*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**

# AUDITORIA INFORMÁTICA A LA SEGURIDAD FÍSICA DEL LABORATORIO MULTIMEDIA DE IDIOMAS UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EL CARMEN (ULEAM)

CASTRO ALAVA JULEXY JAMILETH

**AUTORA:**

A.S. MINAYA MACIAS RENELMO WLADIMIR, MG.

**TUTOR**

EL CARMEN, FEBRER0 2026

# Certificación del director de trabajo de graduación

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

## CERTIFICACIÓN

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

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante Castro Alava Julexy Jamileth, legalmente matriculada en la carrera de Tecnologías de la Información período académico 2025(1)-2025(2), cumpliendo el total de 384 horas, cuyo tema del proyecto es "Auditoria Informática a la seguridad física del Laboratorio Multimedia de Idiomas Universidad Laica Eloy Alfaro De Manabí El Carmen (ULEAM)".

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, 02 de Enero de 2026.

Lo certifico,

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

# Tribunal de sustentación

**Universidad Laica Eloy Alfaro de Manabí**

**Extensión El Carmen**

**Carrera de Ingeniería en Tecnologías de la Información**

**TRIBUNAL DE SUSTENTACIÓN**

**Título del Trabajo de Titulación:**
Auditoria Informática a la seguridad física del Laboratorio Multimedia de Idiomas Universidad Laica Eloy Alfaro De Manabí El Carmen (ULEAM)

**Modalidad:**
Proyector Integrador

**Autor:**
Castro Alava Julexy Jamileth

**Tutor:**
A.S. Minaya Macias Renelmo Wladimir, Mg

**Tribunal de Sustentación:**

- **Presidente:** Ing. Reascos Pinchao Raúl Saed
- **Miembro:** Ing. Pozo Hernández Clara Guadalupe
- **Miembro:** Ing. Mendoza Villamar Roció Alexandra

**Fecha de Sustentación:** 23 Febrero del 2026

## Declaración expresa de autoría

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

# DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: AUDITORIA INFORMÁTICA A LA SEGURIDAD FÍSICA DEL LABORATORIO MULTIMEDIA DE IDIOMAS UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EL CARMEN (ULEAM), corresponde exclusivamente a: CASTRO ALAVA JULEXY JAMILETH con CI. 092903055-9, y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Julexy Castro

**Castro Alava Julexy Jamileth**

**C.I. 092903055-9**

## Dedicatoria

*A mis padres Darwin Castro y Cecibel Alava por siempre apoyarme, cuidarme y acompañarme a lo largo de mi vida estudiantil y personal, gracias por confiar y creer en mí.*

*"Porque, como dijo Akio Furukawa: ´ ¡El sueño de un hijo, es el sueño de sus padres! ¡Si lo cumples, se cumplirá para nosotros! ¡Nuestro sueño es verte cumplir el tuyo! ´".*

***Jamí.***

# Agradecimiento

Este agradecimiento va dirigido a todas aquellas personas que han sido fundamental en la realización y culminación de este proyecto.

Agradezco, a Dios, por darme la fuerza, sabiduría y resistencia para la culminación de esta meta.

A mis padres por nunca abandonarme, apoyarme y aconsejarme constantemente; a mis amigos con los que he compartido aprendizaje y conocimientos.

A los libros, música y anime que me han acompañado a lo largo de mi vida, convirtiéndose en mi refugio y pequeño escape a la realidad. Como dijo Koro-sensei “El estudio no se trata de memorizar, sino de aprender a pensar”.

# Índice de contenidos

# Índice tablas

# Índice de figuras

# Índice de anexos

# Resumen

El presente trabajo de titulación tuvo como objetivo principal realizar una auditoría informática dirigida a la seguridad física del Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. El problema identificado radica en la alta vulnerabilidad de la infraestructura física del laboratorio, caracterizada por la falta en el control de acceso, ausencia de un sistema de vigilancia, además de contar con equipos tecnológicos obsoletos que ya han cumplido su vida útil y riesgos ambientales como filtraciones y falta de mantenimiento. Para el diagnóstico, se empleó una metodología de investigación descriptiva y exploratoria con un enfoque cuantitativo y analítico-sintético. Para ello se aplicaron instrumentos como encuestas a estudiantes, entrevista al coordinador y cuestionarios técnicos basados en los estándares ISO 27001, ISO 27002. Como respuesta a la problemática, se plantea una propuesta de un Plan de Seguridad Física bajo el ciclo de mejora continua (PDCA). Esta incluye la implementación de controles preventivos y correctivos, tales como la gestión de accesos, protección eléctrica, señalética de seguridad, inventarios activos y el uso de protocolos y políticas de seguridad para mitigar riesgos y asegurar la continuidad académica.



**Palabras Claves**: Auditoria, ISO y PDCA.

# Abstract

The main objective of this thesis was to conduct an IT audit focused on the physical security of the Multimedia Language Laboratory at the Eloy Alfaro Lay University of Manabí, El Carmen Extension. The identified problem lies in the high vulnerability of the laboratory's physical infrastructure, characterized by a lack of access control, the absence of a surveillance system, and the use of obsolete technological equipment that has reached the end of its useful life, as well as environmental risks such as leaks and lack of maintenance. For the diagnosis, a descriptive and exploratory research methodology with a quantitative and analytical-synthetic approach was employed. Instruments such as student surveys, an interview with the coordinator, and technical questionnaires based on the ISO 27001 and ISO 27002 standards. As a response to the problem, a Physical Security Plan is proposed, based on the continuous improvement cycle (PDCA). This includes the implementation of preventive and corrective controls, such as the management of accessories, electrical protection, safety signage, active inventories, and the use of security protocols and policies to mitigate risks and ensure academic continuity.



**Keywords:** Audit, ISO and PDCA.

# Capitulo I

## 1.1 Introducción

Actualmente, las instituciones de educación superior han dado mayor importancia la seguridad de la información y la protección de los activos tecnológicos debido al uso constantes de herramientas informáticas en las actividades administrativas, dentro de este contexto, la seguridad física de los laboratorios resulta fundamental, ya que permite garantizar la integridad, disponibilidad y continuidad de los equipos y servicios tecnológicos, además de ofrecer un entorno que respalden el proceso de enseñanza-aprendizaje cuide la salud de los estudiantes.

El laboratorio multimedia es un área indispensable para el desarrollo de actividades académicas; sin embargo, su nivel actual de seguridad física presenta debilidades que lo hacen vulnerables como robos, daños en los equipos, problemas en la infraestructura y accesos no autorizados, generando impactos negativos en el desarrollo de las académicas, estas vulnerabilidades demuestran la necesidad de llevar a cabo una evaluación sistemática de la seguridad física y establecer medidas que permitan prevenir y reducir los riesgos existentes a la mitigación de riesgos existentes.

Como medida de regulación ante la problemática existente, se planteó la implementación de una auditoría informática con base en el estándar ISO 27002, esta herramienta permite identificar, analizar y evaluar los riesgos que están afectando al laboratorio. Al ser un estándar proporciona lineamientos para llevar a cabo buenas prácticas como: llevar el control de seguridad, detectar vulnerabilidades, mejorar gestión de activos.

Este estudio se llevó a cabo haciendo uso de la metodología PDCA e implementando instrumentos de recolección de datos, tales como entrevista, que se le realizó al personal responsable del laboratorio y por otro lado las encuestas que fueron dirigidas a los estudiantes matriculados a la materia de inglés, además también se hizo uso de cuestionarios estructurados. Todas estas herramientas permitieron obtener datos reales sobre las condiciones actuales de seguridad, políticas y el nivel de conocimiento del personal sobre seguridad.

De esta forma, el estudio busca contribuir a la mejora de la gestión de la seguridad, reducir la ocurrencia de incidentes y fortalecer la cultura de protección dentro de la institución.

## 1.2 Presentación del tema

La "AUDITORÍA INFORMÁTICA PARA LA SEGURIDAD FÍSICA EN EL LABORATORIO MULTIMEDIA DE IDIOMAS DE LA ULEAM, EXTENSIÓN EL CARMEN", se enfoca en identificar, evaluar y mitigar los riesgos asociados con la protección de los recursos tecnológicos, infraestructura y equipos físicos. Este proceso incluye el análisis de vulnerabilidades en las instalaciones físicas, el control de accesos, la protección de equipos tecnológicos, y la implementación de medidas de seguridad adecuadas para prevenir daños, pérdidas o interrupciones en el servicio.

## 1.3 Ubicación y contextualización de la problemática

La Universidad Laica Eloy Alfaro de Manabí, fue creada en el año 1985 por el congreso de aquella época, su matriz o central se encuentra ubicada en la ciudad de Manta. La ULEAM– Extensión El Carmen es una universidad pública la cual se encuentra ubicada en el canto El Carmen provincia de Manabí, esta institución educativa cuenta en la actualidad

con 11 carreras en áreas como ingeniería, salud, agropecuaria, educación y contabilidad. Esta institución educativa se ha caracterizado por formar profesionales competentes y emprendedores.

La universidad cuenta con cuatro laboratorios de los cuatro tres están ubicados y asignados a la carrera de TI (Tecnología de la Información) y Software, mientras que el otro se encuentra designado a la facultad de English, específicamente a la opción presencial llamada English Proficiency. Este laboratorio cuenta con 56 consolas en total, la cuales están distribuidas de las siguientes maneras: 6 escritorios con cinto maquinas o consolas en cada uno y 5 escritorio con cuatro máquinas o consolas en cada uno, y la principal que se encuentra en el escritorio del docente.

## 1.4 Planteamiento del problema

### 1.4.1 Problematización

El Laboratorio de English en la actualidad cuenta con un papel importante en la formación académica de los estudiantes, especialmente ya que ayuda a cumplir con el requisito de dominio del B1 “Este es un nivel intermedio según el Marco Común Europeo de Referencia para las Lenguas (MCER). En este nivel, los alumnos son capaces de comunicarse en situaciones cotidianas, entender textos y conversaciones sencillas, y expresar opiniones básicas” (Inglés, 2014) . El cual es un requerimiento importante al momento de titularse.

Sin embargo, su seguridad física enfrenta múltiples amenazas que podrían interrumpir las operaciones de estudio en dicho laboratorio. Entre los principales problemas identificamos el acceso no autorizado, equipos tecnológicos que no han recibido ningún mantenimiento y la infraestructura física dañada del laboratorio, gracias a esto se ha aumentado los errores y defectos técnicos en el personal docente y los estudiantes.

### 1.4.2 Génesis del problema

El génesis del problema radica en la vulnerabilidad que presenta la infraestructura debido a su falta de mantenimiento, este se ve afectado ante eventos como, daños mediante polvo en el sistema operativo, daños hechos por aves e inundaciones. También en el aspecto de factores institucionales el aumento en el registro de los estudiantes ha llevado a una mayor demanda de recursos tecnológicos que pueden conducir a una sobrecarga en los sistemas y aumentar los ataques cibernéticos o la probabilidad de formación de virus.

La falta de infraestructura inadecuada para controlar el crecimiento de estos usuarios también aumenta el riesgo de amenazas informáticas. Juntos, estos factores se encuentran en una situación en la que la seguridad física de los equipos y la infraestructura de laboratorio es mala, lo que amenaza el logro de los objetivos académicos y la capacitación de idiomas adecuada.

### 1.4.3 Estado actual del problema

En la actualidad el laboratorio es funcional, a diferencia de sus equipos, los cuales en la actualidad no funcionan. Debido a esto los estudiantes hacen uso del Laboratorio 1 o Laboratorio 2 del área de TI, para realizar los exámenes o test de ubicación, lo cual suele generar controversia ya que chocan con horas de clases, debido a esto se ha generado un plan para tomar dichas pruebas una vez al mes. Pero aun así no se logra satisfacer la demanda estudiantil.

