recursos en actividades académicas.

La falta de controles de seguridad como es el registro de ingreso, ya que personas sin autorización ingresan a los laboratorios teniendo acceso a todos los dispositivos de los laboratorios y monitoreo en el uso de los equipos sin restricciones. No se lleva un registro de ingreso ni de forma manual ni automática, lo que genera un entorno altamente vulnerable, lo que empeora la situación, ya que no existen responsables del área y no es monitoreada, creando un ambiente más vulnerable.

1.4.2 Génesis del problema

En los últimos meses, se ha evidenciado una serie de deficiencias en los laboratorios de cómputos con respecto al uso y control de los equipos. Se han podido notar diversos problemas como es en la gestión del manejo y el cuidado de los equipos que puede provocar daños profundos a los activos de los laboratorios entre las principales causas son:

Acceso no autorizado: Se ha podido observar que los estudiantes ingresan a los laboratorios sin autorización de acceso y sin restricciones al uso de los equipos, lo cual permite la posibilidad de que le den un mal uso a los equipos como la realización de actividades no académicas, desconexión de los componentes y dejar los equipos fuera de su funcionamiento adecuado. Esta situación es lo que ha provocado varios resultados negativos como daños y pérdidas de equipos dentro de los laboratorios de cómputo.

No existen responsables: Para los laboratorios de cómputo no existe un personal responsable que se encargue de llevar un registro de ingreso a los laboratorios en caso de que ocurra un incidente.

1.4.3 Estado actual del problema

Hoy en día, la infraestructura compuesta por equipos de cómputo, redes y sistemas interconectados son esenciales para el desarrollo académico. Facilita adquirir conocimiento eficiente, ya que tenemos acceso a recursos digitales. Sin embargo, la falta de controles adecuados ha provocado diversos desafíos en temas de seguridad informática como ya se mencionó antes entre los más frecuentes se encuentran el acceso no autorizado y el deterioro de los equipos por falta de controles.

La falta de restricciones ha permitido a los estudiantes utilizar los recursos tecnológicos sin supervisión, lo que ha generado problemas de seguridad y diversas anomalías. Los equipos han sufrido daños, pérdidas y deterioro como consecuencia de las deficiencias en la administración del laboratorio lo que también ha acortado su vida útil de los componentes tecnológicos.

1.5 Diagrama causa – efecto del problema

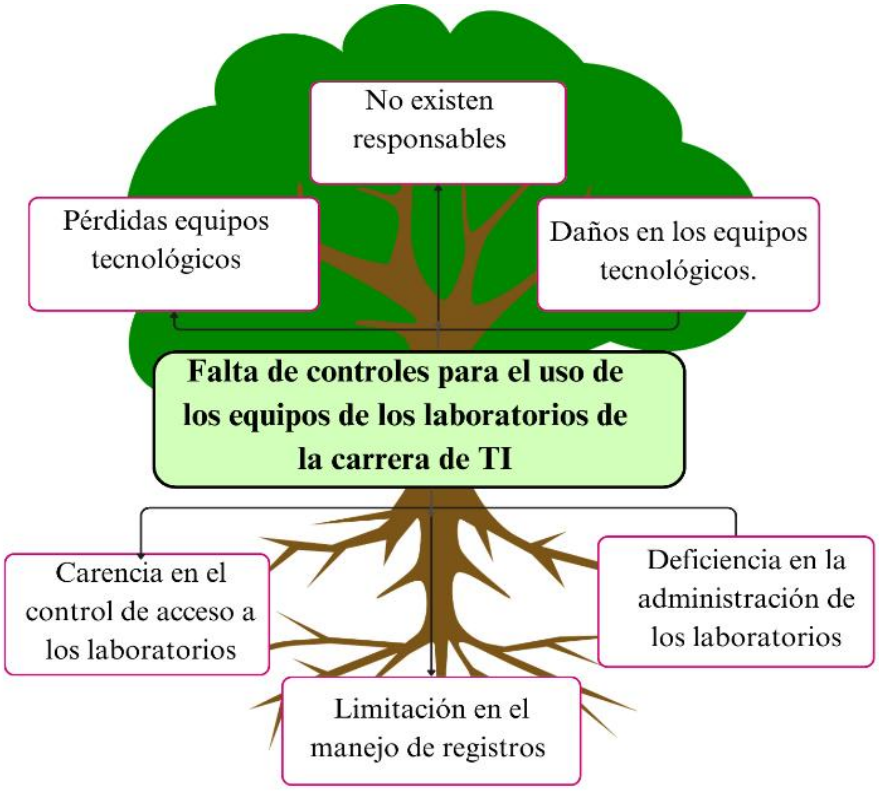


Ilustración 1 Causa-Efecto del Problema

1.6 Objetivos

1.6.1 Objetivo general

Realizar una Auditoría de Seguridad Informática a la Infraestructura Tecnológica de laboratorios de cómputos de las carreras de TI & Software "Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen".

1.6.2 Objetivos específicos

1. Identificar la problemática de investigación para evaluar las vulnerabilidades presentes en la infraestructura tecnológica de los laboratorios de cómputo.
2. Investigar en diferentes fuentes confiables sobre las variables relacionadas con la auditoría de seguridad informática y la infraestructura tecnológica para los equipos de los laboratorios de cómputo.
3. Diagnosticar el estado actual de la infraestructura tecnológica de los laboratorios de cómputos 1 y 2 mediante la aplicación de una auditoría de seguridad informática.
4. Verificar el nivel de seguridad de la infraestructura tecnológica dentro de los laboratorios aplicando una auditoría informática.
5. Elaborar un informe detallado de la Auditoría de Seguridad Informática sobre la infraestructura tecnológica de los laboratorios de cómputo.

1.7 Justificación

La falta de controles de seguridad en los laboratorios de cómputo de las carreras de TI y Software de la ULEAM se ha convertido en un tema que requiere una solución de forma inmediata. La situación actual de los laboratorios no solo afecta el estado de los activos, sino que también limita el desarrollo de las actividades académicas y prácticas de los diferentes niveles de ambas carreras. La falta de medidas de seguridad en los laboratorios dificulta dar soluciones de manera rápida y efectiva lo que conlleva a esta situación a tardará en resolver aumentando el riesgo y daños a los equipos.

La pérdida de infraestructura a causa de daños físicos y el deterioro de los equipos, resulta por diversos factores, tanto ambientales, mantenimiento deficiente o el uso inadecuado, surgiendo situaciones críticas cuando se presentan estos riesgos sin la protección adecuada para estos.

La ejecución de la auditoría demostrará de forma más detallada el estado actual de la seguridad informática dentro de los laboratorios, estableciendo recomendaciones para el mantenimiento continuo de la seguridad, beneficiando a los estudiantes que diariamente utilizan los laboratorios, teniendo un efecto positivo para la comunidad universitaria, al garantizar un entorno seguro y confiable.

1.7.1 Impacto social

Disponer de equipos tecnológicos en buen estado dentro de la institución y en nuestra área es un beneficio considerable para la comunidad universitaria, sobre todo en el área de Tecnologías de Información y Software que tiene como desafío el uso frecuente de dispositivos tecnológicos ya que estos componentes son las herramientas necesaria para realizar cualquier tipo de actividades, es muy importante que todos los equipos esté en óptimo estado y en buena calidad para el desarrollo de actividad.

Mediante la implementación de nuevas medidas de seguridad, deberán adaptarse a las políticas y procedimientos actualizados para el uso de equipos tecnologías en los laboratorios, con la finalidad de garantizar que los laboratorios estén adecuados, incrementando la confianza en la comunidad universitaria. Consecuentemente fortaleciendo la seguridad, contribuyendo a la creación de un ambiente de formación adecuado.

Asegurar que los laboratorios protejan los recursos tecnológicos, crea un sentido de responsabilidad para los estudiantes, profesores y personal informático, promoviendo una cultura de respeto para los recursos institucionales, fortaleciendo el trabajo en equipo, ayudando a reducir el riesgo de pérdida de equipos al garantizar que los procesos respectivos de investigación mejoran no solo la calidad de aprendizaje, sino también la práctica de valores y ética tecnológica.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Las nuevas tecnologías que han surgido tienen un gran impacto en la sociedad moderna, convirtiéndolas en herramientas fundamentales para el día a día de las diferentes áreas, incluyendo a la educación y el desarrollo de estas, permitiendo optar por una mejor organización que cambia la forma en que las personas trabajan dentro de las organización y empresas, también influyen los hábitos diarios de las personas al acceder a ellas en tiempo real, creando entornos sostenibles y eficientes al minimizar procesos que eran complejos.

Estas medidas de seguridad permiten proteger los equipos tecnológicos como es el hardware, evitando lo que son los daños físicos, accesos no autorizados y pérdidas de equipos. La adecuada aplicación de controles para la seguridad ha garantizado que los equipos y datos estén seguros, solo disponibles para los usuarios autorizados, gracias a las medidas que aseguran los recursos para un uso eficiente y seguro.

Igualmente, la implementación de la tecnología en los laboratorios de cómputo ha hecho más necesaria la disposición de sistemas que estén presentes en los trabajos académicos. Por aquello, es importante contar con una infraestructura segura que resguarde los componentes tecnológicos y asegure su disponibilidad únicamente para aquellos que la requieren. Por lo que resulta fundamental realizar revisiones continuas mediante auditorías para asegurar el cumplimiento de normas de seguridad. Estos permiten verificar fallos y mejorar la protección, previniendo problemas que dañen el correcto desempeño de la tecnología en los laboratorios.

1.8.2 Impacto ecológico

La protección ambiental mediante el uso de tecnologías sustentables, defienden las normas y estándares para el mantenimiento adecuado de dispositivos tecnológicos, con la finalidad de prolongar la vida útil de este. Los protocolos de seguridad promueven el correcto funcionamiento, previniendo el deterioro de condiciones ambientales debido a descuidos técnicos

Las prácticas no sólo protegen una cultura tecnológica eficiente y responsable, sino que también ayudan a tomar medidas para cuidar el entorno en que nos rodea, disminuyendo las cargas ambientales institucionales como es el uso excesivo de energía en estas áreas y para así fomentar un mejor desarrollo que sea más sostenible desde los niveles universitario y profesional.

Este proyecto tendrá un impacto ecológico positivo entre ellos es la disminución de recursos por ser eliminar el registro de acceso a los laboratorios de forma escrita lo que permitirá disminuir el uso de papel. En su lugar se implementará un sistema de cámaras de seguridad que registrará automáticamente el acceso de usuario a los laboratorios monitoreando en cada instante, lo que conlleva al reducir el uso de papel reemplazandolo por el monitoreo por cámara.

La implementación de las medidas de seguridad sostenibles transforma el uso de la tecnología para la comunidad universitaria, impulsando un cambio de mentalidad. Mediante la integración de herramientas digitales, reduciendo el consumo de recursos como el papel,

fomentando un compromiso con las buenas prácticas. Contribuyendo a que los estudiantes desarrollen hábitos que puedan adaptar en sus entornos laborales futuros, multiplicando el impacto positivo más allá.

La integración de estas medidas de seguridad, modifican la utilidad de la tecnología, impulsado a un cambio mental, que integra herramientas y la reducción de recursos físicos, fomentando un compromiso con el ambiente y las buenas prácticas, estableciendo costumbre que ayuden a la formación profesional de estos, amplificando un efecto positivo más allá del entorno académico.

CAPÍTULO II

2 MARCO TEÓRICO DE LA INVESTIGACIÓN

2.1 Antecedentes históricos

Auditoría de Seguridad Informática

En este contexto, una auditoría de ciberseguridad es un proceso sistemático diseñado para evaluar la eficacia de los controles de seguridad dentro de una organización. También ayuda a identificar y abordar cualquier problema que pueda afectar la confidencialidad, la integridad y la disponibilidad. En ocasiones, se aceptan riesgos, lo cual es más común en sistemas más nuevos donde la inversión económica supera el riesgo de explotación de una vulnerabilidad (Menéndez, 2023).

Hoy en día, gestionar dispositivos tecnológicos se ha convertido en una práctica común en la vida cotidiana, tanto en el ámbito profesional como en el personal. Esto ha conllevado un aumento de las medidas de seguridad para muchos dispositivos, convirtiéndola en un aspecto fundamental. Esta seguridad incluye protecciones tanto físicas como lógicas, con el objetivo de salvaguardar completamente todos los dispositivos tecnológicos que la requieren (Mata García, 2024).

La auditoría informática es un proceso que nos ayuda a verificar el correcto funcionamiento del sistema de seguridad implementado. Este procedimiento facilita la detección y solución de cualquier problema que pueda afectar los principios básicos de seguridad como son la confidencialidad, integridad y disponibilidad. Mediante esta evaluación, se pueden tomar decisiones informadas para reducir los riesgos asociados a posibles vulnerabilidades, como eliminarlas, minimizar su impacto o en algunos casos aceptarlas (Gómez, 2022).

Infraestructura Tecnológica

Según Smith (2021), entre los años 1960 y 1970, el desarrollo de infraestructura tecnológica produjo avances significativos, iniciando un crecimiento exponencial. Al inicio contaban con sistemas de procesamiento centralizado sólidos, con acceso limitado que era gestionado manualmente, durante esos años la seguridad se centraba en la protección física de los equipos y supervisión del personal autorizado a utilizar las máquinas.

La transformación digital puede describirse como un concepto que integra diferentes perspectivas sobre el cambio digital. Este enfoque reconoce las teorías tradicionales, pero también explora nuevas áreas que requieren flexibilidad, cambio y crecimiento continuo. Asimismo, reconoce que las organizaciones adquieren conocimiento tanto a través de las capacidades cognitivas individuales de sus miembros como de forma colectiva, lo que les permite organizar sus procesos de aprendizaje y adaptarse a los desafíos modernos (Escuder y Palacios, 2023).

2.2 Antecedentes de investigaciones.

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

Este trabajo de investigación se enfocó en realizar una auditoría de seguridad de la información de la infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre. El principal objetivo de esta investigación fue la creación de un informe para evaluar el cumplimiento de los estándares de seguridad, identificando los problemas a través de encuestas y entrevistas, mediante la metodología MAGERIT para auditar un laboratorio de computación. Como resultado, se encontró que los niveles de seguridad están en un 43%, los riesgos críticos como robo de información en un 95% y virus encontrados en los equipos con un 83%, así como peligros como robo, incendio y daños a los equipos. Concluyendo con la elaboración de un informe y una lista de recomendaciones para la reducción de riesgos (Chuez y Michelle, 2022).

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

Esta auditoría ayuda a evaluar la integridad de los recursos tecnológicos de información en la Escuela Técnica Superior Agropecuaria de Manabí, empleando una metodología estructurada según las normas internacionales, dividiendo en tres fases el proyecto, basándose en la seguridad física y lógica de estos recursos, mediante un análisis de los elementos internos y externos de la evaluación con la finalidad de determinar los eventos de mayor relevancia, permitiendo evidenciar hallazgos en la entidad, mostrando los resultados obtenidos del control aplicando lineamientos generales de seguridad. El coeficiente de concordancia de Kendall evidencia un 0,85 de coincidencia, con un bajo control de procedimientos aprobados, siendo conveniente la aplicación de normativas de seguridad rigurosas que permitan minimizar posibles riesgos en la infraestructura tecnológica (Loor y Espinoza, 2014).

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

El propósito de este proyecto académica se encuentra en fortalecer la seguridad tecnológica en las instituciones de educación superior en el Ecuador, mediante el uso de tecnologías emergentes de información e internet, estas tecnologías ofrecen muchos beneficio, pero también traen riesgos físicos y lógicos, como el acceso no autorizado a la información confidencial y los desafíos en el manejo de los dispositivos digitales, factores que pueden ayudar en la creación de entornos de aprendizaje seguros y efectivos, debió a que puedan producir pérdidas y disminuir la calidad de los laboratorios de cómputo. Es crucial la implementación de mecanismos para el control de la seguridad, garantizando la atención, mantenimiento y el uso adecuado de estos. Según (Reyes, 2018) plantea que el objetivo de identificar la vulnerabilidad y sugerir intervenciones para mejorar la seguridad y calidad debe fomentarse para el desarrollo de espacios educativos seguros y funcionales para la comunidad.

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

El propósito de este artículo es demostrar cómo garantizar la integridad, confidencialidad y disponibilidad de la información y los recursos de los laboratorios de la carrera de Tecnologías de la información, mediante un análisis empleando protocolos con el fin de protegerse de amenazas internas y externas, asegurando la continuidad de las actividades investigativas. Se identificó la existencia de protocolos de seguridad con medidas para proteger del acceso no autorizado mediante cámaras de seguridad, sistemas de alarma y cerraduras. También se identificaron vulnerabilidades para la gestión de contraseñas, acceso a los sistemas y la capacitación del personal de seguridad informática, concluyendo que algunos de los laboratorios presentaban vulnerabilidades (Intriago et. al, 2023).

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

Este proyecto de investigación se basa en la creación de un plan estratégico que ayudará a describir y resolver una necesidad relacionada con la seguridad informática del laboratorio de telecomunicaciones. El plan optimizará los procedimientos y políticas para proteger los recursos y equipos informáticos disponibles en el laboratorio de telecomunicaciones del programa de Ingeniería en Computación y Redes. Actualmente, la Universidad Estatal del Sur

de Manabí cuenta con una variedad de equipos tecnológicos, por lo que se necesitan acciones y regulaciones que aseguren la disponibilidad de estos recursos en todo momento. Tanto las técnicas cuantitativas como las cualitativas fueron esenciales para este estudio. A partir de los datos recopilados, se crearon tablas que permitieron identificar la necesidad y elegir la solución más adecuada. Este proyecto sigue un cronograma que ha sido previamente evaluado y respetado dentro del marco de tiempo establecido, y también cuenta con un recurso económico personal del autor (González, 2018).

2.3 Definiciones conceptuales

2.3.1 Auditoría de seguridad Informática

2.3.1.1 Definición de auditoría

Una auditoría es la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos, siendo realizada por una persona independiente y competente que asegure el cumplimiento de las normas, procedimientos y principios de los estándares desempeñados (Arens et. al, 2021).

La auditoría es un proceso continuo que se amplía a la recopilación y revisión de registros históricos de una organización o individuo, confirmando su situación actual. Teniendo como objetivo principal la verificación de la exactitud, la integridad y la autenticidad de los documentos y registros proporcionados para los encargados. También se considera que este proceso nos ayuda a identificar áreas a mejorar y sugiere maneras para fortalecer la gestión organizacional (Hurel et al, 2022).

2.3.1.2 Auditoría informática.

La auditoría informática es un proceso mediante el cual se recopilan y analizan evidencias para evaluar si los sistemas informáticos gestionan adecuadamente los recursos, garantizan la integridad de la información, cumplen eficazmente los objetivos de la organización y optimizan el uso de los recursos. La auditoría de seguridad de la información respalda y garantiza el logro de los objetivos principales de la auditoría, como identificar problemas en una situación, alcanzar objetivos, proteger activos, mantener la integridad de los datos y garantizar la eficiencia y eficacia de la integración de recursos (Chávez y Steven, 2022).

El desempeño de una auditoría informática es muy esencial, sobre todo para las empresas modernas, gracias a que, debido a estas, se puede garantizar la fiabilidad y la seguridad de los sistemas tecnológicos y sus datos, con el objetivo de proteger los activos de

estos mediante una revisión extensa y exhaustiva del sistema y sus procedimientos, con la finalidad de detectar posibles vulnerabilidades. Esto ofrece poder establecer controles y tomar decisiones de manera constante para prevenir el aumento de riesgos en las infraestructuras y la información de los activos (Lucero, 2023).

2.3.1.3 Tipos de auditoría Informáticas

Según el Autor Evilla (2009), existen varios tipos de auditorías informáticas:

A) ***Auditoría informática de explotación:*** Este tipo de auditoría informática considera la información como su principal recurso, la cual debe procesarse y someterse a una verificación preliminar para garantizar su integridad y calidad. Este proceso se lleva a cabo a través de un sistema informático gestionado por software. Una vez obtenido el resultado final, se implementan medidas de control de calidad antes de entregar el producto al cliente o usuario. En algunos casos, el cliente puede participar en la revisión o modificación del producto final.

B) ***Auditoría Informática de Sistemas:*** Esta auditoría se centra en examinar todos los aspectos de la "técnica de sistemas". Con el auge de las telecomunicaciones, existe la necesidad de auditar de forma independiente las comunicaciones, líneas y redes como parte de la infraestructura informática, aunque se mantengan dentro del contexto más amplio de Sistemas.

C) ***Auditoría informática de comunicaciones y redes:*** Esta auditoría considera a los datos como el principal recurso, ya que son procesados y sometidos a una verificación selectiva. Gracias a un examen preliminar, aseguran que la integridad y calidad de estos sea efectiva, el procesamiento se realizó mediante un sistema informático gestionado por software. Obteniendo como resultado establecer medidas de control de calidad antes de entregar el producto al cliente o usuario, pudiendo ser partícipes durante la revisión o modificación del producto final.

D) ***Auditoría informática de desarrollo de proyectos:*** En la integración y desarrollo de proyectos y aplicaciones, los procesos de auditoría son constantes, representando una evolución del análisis y la programación tradicional de estos con un concepto importante. Adicionalmente, el desarrollo abarca diversas áreas responsables, requiriendo procesos informáticos de la empresa.

E) ***Auditoría de la seguridad informática:*** Los principios de la seguridad física y lógica se centran en la protección de sus recursos o activos con soportes, para la prevención de riesgos dentro de edificios o instalaciones que resguardan estos

componentes, se evalúan diversos riesgos consecuentes como posibles incendios, robos y desastres naturales, con la finalidad de poder garantizar la seguridad de los activos tecnológicos.

2.3.1.4 Seguridad Informática

La seguridad de la información se centra en temas como las estrategias para el análisis de riesgos y la evaluación del impacto potencial de estos en el sistema. Para estos análisis, es necesario comprender los factores que influyen en el plan de contingencia, las herramientas para detectarlos y el establecimiento de políticas de seguridad. También incluye los mecanismos tecnológicos para implementar estas políticas, sus auditorías y las herramientas más potentes disponibles en el mercado actual. Estas áreas se abordan a modo de introducción (Postigo, 2020).

La seguridad informática es una disciplina que se basa en políticas y estándares internos y externos establecidos por la empresa. Se encarga de proteger la integridad y privacidad de la información almacenada en un sistema informático contra todo tipo de amenazas, minimizando los riesgos físicos y lógicos que pueda enfrentar el sistema. Si se produce una amenaza a la seguridad, se debe procurar recuperar cualquier información dañada o robada (Baca, 2016).

La seguridad se refiere a proteger la información y los sistemas informáticos del acceso no autorizado, así como a prevenir la destrucción, modificación o divulgación no deseada de dicha información. La información se almacena en dispositivos informáticos para diversos fines. Por ello, es importante proteger el equipo informático y mantenerlo actualizado para garantizar su seguridad frente a las amenazas de seguridad más recientes. Aprenda a mantener sus datos y sistemas a salvo del acceso no autorizado y prepárese para responder ante una brecha de seguridad (Mata, 2024).

2.3.1.4.1 Importancia de la seguridad informática

La seguridad informática se ha convertido en uno de los temas más importantes en la era digital en la que vivimos y tiene como objetivo proporcionar una comprensión general de los conceptos básicos de la seguridad informática, así como de las amenazas y vulnerabilidades a las que se enfrentan los sistemas informáticos ya que es el conjunto de prácticas, herramientas y técnicas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos e información tanto física como lógica (Arango, 2023).

Hoy en día, la seguridad informática se ha vuelto esencial para prevenir fallos inesperados o ataques dirigidos a sistemas y dispositivos tecnológicos. Su objetivo principal es proteger la integridad y el correcto funcionamiento de estos sistemas frente a posibles amenazas. También ayuda a salvaguardar la información confidencial y a garantizar la continuidad operativa de las organizaciones (Álvaro, 2022).

Las políticas de seguridad son un mecanismo para la protección de los sistemas informáticos que se deben incorporar al hardware y software para los puntos más críticos, garantizando su correcta aplicación. Estas políticas permiten un control permanente, alertas tempranas y respuestas inmediatas a cualquier actividad sospechosa. Nos encontramos en una era digital donde la información es el recurso más valioso. La seguridad de estos datos es una necesidad estratégica para garantizar la confianza y continuidad de las operaciones de cualquier organización o institución (Caicedo, 2024).

2.3.1.4.2 Riesgos de seguridad informática

El riesgo de seguridad de la información se refiere al impacto causado por un evento específico y también define la probabilidad potencial de que ocurra y genera ciertos efectos, los cuales se determinan en función de la amenaza y la vulnerabilidad. Para evaluar un riesgo, se consideran factores como la probabilidad de ocurrencia y la gravedad de su impacto para evaluar la debilidad o el nivel de exposición que podría comprometer parcial o totalmente la seguridad de un sistema de información (López, 2017).

Una amenaza se considera cualquier evento accidental o intencional que pueda causar daños al sistema informático. Las vulnerabilidades son muy comunes y se refieren a fallos en sistemas físicos o lógicos. Estas pueden estar relacionadas con aspectos organizacionales como procedimientos mal definidos o desactualizados, falta de políticas de seguridad, el factor humano (falta de formación y concienciación del personal con acceso a los recursos del sistema), el propio equipo, el software y las herramientas lógicas del sistema, así como las ubicaciones físicas y las condiciones ambientales del sistema (Constanza et. al, 2018).

2.3.1.4.3 Acceso no autorizado

Uno de los riesgos más importantes para la ciberseguridad se muestra cuando personas no autorizadas tienen acceso a áreas restringidas, encontrando equipos e información confidencial. Estos factores pueden incrementar el riesgo de controles deficientes y puntos de entrada vulnerables, teniendo como consecuencia estas debilidades físicas, administrativas o de acceso (Torres, 2022).

2.3.1.4.4 Medidas de seguridad perimetral

Según López (2022), las medidas de seguridad dentro de entornos informáticos perimetrales son un riesgo significativo para la seguridad física de los sistemas, siendo un problema clave la falta de sistemas vigilantes debido a la ausencia de cámaras de seguridad. Además, la ciberseguridad puede tener graves consecuencias debido a la integridad y protección de la infraestructura tecnológica.

2.3.1.4.5 Sistemas de vigilancia y monitoreo.

Un sistema de monitoreo asegura una vigilancia constante para la infraestructura tecnológica, ayudando a detectar actividades inusuales, previniendo incidentes de seguridad y tomando medidas oportunas. La gestión para la seguridad es crucial para estos procesos, para el entorno digital, estas herramientas representan una de las principales defensas para proteger los recursos y servicios tecnológicos (López, 2021).

2.3.2 Infraestructura Tecnológica

2.3.2.1 Definición de Infraestructura Tecnológica

La infraestructura es simplemente el conjunto de estructuras e instalaciones de ingeniería que suelen tener una larga vida útil y sirven como base para proporcionar los servicios necesarios para el desarrollo productivo, social, político, militar y personal. Es un factor importante que explica la capacidad de un país para diversificar su economía, expandir el comercio, responder al crecimiento poblacional, reducir la pobreza y mejorar las condiciones ambientales (Bicalho, 2021).

La infraestructura tecnológica es un conjunto de recursos técnicos, físicos, que permiten un correcto funcionamiento para los sistemas informáticos y la comunicación de la organización. Incluyendo la lógica de redes y los servicios necesarios para garantizar el flujo de la información, esta infraestructura es importante para una empresa, respaldando los procesos de producción, ayudando a facilitar la adaptación de nuevas tecnologías, mejorando la eficiencia y productividad empresarial (Cortés, 2021).

2.3.2.2 Importancia de la Infraestructura Tecnológica

Actualmente, la optimización del uso de recursos físicos ha reducido gradualmente los costos y mejorado la eficiencia operativa, recalcando que la tecnología garantice la disponibilidad de los servicios, dado que los sistemas puedan replicarse o ser trasladados de forma sutil al existir fallos, ayudando a reducir la dependencia de hardware específico,

minimiza los riesgos asociados con la durabilidad de los equipos, siendo un factor clave para la modernización de los entornos tecnológicos avanzados (Gallego et. al, 2017).

El uso de infraestructuras tecnológicas es fundamental para ayudar a las organizaciones, mejorando sus procesos optimizan la comunicación garantizando el flujo de la información. En el siglo XXI, la importación de estas ha crecido rápidamente, impulsando el desarrollo de nuevos modelos de negocio ayudando a fomentar la innovación en las empresas para que puedan adaptarse a los entornos globales. Estas se encuentran diseñadas no solo para garantizar el rendimiento y la seguridad de los sistemas, sino también para ser usadas como base a soluciones digitales impulsadas por la productividad y la competitividad (Sánchez, 2023).

Las infraestructuras tecnológicas se encuentran compuestas por recursos físicos, hardware, software, servicios y herramientas que las organizaciones utilizan para garantizar la eficiencia y eficacia de estas. Sirve como base para el desarrollo y la gestión de los procesos operativos, garantizando la disponibilidad de la información, la comunicación y la conectividad necesarias para un rendimiento óptimo en cualquier actividad organizacional. Considerando que el diseño y el mantenimiento adecuado de esta infraestructura es esencial e indispensable para establecer la productividad, seguridad e innovación en el entorno laboral y educativo (Calderón y Álava, 2023)

2.3.2.3 Componentes de la Infraestructura Tecnológica

2.3.2.3.1 Hardware

El hardware es una parte necesaria de la infraestructura tecnológica, por lo que proporciona la base física necesaria para el funcionamiento de los sistemas informáticos. Una configuración de hardware bien diseñada no solo mejora el rendimiento del sistema, sino que también ayuda a gestionar los recursos de forma más eficiente y optimiza la conectividad de la red. Se recomienda invertir en hardware de alta calidad para que así garantice la estabilidad y la escalabilidad de la infraestructura, permitiéndole satisfacer las crecientes demandas del entorno digital (Pérez, 2023).

2.3.2.3.2 Software

Según Humber (2021), el software es la base esencial para desarrollar herramientas o servicios óptimos para el rendimiento de las infraestructuras, automatizando procesos, adaptando cambios y necesidades tecnológicas actuales, siendo un conjunto que permite a los dispositivos realizar tareas al integrar aplicaciones que permiten la comunicación entre

sistemas, garantizando una gestión eficaz del software, también la eficiencia y fortaleciendo la seguridad y estabilidad de todo un ecosistema informático.

2.3.2.3.3 Redes de comunicación

Las redes de comunicación son un componente especial para las infraestructuras tecnológicas, dado que permiten la conexión entre dispositivos y el intercambio de datos, gracias a esto, las máquinas pueden comunicarse entre sí mediante el uso de protocolos seguros, privados y accesibles. Las tecnologías como Ethernet, Wi-Fi y zonas de cobertura son utilizadas en todas partes en el mundo entero, las redes organizadas se gestiona para mejorar el rendimiento y la estabilidad de los servicios, actuando como una defensa contra amenazas, garantizando la continuidad del servicio (Behrouz, 2021).

2.3.2.4 Infraestructura Tecnológica en Laboratorios Educativos

La infraestructura tecnológica de los laboratorios desempeña un papel enorme para la creación de entornos para un aprendizaje eficaz y accesible, permitiendo el acceso a recursos educativos y a herramientas de software desde cualquier lugar y momento. Proporcionar un entorno flexible y escalable permite al docente entregar una experiencia personalizada para el aprendizaje según las necesidades específicas del estudiante, promoviendo la inclusión y el aprendizaje en una era moderna (Buitrago et. al, 2015).

2.3.2.4.1 Mantenimiento y actualización tecnológica.

Según Gutiérrez (2023), proponer un enfoque sistemático es ideal debido a que este permitirá identificar y priorizar las necesidades de un mantenimiento seguro en los sistemas y que se mantengan de manera óptima, demostrando la relevancia de una implementación periódica con la intención de poder adaptarse a los avances tecnológicos y el demandante cambio dentro de los entornos educativos. En el libro “Gestión del mantenimiento de infraestructuras tecnológicas” descubrimos cómo se aborda la necesidad de un mantenimiento y actualización tecnológica continua, siendo fundamental para la productividad de sus infraestructuras.

2.3.2.5 Seguridad Física en la Infraestructura Tecnológica

La importancia de implementar medidas de seguridad centradas en los entornos tecnológicos para la protección de activos como la información que estos contienen. Destacando que la seguridad no está limitada sólo a la tecnología, esta incluye la capacitación del personal comprometido y la creación de nuevos protocolos para la gestión de estos posibles riesgos, mediante la colaboración de diferentes departamentos para la construcción de un

entorno seguro y resiliente, como lo es el uso de tecnologías de videovigilancia y control de acceso (Díaz y Cruz, 2020).

La seguridad física de la infraestructura tecnológica se refiere a la protección ante accesos no autorizados, con la finalidad de prevenir la destrucción o modificación de los equipos. La seguridad informática se encuentra diseñada para usuarios que necesiten una protección sólida en sus dispositivos, es fundamental mantenerlos actualizados y asegurarse de que estén protegidos contra cualquier amenaza de seguridad. Se deben implementar las medidas de seguridad necesarias para ayudar a garantizar la integridad y el funcionamiento continuo de los sistemas tecnológicos (Mata, 2023).

Garantizar la seguridad en la red y para la infraestructura de telecomunicaciones es muy importante debido a que los servicios institucionales deben operar sin interrupciones de manera segura. La " protección de los equipos, el acceso y las zonas sensibles a fallos técnicos o daños por catástrofes naturales". Tomando acciones apropiadas y una adecuada gestión de riesgos se pueden aprovechar mejor las inversiones tecnológicas y los recursos, evitando pérdidas y complicaciones innecesarias según (Olmos, 2020).

2.4 Metodología

2.4.1 Metodología MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos para sistemas de información desarrollada por el Consejo Superior de Administración Electrónica (CSAE), perteneciente al Ministerio de Hacienda y Administraciones Públicas del Gobierno de España. Se creó como respuesta a la creciente constatación de que la administración, y de hecho la sociedad en su conjunto, depende cada vez más de las tecnologías de la información para cumplir su misión. Está estrechamente vinculada al uso generalizado de las tecnologías de la información, que aportan claros beneficios a la ciudadanía, pero también conllevan ciertos riesgos que deben minimizarse mediante medidas de seguridad que fomenten la confianza (Guevara, 2015).

Esta metodología fue utilizada para evaluar, analizar y gestionar los posibles riesgos encontrados en los sistemas informáticos, teniendo como objetivo evaluar el impacto generado que puedan tener los incidentes de seguridad dentro de una organización. Enfocados en ayudar a identificar las amenazas potenciales y reconocer las vulnerabilidades que podrían surgir, permitiendo una mayor comprensión de las posibles acciones preventivas y correctivas que estén adecuadas a cada uno de estos riesgos. Planificando una estrategia para reducir el impacto

de futuros incidentes y mejorar la protección de activos críticos, el uso adecuado de este método ayuda a fortalecer la resiliencia de la organización y garantiza la continuidad de las operaciones (Menéndez, 2022).

2.4.2 Principales características

MAGERIT es una de las metodologías más utilizadas por su versión en español. Algunas de sus principales ventajas incluyen: las decisiones tomadas estarán bien fundamentadas y serán fáciles de defender ofrece un método sistemático para analizar riesgos; facilita la identificación y planificación de las medidas necesarias para reducirlos; y proporciona herramientas que facilitan el análisis de riesgos al permitir la división de activos en diferentes grupos, lo que facilita la identificación de riesgos y la toma de medidas adecuadas para controlarlos (Alvarado et. al, 2018).

2.4.3 Fases de la Metodología Magerit

Según los Autores Ávila y Cuenca (2021) la metodología de Magerit cuenta con cinco fases

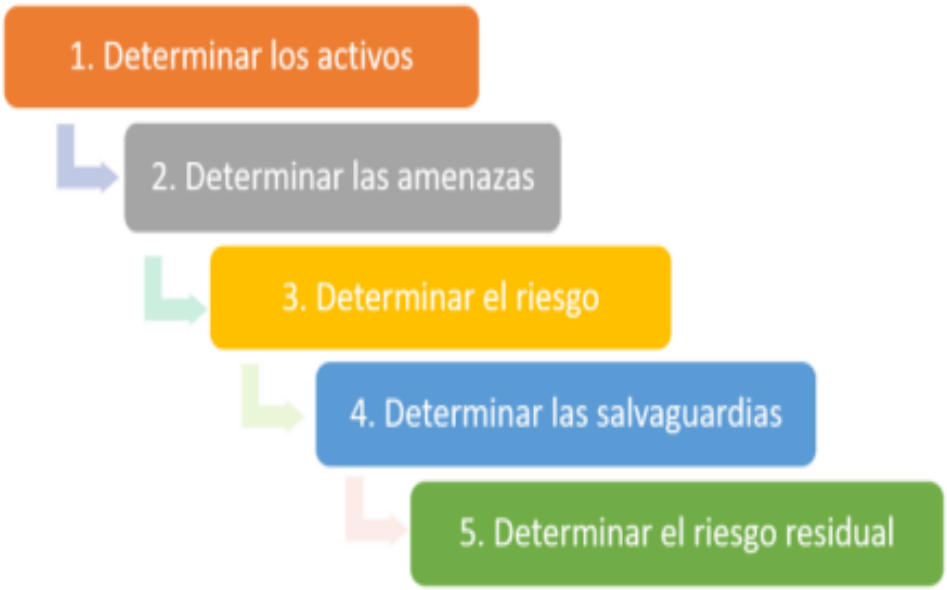


Ilustración 2 Fases de la Metodología MAGERIT

Notas: Cada fase de la Metodología Magerit es crucial para estructurar el análisis, valoración, tratamiento y seguimiento de riesgos. Tomada de (Ávila y Cuenca, 2021)

1. **Determinación de los activos:** Estos activos pueden ser tangibles, como computadoras, servidores o mobiliario, o intangibles, como información, software o la reputación de la empresa. Dado que su importancia ya ha sido reconocida, deben protegerse de daños, pérdidas, accesos no autorizados o cualquier

manipulación que pueda afectar su correcto uso. La comprensión y clasificación adecuada de los activos nos permite saber qué protecciones son necesarias, priorizando las medidas de seguridad adecuadas para aplicarse según su nivel de importancia.

2. **Determinación de las amenazas:** Mediante un análisis de amenazas y vulnerabilidades para la evaluación, diferentes tipos de riesgos pueden afectar a los activos de la institución. Incluyendo los diversos escenarios de desastres naturales, fallos de equipos, errores humanos, ataques intencionales, fallas técnicas y otros incidentes que pueden agravar la situación. Este estudio ayudará a comprender los alcances de cada riesgo y sus posibles impactos para la operación de los laboratorios.
3. **Determinación del riesgo:** Identificar las amenazas y vulnerabilidades que podrían afectar los activos de la institución en situaciones como desastres naturales, fallas internas, errores humanos, ataques intencionales, fallas tecnológicas y combinaciones de eventos que pueden agravar una situación. Esta evaluación muestra el alcance de cada riesgo y cómo puede afectar las operaciones del laboratorio. Además, identificar estos riesgos permite implementar medidas preventivas y de respuesta que reducen la probabilidad de ocurrencia y minimizar sus efectos.
4. **Determinación de salvaguardas.** Este proceso permitió examinar y evaluar las medidas de protección implementadas actualmente en la empresa o institución, ayudando a reducir riesgos existentes, derivados por el uso inadecuado y otros, mediante el uso de procedimientos preventivos y herramientas tecnológicas que garantizan mayor seguridad. Este análisis permitió identificar las posibles mejoras que fortalecen la protección y minimización de las vulnerabilidades y riesgos existentes.
5. **Determinación de riesgo residual.** El análisis de los riesgos existentes es considerado para una verificación de medidas de protección dentro del área, determinando el nivel de riesgo que existe en los activos, se consideran las medidas de seguridad ya implementadas. Gracias a esto, es indispensable para comprender los controles actuales, la eficiencia de su aplicación y si determinan un requerimiento de medidas adicionales para reducir las posibilidades del aumento de amenazas. Garantizando una gestión de seguridad precisa y realista dentro de la empresa.

2.5 Conclusiones de marco teórico.

En este capítulo se realizó una investigación más profunda sobre las variables como son auditoría de seguridad informática e infraestructura tecnológica, apoyándose en fuentes confiables, entre ellas Google Académico y estudios previos relacionados con los temas. Este análisis me permitió comprender de mejor manera la importancia y el objetivo de la auditoría, ya que es una herramienta fundamental para evaluar, controlar y mejorar la seguridad de los sistemas informáticos, la cual nos permite conocer las vulnerabilidades para mitigar riesgos dentro de la infraestructura tecnológica.

Cabe recalcar que una infraestructura tecnológica bien administrada no solo facilita el correcto funcionamiento de los laboratorios de cómputo, sino que también es vital para mantener la integridad, disponibilidad y confidencialidad de la información, pilares esenciales para cualquier institución o empresa. El análisis de otros trabajos similares de investigación me ayudó a poder ver lo valioso de tener estos conocimientos sobre metodologías, estándares y mejores prácticas aplicadas en contextos académicos, mejorando el marco teórico y proporcionando una base clara para el desarrollo de la auditoría en este proyecto.

En conclusión, tras investigar más a fondo, se evidenció que la auditoría y la gestión adecuada de la infraestructura tecnológica están vinculadas para mantener un ambiente seguro y confiable. Estas dos combinaciones son ideales para prevenir incidentes, garantizar la continuidad operativa y fortalecer la confianza de los usuarios. Por ello, este estudio concluye que la aplicación de la auditoría contribuye significativamente a crear un mejor ambiente en los componentes tecnológicos y administrativos de la Universidad Laica Eloy Alfaro, Extensión El Carmen, para así tener un entorno más confiable y seguro.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

En este capítulo se presenta el diseño metodológico que se aplicó en la investigación, indicando las formas de recolección y análisis de la información lo que permitió establecer propuestas de mejora en los controles de seguridad. La metodología organiza el proceso al definir el enfoque, el tipo de estudio y las herramientas utilizadas para obtener los datos. El capítulo inicia con la definición del tipo de investigación y continúa con la explicación de las técnicas empleadas para el procesamiento y análisis de la información recopilada.

3.2 Tipo de investigación

3.2.1 Investigación cualitativa

La investigación cualitativa es multimetódica, naturalista e interpretativa los investigadores cualitativos indagan en situaciones naturales, intentando dar sentido o interpretar los fenómenos en los términos del significado que las personas les otorgan. Este enfoque se centra en el análisis estudiado (Molano et. al, 2021).

Se utilizó un enfoque cualitativo para describir el contexto, las problemáticas de seguridad y justificar la relevancia del proyecto, integrándose al marco teórico mediante el análisis de antecedentes históricos y definiciones conceptuales para fortalecer la base teórica.

3.2.2 Investigación cuantitativa

Según los autores Yucra y Bermedo (2020) afirman que la investigación cuantitativa son términos que se utilizan a menudo en el campo de la ciencia, porque los términos abarcan en sí la estructura de la ciencia cuando el primero utiliza el conocimiento científico, con la validez del conocimiento. La tarea en este análisis es dilucidar la teoría de ambos términos.

El enfoque cuantitativo fue utilizado para un análisis de datos mediante entrevistas, encuestas, observaciones y un análisis resultante, permitiendo la obtención de información precisa y reglamentada para sustentar las conclusiones del proyecto

3.2.3 Investigación descriptiva

Este tipo de investigación tiene como objetivo describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que

permiten establecer la estructura o el comportamiento de los fenómenos en estudio (Guevara et. al, 2020).

En los antecedentes históricos se aplicó una investigación de tipo descriptiva con el fin de analizar la evolución de las variables estudiadas, mientras que en las definiciones conceptuales se desarrollaron los conceptos teorías y estándares fundamentales vinculados con los temas de la investigación.

3.3 Métodos de investigación

3.3.1 Método analítico

El método analítico se define como un enfoque que debe poseer una capacidad productiva para generar su propio objeto de estudio. Sin embargo, una limitación inherente a este método radica en su incapacidad para establecer de manera efectiva una transición adecuada entre las determinaciones sensibles y las determinaciones lógicas. (Herszenbaun, 2022).