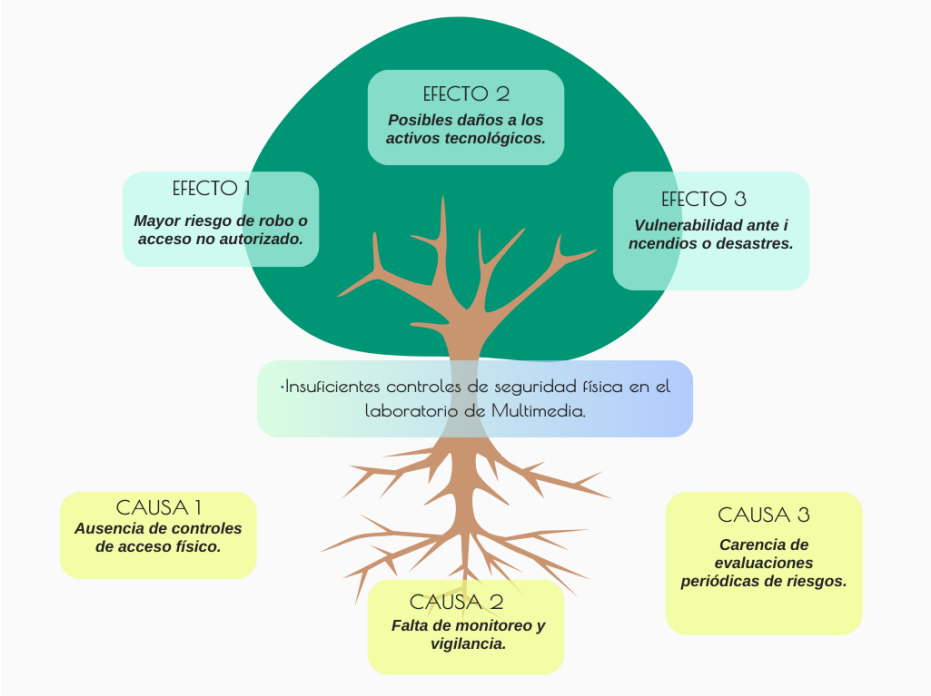
El laboratorio 2 cuenta con 20 computadoras en total, las cuales en la actualidad están en un buen estado de funcionamiento. El laboratorio no tiene vigilancias constantes, a pesar de tener una cámara de seguridad, los días de exámenes son muchos los estudiantes que acuden. Sumándole a ellos también que no todos los docentes pueden ayudar a vigilar ya que también tienen horas laborables se podría decir que no es seguro, y tampoco tan

productivo para los chicos ya que solo es un a hora que se designan para realizar las pruebas de ubicación en English Proficiency llegando así a que varios chicos se queden sin tomar esa materia, por falta de espacio y máquinas.

## 1.5 Diagrama causa – efecto del problema

**Figura 1**

*Árbol de decisión de Causas y Efectos.*



## 1.6 Objetivos

### 1.6.1 Objetivo general

Llevar a cabo una auditoria informática dirigida a la seguridad física del laboratorio multimedia de idiomas en la ULEAM Ext. El Carmen.

### 1.6.2 Objetivos específicos

- Examinar los elementos de riesgo que vulneran la seguridad física del laboratorio.
- Desarrollar un marco contextual teórico del estudio como fundamento a la auditoría de seguridad, con temas explicativos al vínculo con la seguridad en informática en ambientes educativos.
- Implementar auditoría informática aplicando un marco de trabajo y una metodología basada en la norma ISO 27002 y que tenga como objetivo analizar los controles de seguridad física del laboratorio.
- Plantear un diseño metodológico junto con los instrumentos de recolección de datos que permitan diagnosticar el estado actual de la seguridad física en el Laboratorio Multimedia de Idiomas.
- Desarrollar una propuesta en contramedida para reducir los riesgos detectados en la auditoría, a través de medidas correctivas que estén alineadas a la ISO 27002.
- Analizar los resultados obtenidos de la auditoría informática y las herramientas de recolección de datos, para extraer conclusiones y sugerencias que ayuden a retroalimentar la seguridad física del laboratorio.

## 1.7 Justificación

La realización de Auditoria Informática a la Seguridad Física Del Laboratorio Multimedia de Idiomas ULEAM Ext. El Carmen, es importante para garantizar la protección de los recursos tecnológicos y la función correcta que respalda el proceso educativo en el campo del lenguaje. Este laboratorio está equipado con dispositivos que brindan a los estudiantes acceso a plataformas digitales, aplicaciones interactivas y herramientas audiovisuales básicas para desarrollar habilidades lingüísticas.

En la actualidad, la seguridad física del laboratorio es muy vulnerable ya que está expuesta al no autorizado debido a que no cuenta con seguridad la puerta, no tiene cámaras de vigilancias, robo, fallas por humedad o por aves, ya que las ventanas del mismo pasan abiertas, falta de mantenimiento. Estas condiciones pueden ubicar en riesgo el hardware como también la continuidad de la educación de los estudiantes. Mediante esta auditoría informática se procederá a identificar las vulnerabilidades y proponer mejoras que aseguren en la integridad y disponibilidad de los equipos.

Este proyecto busca fomentar la seguridad de los jóvenes ante cualquier desastre o al momento de impartir los conocimientos académicos en el laboratorio. No solo está tratando de reducir los riesgos, sino también para promover el uso de culturas preventivas y responsables en el uso y protección de los recursos informáticos.

### 1.7.1 Impacto tecnológico

La auditoría informática le permite detectar errores en la protección física del equipo, lo que facilitará una medida de ajuste, como el sistema de monitoreo, el control de acceso, la protección de sobretensión y el equipo de movimiento estratégico. Esto aumentará la durabilidad y la confiabilidad del laboratorio de infraestructura de laboratorio y garantizará la operación más segura y continua.

Además, creará una base técnica para mejoras futuras, como la integración de sensores ambientales, supervisión digital, la integración de la ansiedad inteligente y los protocolos de mantenimiento preventivo. De esta manera, el entorno educativo con tecnologías más protegidas y funcionales se reforzará, adaptado a los requisitos modernos relacionados con la enseñanza del lenguaje informático.

### 1.7.2 Impacto social

El impacto social se refleja en mejorar el entorno académico de los maestros y los estudiantes, lo que garantiza que el acceso a los instrumentos tecnológicos no se ve interrumpido por un trauma o abuso físico. Para muchos estudiantes, especialmente aquellos que no tienen acceso a sus equipos, este laboratorio es la principal interacción con las plataformas de educación digital.

Garantizar las condiciones óptimas de seguridad y operación reduce las desigualdades digitales y una mayor inclusión académica. Esta revisión también promueve la comprensión del cuidado de los recursos tecnológicos y el mantenimiento de un entorno educativo seguro y funcional, creando una cultura de responsabilidad y prevención de las universidades.

### 1.7.3 Impacto ecológico

La auditoría contribuye directamente a la sostenibilidad ambiental al identificar riesgos físicos que pueden reducir la vida útil de los equipos, como la humedad, el sobrecalentamiento o la sobrecarga eléctrica. Al evitar daños prematuros en la infraestructura tecnológica, se disminuye la necesidad de reemplazo frecuente y, por ende, la generación de residuos electrónicos, los cuales representan una de las fuentes de contaminación más perjudiciales para el medio ambiente.

Asimismo, las recomendaciones resultantes del proceso de auditoría pueden incluir el uso de equipos de bajo consumo energético, la adecuada ventilación del laboratorio, la correcta distribución del cableado y la implementación de políticas institucionales orientadas al uso eficiente de los recursos tecnológicos. Esto permite fomentar una cultura de responsabilidad ambiental dentro del laboratorio y de la institución.

# Capítulo II

# 2 Marco Teórico

## 2.1 Antecedentes históricos

La auditoría informática ha evolucionado desde su enfoque inicial en procesos contables hasta convertirse en una herramienta clave para la gestión de riesgos tecnológicos. Con el crecimiento de la digitalización, se ha vuelto esencial evaluar no solo la seguridad lógica, sino también la física, especialmente en entornos educativos. Esta evolución ha permitido a las instituciones identificar vulnerabilidades en sus infraestructuras y tomar decisiones informadas para proteger sus recursos tecnológicos (Piattini & Peso, 2021).

La propuesta de auditoria nace de la necesidad de proteger los equipos tecnológicos que se encuentran en el laboratorio y así asegurar la continuidad de las operaciones académicas. Es de conocimiento global que el mantenimiento, el resguardo y protección son fases fundamentales en cualquier empresa o institución, si estos llegan a faltar el nivel de riesgo y perdida sube exhaustivamente, llegando a causar interrupciones en las clases (ISO/IEC 27001, 2023).

Para apoyar estos procesos, se han establecido marcos normativos como ISO 27001, los cuales proporcionan lineamentos claros para la implementación de auditorías informáticas. Estas guías permiten gestionar los riesgos, definir controles físicos y fortalecer la cultura de prevención en las instituciones de educación superior, asegurando así la correcta utilización y disponibilidad de los recursos tecnológicos (Martínez, 2021).

### 2.1.1 Antecedentes de investigaciones relacionadas al tema presentado.

La presente investigación toma como referencia diversos estudios previos relacionados con la auditoria informática, especialmente aquellos enfocados en la seguridad física en entornos educativos. Dichos antecedentes permiten identificar brechas comunes, sustentar la aplicación de metodología adecuadas y justificar la necesidad de auditar las condiciones física de instalaciones que contienen equipos tecnológicos de alta importancia, como el Laboratorio Multimedia de Idiomas de la ULEAM, sede el Carmen.

Ochoa Caicedo (2020), en su tesis *Evaluación de la infraestructura tecnológica bajo estándares ISO 27001 en universidades públicas del Ecuador* la cual fue realizada en la Universidad Central del Ecuador, examinó cómo se gestiona la infraestructura tecnológica en universidades públicas conforme a la norma ISO 27001, detectando que muchas de estas instituciones no cuentan con controles físicos suficientes, lo que pone en peligro la integridad de sus equipos.

Aguilar Rivera (2021) desarrollo su tesis denominada Auditoria de seguridad física y lógica en laboratorios de informática universitarios, en la que evaluó tres laboratorios pertenecientes a una universidad pública en México. Los hallazgos del estudio reflejaron deficiencias importantes en los controles físicos, incluyen la falta de políticas de acceso definidas, la inexistencia de vigilancia y la ausencia de mantenimiento preventivo de los equipos tecnológicos. Basándose en la norma ISO/IEC 27002, concluyó que estas debilidades exponían los activos tecnológicos a riesgos como pérdida, daño o accesos no autorizados. Estos resultados respaldan la importancia de implementar auditorías informáticas.

## 2.2 Definiciones conceptuales

### 2.2.1 Auditoría Informática.

La auditoría informática puede definir como un proceso técnico y organizado orientado a revisar la seguridad y el correcto funcionamiento de los sistemas de información en una entidad. En Ecuador, su implementación resulta fundamental para una administración eficiente de los recursos tecnológicos disponibles, estas actividades tienen como finalidad detectar riesgos, verificar el cumplimiento de normativas vigentes y recomendar medidas correctivas ante posibles fallas. También facilita que la tecnología se utilice de forma alineada con los objetivos institucionales. Aporta información clave para la toma de decisiones estratégicas. Además, fortalece la gobernanza tecnológica y reduce los riesgos operativos (Alcívar, 2024)

De acuerdo con una publicación de la Escuela Superior Politécnica de Chimborazo (ESPOCH), "la auditoría informática implica un proceso de evaluación técnica que debe ser llevado a cabo por profesionales con formación especializada" (Patricio Robalino et al., 2022) . La labor de los auditores informáticos consiste en recopilar y analizar evidencias que permiten determinar el nivel de seguridad de los sistemas de información, en la obra se destaca la necesidad de contar con personal capacitado que contribuya a la protección de los activos digitales dentro de una organización.