Una de las áreas en las que se aplicó el método analítico fue el diagnóstico inicial de los laboratorios. En el marco teórico se consideraron las teorías provenientes de las fuentes consultadas y las interpretaciones obtenidas lo que permitió alcanzar una comprensión más completa del problema. Esta metodología facilitó el análisis de las principales causas y la identificación de sus consecuencias.

3.3.2 Método inductivo

El método inductivo es un tipo de razonamiento que va de lo particular a lo general, de los casos concretos a la formulación de leyes generales. Es muy usado en la enseñanza de idiomas y ciencias porque desarrolla el pensamiento crítico, la participación y el aprendizaje significativo (Palmero, 2021).

El método aplicado permitió analizar situaciones específicas, antecedentes históricos e investigaciones previas, con el propósito de facilitar el estudio de la información y establecer las bases teóricas, así como generar interpretaciones amplias que resulten relevantes para contextos análogos.

3.3.3 Método deductivo

El deductivo es una estrategia de aprendizaje que parte de principios generales o teorías ya establecidas y de allí pasa a casos específicos. Basado en el razonamiento, que ayuda a

entender mejor las cosas abstractas y por lo tanto a tener un aprendizaje ordenado y objetivo (Espinoza, 2023).

El método deductivo fue aplicado en el desarrollo del marco teórico, particularmente en la metodología del proyecto, para estructurar y organizar el análisis.

3.4 Fuentes de información de datos

3.4.1 **Fuentes primarias** – Entrevista

Según el autor Creswell (2020), la entrevista es una de las herramientas más destacadas de la metodología cualitativa, ya que permite recopilar información detallada mediante una conversación estructurada con un individuo. Este método busca crear un ambiente cómodo donde los individuos se sientan cómodos compartiendo historias, perspectivas y opiniones.

La entrevista fue dirigida al coordinador de las carreras de Tecnología de la Información (TI) y Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, con el objetivo de recopilar información relevante sobre la gestión y el funcionamiento de los laboratorios de cómputo.

3.4.2 Fuentes secundaria – Encuesta

La encuesta es una técnica muy usada empleada para investigación debido a su capacidad para recopilar y procesar datos de forma ágil, precisa y eficiente. Este método se caracteriza por ser un procedimiento sistemático diseñado para recolectar información clave relacionada con un tema particular (Salvador, 2020).

Esta encuesta fue aplicada a 149 estudiantes pertenecientes a las carreras de TI & Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, con la finalidad de evaluar las condiciones de seguridad física de los laboratorios de cómputo.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

Según Chamorro et. al (2021), define que una población es el conjunto de elementos que constituyen un objeto de estudio, siendo fundamental que el investigador delimita los elementos para llevar a cabo la investigación.

La encuesta se aplicó a una muestra finita de 149 estudiantes seleccionados de una población total de 242 pertenecientes a las carreras de TI y Software, de los cuales 97 corresponden a la de TI y 145 a la de Software.

3.5.2 Muestra

Según Gutiérrez (2022), la muestra es un conjunto pequeño respecto a la población, que se utiliza regularmente con fines investigativo de estudio, caracterizado por seguir el comportamiento y las tendencias de estos, siendo crucial que la muestra se represente correctamente, significando que esta deberá reflejar las propiedades de la población de origen.

Se escogió a los estudiantes de la carrera de TI & Software para determinar el tamaño de la muestra. En la misma, se aplicó una estadística finita cuya metodología se obtuvo una muestra de 149 encuestados a través de calculadora del tamaño de muestra..

$$n = \frac{N * Z^2 * p * q}{e^2 * (N-1) + Z^2 * p * q}$$

Ilustración 3 Fórmula de Muestra

3.5.3 Análisis de las herramientas de recolección de datos a utilizar

3.5.3.1 Encuesta – Entrevista - Observación / Otras

Las encuestas incluyen 11 preguntas con dos opciones de respuesta, enfocadas en evaluar la seguridad de los laboratorios. Identificar posibles riesgos sobre la situación actual de los laboratorios de cómputos de las carreras de TI & Software en cuanto a seguridad informática de los equipos.

Se diseñó una entrevista dirigida al coordinador de la carrera, compuesta por 12 preguntas, con el fin de recopilar información sobre la seguridad informática de los laboratorios de cómputo.

3.5.3.2 Estructura de los instrumentos de recolección de datos aplicados

La estructura de los instrumentos de recolección de datos utilizados en la investigación fue diseñada de forma organizada para garantizar claridad y pertinencia de la información obtenida. Cada uno de los instrumentos inicia con una portada en la cual se especifica a quién va dirigida y cuál es el objetivo del estudio. Adicional se presenta el cuerpo principal conformado por preguntas estructuradas que permiten obtener información concreta y de fácil análisis. En el caso de la encuesta esta estuvo compuesta por 11 preguntas de tipo cerrado, mientras que la entrevista incluyó 12 preguntas orientadas a profundizar en aspectos clave del estudio.

3.5.4 Plan de recolección de datos

El plan de recolección de datos se diseños de la siguiente manera:

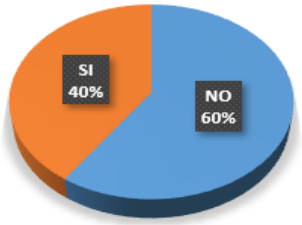
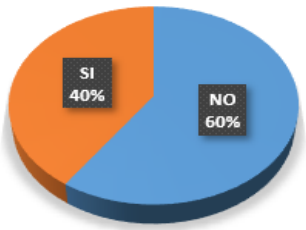
3.6 Análisis y presentación de resultados

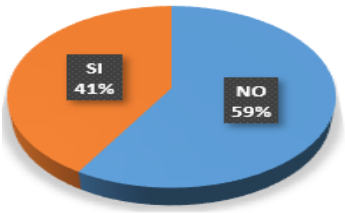
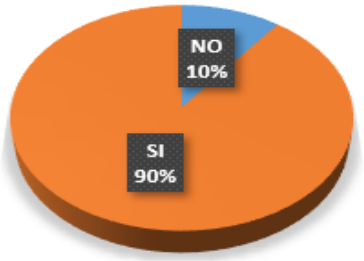
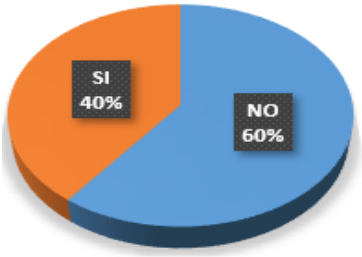
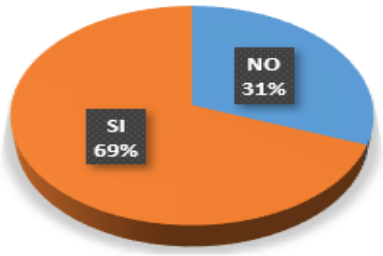
Fecha	Actividad	Instrumento
22/11/2024	Diseño y validación del cuestionario	Encuesta
29/11/2024	Aplicación de encuestas a estudiantes	Encuesta
02/12/2024	Elaboración del formato para la entrevista	Entrevista
09/12/2014	Realización de la entrevista al coordinador	Entrevista
12/12/2024	Análisis de datos	Entrevista-Encuesta

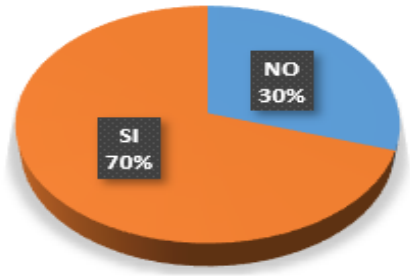
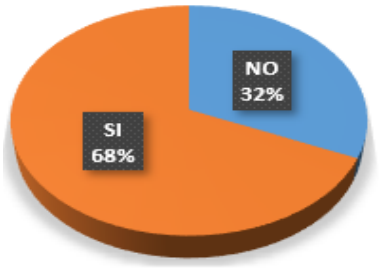
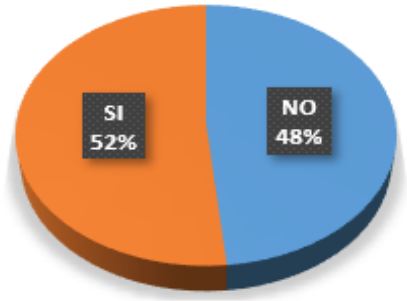
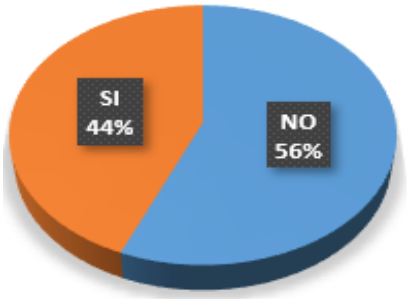
Tabla 2 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos

3.6.1.1 Encuesta aplicada a los estudiantes de las carreras de TI & Software.

N.º	pregunta	Gráfico	Interpretación
1	¿Considera que los laboratorios cuentan con suficientes medidas de seguridad para los equipos?		La mayoría de los estudiantes indicó que los laboratorios carecen de mecanismos adecuados para garantizar la seguridad de los equipos.
2	¿Considera que los equipos del laboratorio están bien asegurados?		La mayoría de los estudiantes indicó que los equipos de los laboratorios no cuentan con protección suficiente.

N.º	pregunta	Gráfico	Interpretación
3	¿Alguna vez ha notado pérdida de algún equipo en los laboratorios durante sus clases?		La mayoría de los estudiantes indicó que no ha observado la desaparición de ningún recurso tecnológico durante sus actividades en los laboratorios.
4	¿Considera que las pérdidas de equipos en el laboratorio afectan la calidad de las clases?		La mayoría de los estudiantes indicó que la desaparición de equipos en los laboratorios impacta negativamente en la calidad de las clases.
5	¿Existen responsables designados para supervisar los laboratorios?		La mayor parte de estudiantes señaló que no se ha designado personal encargado de supervisar los laboratorios.
6	¿Cree que se toman medidas necesarias para evitar daños en los equipos?		La mayoría de los estudiantes señaló que se aplican medidas adecuadas para proteger los equipos y prevenir posibles daños.

N.º	pregunta	Gráfico	Interpretación
7	¿Considera que se realiza un mantenimiento adecuado en los equipos?		Más de la mitad de los estudiantes considera que si existe un mantenimiento adecuado en los equipos.
8	¿Ha observado algún daño en los equipos del laboratorio durante sus prácticas?		La mayor parte de los estudiantes afirmó haber presenciado daños en los equipos durante las prácticas en el laboratorio.
9	¿Cree que los daños en los equipos se reportan de manera oportuna y adecuada para su reparación?		La mayoría de los estudiantes considera que los daños en los equipos siempre se reportan adecuadamente.
10	¿Alguna vez ha tenido problemas para acceder al laboratorio en el horario programado?		La mayor parte de los estudiantes indicó que el acceso al laboratorio en el horario programado no ha presentado dificultades.

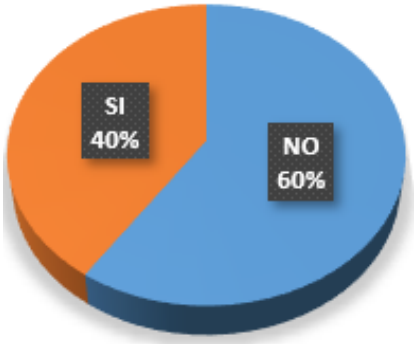
N.º	pregunta	Gráfico	Interpretación
11	¿Considera que la falta de control de acceso afecta la disponibilidad de los equipos?		La gran parte de los estudiantes consideró que la ausencia de mecanismos de control de acceso no afecta la disponibilidad de los recursos tecnológicos.

Tabla 3 Tabulación de encuesta

3.6.1.2 Entrevista aplicada a el Coordinador de la carrera de TI & Software

N.º	preguntas	Respuestas	Interpretación
1	¿Cómo evaluaría la seguridad física de los equipos en los laboratorios?	Es un poco inexistente porque no existe el elemento suficiente que prioricen la seguridad física	Se puede observar que la seguridad física en los laboratorios es deficiente debido a la falta de medidas.
2	En su experiencia, ¿qué tipo de incidentes relacionados con la seguridad de los equipos han ocurrido en los laboratorios?	Lo que se ha se podido observar son las pérdidas de dispositivos como mouse y teclado hubo un caso en particular que se perdieron fuentes internas de un pc.	Se han registrado pérdidas de dispositivos lo que evidencia fallas en el control de seguridad y gestión de equipos.
3	¿Qué opina sobre las medidas que se toman actualmente para prevenir las pérdidas de los equipos?	Considero se puede hacer un mejor trabajo conjuntamente con los docentes, estudiantes y miembros administrativos ya que el proceso actual no es el óptimo para preservar la vida de los equipos	Se reconoce la necesidad de mejorar la gestión de seguridad de los equipos mediante un trabajo conjunto.
4	¿Cree que los equipos del laboratorio están bien protegidos en cuanto a seguridad física?	No están 100% protegidos porque existen accesos externos de estudiantes.	Se observó que los equipos no están completamente protegidos debido al acceso externo de estudiantes
5	¿Existen responsables designados para	Responsable en si no ahí, pero supervisión como tal si	Aunque se realiza una supervisión general, no existe un responsable

N.º	preguntas	Respuestas	Interpretación
	supervisar los laboratorios?	se realiza, pero se reconocen que son un poco distantes.	directo de los laboratorios.
6	¿Qué impacto cree que tendría un mejor control de acceso a los laboratorios en el uso de los equipos?	Tendría un impacto muy positivo tan para el uso, el cuidado y extensión de vida útil de los equipos	Se puede ver que mejorar en las prácticas de seguridad que también tendría un impacto positivo en el uso adecuado.
7	¿Cree que se toman medidas necesarias para evitar daños en los equipos?	Aunque existen medidas, es necesario fortalecerlas debido a la falta de comunicación reciente con los estudiantes.	Aunque existen medidas de seguridad implementadas no se están cumpliendo
8	¿Considera que se realiza un mantenimiento adecuado de los equipos?	Actualmente, el mantenimiento se realiza cada semestre, aunque podría mejorarse.	Se sugiere que se podría hacer un mejor trabajo, la frecuencia de estos para mejorar el mantenimiento
9	¿Ha observado alguna vez situaciones en las que los equipos no estén siendo utilizados de manera adecuada?	Si alguna vez he observado que se encuentran indicios de que los teclados que han sido manipulados, mouse y las pantallas eso ha hecho ver un inicio de que no se ha hecho un correcto uso de los equipos.	Se han observado el mal uso de los equipos, como manipulación en los teclados y pantallas lo que refleja un uso inadecuado
10	¿Considera que la falta de control de acceso afecta la disponibilidad de los equipos?	Sí afecta, debido a que los estudiantes dependen mucho de los dispositivos para realizar sus prácticas.	Se afirma que la falta de control de acceso puede impactar negativamente la disponibilidad de los equipos
11	¿Qué medidas considera más efectivas para mejorar el seguimiento y control del uso de los equipos por parte de los estudiantes?	Ahí iniciativas con los proyectos de titulación que están enfocado para mejorar estos proyectos e incluido su trabajo	Se observó que hay iniciativas vinculadas a proyectos de titulación que buscan mejorar y fortalecer las condiciones.

N.º	preguntas	Respuestas	Interpretación
12	¿Qué opina sobre las medidas de seguridad perimetral, como cámaras en los laboratorios?	Son partes importantes porque actualmente no se puede revisar algún incidente que pueda surgir durante el uso de los equipos y bueno aparte de importante es muy necesario.	Se puede ver qué es crucial contar con un sistema para revisar y gestionar incidencias durante el uso de los equipos.

Tabla 4 Tabulación de Entrevista

3.6.2 Presentación y descripción de los resultados obtenidos

Tomando en cuenta los resultados obtenidos en la pregunta 3 de la entrevista, se considera que las medidas actuales para prevenir las pérdidas de equipos no son óptimas, en la pregunta 3 de la encuesta, varios estudiantes afirmaron haber presenciado ciertas pérdidas de algunos equipos dentro de los laboratorios de cómputos.

Respecto a la pregunta 5 de la encuesta, la mitad de los estudiantes indican que no existe un personal responsable para la supervisión de los laboratorios, coincidiendo con lo señalado en la entrevista correspondiente a la pregunta 5, donde se indica que no hay un responsable directo para los laboratorios de cómputo, pero existe una supervisión general.

En relación con la pregunta 6, la mayoría de los estudiantes considera que se aplican las medidas necesarias para proteger los equipos, sin embargo, persiste la necesidad de reforzar y poner en práctica estas acciones. Este hallazgo coincide con la información obtenida en la entrevista de la pregunta 7, donde se señaló que, aunque las medidas de seguridad para prevenir daños en los equipos existen, su cumplimiento se ve limitado por la falta de comunicación..

3.6.3 Informe final del análisis de los datos

En la investigación se evidenció que los principales problemas en los laboratorios están relacionados con accesos no autorizados, pérdida de equipos y daños por uso inadecuado. Durante la entrevista, el coordinador reconoció que existen medidas de seguridad, pero que muchas veces no se cumplen por falta de comunicación y seguimiento. Esta situación coincide con lo señalado por los estudiantes en la encuesta, quienes expresaron que no existe un control real del ingreso y que incluso han notado la desaparición de equipos. De esta manera, la confrontación de evidencias permite concluir que los problemas se caracterizan principalmente por un control de acceso deficiente, una supervisión limitada de los recursos y la ausencia de medidas efectivas para garantizar la conservación de los equipos.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

Este capítulo presenta el desarrollo de una Auditoría de Seguridad Informática donde se evaluó a los equipos tecnológicos de los laboratorios de cómputo 1 y 2 de la carrera de TI & Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. Para su ejecución, se aplicó la metodología MAGERIT, que ofrece un enfoque estructurado y sistemático para la identificación, evaluación y gestión de riesgos. La implementación de esta metodología permitió obtener un diagnóstico preciso y detallado sobre el estado actual de la seguridad informática en los laboratorios analizados.

4.2 Descripción de la propuesta

La presente propuesta corresponde a una auditoría de seguridad informática física de los equipos en los laboratorios de cómputo 1 y 2 de la carrera de TI & Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. En esta auditoría se llevó a cabo un análisis de riesgo enfocado en el control de acceso de los laboratorios. Para ello, se aplicó la metodología MAGERIT, la cual mediante sus estándares y enfoques permitió identificar el nivel de riesgo de control de acceso y uso de los laboratorios.

4.3 Determinación de recursos

4.3.1 Humanos

La siguiente tabla detalla los recursos humanos que participaron en el desarrollo del proyecto de titulación especificando sus roles y responsabilidades a lo largo del proceso

Cantidad	Recursos	Función	Actividad
1	Ing. Clara Pozo Hernández	Tutora	Participó activamente como guía durante la elaboración de mi trabajo de titulación.
1	Ing. Bladimir Mora	Coordinador de las carreras	Participó como informante clave en la entrevista correspondiente a la fase de diagnóstico.
92	Estudiantes	Estudiantes de las carreras de TI & Softwares.	Participaron en la encuesta destinada al diagnóstico, dentro del capítulo III.
1	Fernanda Basurto	Investigadora	Realizó el proyecto Integrador.

Tabla 5 Recursos humanos

4.3.2 Tecnológicos

La tabla de recursos tecnológicos detalla el conjunto de herramientas informáticas y de comunicación que han sido fundamentales para la ejecución de este proyecto de auditoría de seguridad informática.

Cantidad	Recurso	Actividad
1	Portátil Lenovo core i3 8 GB de RAM	Herramienta clave para la gestión y procesamiento de información.
1	Teléfono Tecno Spark 20C Pro con cámara frontal y trasera	Dispositivo esencial para la recolección de evidencia visual y documental.
8 meses	Conexión de internet	Recurso indispensable para la búsqueda de información y acceso a fuentes académicas.
1	Impresora Epson	Equipo utilizado para la impresión de entrevistas y documentos relevantes para la investigación.
1	Programas de Microsoft Office	Conjunto de herramientas fundamentales para la organización, análisis y presentación de datos.

Tabla 6 Recursos tecnológicos

4.3.3 Económicos

En esta sección se detalla el presupuesto designado para la ejecución de la auditoría de la seguridad informática, incluyendo la inversión en equipos tecnológicos implementados.

Cantidad	Descripción	Precio	Subtotal
1	Portátil Lenovo core i3 8 GB de RAM	$600	$600
1	Teléfono móvil Tecno Spark 20C Pro	$150	$150
8 meses	Internet	$12	$96
1	Impresora	$200	$200
1	Kits de oficina (Lapicero, hojas, etc.)	$20	$20
64 viajes	Transporte	$0.80	$51,20
		Total	$1117,20
		Hora de trabajo	384 h

Tabla 7 Presupuesto

4.4 Etapas del desarrollo de la propuesta

4.4.1 Fase 1 Planificar

4.4.1.1 Programa de Auditoría

Programa de auditoría de seguridad informática en los laboratorios de cómputo de las carreras de TI y Software de la Universidad Laica Eloy Alfaro de Manabí Extensión el Carmen.		
Objetivo • Identificar los riesgos de seguridad física de los equipos de los laboratorios de cómputo 1 y 2 de la carrera de TI & Software de la universidad Laica Eloy Alfaro de Manabí de la Extensión El Carmen. • Evaluar el nivel de seguridad de los equipos de los laboratorios de cómputo de la carrera de TI & Software de universidad Laica Eloy Alfaro de Manabí de la Extensión El Carmen		
Técnicas y Procedimientos	**Ref. a Papel**	**Fecha**
Programa de Auditoría	4.4.1.1	9/5/2025
Revisar la metodología Magerit	4.4.1.2	12/5/2025
Identificar de los activos	4.4.1.3	16/5/2025
Valoración de los activos	4.4.1.4	19/05/2025
Identificar las amenazas	4.4.1.5	26/05/2025
Elaboración de instrumentos	4.4.1.6	2/06/2025
Aplicación de los instrumentos	4.4.1.7	0 9/6/2025
Ejecución	4.4.1.8	13/6/2025
Tabulación	4.4.1.11	16/6/2025
Análisis de resultados	4.4.1.12	20/6/2025
Determinar de riesgo	4.4.1.12.1	23/6/2025
Medidas de Seguridad	4.4.5.2	30/6/2025
Elaboración del informe	5	27/6/2025

Tabla 8 Programa de auditoría

4.4.1.2 Revisión de Magerit

Según la normativa ISO 31000, MAGERIT se integra dentro del Proceso de Gestión de los Riesgos, particularmente en la sección 4.4 sobre la Implementación de la Gestión de los Riesgos, que forma parte del Marco de Gestión de Riesgos. Esta sección establece las directrices para aplicar un enfoque sistemático en la gestión de riesgos, y MAGERIT

proporciona el marco necesario para que los órganos de gobierno puedan tomar decisiones fundamentadas, asegurando la identificación, evaluación y tratamiento de los riesgos derivados del uso de tecnologías de la información (Amutio, 2012)

4.4.1.2.1 Las fases de Magerit

1. **Identificar los activos:** Durante esta etapa definimos la información referente de los datos y servicios estableciendo la importación dentro del sistema, cada uno de los activos fundamentales se determinan los criterios de seguridad que deben aplicarse a los elementos del sistema garantizando su protección y correcto funcionamiento.
2. **Identificar las amenazas:** Durante esta etapa se identificaron las posibles amenazas que pudieran tener un gran impacto en los activos, representadas como eventos o situaciones que puedan ocurrir, para infectar la seguridad, la integridad y la disponibilidad de estos. Enfocados principalmente en analizar aquellos patrones que podrían ocasionar daño y evaluar su impacto al sistema.
3. **Determinar el impacto:** La magnitud del impacto debido al daño que sufren los activos cuando aparece una amenaza, debe ser calculado para analizar el valor de cada activo en los distintos aspectos y la degradación que, provocado por las amenazas, permitiendo estimar su efecto directo en el sistema.
4. **Analizar los riesgos:** En esta fase, se definieron los riesgos exponenciales como daño potencial que puede sufrir un sistema, determinando un análisis clave para el impacto de las amenazas sobre los activos, calculando el nivel de riesgo considerando la probabilidad de que dichas amenazas aparezcan.
5. **Secciones de Medidas de Seguridad:** Durante esta fase se evaluaron los impactos de riesgos a los que los activos se encontrarán expuestos debido a la ausencia de protección, debido a que suele ser inusual encontrar sistemas completamente desprotegidos para este análisis, nos permite comprender las distintas posibilidades consecuentes, para la eliminación de salvaguardas existentes.
6. **Determinar el riesgo e impacto residual:** En esta fase el riesgo residual se define como la situación en la que queda un sistema después de aplicar un conjunto determinado de salvaguardas y evaluar la madurez de su gestión. Se considera que el riesgo ha sido transformado pasando de un nivel potencial inicial a un riesgo residual controlado reflejando la efectividad de las medidas de protección implementadas.

4.4.1.3 Identificar Activos

4.4.1.3.1 Activos físicos

Como primer paso y en cumplimiento de la metodología MAGERIT, se elaboró el inventario de activos clasificados en dos categorías: físicos y lógicos. Esta clasificación facilitó la identificación y organización de los recursos del entorno auditado. En la Tabla 8 se presentan los activos físicos identificados.

Id	Código de serie	Nombre de Activo	Descripción Técnicas	Ubicación De Cómputos	Periféricos Asociados	Marca	Modelo
A01	074213	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1	Monitor LG, Teclado genérico y	LG	9EN336
A02	074504	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A03	074507	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor Dell, Teclado y Mouse	Dell	E1913FS
A04	074497	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A05	074385	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A06	074381	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Mouse y	ASUS	VP228
A07	074494	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228

Id	Código de serie	Nombre de Activo	Descripción Técnicas	Ubicación De Cómputos	Periféricos Asociados	Marca	Modelo
A08	074479	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor LG, Mouse y Sin Teclado	LG	VP228
A09	074506	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor LG, Teclado y Mouse	LG	20MK400H-B
A10	074496	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A11	074501	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado	ASUS	VP228
A12	074500	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A13	074503	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado	ASUS	VP228
A14	074502	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Mouse	ASUS	VP228
A15	074499	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A16	074405	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado	ASUS	VP228
A17	074534	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor LG, Mouse Genius y	LG	W1742ST

Id	Código de serie	Nombre de Activo	Descripción Técnicas	Ubicación De Cómputos	Periféricos Asociados	Marca	Modelo
A18	072002	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor BENQ, Teclado y	BENQ	ET-002-B
A19	074397	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado Y	ASUS	VP228
A20	074095	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado	ASUS	VP228
A21	074079	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Mouse	ASUS	VP228
A22	074408	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A23	074412	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Monitor ASUS, Teclado y	ASUS	VP228
A24	074498	Computadora De Escritorio	Procesador Intel i7, Ram 16MG.	Lab1 Aula 201	Teclado y Mouse Genius	ASUS	VP228
A25	073816	Rack	Estructura metálica para organizar equipos de TI (servidores, red).	Lab1 Aula 201	Switches, Routers y Cableado	Microtk	Crs326-24g-24s+rm
A26	077184	Aire Acondicionado	Controla la temperatura lo que	Lab1 Aula 201	Filtros de Aire	Green Air	Lmvc060cc201

Id	Código de serie	Nombre de Activo	Descripción Técnicas	Ubicación De Cómputos	Periféricos Asociados	Marca	Modelo
			protege a los equipos				
A27		Proyector	Proyección de imágenes o video desde la computadora	Lab1 Aula 201	Control	Epson	EX9240
A28	31120	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor	Dell	D17S
A29	31115	Computada De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A30	31133	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A31	31119	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A32	31130	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A33	31134	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A34	31116	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S

Id	Código de serie	Nombre de Activo	Descripción Técnicas	Ubicación De Cómputos	Periféricos Asociados	Marca	Modelo
A35	31127	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A36	31118	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A37	31125	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A38	31123	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A39	31131	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A40	31129	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A41	31126	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A42	31128	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Au	Mouse, Teclado y Monitor Dell	Dell	D17S
A43	31122	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A44	31132	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S

Id	Código de serie	Nombre de Activo	Descripción Técnicas	Ubicación De Cómputos	Periféricos Asociados	Marca	Modelo
A45	31121	Computadora De Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A46	31125	Computadora de Escritorio	Procesador i7, Ram 16MG	Lab2 Aula 209	Mouse, Teclado y Monitor Dell	Dell	D17S
A47	072001	Rack	Estructura metálica, conexión redundante de energía	Lab2 Aula 209	Switches, Routers y Cableado	Microtk	Crs326-24g-24s+rm
A48	No tiene	Aire Acondicionado	Sistema de climatización para salas de servidores	Lab2 Aula 209	Filtros de Aire control	Green Air	Lmvc060cc201
A49	074483	Proyectores	Proyector HD, conectividad HDMI y Wi-Fi	Lab2 Aula 209	Cables de conexión y Control	Epson	EX9240

Tabla 9 Identificación de activos

4.4.1.3.2 Activos lógicos

La Tabla 9 detalla los activos lógicos de los laboratorios, incluyendo sistemas operativos, software y controles de seguridad de cada uno de los activos de los laboratorios.

Nombre de Activo	Ubicación	Sistema Operativo	Versión SO	Software Instalado	Controles de Seguridad	Observación Técnicas

Computadoras de Escritorios	Lab1	Windows 11	24H2	Office 365, Chrome, IDE Java, VLC	Windows Defender	Las 24 estaciones del Laboratorio 1 cuentan con configuración lógica homogénea.
Rack	Lab1	Sistema embebido		Interfaz web del router y switch	Acceso físico restringido	Contiene switch, patch panel y UPS.
Computadoras de Escritorios	Lab2	Windows 11	24H2	Office 365, Chrome, IDE Java, VLC	Windows Defender	Las 19 estaciones del Laboratorio 1 cuentan con configuración lógica homogénea.
Rack	Lab2	Sistema embebido		Interfaz web del router y switch	firewall de red	Contiene switch, patch panel y UPS.

Tabla 10 Identificación de activos lógicos

4.4.1.4 Valoración de Activos

Una vez definido el inventario de activos, se procedió a su valoración de los activos mediante una escala cualitativa de cinco niveles, detallada tal cual como se muestra en la Tabla 10.

VA	Valor de Activo	Descripción
1	Muy Bajo	Activo con relevancia mínima, su pérdida no afecta las actividades
2	Bajo	Activo tiene poca importancia, su afectación genera molestia menor sin comprometer las actividades.
3	Medio	El activo es necesario para ciertas funciones. Su pérdida puede afectar temporalmente algunos servicios.
4	Alto	Activo crítico para operaciones importantes. Su indisponibilidad causa interrupciones

5	Muy Alto	Activo esencial cuya falla interrumpe actividades y limita el rendimiento académico.

Tabla 11 Valor de activos

Posteriormente, cada activo fue evaluado de acuerdo con los niveles establecidos en la Tabla 10, como se detalla en la Tabla 11.

Tipos de Activos	Ubicación	Valor			
		D	I	C	V.A
Computadoras de Escritorio	Lab1	5	3	4	5
Rack	Lab1	4	4	3	3.6
Aire Acondicionado	Lab1	5	4	3	4
Proyectores	Lab1	1	3	4	2.6
Computadoras de Escritorio	Lab2	5	4	4	4.3
Pantalla	Lab2	1	2	3	2
Rack	Lab2	4	4	3	3.6
Aire Acondicionado	Lab2	5	4	3	4
Proyectores	Lab2	1	3	4	2.6

Tabla 12 Valoración de activos

4.4.1.5 Identificaciones de amenazas

Se consideró cada uno de los activos identificados y se analizaron los posibles peligros a los que podrían estar expuestos, como se detalla en la Tabla correspondiente.

Activos	Amenazas
Computadoras de Escritorio	• Robos • Danos • Incendios • Inundaciones • Malwares
Pantalla	• Robos • Daños
Rack	• Daño • Incendio
Aire Acondicionado	• Daños • Inundaciones

Proyectores	• Robo • Daño

Tabla 13 Identificación de posibles amenazas

4.4.1.6 Elaboración de instrumentos

Con base en los lineamientos de la norma ISO 27001, se diseñaron cinco instrumentos de evaluación cada uno orientado a un grupo específico de riesgos identificados como robo, daño, incendio, inundación y malware. Cada instrumento contiene un total de 25 preguntas de tipo 'sí' o 'no', enfocadas en verificar el cumplimiento de controles asociados a la confidencialidad, integridad y disponibilidad tal como se detalla a continuación.

4.4.1.6.1 Cuestionarios para evaluar riesgos

Se presentan los cuestionarios diseñados para la evaluación de riesgos entre los cuales se consideran amenazas como robo, daño, incendio, inundación y malware. Cada uno de estos cuestionarios está conformado por 25 preguntas orientadas específicamente a su respectivo tema, lo que permite obtener información detallada y precisa sobre los posibles incidentes que podrían afectar a los laboratorios.

Laboratorio N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1
				Pag. 1 - 5
N°	PREGUNTAS: ROBO	SI	NO	Observaciones
1	¿Existen camara de seguridad instalada en los laboratorio?			
2	¿Las camaras de seguridad estan funcionando correctamente?			
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?			
4	¿Existen responsible de la seguridad de los laboratorios?			
5	¿Existen procedimientos para reportar un robo?			
6	¿Se han registrado incidentes previos de robo en los laboratorios?			
7	¿Los activos del laboratorio cuentan con medidas de protección física actualmente?			
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?			
9	¿Los equipos están identificados con códigos o etiquetas?			
10	¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?			
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta area?			
12	Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?			
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?			
14	¿Hay restricciones para la salida de equipos del laboratorio?			
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?			
16	¿Se verifica el estado y funcionamiento de los equipos físicos en los laboratorio?			
17	¿Existe un sistema de comunicación rápida para reportar incidentes?			
18	¿Los accesos principales están bajo vigilancia constante?			
19	¿Se cuenta con sistemas de alarma en los laboratorios?			
20	¿Los equipos están atados o asegurados físicamente?			
21	¿Se han registrado reportes de robo recientemente?			
22	¿Hay dispositivos de rastreo en los equipos?			
23	¿Los laboratorios tienen sensores de movimiento?			
24	¿Existen protocolos claros para la investigación de incidents?			
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?			
Realizado por:		**Observación:**		
Fecha:		**Revisado por:**		

Ilustración 4 Cuestionario de Riesgo

Laboratorio N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 2 - 5		
N°	PREGUNTAS: DAÑO	SI	NO	Observaciones
1	¿Las mesas y superficies de trabajo son adecuadas para los equipos?			
2	¿Se han reportado daños por caídas o golpes?			
3	¿Los teclados, monitores y mouse presentan signos de mal uso?			
4	¿Se realizan inspecciones para detectar desgaste o fallas en los equipos?			
5	¿Los cables y conexiones están organizados adecuadamente?			
6	¿Se cuenta con protección contra sobrecarga eléctrica?			
7	¿Los equipos de los laboratorio se utilizan siguiendo las medidas de seguridad física para prevenir daños			
8	¿Existen registros de mantenimiento preventivo de los equipos?			
9	¿Hay señales visibles de maltrato físico en los equipos?			
10	¿Los equipos están expuestos a humedad o líquidos?			
11	¿Los equipos tienen ventilación suficiente para evitar sobrecalentamientos?			
12	¿Se han identificado equipos con fallas recurrentes?			
13	Se han implementado procedimientos para reportar daños?			
14	¿Los equipos son apagados correctamente después de su uso?			
15	¿Se han reportado incidentes debido al uso inadecuado de los dispositivos en el laboratorio?			
16	¿Se han tomado medidas para reducir el polvo y otras amenazas ambientales?			
17	¿Se da mantenimiento preventivo periódico a los equipos?			
18	¿Los usuarios tienen normas claras sobre el cuidado de los dispositivos?			
19	¿Las conexiones eléctricas son revisadas regularmente?			
20	Se han encontrado problemas en la estructura del laboratorio?			
21	¿El laboratorio tiene cableado estructurado?			
22	¿Se controla la temperatura y ventilación del laboratorio?			
23	¿Se permite el ingreso de alimentos o bebidas?			
24	¿Hay un responsable designado para el cuidado del equipo?			
25	¿Se inspeccionan los equipos al final de cada jornada?			
Realizado por:		**Observación:**		
Fecha:		**Revisado por:**		

Ilustración 5 Cuestionario de Daño

Laboratorio N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 3 - 5
N°	PREGUNTAS: INCENDIO	SI	NO	Observaciones
1	¿El laboratorio cuenta con detectores de humo?			
2	¿Se han instalado extinguidores adecuados para equipos electrónicos?			
3	¿Existe señalización clara de rutas de evacuación?			
4	¿Se han realizado simulacros de incendio en el laboratorio?			
5	¿Las conexiones eléctricas son seguras?			
6	¿Se han revisado los sistemas eléctricos para detectar riesgos?			
7	Se realizan inspecciones técnicas para detectar fallas en el sistema eléctrico?			
8	¿Las tomas de corriente están protegidas contra sobrecargas?			
9	¿Se han registrado incidentes previos relacionados con incendios?			
10	¿Las instalaciones eléctricas están en buen estado?			
11	¿Las rutas de evacuación están despejadas y accesibles?			
12	¿Se realizan inspecciones periódicas para evaluar riesgos de incendio?			
13	¿ ¿El laboratorio cuenta con extintores?			
14	¿Existe una organización estructurada para la disposición de cada equipo en el laboratorio?			
15	¿Existe señalización visible que identifique cada equipo			
16	¿Existen sistemas de ventilación para disipar calor acumulado?			
17	¿La altura de los cables cumple con los estándares de seguridad física?			
18	¿Se almacenan productos inflamables cerca de los equipos?			
19	¿Se revisa el estado de los dispositivos de protección eléctrica?			
20	¿Hay un plan de emergencia en caso de incendio?			
21	¿Se verifica el vencimiento de los extintores?			
22	¿Se realiza limpieza frecuente de polvo y residuos que puedan ser inflamables?			
23	¿El techo y paredes del laboratorio están hechos de materiales resistentes al fuego?			
24	¿Existe un responsable designado para la revisión periódica del equipo contra incendios?			
25	¿Los equipos que generan calor como routers o servidores tienen buena disipación?			

Realizado por:	Observación:
Fecha:	Revisado por:

Ilustración 6 Cuestionario de Incendio

Laboratorio N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 4 - 5		
N°	PREGUNTAS:INUNDACIONES	SI	NO	Observaciones
1	¿Existen registros de inundaciones previas en el área donde se ubica el laboratorio?			
2	¿El laboratorio está ubicado en una zona con riesgo de acumulación de agua por lluvias intensas?			
3	¿Se han identificado posibles puntos de filtración de agua dentro del laboratorio?			
4	¿Existe un sistema de drenaje adecuado en la infraestructura del edificio?			
5	¿Las puertas y ventanas cuentan con sellado contra filtraciones?			
6	¿Hay equipos electrónicos ubicados en áreas bajas susceptibles a inundaciones?			
7	¿Existen sistemas de alerta para detectar acumulación de agua?			
8	¿Los cables eléctricos están protegidos contra humedad y exposición al agua?			
9	¿Se cuenta con un protocolo de emergencia en caso de inundación?			
10	¿Los equipos están elevados em los laboratorios?			
11	¿Las conexiones eléctricas tienen protección contra cortocircuitos por humedad?			
12	¿Se han realizado simulacros de emergencia en caso de inundación?			
13	¿Se han identificado vías seguras de evacuación en caso de inundación?			
14	¿Los documentos físicos importantes están almacenados en áreas protegidas?			
15	¿Los servidores y equipos críticos tienen protección contra humedad?			
16	¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?			
17	¿Se revisa periódicamente el estado de techos y estructuras para prevenir filtraciones?			
18	¿Las áreas de almacenamiento están diseñadas para minimizar riesgos de inundación?			
19	¿Se han tomado medidas estructurales para evitar acumulación de agua en el laboratorio?			
20	¿Los equipos sensibles tienen cubiertas protectoras contra agua?			
21	¿Se han implementado protocolos de inspección después de lluvias fuertes?			
22	¿Los sistemas eléctricos tienen desconexión automática en caso de contacto con agua?			
23	¿Los equipos electrónicos tienen garantías contra daños por humedad?			
24	¿Se han identificado patrones climáticos que podrían aumentar el riesgo de inundación?			
25	¿Se han realizado auditorías previas que recomienden mejoras en la prevención de inundaciones?			

Realizado por:	Observación:
Fecha:	Revisado por:

Ilustración 7 Cuestionario de Inundación

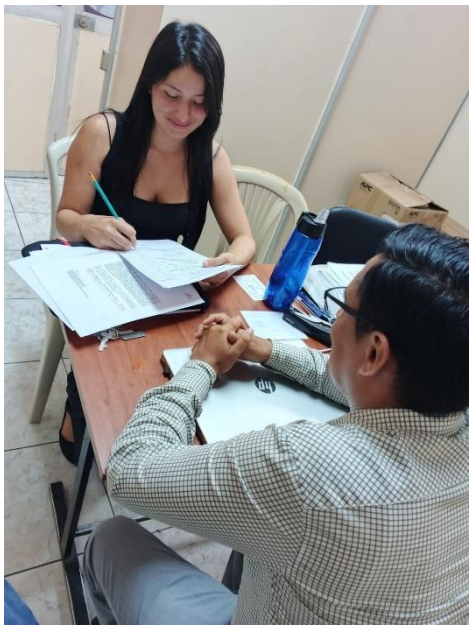
Laboratorio N°	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 5 - 5
N°	PREGUNTAS:MALWARE	SI	NO	Observaciones
1	¿Existe una política de seguridad definida para la protección contra malware?			
2	¿Se cuenta con un software antivirus actualizado en los equipos del laboratorio?			
3	¿Los usuarios tienen restricciones para la instalación de software no autorizado?			
4	¿Se realizan análisis periódicos para detectar posibles infecciones?			
5	¿Existen medidas para prevenir ataques de phishing dentro de la red del laboratorio?			
6	¿Se cuenta con control de acceso para evitar el uso no autorizado de los dispositivos?			
7	¿Los sistemas operativos están actualizados con parches de seguridad?			
8	¿Se han identificado incidentes previos de malware en el laboratorio?			
9	¿Los estudiantes reciben capacitación sobre buenas prácticas de seguridad informática?			
10	¿Las redes Wi-Fi cuentan con medidas de protección contra accesos no autorizados?			
11	¿Se utilizan herramientas de monitoreo para detectar comportamiento sospechoso en los equipos?			
12	¿Existe un procedimiento de respuesta en caso de infección por malware?			
13	¿Se aplican filtros de contenido para prevenir el acceso a sitios maliciosos?			
14	¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?			
15	¿El tráfico de red es monitoreado para detectar actividad sospechosa?			
16	¿Los dispositivos USB están restringidos para evitar infecciones?			
17	Los archivos de instalación y descarga son verificados antes de su uso?			
18	¿Se han realizado auditorías previas que detectaron vulnerabilidades en la seguridad lógica?			
19	Existen políticas de gestión de actualizaciones para reducir riesgos de infección?			
20	¿Se implementan registros de actividad para identificar intentos de acceso sospechosos?			
21	¿Los accesos a cuentas institucionales están protegidos con autenticación de múltiples factores?			
22	¿Los servidores del laboratorio tienen protecciones específicas contra ataques externos?			
23	¿Se han documentado procedimientos de limpieza y eliminación de malware en los equipos?			
24	¿Se cuenta con herramientas de análisis forense para detectar el origen de una infección?			
25	¿Las medidas de seguridad actuales han sido probadas mediante pruebas de penetración?			