Una investigación desarrollada por la Universidad Central del Ecuador resalta que "la auditoría informática ha cobrado mayor relevancia a medida que las tecnologías de la información han evolucionado, convirtiéndose en una herramienta clave para detectar y reducir los riesgos asociados a la pérdida de datos" (Arellano, 2022). La aplicación de metodologías especializadas en 2019 en una institución religiosa fue el enfoque principal del estudio, demostrando que este modelo es adaptable a distintas organizaciones. Los resultados

reflejan que la auditoria permiten establecer controles más eficientes y mejorar la gestión de los recursos tecnológicos.

#### 2.2.1.1 Normativas y estándares (ISO 27001, ITIL)

Estradas & Paéz (2021) explican que "la integración de estos marcos permite fortalecer la protección de la información y alinear los procesos tecnológicos con los objetivos estratégicos de cualquier organización". La auditoría informática es toda una rama de estudio, llena de normas, estándares, políticas y más. Una de estas normas que sobresalen en este tipo de estudios es la ISO 27001 que no es nada más que un proceso que obliga a una organización a gestionar de mejor manera la seguridad de la información. Finalmente, esta ITIL, que es como una guía estandarizada para ver si se cumplen los objetivos de la auditoría.

La integración de estas tres normas en una auditoría tecnológica permite llevar un mejor control y optimizar los procesos, siempre garantizando que se cumpla con las normas propuestas. Lo que destaca Juárez (2020) de estos modelos, es su naturaleza para trabajar en conjunto, lo que favorece su aplicación en auditorías informáticas. Además, su utilización contribuye a una mejor gestión de los recursos tecnológicos y a una mayor protección de los activos.

Los retos al implementar auditorías son constantes lo que aumenta el uso de marcos de trabajo y normas que permitan establecer políticas, responsabilidades y aplicar controles de manera más segura y que garantice resultados. De acuerdo con un estudio publicado en Academia.edu (2023), estos estándares se han consolidado como herramientas esenciales para las auditorías informáticas en entornos digitales cada vez más complejos.

#### 1.1.1.2 Metodologías de auditoría en entornos TI

Como señalan Trujillo et. al (2019), es fundamental apoyarse en buenas prácticas y marcos internacionales ISO para hacer más objetiva y confiable la auditoría. Las auditorías informáticas requieren de metodologías que guíen cada etapa del proceso, desde su planificación hasta la entrega de resultados. No existe una única forma de auditar, ya que cada organización tiene necesidades distintas.

Martínez (2020) propone una auditoría diseñada para ajustarse a la condición real de las organizaciones. Esta auditoría se trabaja bajo una metodología que contempla fases como: análisis del entorno, evaluación de riesgos y revisión de controles, siendo esta útil en instituciones que no aplican de manera estricta los estándares.

En una investigación realizada en la Universidad Estatal del Sur de Manabí, en la cual se aplicó la metodología PDCA para auditar los laboratorios de informática. Y cuyos resultados evidenciaron que este enfoque facilita la identificación de fallas, la aplicación de controles y la optimización de los recursos, lo cual es beneficioso en entornos educativos donde la seguridad y la eficiencia es importante (Sánchez y Toala, 2021).

#### 2.2.1.1 Ciberseguridad y su relación con la auditoría.

La auditoría informática y la ciberseguridad van de la mano pues ambas se complementan, al punto que una auditoria llega a fortalecer la ciberseguridad, es decir permite evaluar si los controles existentes son efectivos frente ante posibles amenazas y de no serlo da opción a mejorar. Mejías (2020) desarrolló una metodología cuyas fases incluyen: análisis de riesgos, identificación de vulnerabilidades y revisión de políticas, con el objetivo de mejorar la seguridad.

Por otro lado, Romero (2021) en su estudio planteó una metodología de gestión de riesgos para la ciberseguridad, aplicada en una empresa del sector minero. Su propuesta tiene fases como: análisis de riesgos, evaluar amenazas y aplicar controles, fortaleciendo así la capacidad de respuesta ante incidentes.

Ormache (2023) en su trabajo, destaca que la auditoría informática cumple un rol importante en el fortalecimiento de la ciberseguridad nacional. A través de la detección de vulnerabilidades y el análisis del cumplimiento normativo, se pueden implementar mejoras efectivas. Esta práctica permite proteger la infraestructura digital del Estado frente a amenazas crecientes. De igual manera, la auditoria impulsa una cultura de control y prevención en el entorno tecnológico, fortalecimiento las prácticas de seguridad, En este contexto, se convierte en una herramienta clave para el desarrollo y la protección de la seguridad digital del país.

#### 2.2.1.2 Auditoría de sistemas y redes.

Las auditorias son clave para mantener los sistemas seguros y no queda atrás una aplicada a redes, ya que van proteger al activo más preciado que son los datos, mientras que as u vez mejoran los procesos operativos. Además, permite identificar deficiencias técnicas y aplicar mejoras constantes. El uso de tecnologías avanzadas refuerza la seguridad, mientras que la capacitación constante del personal se vuelve indispensable frente a la evolución de nuevas amenazas (Bruce, 2025).

Según Contreras (2024), la auditoría de sistemas y redes debe enfocarse en la evaluación de los componentes tecnológicos como: servidores, equipos de red y protocolos. Esta evaluación ayuda a identificar áreas que pueden vulnerar la seguridad y disminuir el desempeño de los servicios. Así mismo, el autor recomienda aplicar marcos de referencia para garantizar cumplir objetivos y dar continuidad operativa.

En el trabajo de Cárdenas (2021), este argumenta que la auditoría informática debe permitir supervisar la seguridad de las redes de datos en tiempo real. Este enfoque facilita la detección temprana y la prevención de posibles amenazas tomando medidas. Además, nos dice que documentar cada hallazgo y recomendación apoya la toma de decisiones y mantener la disponibilidad de los sistemas.

#### 2.2.1.3 Control Interno

Según Torres y Méndez (2021), destacan que los mecanismos de control interno constituyen el principal escudo protector contra amenazas en el ámbito tecnológico. Este sistema integrado combina directrices, protocolos estandarizados y metodologías operativas orientadas a: salvaguardar los activos organizacionales, preservar la calidad de los datos, y alinear las operaciones con los fines institucionales.

En el ámbito de la educación superior, el control interno en los entornos informáticos abarca diversas áreas, que van desde la protección física de los equipos hasta la administración de usuarios, contraseñas, copias de seguridad, licencias de software y accesos remotos. El control interno, cuando se aplica de manera apropiada, garantiza el correcto funcionamiento de los sistemas utilizados tanto en la gestión académica como administrativa, asegurando niveles adecuados de seguridad y eficiencia. Además, favorece la ejecución de auditorías periódicas, ya que permite contar con trazabilidad y documentación de respaldo de los procesos institucionales (Guzmán & Rivera, 2021).

Dentro de los modelos más reconocidos para la evaluación del control interno se encuentra el COSO, desarrollado por el Committee of Sponsoring Organizations of the Treadway Commission. Este enfoque establece cinco pilares esenciales: el entorno de control, la identificación y análisis de riesgos, las actividades de control, la comunicación de la información y la supervisión continua. Estos elementos pueden ser aplicados en todos los

niveles institucionales y adaptados a contextos tecnológicos, lo que permite fortalecer la gobernanza de las tecnologías de la información y mejorar la gestión de riesgos (Muñoz & Cedeño, 2020).

### 2.2.2 Seguridad Física

Seguridad física es el conjunto de medidas preventivas y correctivas diseñadas para proteger los recursos tecnológicos, instalaciones y personal de una organización frente a amenazas físicas como accesos no autorizados, robos, desastres naturales o sabotajes. Su objetivo es garantizar la integridad, disponibilidad y continuidad operativa de los activos informáticos (Bruce, 2025).

Según Tenorio (2024), la seguridad física en entornos informáticos no solo se limita a la protección de equipos, sino que abarca un conjunto integral de medidas como el control de accesos, la video vigilancia y los planes de contingencia. Estas acciones deben alinearse a la ISO 27001, que proporciona la guía para la gestión de la seguridad. De esta manera, se busca asegurar los activos, prevenir accesos no autorizados y mantener la continuidad operativa.

Según la Universidad Técnica de Machala (2024), una auditoría informática enfocada en la seguridad física facilita la detección de vulnerabilidades en los sistemas de protección de los equipos. A través de esta evaluación, se pueden identificar riesgos como accesos indebidos, fallas en la vigilancia o ausencia de protocolos ante emergencias. Esta información es clave para tomar decisiones estratégicas que fortalezcan la seguridad institucional. Además, se promueve una cultura preventiva que protege los activos informáticos frente a amenazas.

#### 2.2.2.1 Protección de centros de datos y salas de servidores.

La seguridad en los centros de datos y en las salas de servidores se basa principalmente en la aplicación de medidas físicas y técnicas para proteger los equipos críticos de procesamiento y almacenamiento de información. El objetivo es claro y es evitar accesos no autorizados, sabotajes y asegurar la continuidad de los servicios tecnológicos (Torres & Méndez, 2021).

Flores (2024) menciona que la auditoría informática debe realizar una evaluación detallada de este tipo de espacios, debido a que cualquier debilidad compromete gravemente la disponibilidad y la seguridad. La protección de centros de datos y salas de servidores son fundamentales, ya que allí se concentran equipos esenciales como servidores, dispositivos de red y sistemas de almacenamiento, los cuales son indispensables para el funcionamiento informático. Y garantizar su protección es muy necesario, por eso se aplican mecanismos como controles de acceso, cerraduras electrónicas, monitoreo ambiental y sistemas de detección de incendios.

Moncayo y Llerena (2021) en su trabajo aportan que es necesario implementar controles estructurales, ambientales y de acceso que garanticen la integridad, disponibilidad y confidencialidad de los datos. La correcta aplicación de estas medidas contribuye a reducir riesgos operativos y a fortalecer la resiliencia tecnológica.

#### 2.2.2.2 Controles de acceso biométricos y vigilancia.

El tema de controles de acceso es uno de los pilares de la seguridad, su importancia en las instituciones es cada vez más trascendente. El acceso biométrico como huella, iris o facial, por un lado, es cada vez más visto en hogares y empresas por su eficiencia y la vigilancia usando sistemas de video vigilancia es ya casi una necesidad primaria en ciudades con índices de delincuencia alto. Su implementación reduce considerablemente el riesgo de

accesos no autorizados y facilita el registro y seguimiento de eventos (Guzmán & Rivera, 2021).

Buenaño et. al (2021) expresa en su trabajo que los sistemas de acceso que usan datos biométricos de control permiten verificar la identidad de los usuarios. A diferencia de los métodos tradicionales, estos sistemas no dependen de tarjetas o contraseñas, lo que incrementa la seguridad. Su aplicación en instituciones contribuye a un mayor control de acceso y disminuye el riesgo de suplantación de identidad.

Por otro lado, según Echeverría (2022) la integración de tecnologías biométricas con sistemas de notificación y monitoreo en red, usando una placa Raspberry Pi, permite desarrollar soluciones más eficientes. Estos sistemas no solo controlan el acceso físico, sino que también generan alertas en tiempo real, fortaleciendo la capacidad de respuesta.