Realizado por:	Observación:
Fecha:	Revisado por:

Ilustración 8 Cuestionario de Malware

4.4.2 Aplicación de la Auditoría.

Para llevar a cabo la auditoría se realizó una revisión exhaustiva de las instalaciones de los laboratorios para verificar su estado actual. Adicionalmente, se contó con la colaboración del Ing. Bladimir Mora, coordinador de las carreras de TI y Software, quien apoyó el desarrollo de la auditoría respondiendo las preguntas de la entrevista de evaluación correspondientes. Esta fase permitió contrastar las observaciones con el conocimiento administrativo y operativo del entorno.



4.4.2.1 Ejecución

Mediante la ejecución de la auditoria, llevada a cabo con la aplicación de un cuestionario compuesto por 25 preguntas diseñadas cuidadosamente, para conseguir evaluar los controles de seguridad física en los laboratorios. Conjunto a la colaboración del coordinador de carrera, logramos acceder a la información necesaria, cada uno de las preguntas abordan aspectos clave relacionados con amenazas significativas como el daño físico, riesgo a incendio, inundación y la presencia de malware, obteniendo un diagnóstico claro e íntegro del estado actual de la seguridad de la infraestructura tecnológica evaluada.

4.4.2.1.1 Evidencias de Cuestionarios llenos.

Se adjunta únicamente el cuestionario correspondiente al riesgo de robo los demás cuestionarios llenos pueden ser consultados en el Anexo G, ubicado al final del documento.

Laboratorio N° 1	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 1 - 5
N°	PREGUNTAS: ROBO	SI	NO	Observaciones
1	¿Existen camara de seguridad instalada en los laboratorio?	X		
2	¿Las camaras de seguridad estan funcionando correctamente?	X		
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?		X	
4	¿Existen responsible de la seguridad de los laboratorios?	X		
5	¿Existen procedimientos para reportar un robo?	X		
6	¿Se han registrado incidentes previos de robo en los laboratorios?		X	
7	¿Los activos del laboratorio cuentan con medidas de protección física actualmente?		X	
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?		X	
9	¿Los equipos están identificados con códigos o etiquetas?		X	
10	¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?		X	
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta area?	X		
12	Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?		X	
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?		X	
14	¿Hay restricciones para la salida de equipos del laboratorio?	X		
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?	X		
16	¿Se verifica el estado y funcionamiento de los equipos físicos en los laboratorio?	X		
17	¿Existe un sistema de comunicación rápida para reportar incidentes?		X	
18	¿Los accesos principales están bajo vigilancia constante?		X	
19	¿Se cuenta con sistemas de alarma en los laboratorios?		X	
20	¿Los equipos están atados o asegurados físicamente?		X	
21	¿Se han registrado reportes de robo recientemente?		X	
22	¿Hay dispositivos de rastreo en los equipos?		X	
23	¿Los laboratorios tienen sensores de movimiento?		X	
24	¿Existen protocolos claros para la investigación de incidents?		X	
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?	X		
Realizado por: Fernanda Elizabeth Basurto Muñoz		**Observación:**		
Fecha: 30/05/2025		**Revisado por:** Ing. Clara Guadalupe Pozo Hernández		

Ilustración 9 Cuestionario de Riesgo lleno

Ilustración 12 Respuesta Lab1 Malware

Ilustración 14 Respuesta Lab 2 de Daño

Ilustración 13 Respuesta Lab2 Riesgo

4.4.2.2 Revisión de controles físicos

En siguientes tablas se presentan de manera estructurada los principales riesgos identificados en la infraestructura tecnológica de los laboratorios. En ellas se detallan amenazas relevantes como el daño físico a los equipos, el riesgo de incendios, posibles inundaciones y la presencia de malware. Esta tabla permite visualizar de forma clara y sintética los puntos críticos detectados.

Robo	
Dentro de los establecimientos existen cámara, pero solo en el laboratorio 1 funciona de forma correcta 	No existen registro de ingresos 

Tabla 14 Riesgo de Robo

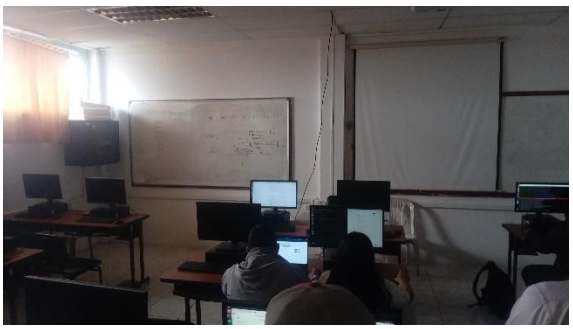
Daños	
No se lleva el control del uso de los dispositivos dentro de los laboratorios, existen ocasiones donde los equipos quedan encendidos. 	Los cables están bien estructurados entre la interconexión de los equipos dentro de los laboratorios. 

Tabla 15 Riesgo de Daños

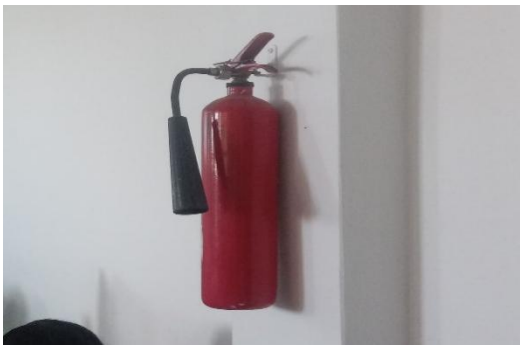
Incendios	
No existe ningún detector de humo en el área de los laboratorios en caso de un incendio. 	Los extintores están a la vista, pero están vencidos 

Tabla 16 Riesgo de Incendio

Inundación	
El techo de los laboratorios está en buenas condiciones en caso de lluvias 	Las ventanas no cuentan con sellados contra filtraciones de agua 

Tabla 17 Riesgo de Inundación

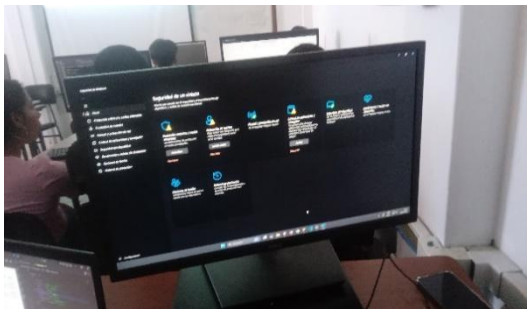
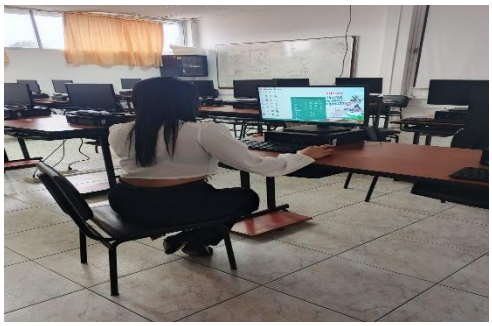
Malware	
Todas las computadoras de los laboratorios cuentan con el antivirus de Windows Defender. 	Ninguna computadora cuenta con algún usuario ni contraseña para evitar el uso no autorizado 

Tabla 18 Riesgo de Malware

4.4.2.3 Tabulación

Se empleó la herramienta de Excel para organizar los datos recopilados a partir de la matriz de evaluación de controles de seguridad aplicado en los laboratorios de las carreras de Software y TI contando además con el valioso apoyo del coordinador de dichas carreras.

4.4.2.3.1 Niveles para tabular

Para la tabulación de los cuestionarios aplicados se definieron tres niveles de evaluación con el fin de clasificar objetivamente las respuestas obtenidas.

- 1= Seguridad: la respuesta demuestra que se cuenta con controles adecuados.
- 2= Se usa cuando la pregunta no es relevante o la respuesta no está relacionada con seguridad o riesgo.
- 0 = Riesgo: asignado cuando la respuesta evidencia la ausencia de controles

Niveles	
0	Riesgo
1	Seguridad
2	No aplica

Tabla 19 Niveles de Tabulación

4.4.2.4 Tabulación de Datos

Se prosiguió a evaluar cada pregunta como antes se mencionó con la escala de 0,1 y 2.

Riesgo de Robo			
N°	Preguntas	Lab 1	Lab 2
1	¿Existen camara de seguridad instalada en los laboratorio?	1	0
2	¿Las camaras de seguridad estan funcionando correctamente?	1	0
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?	0	0
4	¿Existen responsible de la seguridad de los laboratorios?	1	1
5	¿Existen procedimientos para reportar un robo?	1	1
6	¿Se han registrado incidentes previos de robo en los laboratorios?	1	0
7	¿Los activos del laboratorio cuentan con medidas de protección física actualmente?	0	0
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?	0	0
9	¿Los equipos están identificados con códigos o etiquetas?	0	1
10	¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?	0	0
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta area?	1	0
12	Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?	0	0
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?	0	0
14	¿Hay restricciones para la salida de equipos del laboratorio?	1	1
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?	1	0
16	¿Se verifica el estado y funcionamiento de los equipos físicos en los laboratorio?	1	1
17	¿Existe un sistema de comunicación rápida para reportar incidentes?	0	0
18	¿Los accesos principales están bajo vigilancia constante?	0	0
19	¿Se cuenta con sistemas de alarma en los laboratorios?	0	0
20	¿Los equipos están atados o asegurados físicamente?	0	0
21	¿Se han registrado reportes de robo recientemente?	1	1
22	¿Hay dispositivos de rastreo en los equipos?	0	0
23	¿Los laboratorios tienen sensores de movimiento?	0	0
24	¿Existen protocolos claros para la investigación de incidents?	0	0
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?	0	0
	Total controles no aplica (2)	**0**	**0**
	Total de controles Evaluados	**25**	**25**
	Seguridad (1)	**10**	**6**
	Riesgo (0)	**15**	**19**
	Porcentaje de Seguridad	**40%**	24%
	Porcentaje de Riesgo	**60%**	**76%**
		100%	100%

Ilustración 16 Evidencias de la Tabulación de Robo

Riesgo de Daño			
N°	Preguntas	Lab 1	Lab 2
1	¿Las mesas y superficies de trabajo son adecuadas para los equipos?	1	1
2	¿Se han reportado daños por caídas o golpes?	1	1
3	¿Los teclados, monitores y mouse presentan signos de mal uso?	0	1
4	¿Se realizan inspecciones para detectar desgaste o fallas en los equipos?	1	1
5	¿Los cables y conexiones están organizados adecuadamente?	1	1
6	¿Se cuenta con protección contra sobrecarga eléctrica?	0	0
7	¿Los equipos de los laboratorio se utilizan siguiendo las medidas de seguridad física para prevenir daños	1	1
8	¿Existen registros de mantenimiento preventivo de los equipos?	0	0
9	¿Hay señales visibles de maltrato físico en los equipos?	1	1
10	¿Los equipos están expuestos a humedad o líquidos?	1	0
11	¿Los equipos tienen ventilación suficiente para evitar sobrecalentamientos?	1	1
12	¿Se han identificado equipos con fallas recurrentes?	0	0
13	Se han implementado procedimientos para reportar daños?	1	1
14	¿Los equipos son apagados correctamente después de su uso?	0	0
15	¿Se han reportado incidentes debido al uso inadecuado de los dispositivos en el laboratorio?	1	1
16	¿Se han tomado medidas para reducir el polvo y otras amenazas ambientales?	0	0
17	¿Se da mantenimiento preventivo periódico a los equipos?	1	1
18	¿Los usuarios tienen normas claras sobre el cuidado de los dispositivos?	0	0
19	¿Las conexiones eléctricas son revisadas regularmente?	0	0
20	Se han encontrado problemas en la estructura del laboratorio?	0	1
21	¿El laboratorio tiene cableado estructurado?	1	1
22	¿Se controla la temperatura y ventilación del laboratorio?	1	1
23	¿Se permite el ingreso de alimentos o bebidas?	1	1
24	¿Hay un responsable designado para el cuidado del equipo?	0	0
25	¿Se inspeccionan los equipos al final de cada jornada?	0	0
	Total controles no aplica (2)	**0**	**0**
	Total de controles Evaluados	**25**	**25**
	Seguridad (1)	**14**	**15**
	Riesgo (0)	**11**	**10**
	Porcentaje de Seguridad	**56%**	60%
	Porcentaje de Riesgo	**44%**	**40%**
		100%	100%

Ilustración 17 Evidencias de la Tabulación de Daño

Riesgo de Incendio			
N°	Preguntas	Lab 1	Lab 2
1	¿El laboratorio cuenta con detectores de humo?	0	0
2	¿Se han instalado extinguidores adecuados para equipos electrónicos?	0	0
3	¿Existe señalización clara de rutas de evacuación?	1	1
4	¿Se han realizado simulacros de incendio en el laboratorio?	0	0
5	¿Las conexiones eléctricas son seguras?	1	1
6	¿Se han revisado los sistemas eléctricos para detectar riesgos?	0	0
7	Se realizan inspecciones técnicas para detectar fallas en el sistema eléctrico?	0	0
8	¿Las tomas de corriente están protegidas contra sobrecargas?	1	1
9	¿Se han registrado incidentes previos relacionados con incendios?	1	1
10	¿Las instalaciones eléctricas están en buen estado?	1	1
11	¿Las rutas de evacuación están despejadas y accesibles?	1	1
12	¿Se realizan inspecciones periódicas para evaluar riesgos de incendio?	0	0
13	¿ ¿El laboratorio cuenta con extintores?	0	1
14	¿Existe una organización estructurada para la disposición de cada equipo en el laboratorio?	1	1
15	¿Existe señalización visible que identifique cada equipo	0	0
16	¿Existen sistemas de ventilación para disipar calor acumulado?	1	1
17	¿La altura de los cables cumple con los estándares de seguridad física?	1	1
18	¿Se almacenan productos inflamables cerca de los equipos?	1	1
19	¿Se revisa el estado de los dispositivos de protección eléctrica?	0	0
20	¿Hay un plan de emergencia en caso de incendio?	0	0
21	¿Se verifica el vencimiento de los extintores?	0	0
22	¿Se realiza limpieza frecuente de polvo y residuos que puedan ser inflamables?	1	1
23	¿El techo y paredes del laboratorio están hechos de materiales resistentes al fuego?	0	0
24	¿Existe un responsable designado para la revisión periódica del equipo contra incendios?	0	0
25	¿Los equipos que generan calor como routers o servidores tienen buena disipación?	1	1
	Total controles no aplica (2)	**0**	**0**
	Total de controles Evaluados	**25**	**25**
	Seguridad (1)	**12**	**13**
	Riesgo (0)	**13**	**12**
	Porcentaje de Seguridad	**48%**	52%
	Porcentaje de Riesgo	**52%**	**48%**
		100%	100%

Ilustración 18 Evidencias de la Tabulación de Incendio

Riesgo de Inundación			
N°	Preguntas	Lab 1	Lab 2
1	¿Existen registros de inundaciones previas en el área donde se ubica el laboratorio?	1	1
2	¿El laboratorio está ubicado en una zona con riesgo de acumulación de agua por lluvias intensas?	1	1
3	¿Se han identificado posibles puntos de filtración de agua dentro del laboratorio?	1	0
4	¿Existe un sistema de drenaje adecuado en la infraestructura del edificio?	1	0
5	¿Las puertas y ventanas cuentan con sellado contra filtraciones?	0	0
6	¿Hay equipos electrónicos ubicados en áreas bajas susceptibles a inundaciones?	1	1
7	¿Existen sistemas de alerta para detectar acumulación de agua?	0	0
8	¿Los cables eléctricos están protegidos contra humedad y exposición al agua?	1	1
9	¿Se cuenta con un protocolo de emergencia en caso de inundación?	0	0
10	¿Los equipos están elevados en los laboratorios?	0	1
11	¿Las conexiones eléctricas tienen protección contra cortocircuitos por humedad?	0	0
12	¿Se han realizado simulacros de emergencia en caso de inundación?	0	0
13	¿Se han identificado vías seguras de evacuación en caso de inundación?	0	0
14	¿Los documentos físicos importantes están almacenados en áreas protegidas?	0	0
15	¿Los servidores y equipos críticos tienen protección contra humedad?	0	0
16	¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?	0	0
17	¿Se revisa periódicamente el estado de techos y estructuras para prevenir filtraciones?	0	0
18	¿Las áreas de almacenamiento están diseñadas para minimizar riesgos de inundación?	1	1
19	¿Se han tomado medidas estructurales para evitar acumulación de agua en el laboratorio?	0	0
20	¿Los equipos sensibles tienen cubiertas protectoras contra agua?	0	0
21	¿Se han implementado protocolos de inspección después de lluvias fuertes?	0	0
22	¿Los sistemas eléctricos tienen desconexión automática en caso de contacto con agua?	0	0
23	¿Los equipos electrónicos tienen garantías contra daños por humedad?	0	0
24	¿Se han identificado patrones climáticos que podrían aumentar el riesgo de inundación?	1	0
25	¿Se han realizado auditorías previas que recomienden mejoras en la prevención de inundaciones?	0	0
	Total controles no aplica (2)	**0**	**0**
	Total de controles Evaluados	**25**	**25**
	Seguridad (1)	**8**	**6**
	Riesgo (0)	**17**	**19**
	Porcentaje de Seguridad	**32%**	24%
	Porcentaje de Riesgo	**68%**	**76%**
		100%	100%

Ilustración 19 Evidencias de la Tabulación de Imnundación

4.4.2.5 Análisis de Resultados

Para la obtención de la matriz de riesgo, se consideró en primer lugar el nivel de impacto, como parámetro fundamental para la evaluación. Este fue determinado con base en los criterios establecidos, los cuales se detallan a continuación:

Valor De Impacto	Descripción
1	No afecta las actividades, estas continúan con normalidad y sin alteraciones.
2	Genera afectaciones leves que no interrumpen el desarrollo normal de las actividades.
3	Provoca una interrupción parcial, breve y controlada que afecta momentáneamente las actividades.
4	Impacta significativamente ocasionando la detención temporal de las actividades.
5	Produce un impacto grave que paraliza completamente las actividades.

Tabla 25 Valoración de Impacto

El impacto fue calculado utilizando los niveles previamente establecidos, evaluando las siguientes dimensiones: confidencialidad, disponibilidad e integridad, tal como se detalla en la tabla.

Riesgos	Confidencialidad	Disponibilidad	Integridad	Valor de Impacto
Robo	3	5	3	4
Daño	2	4	2	3
Incendio	3	5	3	4
Inundación	2	4	3	3
Malware	3	5	3	4

Tabla 26 Cálculo de Valor de Impacto

Para la valoración del riesgo, se consideraron los porcentajes obtenidos en los controles asociados a los riesgos identificados: robo, incendio, inundación, daño de equipo y malware. A partir de los cuestionarios aplicados en los laboratorios 1 y 2, se calculó un promedio general de los resultados. Estos valores fueron evaluados conforme a una escala de clasificación, en función del rango porcentual correspondiente, tal como se muestra en la siguiente tabla.

Nivel	Aparación	Nivel de Riesgo
1	Más Bajo	1 – 10%
2	Bajo	11% - 30
3	Medio	31% - 50
4	Alto	51 - 75
5	Más Alto	75

Tabla 20 Nivel de Riesgo

A continuación, se muestra la matriz de la gravedad de Impacto mencionando los niveles ya calificados.

LEYENDA							
			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
APARICIÓN (probabilidad)	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal.Se vigilará aunque no requiere medidas preventivas de partida.

Gravedad de Impacto

Siguiendo los pasos mencionados una vez obtenido la probabilidad y la gravedad se conoció el nivel del riesgo es de esa manera que se desarrolló la matriz de riesgos

MATRIZ DE RIESGOS				
RIESGO	Aparición probabilidad	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
Robo	4	4	16	Muy grave
Daño	4	3	12	Importante
Incendio	3	3	9	Importante
Inundación	3	4	12	Importante
Malware	4	4	16	Muy grave

Ilustración 20 Matriz de Riesgo

CAPÍTULO V

5 INFORME DE AUDITORÍA

Tipo de Auditoría: Auditoría de Seguridad Informática

Dirigido a: Dr. Temístocles Bravo Decano de la ULEAM Extensión El Carmen

Objetivos:

- Identificar los riesgos de seguridad física de los equipos de los laboratorios de cómputo 1 y 2 de la carrera de TI & Software de la universidad Laica Eloy Alfaro de Manabí de la Extensión El Carmen.
- Evaluar el nivel de seguridad de los equipos de los laboratorios de cómputo de la carrera de TI & Software de universidad Laica Eloy Alfaro de Manabí de la Extensión El Carmen

Alcance:

La presente auditoría fue desarrollada a partir de un conjunto de tareas específicas, adaptadas de acuerdo con los lineamientos establecidos por la metodología MAGERIT.

- ❖ Revisar la metodología Magerit
- ❖ Inicio de Auditoria
- ❖ Identificar de los activos
- ❖ Valoración de los activos
- ❖ Identificar las amenazas
- ❖ Elaboración de instrumentos
- ❖ Aplicación de los instrumentos
- ❖ Ejecución
- ❖ Tabulación y análisis de resultados
- ❖ Determinar de riesgo
- ❖ Medidas de Seguridad
- ❖ Elaboración del informe

Personal Relacionado:

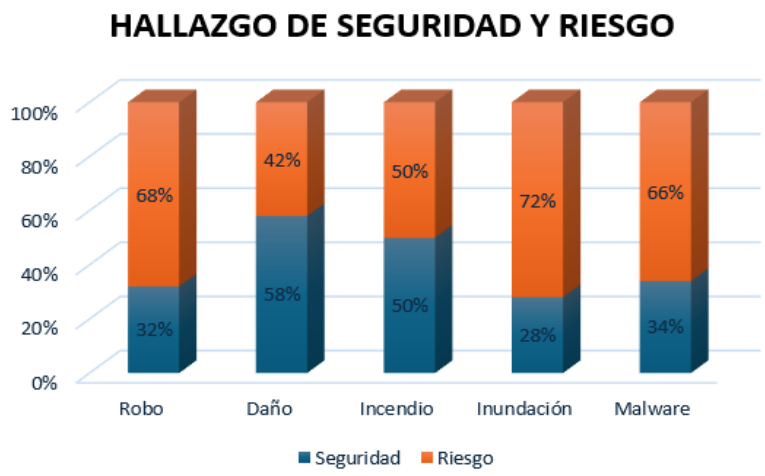
Coordinador de las carreras de TI & Software**.**

Estudiante de las carreras de TI & Software.