#### 2.2.2.3 Normativas de seguridad física ISO 27002.

La norma ISO 27002 llego para complementar a la ISO 27001 y proporciona lineamientos en la implementación de controles para la protección física y ambiental de los activos, se resume como una guía para fortalecer la seguridad. Esta versión organiza sus controles en cuatro categorías: organizativos, relacionados con las personas, físicos y tecnológicos. Los controles físicos son fundamentales para prevenir accesos no autorizados y reducir riesgos derivados de factores ambientales o incidentes internos (ISOtools, 2022).

Entre los controles más importantes se incluyen:

- **Perímetros de seguridad física (7.1):** Establecer y proteger áreas que contienen activos críticos.
- **Control de entrada física (7.2):** Asegurar que solo personal autorizado acceda a zonas restringidas.

- **Monitoreo físico (7.4):** Implementar sistemas de vigilancia para detectar accesos indebidos.
- **Protección ante amenazas físicas y ambientales (7.5):** Incorporar medidas contra incendios, inundaciones y sabotajes (Lopez, 2021-2022).

Narváez (2024) señala que "ISO/IEC 27002:2022 proporciona directrices para aplicar controles físicos y ambientales que salvaguarden activos críticos frente a accesos no autorizados y riesgos naturales" (pág. 45). La norma contempla una serie de controles específicos enfocados en la seguridad física, tales como la protección del perímetro y la vigilancia permanente de las áreas críticas.

La adopción de estos controles contribuye a proteger la integridad, disponibilidad y confidencialidad de la información, evitando que vulnerabilidades físicas impacten en la operación institucional. Además, impulsa una cultura de prevención que refuerza la capacidad de respuesta organizacional ante riesgos físicos y tecnológicos (Group E. , 2023).

#### 2.2.2.4 Resiliencia física ante desastres naturales.

Es el poder que tiene la infraestructura para soportar, adaptarse y recuperarse ante eventos de riesgo de origen natural como son los incendios, inundaciones o terremotos entre los más comunes. Para que una infraestructura llegue a tener un nivel alto de resiliencia es necesario una buena planificación al momento de construir. Por lo tanto, implica contar con planes de emergencia, rutas de evacuación, sistemas de respaldo y una cultura enfocada en la prevención. Su objetivo principal es minimizar los efectos de los desastres y asegurar la continuidad de los servicios (Payano, 2021).

De acuerdo con Lahm, y Micah (2024), las nuevas tecnologías y la llegada del internet de las cosas, que introdujo muchos sensores y soluciones basadas en inteligencia

artificial son grandes alternativas a herramientas que pueden mejorar la resiliencia de las infraestructuras ante este tipo de eventos. Con estas nuevas tecnologías se facilita el monitoreo constante y ayudan a anticipar fallas, además de apoyar la toma de decisiones durante emergencias. Estas tecnologías constituyen un avance significativo en la gestión del riesgo físico.

Rivera (2021) afirma que la resiliencia frente a desastres naturales debe basarse en una planificación anticipada, que integre tanto personal capacitado, recursos logísticos y protocolos de respuesta. En el contexto de seguridad física, esto implica preparar infraestructuras que puedan resistir eventos extremos y mantener su funcionalidad operativa. Además, resalta la importancia de la cooperación interinstitucional y el uso de tecnologías para mejorar la capacidad de respuesta. Esta visión integral permite reducir el impacto de los fenómenos naturales y proteger tanto a las personas como a los activos críticos de una organización.

#### 2.2.2.5 Amenazas y Riesgos a la Seguridad Física

Las amenazas y riesgos a la seguridad física representan uno de los mayores desafíos para cualquier organización que dependa de activos tecnológicos y de infraestructura para su operación. La seguridad física se enfrenta a un amplio espectro de amenazas, tanto intencionales como accidentales, que pueden comprometer la integridad, disponibilidad y confidencialidad de los recursos. Comprender la naturaleza de estas amenazas y los riesgos asociados es fundamental para diseñar estrategias efectivas de protección y mitigación (Lahm et al., 2024).

#### *2.2.2.5.1 Tipos de Amenazas a la Seguridad Física*

Las amenazas se pueden clasificar en dos grandes categorías:

**a) Amenazas Intencionales:**

Las amenazas intencionales constituyen actos maliciosos ejecutados por personas u organizaciones con fines destructivos o ilícitos. Estas acciones deliberadas abarcan desde intrusiones no autorizadas y actos vandálicos hasta robos de hardware, sabotajes laborales, ataques terroristas y operaciones dirigidas contra instalaciones críticas. Un caso paradigmático sería el de un intruso que penetra en un centro de datos para comprometer equipos sensibles o sustraer información confidencial, lo que podría desencadenar la fuga de datos estratégicos y paralizar operaciones esenciales (Hernández et al., 2021).

b) **Amenazas Accidentales o Naturales**:

Los incidentes de origen no intencional representan riesgos significativos para los sistemas informáticos, pese a no ser provocados por acciones humanas. Entre estos fenómenos se encuentran catástrofes naturales como sismos, inundaciones e incendios, así como fallas tecnológicas que incluyen cortes eléctricos, sobretensiones o explosiones accidentales. La ausencia de protocolos de prevención ante estos eventos puede ocasionar daños severos, no solo en la infraestructura física, sino también en la integridad de los datos y en la estabilidad financiera de las organizaciones (ISO, 2022).

### 2.2.3 Categoría conceptual actualizados vinculados al tema planteado

En el marco de la auditoría informática aplicada a la seguridad física, se han desarrollado nuevas categorías conceptuales que fortalecen la gestión de riesgos en entornos educativos. Uno de estos conceptos es la resiliencia operativa institucional, entendida como la capacidad de una universidad para mantener sus funciones críticas ante eventos

disruptivos. En el caso de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, esta resiliencia se vuelve esencial para garantizar la continuidad académica, especialmente en espacios como el Laboratorio Multimedia de Idiomas, donde se desarrollan actividades clave para la formación lingüística de los estudiantes.

Otro concepto importante dentro del ámbito educativo son los espacios físicos y digitales necesarios para el desarrollo y aprendizaje. Estos entornos, como los laboratorios, requieren medidas de seguridad física avanzadas que incluyen controles de acceso biométricos, sistemas de video vigilancia y monitoreo de las condiciones ambientales. En este contexto, la ULEAM Ext. El Carmen, al ser una institución pública con una alta población estudiantil, debe dar prioridad a la protección de estos espacios con el fin de evitar interrupciones en el servicio.

De igual manera, mediante una auditoría se busca soluciones preventivas, ya que esta está orientada a la anticipación de riesgos mediante evaluaciones periódicas y el uso de normas como la ISO 27002. Esto permite que la universidad identifique vulnerabilidades antes de que se conviertan en incidentes graves. Evitando gastos elevados para la institución.

## 2.3 Conclusiones relacionadas al marco teórico en referencia al tema planteado.

Como parte de lo mostrado en el marco teórico, se concluye que la auditoría informática constituye una herramienta para fortalecer la seguridad física en instituciones como la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. Haciendo revisión a investigaciones previas y normativas, se muestra que muchas universidades enfrentan dificultades relacionadas con accesos no autorizados, falta de mantenimiento y ausencia de controles.

La aplicación de normas como ISO 27001 y 27002 permitió establecer políticas claras, gestionar riesgos y alinear la seguridad con los objetivos. En el caso específico de la ULEAM Ext. El Carmen, estas herramientas resultan fundamentales para proteger espacios como el Laboratorio multimedia de idiomas, donde se desarrollan actividades académicas para la formación de los estudiantes.

Finalmente, se destaca la importancia de integrar tecnologías emergentes como sistemas de acceso con datos biométricos, sensores usados en el internet de las cosas y plataformas de video vigilancia que implemente notificaciones. Estas soluciones no solo mejoran la capacidad de respuesta ante amenazas físicas, sino que también fortalecen la resiliencia institucional frente a desastres naturales y fallos operativos. En conclusión, el marco teórico respalda la necesidad de implementar auditorías informáticas integrales que aborden tanto la seguridad física como la lógica, promoviendo una cultura de prevención, control y mejora continua en la ULEAM.

# Capítulo III

## 3 Marco investigativo

### 3.1 Introducción

El desarrollo de auditorías informáticas aplicadas a la seguridad física en entornos universitarios requiere un planteamiento metodológico rigoroso que garantice la obtención de información certera y relevante para el análisis. La metodología define las herramientas y procedimientos mediante los cuales se recopilan, procesan y analizan los datos que permiten evaluar el estado actual de la seguridad física del laboratorio, así como determinar vulnerabilidades y riesgos. Este capítulo es fundamental para asegurar la validez científica y la confiabilidad de los resultados obtenidos, elementos indispensables para la formulación de recomendaciones pertinentes y efectivas en el contexto de la Universidad Laica Eloy Alfaro de Manabí.

Además, la metodología orienta el proceso investigativo, asegurando que la auditoría informática se ejecute siguiendo criterios técnicos y éticos específicos para un entorno educativo. Se adapta a las particularidades que implican la protección de recursos tecnológicos en instituciones académicas, integrando aspectos técnicos y humanos en el análisis. Por ello, contar con un marco metodológico sólido facilita la replicabilidad del estudio y la aplicación de sus conclusiones en la mejora continua de la seguridad física en los laboratorios universitarios.

### 3.2 Tipo de investigación

#### 3.2.1 Investigación Descriptiva

Este tipo de investigación permite recopilar datos sistemáticos sobre las condiciones existentes y analizarlos con el fin de implementar cambios que mejoren la protección de los recursos. Este enfoque resulta idóneo en contextos tecnológicos educativos debido a su

capacidad para describir fenómenos presentes y aportar conocimientos que favorecen la toma de decisiones basadas en evidencia (Alcívar, 2024).

Para la presente auditoría informática, eligió un enfoque de investigación descriptivo con una orientación aplicada, ya que fue necesario caracterizar detalladamente la situación actual de la seguridad física en el laboratorio multimedia y luego se propuso soluciones prácticas para dar salida a la problemática planteada.

### 3.2.2 Investigación Exploratoria

Tal como lo plantea Arellano (2020), en su tesis desarrollada en la Universidad Central del Ecuador, "la investigación exploratoria permite adaptar el marco metodológico a las necesidades reales de cada organización, facilitando el análisis de riesgos y la mejora de los procesos informáticos" (pág. 56). Este tipo de investigación se centra en analizar puntos que saben pasar desapercibidos y darles seguimiento para tener una visión más amplia del tema de estudio. En este tipo de investigaciones de auditoria informática sirve de ayuda para la identificación temprana de riesgos o malas prácticas que lleven a generar problemas estructurales.

De acuerdo con ello se escogió este enfoque él fue encaminado a la necesidad de comprender el entorno que rodea el proyecto, esto facilitó tener información previa y sacar hipótesis. En la auditoría que se realizó, la investigación exploratoria ha permitió detectar fallas en la cultura organizacional, desconocimiento de protocolos y vulnerabilidades que afectaban la protección de los recursos tecnológicos.

## 3.3 Métodos de investigación

### 3.3.1 Método Cuantitativo

De acuerdo con Tenorio (2025) , este método permite obtener datos numéricos que, al ser analizados estadísticamente, facilitan la identificación de patrones y tendencias en la percepción y aplicación de normas de seguridad física. El enfoque cuantitativo es fundamental en auditorías informáticas para garantizar objetividad en la evaluación y medir la efectividad de controles y protocolos establecidos en el entorno evaluado.