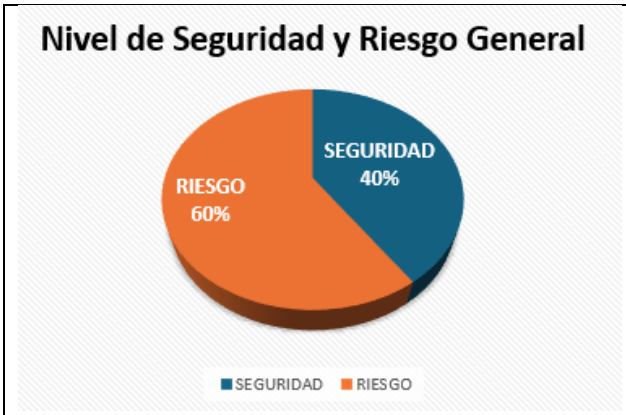
Los resultados obtenidos manifiestan que los equipos de los laboratorios se encuentran en riesgo alto, dado a una serie de exposiciones a amenazas, mediante la metodología MAGERIT se concluyó que, en este tipo de situaciones, requiere la aplicación de medidas urgentes para reducir las vulnerabilidades con el fin de proteger la infraestructura tecnológica del complejo.

5.1 Hallazgos

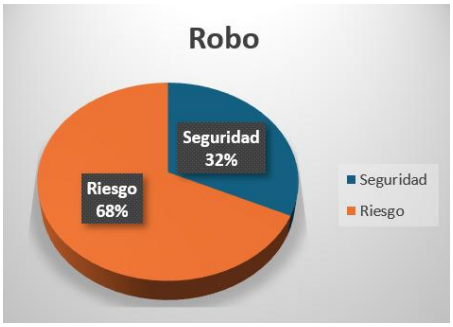
El gráfico evidencia que los laboratorios presentan niveles de riesgo entre importante y muy grave frente a amenazas como inundación, robo y malware lo que revela una alta vulnerabilidad y deficiencias en las medidas de protección. Aunque incendio y daño presentan riesgos más equilibrados también requieren atención. En conjunto los resultados destacan la urgente necesidad de reforzar la seguridad física y optimizar los protocolos existentes y aplicar medidas correctivas alineadas con la metodología MAGERIT.



Resultados de Riesgos y Seguir



Los resultados indican que los equipos del laboratorio presentan un riesgo alto lo que evidencia una exposición significativa a amenazas. Esta situación requiere medidas urgentes para reducir las vulnerabilidades.

Robo debido a:	**Robo**
	• No existen cámara de seguridad • Falta de medidas de seguridad • No cuenta con sistemas de alarmas • No existe un control de acceso • No cuentan con dispositivos de rastreo • No existen protocolos para incidentes
El riesgo frente al robo ha sido clasificado en un nivel alto, correspondiente a un riesgo muy importante. Esta situación se debe a graves deficiencias en la seguridad física, como la falta de cámaras de videovigilancia, sistemas de alarma y controles de acceso efectivos.	
Daño debido a:	**Daño**
	• No tener registros de mantenimiento previos. • El uso inadecuado de los dispositivos • Mal control de revisión eléctrica • No existe responsable del área • Fallas frecuentes en equipos • Problemas de estructuras
El daño de los equipos representa un riesgo muy importante debido a una falta de mantenimiento y mala gestión técnica. Aunque existe una protección básica, es recomendado reforzar los controles para evitar incidentes.	
Incendio debido a:	**Incendio**
	• No existen detectores de humo • No existen revisión de los extintores • No existen un plan de emergencia • No existen responsables para revisión contra incendio.

El riesgo de incendio ha sido clasificado en un nivel medio. Este nivel se origina por la ausencia de detectores de humo, la falta de mantenimiento de extintores, la inexistencia de planes de emergencia y la ausencia de personal designado.

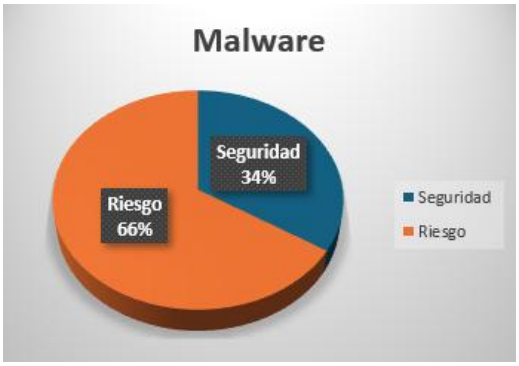
Inundación debido a:

Inundación

- No existe un plan de emergencia
- No existen sellos contra filtraciones
- No existen medidas físicas
- No existen protocolos en caso de lluvias

El riesgo de inundación es muy importante debido a la ausencia de medidas físicas y protocolos adecuados. La seguridad actual es baja por lo que se requiere una intervención urgente para proteger las instalaciones.

Malware debido a:



Malware

- No existen protección de acceso
- Los archivos de instalación no son verificados

El riesgo de infección por malware ha sido clasificado como alto, lo que corresponde a un riesgo muy importante según la escala establecida.

5.1.1 Opinión

Una vez finalizada la auditoría se pudo verificar los principales riesgos expuesto como: Robo, Daño, Incendio, inundación y Malware. En lo que se obtuvo como resultado un nivel general que existe riesgo muy importante por lo cual es necesario tomar medidas preventivas, para regular la situación y con respecto a la seguridad.

Ilustración 21 Evidencia de Nivel General de Riesgo

Después de obtener los resultados de cada amenaza examinada se evaluaron cada uno de los riesgos aplicando para conocer el nivel de seguridad de los equipos de los laboratorios de cómputo de la carrera de TI & Software de universidad Laica Eloy Alfaro de Manabí de la Extensión El Carmen, para ellos se realizó una matriz de riesgo en lo que se obtuvo los siguientes resultados.

MATRIZ DE RIESGOS	
RIESGO	**Nivel de Riesgo**
Robo	Muy grave
Daño	Importante
Incendio	Importante
Inundación	Importante
Malware	Muy grave

Ilustración 22 Matriz y Nivel de Riesgo

5.1.2 Conclusiones

El desarrollo de esta auditoría de seguridad informática en los laboratorios de cómputo de la carrera de TI y Software permitió reconocer con exactitud las vulnerabilidades físicas que impactan en la infraestructura. El proceso reveló la ausencia de controles de acceso, ausencia de personal a cargo de los laboratorios y fallas en la comunicación interna sobre el uso y cuidado de los equipos. En este trabajo se demostró claramente que la aplicación de metodologías como MAGERIT no solo facilita la identificación y valoración de riesgos, sino que también nos ayuda a tomar en cuenta la implementación de medidas preventivas, contribuyendo a un mejor entorno académico más seguro, confiable y eficiente.

5.1.3 Recomendaciones

- Implementar un control de acceso efectivo que exista alguna restricción para ingresar a los laboratorios que autentique el ingreso, acompañado de un registro automatizado que permita monitorear de forma continua el ingreso y salida de usuarios en los laboratorios.
- Que exista un responsable directo para la supervisión de los laboratorios, encargado del cumplimiento de las políticas de uso, la gestión de incidentes y el control.
- Que existan mantenimientos más a menudo para que de manera que se prolongue la vida útil de los equipos y se reduzcan fallas técnicas
- Instalaciones de cámaras dentro de los laboratorios para que así se permita el monitoreo en tiempo real y el respaldo de grabaciones para la investigación de incidentes.
- Aplicar políticas de seguridad que integren medidas físicas y lógicas, así como protocolos claros para reporte de incidentes.
- se recomienda poner en práctica el manual → Ver en el anexo F **Manual de guías de buenas prácticas**

5.1.3.1 Implementación de medidas de seguridad

Dentro de las medidas preventivas evaluadas, se determinó que la instalación de cámaras de seguridad es la medida más viable y efectiva, ya que se podrá tener una vigilancia continua de quién ingresa a los laboratorios. Esto permitirá monitorear en tiempo real el acceso a los laboratorios.

Opciones de Cámaras	
Cámaras	**Características**
Axis P1467-LE 	❖ **Marca/Modelo:** Axis P1467-LE ❖ **Tipo:** Bullet Network Camera ❖ **Resolución:** 5 MP ❖ **Ángulo de visión:** 107° ❖ **Conectividad:** PoE / Ethernet ❖ **Observaciones**: Tecnología Lightfinder para excelente visión nocturna, ideal para áreas con poca luz.
Reolink RLC-811A 	❖ **Marca/Modelo:** Reolink RLC-811A ❖ **Tipo:** Bullet Camera PoE ❖ **Resolución:** 4K ❖ **Ángulo de visión:** 87.5° ❖ **Conectividad:** PoE / Ethernet ❖ **Observaciones:** Color Night Vision, alta resolución, buena cobertura de exterior.
Hikvision DS-2CD1023G2-LIU 	❖ **Resolución:** 2 MP (1080p) ❖ **Ángulo de visión:** 103° ❖ **Conectividad:** RJ45 / ONVIF ❖ **Características destacadas:** - Smart Hybrid Light para visión nocturna clara. - Audio bidireccional y ranura para tarjeta microSD de hasta 512 GB. - Resistente a agua y polvo (IP67). - Compresión H.265+ para eficiencia en el uso del ancho de banda.

Tabla 21 Implementación de cámara

5.1.3.1.1 Elección de cámara

Para la instalación se eligió la cámara Hikvision DS-2CD1023G2-LIU, ya que tiene una amplia cobertura de 103°, una buena resolución de 2 MP y facilidad de integración con sistemas ONVIF (estándar que permite la compatibilidad entre dispositivos); también se tomó en cuenta su durabilidad y calidad, garantizando seguridad, funcionamiento constante y facilidad de mantenimiento de manera económica. Su tecnología avanzada también permite una visión clara en condiciones de baja iluminación, asegurando vigilancia continua en todo momento.

5.1.3.1.2 Materiales

- Cámara Hikvision DS-2CD1023G2-LIU
- Cables de red RJ45 / Ethernet
- Tornillería y anclajes
- Computadora
- Conectores RJ45
- Ponchadora

5.1.3.1.3 Instalación

Para llevar a cabo la instalación de la cámara, se tomó en cuenta cuáles podrían ser los puntos clave para instalarla; en este caso, se instaló en la parte alta, donde cubre toda el área del pasillo y claramente se puede visualizar el laboratorio. A continuación, se muestran los detalles.

Ilustración 23 Proyección

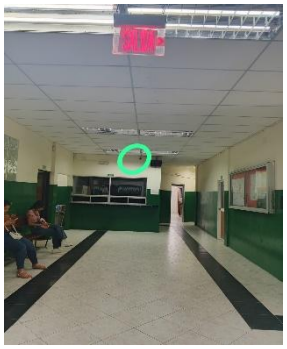
Punto de instalación de la cámara. 	Se prosiguió con la instalación de los cables desde el punto donde iba la cámara hasta eL NVR. 	Se realizó la instalación de la cámara. 
Se procede a configurar la cámara, asignando la IP y los permisos de acceso. 	Se observa ángulo de visión de la cámara instalada. 	Las cámaras se visualizan en tiempo real desde la computadora conectada. 

Tabla 22 Instalación de cámara

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Sin duda, la auditoría de seguridad informática realizada utilizando la metodología MAGERIT, junto con la aplicación de encuestas y entrevistas, permitió obtener un diagnóstico claro y preciso sobre el estado de la seguridad física y lógica en los laboratorios 1 y 2. Los resultados, provenientes tanto de estudiantes como del coordinador, fueron coherentes y evidenciaron deficiencias importantes que afectan el correcto funcionamiento y protección de los recursos tecnológicos. Este proceso evidenció con las respectivas pruebas que combinar diferentes métodos brinda una visión más completa y detallada, ayudando a identificar problemas en pueden llevarse a convertir en un gran problema.

Durante este análisis, se identificó varios riesgos críticos como robo, malware e inundaciones dentro de las instalaciones, representando una amenaza mayo para la confidencialidad, la integridad y la disponibilidad de los activos, además de distintos riesgos ocasionados por mal uso de los activos e incendio, clasificados con un nivel medio-alto, teniendo un impacto considerable en la operatividad de los laboratorios. Demostrando así que no solo provienen riesgos de factores externos sino también de malas prácticas del día a día en el entorno académico, tomando en cuenta la importancia de implementar medidas preventivas más rigurosas.

También se elaboró una propuesta de un manual de buenas prácticas junto con la aplicación de la metodología MAGERIT ofrece un marco sólido para mejorar la seguridad, siempre que se garantice una asignación clara de responsabilidades, un presupuesto definido y un seguimiento constante, permitiendo a la institución contar con una hoja de ruta clara para priorizar acciones, establecer responsables y medir el impacto real de las medidas adoptadas.

6.2 Recomendaciones

- Implementación de Manual de Buenas Prácticas para los estudiantes y la comunidad universitaria en general para ponerlo en práctica de manera efectiva para así fomentar una cultura de responsabilidad en el uso de los recursos tecnológicos con único propósito de promover un ambiente de trabajo más seguro mejorando la seguridad de toda la comunidad académica.
- Instalaciones de videovigilancia con cámaras en áreas clave y puntos ciegos hacia los laboratorios, que permita una vigilancia legible, también establecer protocolos para el manejo y acceso, garantizando el uso correcto de estas.
- Realizar un etiquetado para activos tecnológicos, necesario para realizar una sistematización de inventarios de cada laboratorio, que facilite el control, seguimiento y detección de pérdidas, asegurando una gestión ordenada y eficiente para los recursos tecnológicos.
- Que exista un responsable directo para la supervisión de los laboratorios, encargado del cumplimiento de las políticas de uso, la gestión de incidentes y el control.

BIBLIOGRAFÍA

Alvarado-Zabala, J., Pacheco-Guzmán, J., y Martillo-Alchundia, I. (2018, noviembre). *El análisis y gestión de riesgos en gobiernos de TI desde el enfoque de la metodología MAGERIT*. Revista Contribuciones a las Ciencias Sociales. Grupo eumed.net. https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html

Álvaro, V. (2022). *Auditoría de seguridad informática* . Bogotá: Ediciones de la U.

Amutio, M. A. (2012*). Metodología de análisis y gestión de riesgos de los sistemas de información.* Ministerio de Hacienda y Administraciones Públicas.

Anderson, R. (2023). *La industria de los videojuegos*. México: Tech Journal.

Arango Gómez, O. D. (2023*). El ABC de la seguridad informática: Guía práctica para entender la seguridad digital.* Bogotá: Autores Editores.

Arens, A. A., Elder, R. J., y Beasley, M. S. (2007). *Auditoría*: Un enfoque integral (11.ª ed.). Madrid: Pearson Educación.

Arias, H. A. (2010). Auditoría informática y gestión de tecnologías de información y comunicación (TICs).

Ávila, R., y Cuenca, J. P. (2021, 4 de diciembre). *Fases de MAGERIT* [PDF]. Ciencias Técnicas y Aplicadas. https://dialnet.unirioja.es/descarga/articulo/8384035.pdf

Baca Urbina, G. (2016). *Introducción a la seguridad informática* (1.ª ed.). México: Grupo Editorial Patria.

Behrouz, A. (2021). *Comunicaciones de Datos y Redes de Computadoras.* México: McGraw-Hill.

Bicalho, F. W. (2021). *Infraestructura resiliente: un imperativo para el desarrollo sostenible en América Latina y el Caribe* (Serie Comercio Internacional No. 160). Comisión Económica para América Latina y el Caribe (CEPAL). https://repositorio.cepal.org/handle/11362/46646

Buitrago, S., Alfonso, F., Ballesteros, J., y González, J. (2015*). Plataforma Cloud Computing como infraestructura tecnológica para laboratorios virtuales, remotos y adaptativos.* Revista Científica, 23.

Caicedo, C. (2024). Políticas de seguridad en la infraestructura tecnológica de instituciones de salud. Revista Científica de Salud BIOSANA, 1. https://soeici.org/index.php/biosana/article/download/102/189/444

Calderón Parrales, A. P., & Álava Cruzatty, J. E. (2023). *Diseño de infraestructura tecnológica para fortalecer la conectividad en el Malecón de Puerto Cayo.* Revista Científica Arbitrada Multidisciplinaria pentaciencias. https://doi.org/10.59169/pentaciencias.v5i5.763

Cano, M. A. (2011). *Interacción de microorganismos benéficos en plantas*. *Una Revisión*.

Chamorro, R., Oseda, M., Mucha, L., y Alania, R. (2021). *Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado.* Revista Científica de Ciencias Sociales y Humanidades, 51, 50–57. https://doi.org/10.37711/desafios.2021.12.1.253

Chávez, T., y Steven, A. (2022). *Auditoría informática en la empresa Distribuidora los Paisas.* Ecuador: Contabilidad y Auditoría C.P.A.

Chuez, P., y Michelle, L. (2022). *Auditoría de seguridad informática para infraestructura tecnológica en la Unidad Educativa Antonio José de Sucre en el periodo 2022.*

Constanza, D., Torres, N., y Peña, Y. (2018*). Diseño de políticas de seguridad informática para la empresa.* Neiva: Seguridad Informática.

Cortés, F. (2021). *Infraestructura Tecnológica: Claves para su Desarrollo en las Empresas.* Madrid: Ediciones Empresariales.

Creswell, W. (2020). *La entrevista como herramienta de recolección de datos.* California: Sage Publications.

Díaz, C., y Cruz, J. (2020). *Importancia de la seguridad física en la infraestructura de redes, centros de datos y telecomunicaciones de las instituciones de educación superior.* Tecnología e Innovación en Educación Superior, 3, 3–5.

Escuder, A., y Palacios, N. (2023). *Horizontes de La Transformación Digital.* Bolivia: dig-umsa-bo.

Espinoza, E. (2023). *La enseñanza de las ciencias sociales mediante el método deductivo. Revista Mexicana de Investigación e Intervención Educativa*, 2(2), 34–41.

Evilla, J. (2009). *Tipos y clases de auditorías informáticas.* Puerto Rico: Attribution Non-Commercial.

Gallego, A., Jaramillo, B., y Montenegro, C. (2017). *Virtualización de infraestructura tecnológica*. Colombia: Editorial Universidad Distrital Francisco José de Caldas (UD).

Giménez, J. (2023). Seguridad informática. Buenos Aires, Argentina: 1C Editorial.

Gómez, V. (2022). *Auditoría de seguridad informática.* España: Ediciones de la U.

González, D. (2018). *Diseño de un plan estratégico de seguridad informática para la protección de los recursos informáticos en el laboratorio de telecomunicaciones de la carrera de ingeniería en computación y redes.* Ciudad, País: Universidad XYZ.

González, J. (2012). *MAGERIT – versión 3.0.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Guevara, G., Verdesoto, A., y Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimenta es, participativas, y de investigación-acción). *Revista Científica Mundo de la Investigación y el Conocimiento*, 166.

Revista Científica Mundo de la Investigación y el Conocimiento, 166, 12–20.

Guevara, J. (2015). Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Perú: Magerit.Gutiérrez, L. (2023). *Gestión del mantenimiento de infraestructuras tecnológicas.* Madrid, España: Pearson.

Gutiérrez, M. (2022). *Muestra estadística.* Madrid: Etecé.

Harris y Laura. (2021). *Una revisión completa.* Barcelona: Gamer's Digest.

Herszenbaun, M. (2022). *Método analítico y la carencia de síntesis en "El conocer analítico" de la.* Madrid: Nuevo Itinerario.

Humbert, J. P. (2021). *Infraestructura de TI: Fundamentos y Prácticas.* México: Pearson Educación.

Hurel, R., Barrionuevo, C., Román, L., & Marcillo, P. (12 de Diciembre de 2022). Fundamentosde la auditoría: Una aproximación del estado del arte. *Audit Fundamentals*, pág. 247.

Intriago, J., Quimis, S., Choez, A., y Marcillo, J. (2023). *Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información.*

Jesús García Brunton, O. P. (2018). Influencia del cambio climático en la mejora genética de plantas. *Sociedad Española de Ciencias Hortícolas*.

Johnson, & Pedro. (2023). *Análisis del mercado de servicios de juegos en la nube.* Buenos Aires: Digital Entertainment Review.

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

López, C. (2021). *Seguridad Informática: Un Enfoque Integral.* Madrid: Ediciones Díaz de Santos.

López, M. (2022). *Medidas de seguridad perimetral en instalaciones informáticas.* Madrid: Seguridad Digital.

López, R. (2017). *Seguridad informática.* San Marco: Fundamentos de seguridad informática.

Lucero, L. (2023). *El rol de la auditoría informática en la era de la protección de datos personales Ecuador.* Argentina: Technology Rain Journal ISSN.

Mata García, E. (2024). *Seguridad de Equipos Informáticos.* Venezuela: Ra-Ma S.A.

Mata, A. (2023). *Seguridad en Equipos Informáticos. Actualizado 2023.* España: Segunaad.

Mata, A. (2024). *Seguridad de Equipos Informáticos.* Madrid: Ra.Ma 2023.

Medina, E., Medina, L., & Rivera, D. (2020). *Fundamentos teórico-conceptuales de la auditoría de procesos.* Camagüey: Rev retos vol.14 no.1.

Menéndez, S. (11 de Mayo de 2022). Auditoría de la Seguridad Informática. *Auditoría de la Seguridad Informática*, pág. 43.

Menéndez, S. C. (2023). *Auditoría de Seguiridad Informática.* Madrid: Ra-ma Editorial.

Mercedes Marqués. (2011). *Bases de datos.*

Metcalfe, R. (2015). *Information Security - Evolution.* Estados Unidos: Simon & Schuster.

MICROORGANISMO, I. P. (1999).

Miller y Tomás. (2021). *El auge y la caída de Google Stadia.* Madrid: Video Game Insights.

Molano, M., Valencia, A. M., y Apraez, M. (2021). Características e importancia de la metodología cualitativa en la investigación científica. *Semillas del Saber*, 20 al 21.