Se utilizó principalmente el método cuantitativo dado que la recolección de datos se realizó mediante encuestas estructuradas dirigidas a los estudiantes. Para con los datos obtenidos poder entender donde se centran los riesgos de la seguridad del laboratorio.

### 3.3.2 Analítico – Sintético

El método analítico-sintético, el cual permite examinar un fenómeno dividiéndolo en sus partes esenciales para comprenderlo con mayor profundidad. A través del análisis, se identificaron los componentes clave que conforman la auditoría informática, como los controles físicos, las políticas de seguridad y los riesgos asociados. Posteriormente, mediante el proceso sintético, se integraron estos elementos para entender cómo interactúan entre sí y cómo influyen (Alcívar, 2024).

En el desarrollo de esta investigación se empleó en el funcionamiento general del sistema de seguridad del laboratorio. Este enfoque metodológico facilitó una visión más clara y estructurada del objeto de estudio, permitiendo no solo detectar debilidades específicas, sino también proponer mejoras que respondan a la realidad institucional.

## 3.4 Fuentes de información de datos

### 3.4.1 Fuentes primarias Encuesta

En la investigación realizada por Tenorio (2024), se resalta la importancia de la encuesta como instrumento clave para obtener datos directamente de estudiantes, docentes y técnicos, con el fin de evaluar su percepción, conocimiento y adherencia a las normativas de seguridad física. Este método posibilita la identificación de debilidades y aspectos críticos en los controles y procesos vigentes, lo que es esencial para diseñar estrategias que fortalezcan la seguridad del laboratorio.

Así, en la presente auditoría, la encuesta aplicada a los usuarios del laboratorio multimedia contribuyo a la recopilación de información relevante y actualizada sobre el cumplimiento de las medidas de seguridad, complementando la información obtenida mediante entrevistas y observación para lograr un análisis integral de la protección física en el centro de estudios.

### 3.4.2 Fuentes secundarias Entrevista

Según Silva (2020) “su aplicación en esta investigación permitió profundizar en aspectos humanos y organizacionales que influyen en la seguridad física del laboratorio, complementando los datos obtenidos por otros medios. Esta técnica se adapta a las condiciones reales de cada institución, facilitando la identificación de factores que inciden directamente en la gestión tecnológica” (pág. 58).

La entrevista fue herramienta metodológica que nos permitió obtener información directa de los participantes mediante una conversación previamente estructurada, a través de este proceso, se logró recopilar opiniones, experiencias y conocimientos que no siempre se evidencian en instrumentos cuantitativos como encuestas.

## 3.5 Estrategia Operacional Para La Recolección De Datos

### 3.5.1.1 Población

Esta técnica es adecuada para estudios descriptivos donde se requiere información específica y de primera mano, en especial en contextos institucionales limitados en tiempo o recursos, se garantizará que la muestra representativa refleje adecuadamente la diversidad de perfiles involucrados en la seguridad física del laboratorio (Alcívar, 2024).

La población la cual fue nuestro objeto de estudio estuvo constituida por el personal administrativo, técnico y los usuarios habituales del laboratorio multimedia de idiomas. Para la selección de la muestra, se empleó un muestreo no probabilístico por conveniencia, considerando la accesibilidad y disponibilidad de los participantes durante el periodo de recolección de datos.

### 3.5.1.2 Muestreo

Según Alcívar Rivas (2024), este método resulta eficiente en el ámbito educativo debido a que permite obtener datos de los usuarios que hacen uso del laboratorio o del personal que da mantenimiento, es decir los usuarios prioritarios de los que se podrá obtener mejor calidad de datos, aunque su limitación viene de generalizar los resultados. El mismo se utilizó un muestreo no probabilístico por conveniencia para seleccionar a los participantes de la auditoría informática, debido a que esta técnica prioriza la accesibilidad y disposición de las personas involucradas en el estudio, lo cual facilita la recolección de información en un contexto institucional donde la disponibilidad puede ser limitada.

En este caso el tamaño de nuestra muestra correspondió a aquellos estudiantes que se encontraban actualmente matriculados en los niveles de Ingles A1, A2 y B1 de la ULEAM Ext. El Carmen y correspondieron a carreras como Agropecuaria, Enfermería, Tecnología

de la Información y Educación, al realizar esta encuesta con un margen de error del 5% nuestro tamaño de muestra fue de 50 respuestas.

#### 3.5.1.3 Estructura de los instrumentos de recolección de datos aplicados

Como base de la recolección de datos en este proyecto se emplearon 2 instrumentos: la primera una encuesta dirigida principalmente a los estudiantes de la ULEAM Ext. El Carmen, específicamente los cursos A1, A2 y B1, de la materia de inglés. La misma que es vista por diferentes carreras. Y la otra es una entrevista aplicada al docente que es responsable del área de idiomas.

La encuesta consta de 12 preguntas con opción múltiple, con estas preguntas se busca obtener datos sobre el punto de vista, conocimiento y experiencias de los estudiantes respecto a la problemática del estudio. Este instrumento permitió obtener una visión general del nivel de comprensión y las dificultades comunes que enfrentan los estudiantes en el proceso de adquisición del idioma.

Por su parte, la entrevista al docente encargado del área de idiomas incluyó 12 preguntas abiertas, formuladas con el objetivo de profundizar en aspectos cualitativos relacionados con la planificación académica, metodologías empleadas, retos institucionales y estrategias pedagógicas implementadas para mejorar el aprendizaje del inglés en los distintos niveles. La entrevista permitió obtener información valiosa desde la perspectiva del docente, complementando los datos obtenidos en las encuestas.

Ambos instrumentos fueron elaborados en función de los objetivos específicos de la investigación, garantizando su pertinencia y coherencia con el enfoque metodológico del estudio.

**Tabla 1**

*Tabla de Instrumento de Recolección de Datos.*

| Técnica | Instrumento | Fuente | Responsable | Fecha |
|---|---|---|---|---|
| **Entrevista** | Guía de entrevista | Ing. Roman Loor Michael Argenis | Julexy Jamileth Castro Alava | 06/08/2025 |
| **Encuesta** | Cuestionario | Estudiantes de las carreras de las diversas carreras que están matriculado en la materia de English. | Julexy Jamileth Castro Alava | 28/07/2025 hasta 14/08/2025 |

### 3.5.2 Plan de recolección de datos

La recolección de datos de esta investigación se planificó considerando tanto la disponibilidad de los participantes como la pertinencia de la información a obtener. Para llevar a cabo este plan de recolección se plantearon 2 fases: una es la aplicación del primer instrumento que es la encuesta a los estudiantes y la segunda es la aplicación de la entrevista al docente designado.

La primera fase se aplicó a los estudiantes de las carreras de agropecuaria, enfermería, tecnologías de la información y educación, específicamente en la materia que todos cursan en común que es inglés y a los cursos de A1, A2 y B1. Esta fase se dio inicio el 28 de julio hasta su fin el 14 de agosto de 2025. Pera agilizar esta fase se usó un formulario digital usando la herramienta de Google Forms.

La segunda fase por otro que corresponde a la entrevista hacia el docente responsable del área de idiomas. Esta se llevó a cabo el 6 de agosto del 2025 en su oficina en las

instalaciones de la ULEAM Extensión El Carmen, la misma se aplicó de manera presencial y las respuestas fueron grabadas para posteriormente ser trascritas, y donde se las pudo analizar de mejor manera.

De esta forma, el plan de recolección de datos contempló no solo el orden y la temporalidad de las actividades, sino también las condiciones necesarias para asegurar la validez de la información, procurando que los resultados reflejen de manera precisa las percepciones de los estudiantes y la experiencia del docente.

## 3.6 Análisis y presentación de resultados

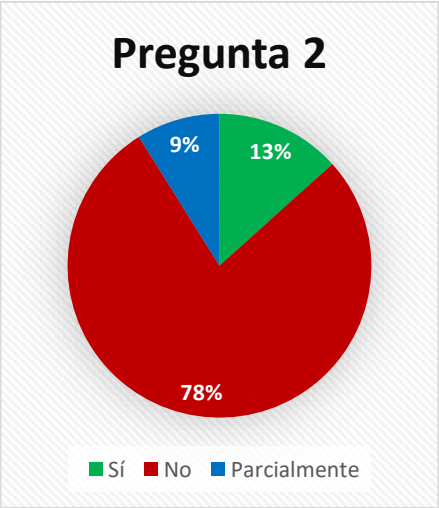
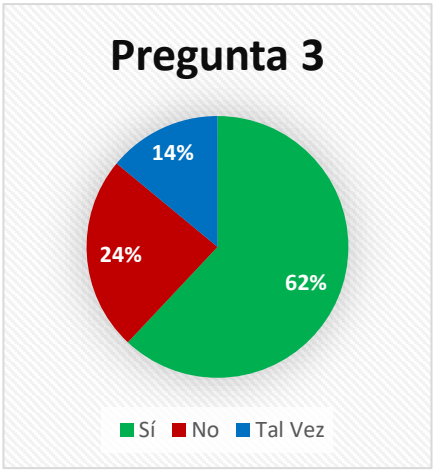
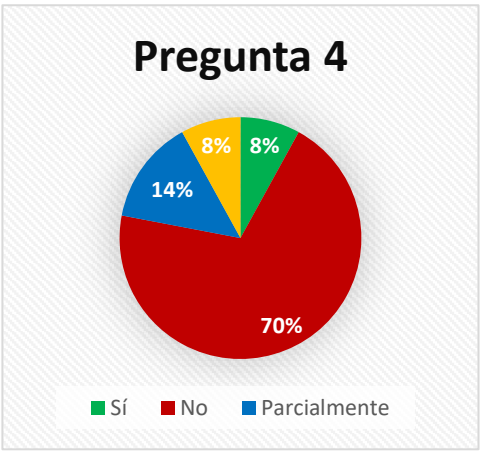
### 3.6.1 Tabulación y análisis de los datos

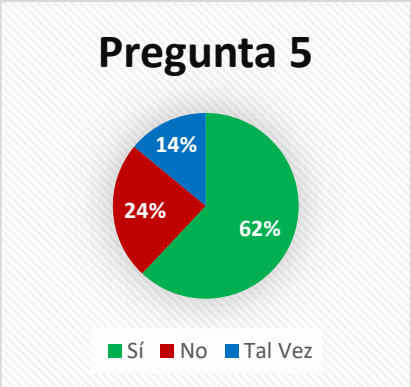
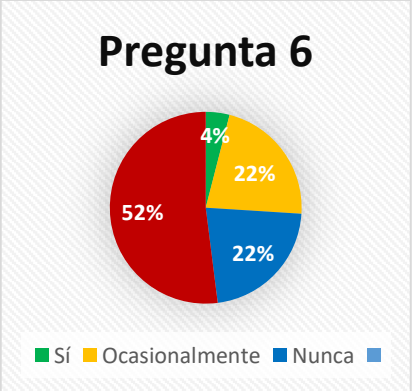
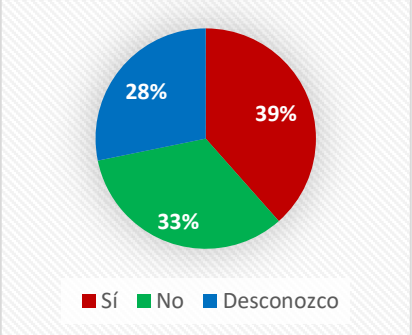
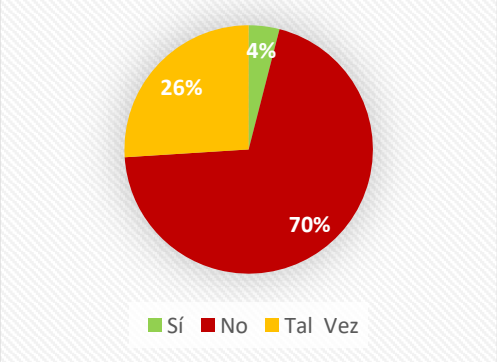
#### 3.6.1.1 Encuesta los estudiantes de las carreras matriculados en English.

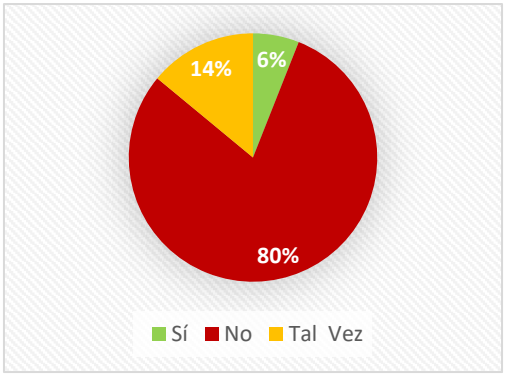
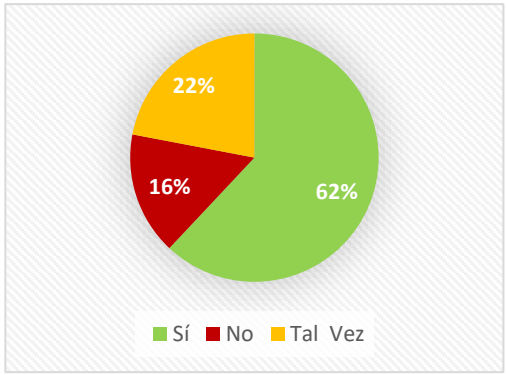
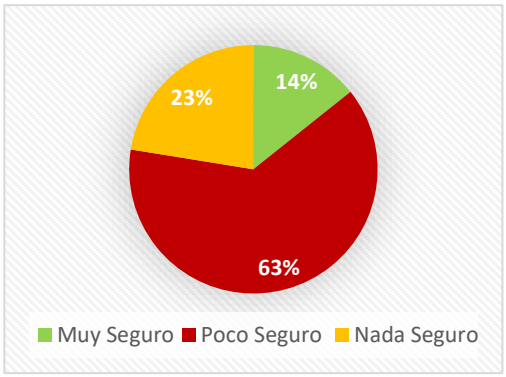
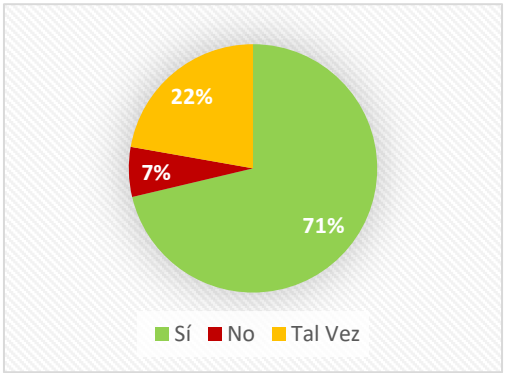
**Tabla 2**

*Resultado del método de investigación (Encuesta).*

| Pregunta | Gráfica | Análisis |
|---|---|---|
| 1. **¿Ha notado problemas técnicos que hagan fallar los equipos del Laboratorio?** |  | Casi la mitad de los estudiantes ha notado problemas técnicos en los equipos del laboratorio, y un poco menos de la otra mitad dice a ver visto fallos ocasionales lo que evidencia una falta de mantenimiento. |

| Preguntas | Gráfica | Análisis |
|---|---|---|
| **2. ¿Considera usted que los equipos tecnológicos del laboratorio están en buen estado?** |  | Los resultados muestran que una cuarta parte de los estudiantes considera que los equipos no se encuentran en buen estado, y la mitad dice que esta parcialmente bien lo que afecta directamente la calidad del aprendizaje y la continuidad académica. |
| **3. ¿ha visto dar mantenimientos a los equipos del Laboratorio?** |  | Mas de la mitad de los estudiantes ha visto dar mantenimientos a los equipos mientras que una cuarta parte no lo ha visto. |
| **4. ¿Considera que el laboratorio cuenta con medidas adecuadas de seguridad para los equipos?** |  | Se identificó que casi la totalidad de los estudiantes considera que el laboratorio no cuenta con medidas adecuadas de seguridad física como cerraduras seguras, cámaras funcionales o control de accesos. |

| Pregunta | Gráfica | Análisis |
|---|---|---|
| **5. ¿Ha escuchado o presenciado de accesos no autorizados al laboratorio?** |  | Un número considerable y pasado de la mitad de los estudiantes ha presenciado accesos no autorizados, lo que representa un riesgo. |
| **6. ¿Considera usted que la infraestructura del laboratorio recibe un mantenimiento adecuado?** |  | La mitad de los estudiantes no tiene conocimiento del mantenimiento a la infraestructura, y una cuarta parte ve que lo hacen ocasionalmente. |
| **7. ¿Conoce de incidentes como robos o daños en el laboratorio?** |  | Existen percepciones divididas respecto a incidentes en el laboratorio, pues un poco menos de la mitad si conoce de estos incidentes y el resto lo desconoce o no a visto. |
| **8. ¿Considera usted que el laboratorio está preparado ante desastres naturales?** |  | La mayoría considera que el laboratorio no está preparado para enfrentar eventos, lo que compromete la resiliencia operativa. |

| Pregunta | Gráfica | Análisis |
|---|---|---|
| **9. ¿Ha recibido alguna capacitación sobre normas de seguridad física para cuidar el laboratorio?** |  | Se evidencia una falta de capacitación sobre normas de seguridad física, lo que limita la cultura preventiva entre los usuarios. |
| **10. ¿Cree que implementar controles de acceso biométricos y video vigilancia aumentará la seguridad?** |  | Mas de la mitad de los estudiantes ven como necesaria la implementación de sistemas biométricos y video vigilancia para mejorar la protección del laboratorio. Y menos de la cuarta parte se opone. |
| **11. ¿Qué tan seguro se siente al utilizar el laboratorio?** |  | La gran mayoría no se siente segura al utilizar el laboratorio, lo que refleja una baja confianza en las condiciones actuales. |
| **12. ¿Ve útil hacer auditorías periódicas para evaluar la seguridad física del laboratorio?** |  | Casi la mayoría señalo que realizar auditorías periódicas es útil para evaluar y mejorar la seguridad física del laboratorio. |

### 3.6.2 Presentación y descripción de los resultados obtenidos.

#### 3.6.2.1 Entrevista a Coordinador de English.

**Tabla 3**

*Resultado al Instrumento de Investigación (Entrevista).*

| Preguntas | Respuestas | Análisis |
|---|---|---|
| 1. **¿Cuál es su cargo actual dentro de la universidad y desde cuándo lo desempeña?** | "Me desempeño como docente de la carrera de la Educación básica, además soy responsable de en la extensión desde el 2011". | El docente describe su rol desempeñado dentro de la universidad |
| 2. **Desde su experiencia, ¿con qué frecuencia se presentan fallas o problemas técnicos en los equipos del laboratorio?** | "El laboratorio de English fue utilizado por la carrera de Idiomas en la extensión el cual finalizo aproximadamente en el año 2015". | Nos hace saber el tiempo de uso que se le dio al laboratorio por parte de la carrera de idiomas. |
| 3. **¿Considera que el laboratorio es seguro?** | "Parcialmente seguro, ya que cuenta con una puerta que resguardaba los equipos del laboratorio. No obstante, existía la posibilidad de que alguien ingresara por las ventanas laterales." | No lo considera seguro del todo porque existen posibilidades altas de irrupciones. |

| | | | |
|---|---|---|---|
| **4.** | **¿Considera que el laboratorio está preparado para enfrentar desastres naturales como inundaciones o incendios? ¿Qué medidas existen actualmente?** | "No cumple con las condiciones ante eventos como lo es el incendio." | Concluyó en que no tiene |
| **5.** | **¿Cree que sería beneficioso implementar sistemas de control de acceso biométrico o video vigilancia? ¿Por qué?** | "Si, ya que al no contar con seguro se vuelve viable para el robo, o la perdida de objetos." | Nos dijo que si, por la inseguridad visible. |
| **6.** | **¿Considera que el laboratorio cuenta con medidas adecuadas de seguridad física, como cerraduras, cámaras o controles de acceso? ¿Por qué?** | "No el laboratorio no cuenta con ninguna medida de seguridad". | Nos hizo saber que no existen medidas |

| Preguntas | Respuestas | Análisis |
|---|---|---|
| **7. ¿Se brinda capacitación o información al personal y usuarios sobre normas de seguridad física en el laboratorio? ¿Con qué frecuencia?** | "Al principio si se realizaba capacitación y se realizó manuales los cuales estaban pegados en la pared, para que sean observados y leído siempre que se utilizaba el laboratorio, actualmente ya no se realiza". | Con el tiempo la capacitación se dejó atrás y se remplazó por manuales. |
| **8. ¿Ha ocurrido algún incidente relacionado con robos, humedad o polvo? ¿Cómo se ha gestionado?** | "De robo no, de polvo si ya que no se realiza limpieza en esta área, entonces los muebles y equipos son afectados". | Si hay antecedentes en polvo, por la falta de limpieza en los laboratorios. |
| **9. ¿Cómo evalúa el estado actual de la infraestructura del laboratorio (puertas, ventanas, techos, etc.) en relación con las normas técnicas de mantenimiento?** | "El laboratorio es disfuncional, como se ha señalado anteriormente: su estado no es el más adecuado y su infraestructura tampoco resulta apropiada para que los estudiantes reciban clases." | No es se encuentra en un estado apropiado y su infraestructura ya tiene mucho tiempo. |
| **10. ¿Con qué frecuencia se realiza mantenimiento a los equipos? ¿Existe un cronograma establecido o se hace de forma reactiva?** | "Actualmente no se cuenta con mantenimiento en los equipos, pero, cuando funcionaban, sí se les realizaba de manera periódica." | Ya no se realizan por su no uso, pero antes si se les realizaba. |

| | | |
|---|---|---|
| 11. **¿Ha tenido conocimiento de accesos no autorizados al laboratorio? ¿Cómo se ha manejado esa situación?** | "Sí, ha habido ocasiones en la cual se ha tenido ingreso de estudiantes que no pertenecen o que no toman la materia." | Si han existido antecedentes. |
| 12. **¿Cuál es el estado general de los equipos tecnológicos del laboratorio? ¿Están todos operativos o hay algunos fuera de servicio?** | "No existen; está en desuso, ya que cumplieron su vida útil." | Ya cumplieron su vida útil |
| 13. **¿Considera útil realizar auditorías periódicas para evaluar la seguridad física del laboratorio?** | "Por supuesto, si hubiera la manera de contar con un nuevo laboratorio si nos gustaría que contemos con auditorias periódicas para gestionar posibles daños." | Si, sería bueno prevenir antes que lamentar. |

### 3.6.3 Presentación y descripción de los resultados obtenidos del Cuestionario de requisito según norma ISO 27001

La aplicación del cuestionario de requisitos basado en la norma ISO 27001 reveló una situación alarmante en la seguridad física del Laboratorio, evidenciando una brecha significativa entre las salvaguardas actuales y los estándares internacionales. A través de las fases de planificación y verificación descritas en el capítulo IV, se determinó que el laboratorio carece de mecanismos para controlar el acceso, como sistemas biométricos, de tarjetas o videovigilancia. Los resultados generales muestran un nivel de riesgo alarmante

del 74% frente a un escaso 26% de seguridad, lo que resalta la vulnerabilidad y la urgencia de implementar las salvaguardas propuestas en el marco del ciclo PDCA.