Olmos, J. (2020). Importancia de la Seguridad Física en la Infraestructura de Redes, Centros de Datos y Telecomunicaciones de las Instituciones de Educación . *Revista de Tecnología e Innovación en Educación Superior*, Imnovaciones.

Ortega, F., y Salazar, J. (2016). *Auditoría informática a los procesos y organización del área de sistemas en la Empresa Agropez Ltda de la Ciudad de Ipiales.* FIALES: Universidad de Nariño.

Palacios . (2020). *Seguridad informática.* Paola Paz Otero. Obtenido de https://www.google.com.ec/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es-419&gbpv=1

Palmero, S. (2021). *La enseñanza del componente gramatical: el método deductivo e inductivo.* Madrid: El método deductivo e inductivo.

Patel, y Karen. (2022). *La plataforma de juegos en la nube de Google.* Santiago: Cloud Gaming Review.

Pérez, A. (2021). *Amenazas físicas a la seguridad informática.* Madrid: Editorial Ciberseguridad.

Pérez, J. (2023). *La importancia del hardware en la infraestructura tecnológica.* Quito: Revista de Tecnología y Sociedad.

Postigo, A. (2020). *Seguridad informática.* España: Maria José López Raso.

Postigo, A. (2020). *Seguridad informática.* España: Cavel Industria Gráfica.

Rafael, O. (11 de Diciembre de 2023). *https://blog.hubspot.es/*. Obtenido de Tipos de auditoría: cuáles son y ejemplos: https://blog.hubspot.es/marketing/tipos-auditoria

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

Rivas, R. (1999). Interacciones planta microorganismo. *Interacciones Planta Microorganismo*.

Salvador Oliván, J. A. (2020). Encuesta y Diseños de Investigación. *Revista Española de Documentación Científica*, 12.

Sánchez, M. (2023). *La revolución digital: importancia de la infraestructura tecnológica en el siglo XXI.* Estados Unidos: Editorial Tecnología y Sociedad.

Smith, J. (2020). *The Future of Gaming: A Deep Dive into Google Stadia.* Estados Unidos: Tech Review.

Smith, J. (2021). *Evolución de la Infraestructura Tecnológica en Laboratorios de Cómputo.* Estados Unidos: Tecnológica.

Torres, L. (2022). Seguridad física en instalaciones informáticas. *Revista de Seguridad y Protección Informática*, 28-38.

Vegas. (1998).

Yucra, T., & Bermedo, L. Z. (2020). Revista Científica Mundo de la Investigación y el Conocimiento, 166, 12–20.

Guevara, J. (2015). Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Perú: Magerit.

ANEXOS

Anexo A Aprobación de tema

Universidad Laica Eloy Alfaro de Manabí

Periodo 2024-2025(2) - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Estimad@
Docente y Estudiante
Uleam

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

Tema: AUDITORIA DE SEGURIDAD INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DE LABORATORIOS DE CÓMPUTOS DE LA CARRERA DE TI "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN".

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

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

Apellidos y nombres del tutor asginado: POZO HERNANDEZ CLARA GUADALUPE

Apellidos y nombres del estudiante: BASURTO MUÑOZ FERNANDA ELIZABETH

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2024-2025(2)

Anexo B Instrumento entrevista

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ — *Ingeniería en Tecnologías de la Información*

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ — *Ingeniería en Tecnologías de la Información*

Entrevista Dirigida A: Ing. Bladimir Mora Coordinador de las carreras de TI & Software.

OBJETIVO: Identificar posibles riesgos sobre la situación actual de los laboratorios de cómputos de las carreras de TI & Software en cuanto a seguridad Informática de los equipos.

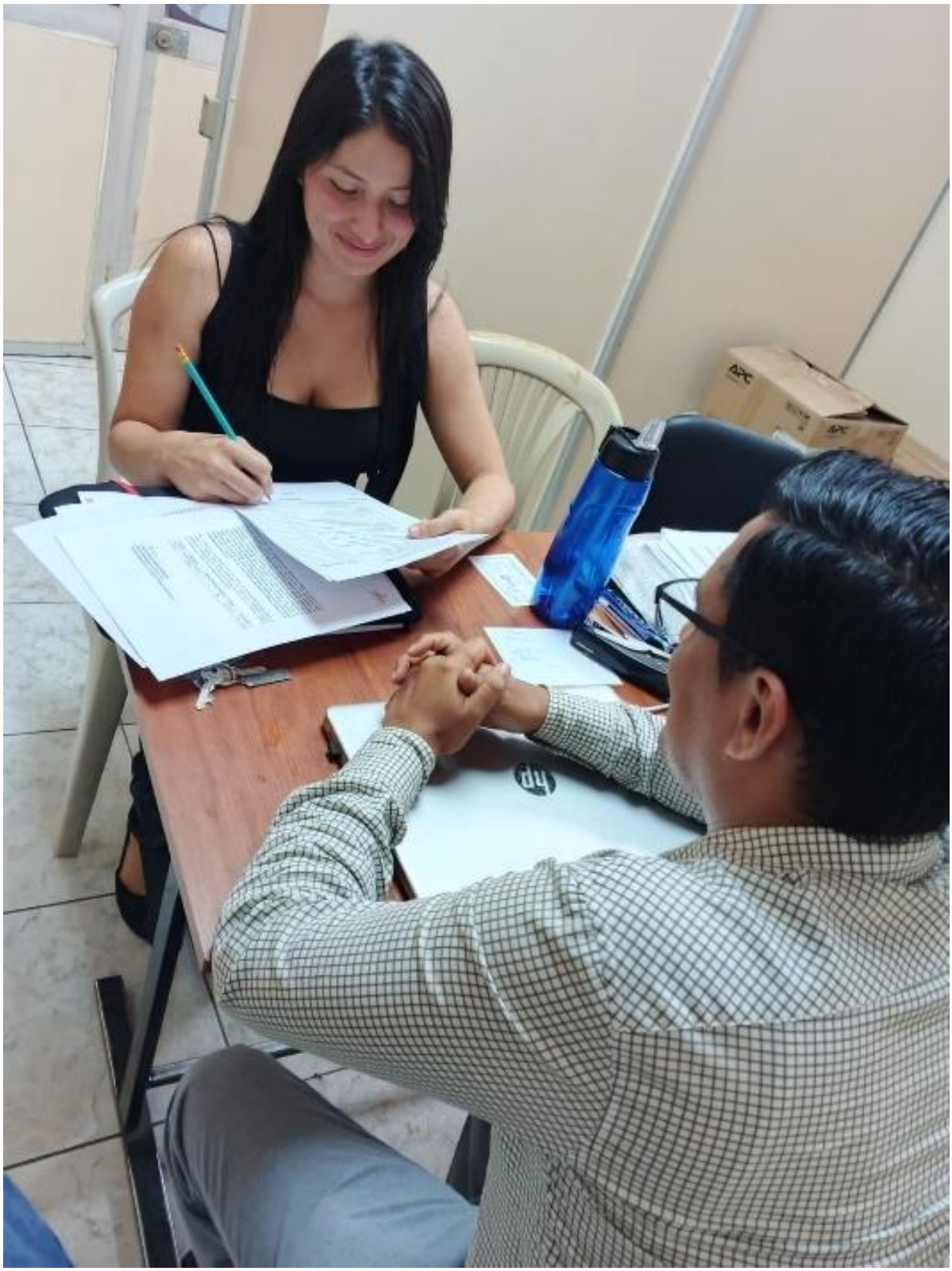
1. **¿Cómo evaluaría la seguridad física de los equipos en los laboratorios?**
2. **En su experiencia, ¿qué tipo de incidentes relacionados con la seguridad de los equipos han ocurrido en los laboratorios?**
3. **¿Qué opina sobre las medidas que se toman actualmente para prevenir el daño de los equipos?**
4. **¿Cree que los equipos del laboratorio están bien protegidos en cuanto a seguridad física?**
5. **¿Existen responsables designados para supervisar los laboratorios?**
6. **¿Cree que se toma medidas necesarias para evitar daños en los equipos?**
7. **¿Qué impacto cree que tendría un mejor control de acceso a los laboratorios en el uso de los equipos?**
8. **¿Considera que se realiza un mantenimiento adecuado de los equipos?**
9. **¿Ha observado alguna vez situaciones en las que los equipos no estén siendo utilizados de manera adecuada?**
10. **¿Considera que la falta de control de acceso afecta la disponibilidad de los equipos?**
11. **¿Qué medidas considera más efectivas para mejorar el seguimiento y control del uso de los equipos por parte de los estudiantes?**
12. **¿Qué opina sobre las medidas de seguridad perimetral, como cámaras en los laboratorios?**

Anexo C Instrumento encuesta

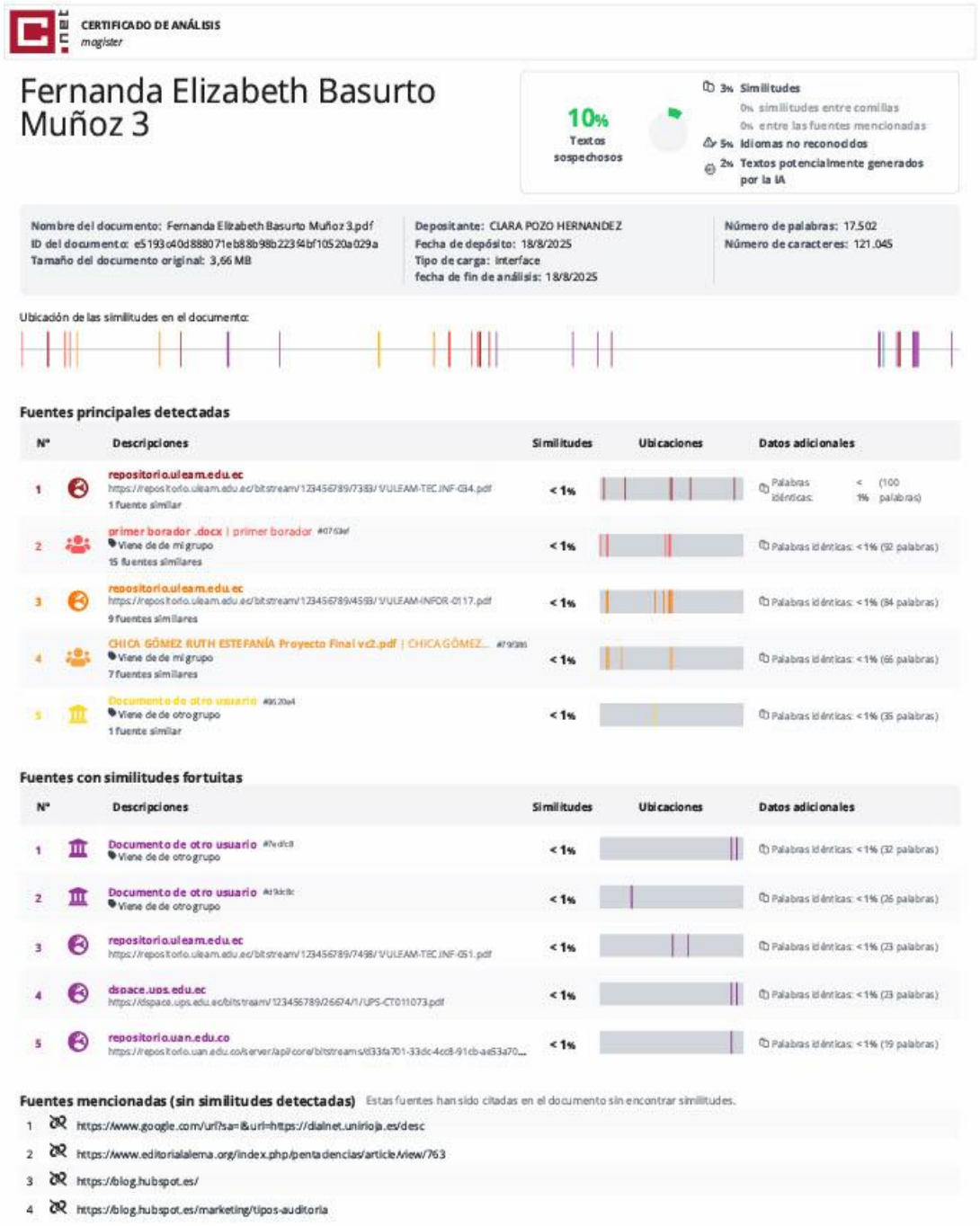
Laboratorio N°	**CUESTIONARIO DE IDENTIFICACION DE RIESGO**			**C1**
				Pag. 1 - 5
N°	**PREGUNTAS: ROBO**	**SI**	**NO**	**Observaciones**
1	¿Existen camara de seguridad instalada en los laboratorio?			
2	¿Las camaras de seguridad estan funcionando correctamente?			
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?			
4	¿Existen responsible de la seguridad de los laboratorios?			
5	¿Existen procedimientos para reportar un robo?			
6	¿Se han registrado incidentes previos de robo en los laboratorios?			
7	¿Los activos del laboratorio cuentan con medidas de protección física actualmente?			
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?			
9	¿Los equipos están identificados con códigos o etiquetas?			
10	¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?			
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta area?			
12	Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?			
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?			
14	¿Hay restricciones para la salida de equipos del laboratorio?			
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?			
16	¿Se verifica el estado y funcionamiento de los equipos físicos en los laboratorio?			
17	¿Existe un sistema de comunicación rápida para reportar incidentes?			
18	¿Los accesos principales están bajo vigilancia constante?			
19	¿Se cuenta con sistemas de alarma en los laboratorios?			
20	¿Los equipos están atados o asegurados físicamente?			
21	¿Se han registrado reportes de robo recientemente?			
22	¿Hay dispositivos de rastreo en los equipos?			
23	¿Los laboratorios tienen sensores de movimiento?			
24	¿Existen protocolos claros para la investigación de incidents?			
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?			

Realizado por:	**Observación:**
Fecha:	**Revisado por:**

Anexo D Fotografía 7



Anexo E Certificado de coincidencia académica



CERTIFICADO DE ANÁLISIS
magister

Fernanda Elizabeth Basurto Muñoz 3

10% Textos sospechosos

3% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
5% Idiomas no reconocidos
2% Textos potencialmente generados por la IA

Nombre del documento: Fernanda Elizabeth Basurto Muñoz 3.pdf
ID del documento: e5193c40d888071eb88b98b22354bf10520a029a
Tamaño del documento original: 3,66 MB

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 18/8/2025
Tipo de carga: interface
fecha de fin de análisis: 18/8/2025

Número de palabras: 17.502
Número de caracteres: 121.045

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/7389/1/ULEAM-TEC.INF-034.pdf 1 fuente similar	< 1%		Palabras idénticas: < 1% (100 palabras)
2	primer borador .docx | primer borador Viene de de mi grupo 15 fuentes similares	< 1%		Palabras idénticas: < 1% (52 palabras)
3	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/4593/1/ULEAM-INFOR-0117.pdf 9 fuentes similares	< 1%		Palabras idénticas: < 1% (34 palabras)
4	CHICA GÓMEZ RUTH ESTEFANÍA Proyecto Final v2.pdf | CHICA GÓMEZ... Viene de de mi grupo 7 fuentes similares	< 1%		Palabras idénticas: < 1% (66 palabras)
5	Documento de otro usuario Viene de de otro grupo 1 fuente similar	< 1%		Palabras idénticas: < 1% (35 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (32 palabras)
2	Documento de otro usuario Viene de de otro grupo	< 1%		Palabras idénticas: < 1% (26 palabras)
3	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/7498/1/ULEAM-TEC.INF-051.pdf	< 1%		Palabras idénticas: < 1% (23 palabras)
4	dspace.ups.edu.ec https://dspace.ups.edu.ec/bitstream/123456789/26674/1/UPS-CT011073.pdf	< 1%		Palabras idénticas: < 1% (23 palabras)
5	repositorio.uan.edu.co https://repositorio.uan.edu.co/server/api/core/bitstreams/d33fa701-33dc-4cc8-91cb-ae53a70...	< 1%		Palabras idénticas: < 1% (19 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.google.com/url?sa=i&url=https://dialnet.unirioja.es/desc
2 https://www.editorialalema.org/index.php/pentaciencias/article/view/763
3 https://blog.hubspot.es/
4 https://blog.hubspot.es/marketing/tipos-auditoria


Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ
MANUAL DE POLÍTLCAS DE SEGURIDAD DE BUENAS PRÁCTICAS PARA LOS LABORATORIOS DE CÓMPUTOS
Tecnologia De La Informacion – Uleam Extensión El Carmen
Presentado por:
Fernanda Basurto

ÍNDICE

INTRODUCCION

El presente manual tiene como objetivo establecer un conjunto de políticas y buenas prácticas orientadas a proteger la infraestructura tecnológica de los laboratorios de la carrera de las Carreras de TI & Software de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. La seguridad física y lógica es vital para garantizar la continuidad operativa, la protección de los activos y la seguridad.

En un entorno educativo donde la tecnología juega un papel central en el proceso de enseñanza-aprendizaje, resulta imprescindible contar con medidas preventivas y correctivas que minimicen el impacto de eventos que puedan comprometer la disponibilidad, integridad y confidencialidad de los recursos tecnológicos. Este documento se fundamenta en la metodología MAGERIT, permitiendo identificar, analizar y gestionar los riesgos asociados a los activos informáticos de los laboratorios.

Así mismo, se busca establecer lineamientos claros que orienten al personal docente, técnico y estudiantil en el correcto uso, mantenimiento y protección de los equipos, promoviendo una cultura de seguridad institucional que fortalezca la gestión educativa y administrativa de los entornos tecnológicos.

OBJETIVOS

Plantear procedimientos y medidas de seguridad que reduzcan riesgos en los laboratorios informáticos e inculcar el uso adecuado de los recursos tecnológicos

ALCANCE

Este manual se aplica a todos los laboratorios de informática de la carrera de TI y Software de la ULEAM, incluyendo el equipo de cómputo, periféricos, infraestructura de red, software institucional y a todo el personal que haga uso de estas instalaciones.

DEFINICIONES

1 LABORATORIOS DE COMPUTOS

1.1 Equipos De Computos

Los equipos de cómputo constituyen el principal recurso de los laboratorios informáticos. Cada unidad debe mantenerse en condiciones óptimas para su uso. Es necesario establecer buenas prácticas en cuanto al encendido, apagado, limpieza y mantenimiento preventivo.

- Cada equipo debe contar con un número de etiqueta visible.
- Los mantenimientos preventivos deben realizarse al menos una vez cada semestre.
- El acceso a los equipos debe estar autorizado por la persona encargada.

1.2 PERIFERICOS

Los periféricos complementan el uso del equipo principal en los laboratorios y son fundamentales para el desarrollo de prácticas académicas. Estos incluyen proyectores, teclados, ratones, pantallas y otros dispositivos externos conectados a los equipos de cómputo. Su uso debe estar sujeto a normas estrictas para garantizar su conservación y funcionamiento adecuado.

2 RESPONSABLES

- **Laboratorista:** Supervisión, mantenimiento, control de uso y reporte de fallas.
- **Docentes:** Control y supervisión del uso académico de los periféricos durante clases.
- **Estudiantes:** Uso adecuado notificación de daños o problemas, respeto a las normas de conservación.

3 POLITICAS DE SEGURIDAD

1. **Política de Control de Acceso Físico**
   - ❖ El ingreso a los laboratorios estará restringido únicamente a personal autorizado.
   - ❖ El personal técnico será responsable del control y supervisión de accesos fuera del horario académico.
   - ❖ Los laboratorios deben permanecer cerrados cuando no estén en uso.
   - ❖ Se llevará un registro de ingreso y salida del personal y usuarios externos atraves de monitoreo de videovigilancia.
   - ❖ No se permite el ingreso a usuarios sin acompañamiento del personal responsable.
2. **Política de Seguridad de Equipos**
   - ❖ No se permite el movimiento, apertura ni modificación de los equipos sin autorización.
   - ❖ Los usuarios deben manipular el hardware con cuidado; está prohibido el consumo de alimentos o bebidas cerca de los equipos.
   - ❖ Los equipos deben apagarse correctamente al finalizar su uso.
   - ❖ No se permite colocar objetos pesados sobre los equipos o monitores.
   - ❖ Se debe evitar el contacto directo con puertos o componentes internos sin conocimiento técnic

3. Política de Instalación y Uso de Software

- Solo descargar software autorizados.
- El uso de software será exclusivamente académico.
- Se debe usar software libre o educativo, siempre que cumpla con los fines del laboratorio.
- Prohibido descargar archivos ejecutables desde fuentes no confiables.
- Cualquier solicitud de nuevo software debe ser verificada.

4. Política de Prevención ante Malware

- No se permite el uso de dispositivos USB sin previa autorización y análisis antivirus.
- Todos los equipos deberán contar con un sistema antivirus activo y configurado para análisis automáticos diarios.
- Los sistemas operativos y programas deben mantenerse actualizados regularmente.
- Está prohibido acceder a sitios web de dudosa procedencia o que representen riesgos.
- Se proporcionarán guías prácticas y recomendaciones visibles sobre el uso seguro de los dispositivos.

5. Política de Uso Responsable

- Los usuarios deben mantener un comportamiento respetuoso y ordenado dentro del laboratorio.
- Está prohibido modificar la configuración de los equipos sin autorización.
- Se debe evitar cualquier actividad que genere ruido o distracción para otros usuarios.
- Las sillas, mesas y demás mobiliario deben ser usados de forma adecuada.
- Se prohíbe el uso de los equipos para actividades no académica.

6. Política de Responsabilidad del Usuario

- El usuario debe verificar que el equipo asignado esté en buen estado al iniciar su sesión.
- Cualquier incidente debe ser reportado inmediatamente al personal técnico.
- Los usuarios deben guardar su información en medios personales, ya que los equipos se reinician regularmente.
- Está prohibido cambiar contraseñas administrativas o restringir el acceso a otros usuarios.
- Al finalizar su uso, el usuario debe cerrar sesión y dejar su puesto limpio y ordenado.

4 CONTROLES PARA PRVENIR RIESGOS

RIESGO	DESCRIPCIÓN	PREVENCIÓN
Robo	Pérdida de activos debido al acceso no autorizado.	• Instalar cámara de seguridad • Implementar medidas de seguridad • Regular el control de acceso • Poner en practica los protocolos en caso de incidente.
Daño	Deterioro de equipos tecnológicos por mal uso, accidentes o falta de mantenimiento	• Llevar un registro de mantenimiento • Delegar a un responsables para esta áreas • Revision frecuentes a los equipos • Revision de área
Incendio	Daños a instalaciones por fuego o cortocircuito.	• Revision de extintores • Elaborar un plan de emergencias
Inundacion	Filtración de agua por techos o tuberías, afectando equipos.	• Realizar un plan de emergencia • Poner en protica las medidas existentes
Malware	Infección por software malicioso debido a malas prácticas.	• Tener en cuenta los archivos a instalarse

5 ANEXOS

Formato para llevar el registro de mantenimiento de los laboratorios

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

EXTENSIÓN EL CARMEN

TECNOLOGIA DE LA INFORMACIÓN

BITÁCORA DE MANTENIMIENTO PREVENTIVO A EQUIPO DE

CARRERA:	TECNOLOGÍA DE LA INFORMACIÓN
LABORATORIO:	COMPUTO 1
NÚMERO DE AULA:	201

DESCRIPCIÓN DEL EQUIPO	N.º de Inventario	Fecha de Inicio (Mantenimiento)	Fecha de Término (Mantenimiento)	Equipos en servicio (Sí/No)	Estado del Mantenimiento	Fecha estimada del próximo mantenimiento	Descripción general del mantenimiento realizado	Persona o empresa que realizó el mantenimiento	Supervisor (Nombre y Firma)

Revisón: _____ RESPONSABLE DE LABORATORIO: _____

Ilustración 1Formato de mantenimiento

Anexo G Cuestionarios llenos.

Laboratorio N° 1	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 1 - 5
N°	PREGUNTAS: ROBO	SI	NO	Observaciones
1	¿Existen camara de seguridad instalada en los laboratorio?	X		
2	¿Las camaras de seguridad estan funcionando correctamente?	X		
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?		X	
4	¿Existen responsible de la seguridad de los laboratorios?	X		
5	¿Existen procedimientos para reportar un robo?	X		
6	¿Se han registrado incidentes previos de robo en los laboratorios?		X	
7	¿Los activos del laboratorio cuentan con medidas de protección física actualmente?		X	
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?		X	
9	¿Los equipos están identificados con códigos o etiquetas?		X	
10	¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?		X	
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta area?	X		
12	Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?		X	
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?		X	
14	¿Hay restricciones para la salida de equipos del laboratorio?	X		
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?	X		
16	¿Se verifica el estado y funcionamiento de los equipos físicos en los laboratorio?	X		
17	¿Existe un sistema de comunicación rápida para reportar incidentes?		X	
18	¿Los accesos principales están bajo vigilancia constante?		X	
19	¿Se cuenta con sistemas de alarma en los laboratorios?		X	
20	¿Los equipos están atados o asegurados físicamente?		X	
21	¿Se han registrado reportes de robo recientemente?		X	
22	¿Hay dispositivos de rastreo en los equipos?		X	
23	¿Los laboratorios tienen sensores de movimiento?		X	
24	¿Existen protocolos claros para la investigación de incidents?		X	
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?	X		
Realizado por: Fernanda Elizabeth Basurto Muñoz		**Observación:**		
Fecha: 30/05/2025		**Revisado por:** Ing. Clara Guadalupe Poo Hernández		

Laboratorio N° 1	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 2 - 5
N°	PREGUNTAS: DAÑO	SI	NO	Observaciones
1	¿Las mesas y superficies de trabajo son adecuadas para los equipos?	X		
2	¿Se han reportado daños por caídas o golpes?		X	
3	¿Los teclados, monitores y mouse presentan signos de mal uso?	X		
4	¿Se realizan inspecciones para detectar desgaste o fallas en los equipos?	X		
5	¿Los cables y conexiones están organizados adecuadamente?	X		
6	¿Se cuenta con protección contra sobrecarga eléctrica?		X	
7	¿Los equipos de los laboratorio se utilizan siguiendo las medidas de seguridad física para prevenir daños	X		
8	¿Existen registros de mantenimiento preventivo de los equipos?		X	
9	¿Hay señales visibles de maltrato físico en los equipos?		X	
10	¿Los equipos están expuestos a humedad o líquidos?		X	
11	¿Los equipos tienen ventilación suficiente para evitar sobrecalentamientos?	X		
12	¿Se han identificado equipos con fallas recurrentes?	X		
13	Se han implementado procedimientos para reportar daños?	X		
14	¿Los equipos son apagados correctamente después de su uso?		X	
15	¿Se han reportado incidentes debido al uso inadecuado de los dispositivos en el laboratorio?		X	
16	¿Se han tomado medidas para reducir el polvo y otras amenazas ambientales?		X	
17	¿Se da mantenimiento preventivo periódico a los equipos?	X		
18	¿Los usuarios tienen normas claras sobre el cuidado de los dispositivos?		X	
19	¿Las conexiones eléctricas son revisadas regularmente?		X	
20	Se han encontrado problemas en la estructura del laboratorio?	X		
21	¿El laboratorio tiene cableado estructurado?	X		
22	¿Se controla la temperatura y ventilación del laboratorio?	X		
23	¿Se permite el ingreso de alimentos o bebidas?		X	
24	¿Hay un responsable designado para el cuidado del equipo?		X	
25	¿Se inspeccionan los equipos al final de cada jornada?		X	

Realizado por:	Observación:
Fernanda Elizabeth Basurto Muñoz	
Fecha: 30/05/2025	**Revisado por:** Ing. Clara Guadalupe Pozo Hernández

Laboratorio N° 1	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 3 - 5
N°	PREGUNTAS: INCENDIO	SI	NO	Observaciones
1	¿El laboratorio cuenta con detectores de humo?		X	
2	¿Se han instalado extinguidores adecuados para equipos electrónicos?		X	
3	¿Existe señalización clara de rutas de evacuación?	X		
4	¿Se han realizado simulacros de incendio en el laboratorio?		X	
5	¿Las conexiones eléctricas son seguras?	X		
6	¿Se han revisado los sistemas eléctricos para detectar riesgos?		X	
7	Se realizan inspecciones técnicas para detectar fallas en el sistema eléctrico?		X	
8	¿Las tomas de corriente están protegidas contra sobrecargas?	X		
9	¿Se han registrado incidentes previos relacionados con incendios?		X	
10	¿Las instalaciones eléctricas están en buen estado?	X		No existe inspecciones pictografiables
11	¿Las rutas de evacuación están despejadas y accesibles?	X		
12	¿Se realizan inspecciones periódicas para evaluar riesgos de incendio?		X	
13	¿¿El laboratorio cuenta con extintores?		X	
14	¿Existe una organización estructurada para la disposición de cada equipo en el laboratorio?	X		
15	¿Existe señalización visible que identifique cada equipo	X		
16	¿Existen sistemas de ventilación para disipar calor acumulado?	X		
17	¿La altura de los cables cumple con los estándares de seguridad física?	X		
18	¿Se almacenan productos inflamables cerca de los equipos?		X	
19	¿Se revisa el estado de los dispositivos de protección eléctrica?		X	
20	¿Hay un plan de emergencia en caso de incendio?		X	
21	¿Se verifica el vencimiento de los extintores?		X	
22	¿Se realiza limpieza frecuente de polvo y residuos que puedan ser inflamables?	X		
23	¿El techo y paredes del laboratorio están hechos de materiales resistentes al fuego?		X	
24	¿Existe un responsable designado para la revisión periódica del equipo contra incendios?		X	
25	¿Los equipos que generan calor como routers o servidores tienen buena disipación?	X		

Realizado por: Fernanda Elizabeth Basurto Muñoz	Observación:
Fecha: 30/05/2025	Revisado por: Ing. Clara Guadalupe Rojo Hernández

Laboratorio N° 1	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 4 - 5		
N°	PREGUNTAS:INUNDACIONES	SI	NO	Observaciones
1	¿Existen registros de inundaciones previas en el área donde se ubica el laboratorio?		X	
2	¿El laboratorio está ubicado en una zona con riesgo de acumulación de agua por lluvias intensas?		X	
3	¿Se han identificado posibles puntos de filtración de agua dentro del laboratorio?		X	
4	¿Existe un sistema de drenaje adecuado en la infraestructura del edificio?	X		
5	¿Las puertas y ventanas cuentan con sellado contra filtraciones?		X	
6	¿Hay equipos electrónicos ubicados en áreas bajas susceptibles a inundaciones?		X	
7	¿Existen sistemas de alerta para detectar acumulación de agua?		X	
8	¿Los cables eléctricos están protegidos contra humedad y exposición al agua?	X		
9	¿Se cuenta con un protocolo de emergencia en caso de inundación?		X	
10	¿Los equipos están elevados em los laboratorios?		X	
11	¿Las conexiones eléctricas tienen protección contra cortocircuitos por humedad?		X	
12	¿Se han realizado simulacros de emergencia en caso de inundación?		X	
13	¿Se han identificado vías seguras de evacuación en caso de inundación?		X	
14	¿Los documentos físicos importantes están almacenados en áreas protegidas?		X	
15	¿Los servidores y equipos críticos tienen protección contra humedad?		X	
16	¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?		X	
17	¿Se revisa periódicamente el estado de techos y estructuras para prevenir filtraciones?		X	
18	¿Las áreas de almacenamiento están diseñadas para minimizar riesgos de inundación?	X		
19	¿Se han tomado medidas estructurales para evitar acumulación de agua en el laboratorio?		X	
20	¿Los equipos sensibles tienen cubiertas protectoras contra agua?		X	
21	¿Se han implementado protocolos de inspección después de lluvias fuertes?		X	
22	¿Los sistemas eléctricos tienen desconexión automática en caso de contacto con agua?		X	
23	¿Los equipos electrónicos tienen garantías contra daños por humedad?		X	
24	¿Se han identificado patrones climáticos que podrían aumentar el riesgo de inundación?		X	
25	¿Se han realizado auditorías previas que recomienden mejoras en la prevención de inundaciones?		X	

Realizado por: Fernanda Elizabeth Basurto Haïze	Observación:
Fecha: 30/05/2025	Revisado por: Ing. Clara Guadalupe Poo Hernández

Laboratorio Nº 2	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 1 - 5
Nº	PREGUNTAS: ROBO	SI	NO	Observaciones
1	¿Existen camara de seguridad instalada en los laboratorio?	X		
2	¿Las camaras de seguridad estan funcionando correctamente?		X	
3	¿Se dispone de cerraduras de alta seguridad en las puertas de los Laboratorios?		X	
4	¿Existen responsible de la seguridad de los laboratorios?	X		
5	¿Existen procedimientos para reportar un robo?	X		
6	¿Se han registrado incidentes previos de robo en los laboratorios?	X		
7	¿Los activos del laboratorio cuentan con medidas de protección física actualmente?		X	
8	¿Existe un control de acceso restringido para el ingreso a los laboratorios?		X	
9	¿Los equipos están identificados con códigos o etiquetas?	X		
10	¿Se mantiene un registro actualizado de las personas que acceden a los laboratorios?		X	
11	¿Existe un sistema de registro actualizado sobre el ingreso a esta area?	X		
12	Los estudiantes apagan y almacenan correctamente los equipos al finalizar sus actividades en el laboratorio?		X	
13	¿Los estudiantes externos firman un registro antes de ingresar a los laboratorios?		X	
14	¿Hay restricciones para la salida de equipos del laboratorio?	X		
15	¿Existen mecanismos para monitorear la actividad dentro del laboratorio?		X	
16	¿Se verifica el estado y funcionamiento de los equipos físicos en los laboratorio?	X		
17	¿Existe un sistema de comunicación rápida para reportar incidentes?		X	
18	¿Los accesos principales están bajo vigilancia constante?		X	
19	¿Se cuenta con sistemas de alarma en los laboratorios?		X	
20	¿Los equipos están atados o asegurados físicamente?		X	
21	¿Se han registrado reportes de robo recientemente?		X	
22	¿Hay dispositivos de rastreo en los equipos?		X	
23	¿Los laboratorios tienen sensores de movimiento?		X	
24	¿Existen protocolos claros para la investigación de incidents?		X	
25	¿Se aplican sanciones o medidas disciplinarias en casos de hurto?		X	

Realizado por:	Observación:
Fernanda Elizabeth Basurto Muñoz	
Fecha: 30/05/2025	**Revisado por:** Ing. Clara Guadalupe Paz Hernández

Laboratorio Nº 2	CUESTIONARIO DE IDENTIFICACION DE RIESGO	C1 Pag. 2 - 5		
Nº	PREGUNTAS: DAÑO	SI	NO	Observaciones
1	¿Las mesas y superficies de trabajo son adecuadas para los equipos?	X		
2	¿Se han reportado daños por caídas o golpes?		X	
3	¿Los teclados, monitores y mouse presentan signos de mal uso?		X	
4	¿Se realizan inspecciones para detectar desgaste o fallas en los equipos?	X		
5	¿Los cables y conexiones están organizados adecuadamente?	X	\	
6	¿Se cuenta con protección contra sobrecarga eléctrica?		X	
7	¿Los equipos de los laboratorio se utilizan siguiendo las medidas de seguridad física para prevenir daños	X		
8	¿Existen registros de mantenimiento preventivo de los equipos?		X	
9	¿Hay señales visibles de maltrato físico en los equipos?		X	
10	¿Los equipos están expuestos a humedad o líquidos?	X		
11	¿Los equipos tienen ventilación suficiente para evitar sobrecalentamientos?	X		
12	¿Se han identificado equipos con fallas recurrentes?	X		
13	Se han implementado procedimientos para reportar daños?	X		
14	¿Los equipos son apagados correctamente después de su uso?		X	
15	¿Se han reportado incidentes debido al uso inadecuado de los dispositivos en el laboratorio?		X	
16	¿Se han tomado medidas para reducir el polvo y otras amenazas ambientales?		X	
17	¿Se da mantenimiento preventivo periódico a los equipos?	X	\	
18	¿Los usuarios tienen normas claras sobre el cuidado de los dispositivos?		X	
19	¿Las conexiones eléctricas son revisadas regularmente?	\	X	
20	Se han encontrado problemas en la estructura del laboratorio?		X	
21	¿El laboratorio tiene cableado estructurado?	X		
22	¿Se controla la temperatura y ventilación del laboratorio?	X		
23	¿Se permite el ingreso de alimentos o bebidas?		X	
24	¿Hay un responsable designado para el cuidado del equipo?		X	
25	¿Se inspeccionan los equipos al final de cada jornada?		X	

Realizado por:	Observación:
Fernanda Elizabeth Basurto Muñoz	
Fecha: 30/05/2025	**Revisado por:** Ing. Clara Guadalupe Pazo Hernández

Laboratorio N° 2	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 3 - 5
N°	PREGUNTAS: INCENDIO	SI	NO	Observaciones
1	¿El laboratorio cuenta con detectores de humo?		X	
2	¿Se han instalado extinguidores adecuados para equipos electrónicos?		X	
3	¿Existe señalización clara de rutas de evacuación?		X	
4	¿Se han realizado simulacros de incendio en el laboratorio?		X	
5	¿Las conexiones eléctricas son seguras?	X		
6	¿Se han revisado los sistemas eléctricos para detectar riesgos?		X	
7	Se realizan inspecciones técnicas para detectar fallas en el sistema eléctrico?		X	
8	¿Las tomas de corriente están protegidas contra sobrecargas?	X		
9	¿Se han registrado incidentes previos relacionados con incendios?		X	
10	¿Las instalaciones eléctricas están en buen estado?	X		
11	¿Las rutas de evacuación están despejadas y accesibles?	X		
12	¿Se realizan inspecciones periódicas para evaluar riesgos de incendio?		X	
13	¿¿El laboratorio cuenta con extintores?	X		
14	¿Existe una organización estructurada para la disposición de cada equipo en el laboratorio?	X		
15	¿Existe señalización visible que identifique cada equipo		X	
16	¿Existen sistemas de ventilación para disipar calor acumulado?	X		
17	¿La altura de los cables cumple con los estándares de seguridad física?	X		
18	¿Se almacenan productos inflamables cerca de los equipos?		X	
19	¿Se revisa el estado de los dispositivos de protección eléctrica?		X	
20	¿Hay un plan de emergencia en caso de incendio?		X	
21	¿Se verifica el vencimiento de los extintores?		X	
22	¿Se realiza limpieza frecuente de polvo y residuos que puedan ser inflamables?	X		
23	¿El techo y paredes del laboratorio están hechos de materiales resistentes al fuego?		X	
24	¿Existe un responsable designado para la revisión periódica del equipo contra incendios?		X	
25	¿Los equipos que generan calor como routers o servidores tienen buena disipación?	X		

Realizado por: Fernanda Elizabeth Basurto Muñoz	**Observación:**
Fecha: 30/05/2025	**Revisado por:** Ing. Clara Guadalupe Pozo Hernández

Laboratorio N° 2	CUESTIONARIO DE IDENTIFICACION DE RIESGO			C1 Pag. 4 - 5
N°	**PREGUNTAS:INUNDACIONES**	**SI**	**NO**	**Observaciones**
1	¿Existen registros de inundaciones previas en el área donde se ubica el laboratorio?		X	
2	¿El laboratorio está ubicado en una zona con riesgo de acumulación de agua por lluvias intensas?		X	
3	¿Se han identificado posibles puntos de filtración de agua dentro del laboratorio?	X		
4	¿Existe un sistema de drenaje adecuado en la infraestructura del edificio?		X	
5	¿Las puertas y ventanas cuentan con sellado contra filtraciones?		X	
6	¿Hay equipos electrónicos ubicados en áreas bajas susceptibles a inundaciones?		X	
7	¿Existen sistemas de alerta para detectar acumulación de agua?		X	
8	¿Los cables eléctricos están protegidos contra humedad y exposición al agua?	X		
9	¿Se cuenta con un protocolo de emergencia en caso de inundación?		X	
10	¿Los equipos están elevados em los laboratorios?	X		
11	¿Las conexiones eléctricas tienen protección contra cortocircuitos por humedad?		X	
12	¿Se han realizado simulacros de emergencia en caso de inundación?		X	
13	¿Se han identificado vías seguras de evacuación en caso de inundación?		X	
14	¿Los documentos físicos importantes están almacenados en áreas protegidas?		X	
15	¿Los servidores y equipos críticos tienen protección contra humedad?		X	
16	¿Existen medidas físicas para prevenir ataques de ransomware en los equipos del laboratorio?		X	
17	¿Se revisa periódicamente el estado de techos y estructuras para prevenir filtraciones?		X	
18	¿Las áreas de almacenamiento están diseñadas para minimizar riesgos de inundación?	X		
19	¿Se han tomado medidas estructurales para evitar acumulación de agua en el laboratorio?		X	
20	¿Los equipos sensibles tienen cubiertas protectoras contra agua?		X	
21	¿Se han implementado protocolos de inspección después de lluvias fuertes?		X	
22	¿Los sistemas eléctricos tienen desconexión automática en caso de contacto con agua?		X	
23	¿Los equipos electrónicos tienen garantías contra daños por humedad?		X	
24	¿Se han identificado patrones climáticos que podrían aumentar el riesgo de inundación?		X	
25	¿Se han realizado auditorías previas que recomienden mejoras en la prevención de inundaciones?		X	

Realizado por: Fernanda Elizabeth Basurto Muñoz	**Observación:**
Fecha: 30/05/2025	**Revisado por:** Ing. Clara Guadalupe Pozo Hernández

GLOSARIO

Auditoría: Proceso sistemático para evaluar y verificar el cumplimiento de normas.

Infraestructura Tecnológica: Conjunto de hardware, software y redes

Vulnerabilidad: Debilidad en un sistema que puede ser explotada.

Riesgo: Probabilidad de que una amenaza cause un daño.

Integridad: Asegurar que los datos no han sido alterados.

COBIT: Marco de trabajo para la gestión y gobierno de TI.

ISO 27001: Norma para sistemas de gestión de seguridad de la información.

Amenaza: Posible evento que podría causar daño.

Controles de Seguridad: Medidas para mitigar riesgos.

Monitoreo: Supervisión constante de un sistema.

Plan de Contingencia: Estrategia para responder a incidentes.

Políticas de Seguridad: Reglas para proteger los recursos.

Metodología: Conjunto de pasos para realizar una investigación.

TI: Abreviatura de Tecnología de la Información.

Auditoría Física: Evaluación de la seguridad del hardware e instalaciones.

Firewall: Dispositivo que filtra el tráfico de red.

Antivirus: Software para proteger contra programas maliciosos.

Backup: Copia de seguridad de la información.

Cifrado: Proceso de codificación de datos para protegerlos.

Autenticación: Proceso de verificar la identidad de un usuario.

Autorización: Conceder permisos para acceder a recursos.

VPN: Red privada virtual.

IDS (Sistema de Detección de Intrusos): Herramienta para detectar actividad sospechosa.

Phishing: Ataque para obtener información confidencial.

Malware: Software malicioso.

Ransomware: Ataque que bloquea el acceso a datos.

Parche de Seguridad: Actualización para corregir vulnerabilidades.

Análisis de Riesgos: Proceso para identificar y evaluar riesgos.

Auditor: Persona que realiza una auditoría.

Deterioro: Daño físico de los equipos.

Activos: Recursos valiosos de la organización.

Redes: Infraestructura que conecta equipos.

Servidor: Computadora que provee servicios a otros equipos.

Protocolo: Conjunto de reglas para la comunicación.

Gestión de Incidentes: Proceso para manejar y resolver problemas de seguridad.

Análisis Forense: Investigación de un incidente de seguridad.

Ciberseguridad: Protección de sistemas y redes en el ciberespacio.

Dispositivo Periférico: Equipo auxiliar conectado a la computadora.

Sistemas Operativos: Software principal de una computadora (ej: Windows).

Control de Acceso: Mecanismo para restringir el acceso a recursos.

Génesis: Origen o inicio de un problema.

Mitigación: Acciones para reducir el impacto de un riesgo.