En cuanto a la identificación detallada de amenazas, la evaluación arrojó que los riesgos de "Malware" y "Daño de equipos" son los de riego más alto, que entran en el nivel de "Muy Graves", estas se dan ya que no se hace un debido mantenimiento. Asimismo, se identificaron deficiencias graves en la protección ambiental, como la ausencia de detectores de humo y extintores, así también una alta vulnerabilidad ante robos. Estos hallazgos, sustentados en la matriz de riesgos y la observación de campo, confirman que la infraestructura actual no cumple con los requisitos de seguridad física necesarios para garantizar la continuidad de las actividades académicas.

### 3.6.4 Presentación y descripción de los resultados obtenidos

Los resultados obtenidos evidencian que la seguridad física del laboratorio presenta deficiencias significativas. En la encuesta, la mayoría de los estudiantes indicó desconocer el estado técnico de los equipos, aunque un porcentaje menor reconoció fallas frecuentes, lo que refleja falta de mantenimiento y comunicación institucional. Además, se percibe ausencia de medidas de seguridad física, como cerraduras y cámaras, y una baja preparación ante riesgos como robos o desastres naturales. Por otro lado, la entrevista al docente responsable confirmó que el laboratorio se encuentra en desuso, sin mantenimiento ni controles de acceso, y que los equipos han cumplido su vida útil. Estos hallazgos coinciden en la necesidad urgente de implementar acciones correctivas para garantizar la funcionalidad y seguridad del espacio.

### 3.6.5 Informe final del análisis de los datos

Una de las principales causas del problema identificado fue el deterioro de los equipos tecnológicos por falta de mantenimiento, lo cual ha generado fallas constantes en el laboratorio.

Los resultados obtenidos de la aplicación de la encuesta dieron a conocer el desconocimiento de parte de los estudiantes hacia el tema de la condición actual del estado del laboratorio, todo eso nos lleva a pensar, además se sienten inseguros en su espacio académico y piensan que la infraestructura no cumple con lo necesario para soportar algún evento de origen natural. La entrevista complementa los resultados y el docente responsable nos manifestó que el laboratorio actualmente no está en uso debido a que los equipos han alcanzado el final de su vida útil y necesitarían ser remplazados, reafirmando así la necesidad de implementar medidas correctivas para dar mejor funcionamiento y rendimiento.

# Capítulo IV

## 4 Marco propositivo

El presente capítulo desarrolla la propuesta de implementación de un Plan de Seguridad Física, orientado a fortalecer la protección integral de los activos tecnológicos, la infraestructura y los procesos operativos del Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí. Esta propuesta surge como respuesta a las vulnerabilidades detectadas durante el diagnóstico situacional y el análisis de riesgos, aplicando metodologías reconocidas internacionalmente para la gestión de seguridad de la información.

La problemática planteada se evidencia en los capítulos anteriores mediante la aplicación de los instrumentos, por ello se plantea el uso de las normas ISO 27001, 27002 y metodologías como PDCA, los cuales además de poder trabajar juntos nos dan una guía completa para una correcta gestión de riesgos. Además, garantiza la integridad y disponibilidad de la información para los estudiantes.

En este capítulo se plantea detallar los recursos tanto económicos, humanos y tecnológicos usados en la implementación del proyecto, también se distribuye los roles con sus responsabilidades en el proyecto, para a continuación llevar a cabo cada una de las etapas de la metodología planteada.

Así mismo, se presenta la propuesta de implementación basada en el ciclo de mejora continua (PDCA), que permitió evaluar los resultados obtenidos y aplicar acciones correctivas y preventivas. Este enfoque asegura que la seguridad física del laboratorio no sea un proceso estático, sino dinámico y adaptable a nuevas amenazas, contribuyendo al fortalecimiento de la infraestructura tecnológica y al cumplimiento de los estándares

internacionales. Entre las cuales encontramos la etapa de planificar, donde se plantea el pan de la auditoria. La etapa de hacer, donde se efectúa el cuestionario de cumplimiento y análisis de entorno. La etapa de verificar, donde se identifican riesgos y se hace la matriz. Finalmente, la etapa actuar, donde se calcula el impacto y se interpreta los riesgos.

## 4.1 Introducción a la propuesta

La propuesta que se presenta en el siguiente capítulo surge como respuesta a diversos hallazgos identificados en auditorías aplicadas en laboratorios que presentan deficiencias significativas en cuanto a la seguridad física. Durante estos procesos se han detectado riesgos que abarcan desde accesos no controlados, ausencia de sistemas de monitoreo, hasta incidentes relacionados con factores ambientales y la falta de controles eléctricos adecuados. Cada una de las situaciones detectadas constituye un riesgo relevante para la integridad de los equipos y para la continuidad operativa del laboratorio, afectando directamente la calidad, disponibilidad y confiabilidad de los servicios tecnológicos que allí se prestan.

Estas vulnerabilidades no solo comprometen los recursos físicos, sino también la información y los procesos académicos que dependen del adecuado funcionamiento del laboratorio.

Se hace evidente la necesidad de implementar medidas para reforzar la seguridad física, para asegurar que el entorno que rodea los equipos sea seguro para los mismos y para quienes hacen uso del espacio. Así si existe un evento inesperado se tenga controles y procedimientos organizados que permitan disminuir estas las amenazas.

Asegurar condiciones apropiadas para la protección de las instalaciones del Laboratorio de la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen es el objetivo principal al que se quiere llegar. Para lograrlo, la aplicación de buenas prácticas es parte fundamental y estas deben estar basadas en las normativas ya propuestas, las cuales sirvieron como guía para la implementación de control efectivos. Con ello, se busca garantizar la continuidad de las actividades, contribuyendo al desarrollo académico de los estudiantes.

## 4.2 Identificación de recursos necesarios:

Para continuar con la propuesta orientada a la mejora de la seguridad física del laboratorio de idiomas de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen se identificaron los diferentes recursos humanos, tecnológicos y económicos utilizados durante todo el proceso de auditoria informática. Para ello se ubica la clasificación de estos elementos con la finalidad de garantizar la viabilidad operativa y financiera, para lo cual se detallan los siguientes recursos:

### 4.2.1 Recursos Humanos

Estos recursos hacen referencia a todas las personas que participaron sea de forma directa o indirecta dentro del proceso de auditoría, mediante el aporte de conocimientos técnicos, asesorías o apoyo dentro de la recopilación de la información. Con la ayuda de los actores se pudo realizar un diagnóstico real que sirvió para la construcción de la propuesta.

**Tabla 4**

*Roles, recursos humanos*

| Rol | Responsabilidades |
|---|---|
| **Autora** | Ejecución de la auditoría, recolección de datos, análisis de riesgos y elaboración del informe final. |
| **Coordinador de Inglés** | Da información técnica sobre el laboratorio y respuesta a la entrevista aplicada. |
| **Tutor de Proyecto** | Asesoría técnica, revisión de los instrumentos de investigación y guía metodológica. |
| **Estudiantes de Inglés** | Dan su participación en encuestas realizadas para evaluar la seguridad y estado de los equipos. |

### 4.2.2 Recursos Tecnológicos

Los recursos tecnológicos corresponden a los equipos y herramientas digitales que permitieron ejecutar un análisis de evidencias, generar documentación y elaborar informes que son de apoyo para el desarrollo de la auditoria informática de la seguridad física.

**Tabla 5**

*Equipo tecnológico*

| Equipo | Función |
|---|---|
| **Hardware** | Equipos de cómputo utilizados para la tabulación de datos y redacción del proyecto. |
| **Internet** | Herramientas indispensables para la investigación. |
| **Cuestionarios Forms** | Instrumentos estructurados de google para la recolección de datos. |
| **Paquete de Office** | Necesario para realizar el documento y cálculos de los resultados. |

### 4.2.3 Recursos Económicos

Estos recursos son los diversos costos asociados que se encuentran estrechamente relacionados a los costos de operación de los equipos tecnológicos junto con los materiales que se consideran necesarios para tareas como la elaboración de informes. Los valores representan una forma en la que los recursos han sido utilizados, sea de manera directa o indirecta durante todo el proceso de investigación e implementación de la propuesta.

**Tabla 6**

*Recursos Económicos*

| Cantidad | Descripción | Costo Unitario | Sub total |
|---|---|---|---|
| **60** | Transporte | $1,00 | $60 |
| **1** | Computadora | $600 | $600 |
| **1** | Impresión | $50 | $50 |
| **6 meses** | Internet | $22 | $132 |
| **1** | Gastos varios | $50 | $50 |
| | | **Valor Total** | $892 |

## 4.3 Descripción técnica de la propuesta de seguridad informática

La siguiente propuesta está orientada a la implementación de una auditoria informática para seguridad física en el laboratorio de idiomas de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, basado en controles preventivos y correctivos orientados a la mejora de los mecanismos de protección tales como accesos no autorizados, incidentes ambientales, fallos eléctricos y riesgos operativos.

Esto debido a que por falta de mantenimiento y de actualizaciones le Software con el cual se trabajaba o dependía las consolas para la realización de actividades tales como listenning y Reading dejo de funcionar, al ocurrir este suceso no se pudo recuperar los datos ya guardado o en este caso el respaldo. También debido a la falta de limpieza o aseo al aula o laboratorio, los equipos y muebles se vieron afectado por el polvo, ocasionando así su deterioro rápidamente.

La propuesta consiste en diseñar un plan de mejora a la seguridad física ya que esto factores representan amenazas significativas que pueden ocasionar pérdida de información,

interrupción de actividades académicas y deterioro de equipos, por lo que se requiere una intervención integral basada en buenas prácticas y estándares internacionales como ISO/IEC 27001 y lineamientos de auditoría informática.

Para ello se plantean diferentes soluciones efectivas que incluyen:

- Gestión del control de acceso al laboratorio.
- Implementación de UPS y reguladores de voltaje para protección eléctrica.
- Equipamiento de señaléticas de seguridad y normativas a seguir dentro del laboratorio.
- Registros que lleven el inventario con etiquetado de activos que posee el laboratorio.
- Instancia de procedimientos de emergencia ante desastres como incendios o inundaciones.

Además, ya que la mayoría de estudiantes han desconocido y desconocen de las políticas se plantea integración de mecanismos de supervisión, implementación de protocolos y políticas de seguridad, además de auditoría continua, con el fin de evaluar periódicamente el cumplimiento de los controles implementados y realizar ajustes cuando sea necesario. Con esto se asegura que las medidas preventivas que se implementaron no solo den resultados a corto plazo, sino que se puedan adaptar a las nuevas amenazas que aparecen y a los constantes cambios que se generan en la infraestructura y equipos.

El objetivo a futuro es disminuir los riegos que traen los activos tecnológicos y toda la infraestructura que trae detrás, generando un entorno confiable para el desarrollo de las actividades académicas de los estudiantes de la universidad.

### 4.4 Clasificación de recursos para implementación:

Para la implementación de la propuesta se requieren diferentes recursos distribuidos en diferentes áreas, estas son:

### 4.4.1 Recursos humanos y roles de responsabilidad

Los recursos humanos hacen referencia a todas las personas que participaron de manera directa e indirecta en el desarrollo del proceso de auditoría informática y en la formulación de la propuesta orientada al fortalecimiento de la seguridad física del Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen.

El factor humano es indispensable, pues hace posible muchas de las tareas como por ejemplo la recopilación de datos, además aporta experiencia y apoyo en la aplicación de los instrumentos de recolección de datos. Por eso gracias al trabajo coordinado entre los diferentes implicados en este estudio, se obtuvo una visión completa de la situación del laboratorio, facilitando la identificación de riesgos.

La participación de los roles involucrados dio una idea más clara de la situación actual, que sirvió como base para el planteamiento de una propuesta acorde a las necesidades. Este trabajo en conjunto permitió identificar riesgos como por ejemplo los accesos no autorizados, fallas eléctricas y amenazas ambientales que pueden existir en el cantón.

**Tabla 7**

*Recursos Humanos y Responsabilidades.*

| Cantidad | Recursos | Función |
|---|---|---|
| **1** | Wladimir Minaya, Mg. | Tutor del Proyecto de Titulación |
| **1** | Ing. Román Loor Michael | Docente y encargado de Ingles. |
| **50** | Estudiantes de la ULEAM | Colaboradores en la realización de recolección de datos como lo fue la encuesta. |
| **1** | Castro Julexy | Auditora. |

### 4.4.2 Recursos tecnológicos e infraestructura

Los recursos tecnológicos corresponden al conjunto de equipos y herramientas digitales que hicieron posible la ejecución del proceso de auditoría informática y la formulación de la propuesta orientada al fortalecimiento de la seguridad física del Laboratorio Multimedia de Idiomas. Estos recursos permitieron organizar y analizar la información recopilada, así como reunir las evidencias necesarias para respaldar el desarrollo del estudio y la elaboración de la documentación técnica correspondiente.

En este apartado se incluyen los equipos de cómputo que fueron utilizados dentro del laboratorio. De igual manera, se emplearon herramientas digitales para la redacción del informe final y la estructuración de la propuesta, cumpliendo con los lineamientos académicos y técnicos establecidos.

La correcta utilización de los recursos tecnológicos contribuyó a detectar vulnerabilidades, riesgos y falencias relacionadas con la seguridad física, además de apoyar el planteamiento de soluciones acordes a las normativas internacionales de seguridad de la información. Gracias a ello, se logró formular una propuesta integral orientada a la protección de los activos tecnológicos y la continuidad operativa del laboratorio.

**Tabla 8**

*Recursos Tecnológicos Utilizados***.**

| Cantidad | Recurso |
|---|---|
| **1** | Portátil HP Intel Inside, con 4GB. |
| **1** | Celular Infinix almacenamiento de 256 GB y 16 de RAM. Con cámara de 48Mp. |
| **1** | Paquete de Microsoft Office |
| **12 meses** | Internet |

### 4.4.3 Recursos económicos y presupuesto requerido

Los recursos económicos comprenden los costos asociados al desarrollo de la auditoría informática y a la implementación de la propuesta orientada al fortalecimiento de la seguridad física del Laboratorio. Además, se especifica costos relacionados a la compra de dispositivos para protección eléctrica, sistemas de control de acceso, señaléticas de seguridad y herramientas tecnológicas necesarias para proteger los equipos del laboratorio, prevenir accidentes y asegurar la continuidad.

La identificación de estos costos permite analizar la viabilidad del proyecto y garantizar que las acciones propuestas puedan ejecutarse de manera realista y sostenible dentro de la ULEM, Extensión El Carmen. Una planificación financiera adecuada contribuye a que las medidas de seguridad se implementen sin afectar la operatividad institucional, fortaleciendo la infraestructura tecnológica y protegiendo los activos físicos del laboratorio.

**Tabla 9**

*Recurso Económicos y presupuesto requerido.*

| Cantidad | Descripción | Precio Unitario | Subtotal |
|---|---|---|---|
| **1** | Portátil Hp Intel Inside | $ 280,00 | $ 280,00 |
| **1** | Celular marca Infinix | $ 180,00 | $ 180,00 |
| **1** | Impresora Epson | $ 300,00 | $ 300,00 |
| **1** | Resma De Papel Bond | $ 5,00 | $ 5,00 |
| | **Total** | | **$ 765,00** |

## 4.5 Etapas de acción para el desarrollo de la propuesta:

### 4.5.1 FASE I (PLANIFICAR).

#### 4.5.1.1 Programa de Auditoría

**Tabla 10**

*Programa de Auditoría*

| **Programa de auditoría informática a la seguridad física del laboratorio multimedia de idiomas universidad laica Eloy Alfaro De Manabí El Carmen (ULEAM).** |
|---|

**Objetivos**

1. Identificar los principales riesgos físicos que afectan la integridad de los activos informáticos del Laboratorio Multimedia.
2. Evaluar el nivel actual de cumplimiento de las normas ISO/IEC 27001 e ISO/IEC 27002 relacionadas con la seguridad física y ambiental.

| **Técnicas y procedimientos** | **Referencia a papel de trabajo** | **Fecha** |
|---|---|---|
| 4.5.2.1 Elaborar cuestionario de Requisitos según Normas ISO 27001 | C1 | 08/10/2025 |
| 4.5.4.1 Elaborar Cuestionarios de Identificación de Riesgos | C2 | 20/10/2025 |
| 4.5.4.1 Responder el cuestionario | C2 | 23/10/2025 |
| 4.5.4.1 Entrevista a encargado para llenar cuestionario. | C1 | 23/10/2025 |

| | | |
|---|---|---|
| 4.5.4.1.3 Identificación de Riesgo. | R1 | 30/10/2025 |
| 4.5.4.1.4 Valoración de riesgo | R2 | 10/11/2025 |
| 4.5.5.1 Calcular impacto | R3 | 15/11/2025 |
| 5.4.1 Calcular nivel de seguridad | | 18/11/2025 |
| Elaborar plan de contramedida | | 28/01/2026 |

| | |
|---|---|
| **Elaborado por:**<br>• Castro Alava Julexy Jamileth | **Revisado por:**<br>Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>06/10/2025 | **Firma**: |

### 4.5.1.2 Plan de auditoria Informática Modelo PDCA

El plan de auditoría informática basado en el modelo PDCA (Planificar, Hacer, Verificar y Actuar) establece una metodología cíclica que garantiza la mejora continua en los procesos de seguridad física y operativa del laboratorio. Este enfoque busca que las actividades de auditoría no se realicen de manera aislada, sino que formen parte de un proceso continuo de revisión, mejora y control de la seguridad física.

Durante la etapa de Planificación se establecen los objetivos de la auditoría, el alcance del análisis y los criterios de evaluación, además de definir los recursos humanos, tecnológicos y económicos necesarios, el cronograma de trabajo y los indicadores que permitieron medir los resultados obtenidos.

Durante la etapa de Hacer, se ejecutan las actividades programadas, aplicando los instrumentos de evaluación previamente diseñados. En esta fase se lleva a cabo la recopilación de evidencias, inspección física del laboratorio, revisión de controles existentes y levantamiento de información sobre riesgos potenciales. Siempre tomando de guía los que establece la norma guía que tomo el proyecto.

Está etapa de Verificar evalúa los resultados obtenidos para posteriormente compararlos con los procesos actuales con lo que se pudo encontrar falencias o amenazas directas a la seguridad física. Como resultado de este proceso, se genera un informe que evidencia el nivel de cumplimiento alcanzado, permitiendo determinar su efectividad.

En la fase de Actuar se definen acciones correctivas y preventivas dirigidas a mejorar la seguridad física y operativa del laboratorio, las cuales incluyen la aplicación de nuevos controles, la actualización de procedimientos y la capacitación del personal involucrado. Asimismo, se establece un sistema de seguimiento que permite mantener las mejoras en el tiempo y asegurar la continuidad del ciclo PDCA frente a posibles nuevas amenazas.

La aplicación de este modelo contribuye a optimizar la seguridad del laboratorio y a fortalecer una cultura institucional enfocada en la prevención y el cumplimiento de estándares internacionales de seguridad de la información.

**Tabla 11**

*Modelo PDCA (Fases de la ISO/IEC 27002).*

| FASE | ACTIVIDADES | INSTRUMENTOS/CONTROLES |
|---|---|---|
| **Planificar** | Identificación de riesgos, análisis de vulnerabilidades, revisión ISO/PDCA | Planificar auditoria y fases a seguir. |
| **Hacer** | Diseño de controles físicos e implementación | Implementación Controles físicos ISO 27002 (accesos, CCTV, inventario, incendios, etc.) |
| **Verificar** | Ejecución de auditoría, verificación de controles, inspección | Cuestionarios ISO 27001 / 27002 / PDCA y Matriz de Riesgo. |
| **Actuar** | Mejora continua, KPIs, ajustes | Indicadores de monitoreo, análisis de incidentes |

#### 4.5.1.3 Revisión de la norma ISO/IEC 27002 para contextualizar los controles físicos aplicables.

La norma ISO/IEC 27002 establece un conjunto de controles de seguridad de la información organizados en cuatro dominios: organizativos, de personas, tecnológicos y físicos. En el contexto del Laboratorio Multimedia de Idiomas de la ULEAM, los controles físicos son especialmente relevantes, ya que están orientados a proteger los activos tecnológicos frente a accesos no autorizados, daños ambientales y otras amenazas que puedan comprometer la integridad de la infraestructura y la continuidad operativa.

La norma ISO 27002 en su sección 7 contempla medidas para proteger las instalaciones, controlando el acceso no deseado y anticipando posibles amenazas que podrían llegar a afectar la seguridad de los equipos. Para llevarlo a cabo se usaron medidas como zonas seguras, acceso biométrico, instalación de cámaras y protocolos ante emergencias.

Al tomar estas medidas en el laboratorio nos permite tener un panorama claro y un paso firme en la gestión de la seguridad física, al estar estás alineadas la guía expuesta por las normas asegura un mejor manejo, ya que la misma recalca que es importante tomar medidas preventivas en conjunto y con supervisión constante.

De esta manera, la revisión de la norma ISO 27002 además de incentivar la aplicación de controles preventivos, también evaluar el estado actual e identifica lo que debe ser corregido. De esta manera, se asegura que la propuesta de seguridad física no sea aislada, sino parte de un sistema integral que fortalezca la protección de los activos tecnológicos y contribuya a la mejora continua en la gestión de la seguridad de la información.

**Tabla 12**

*Control Físicos Norma Mediante ISO/IEC 27002*

| ÍTEMS # | NOMBRE | DESCRIPCIÓN |
|---|---|---|
| **7.1** | **Perímetros de seguridad física.** | Delimitación de zonas seguras para restringir el acceso a áreas donde se almacenan o procesan datos sensibles. |
| **7.2** | **Control de entrada física.** | Implementación de sistemas que regulen el acceso a las instalaciones, como tarjetas de identificación, lectores biométricos o vigilancia. |
| **7.3** | **Seguridad de oficinas, salas e instalaciones.** | Diseño de espacios físicos que minimicen el riesgo de intrusión o daño a los activos. |
| **7.4** | **Supervisión de la seguridad física.** | Monitoreo continuo mediante cámaras y sistemas de registro para detectar accesos no autorizados. |
| **7.5** | **Protección contra amenazas físicas y ambientales.** | Medidas contra incendios, inundaciones, terremotos y sabotajes. |
| **7.6** | **Trabajo en áreas seguras.** | Control del personal que opera en zonas críticas, asegurando que solo personas autorizadas tengan acceso. |
| **7.7** | **Política de escritorio y pantalla despejados.** | Buenas prácticas para evitar la exposición de información sensible cuando los equipos no están en uso. |

### 4.5.2 FASE II (HACER)

#### 4.5.2.1 Cuestionario para el cumplimiento de requisito (Instrumento utilizado.)

El cuestionario para el cumplimiento de requisitos es un instrumento fundamental dentro del proceso de auditoría informática, ya que permite evaluar de manera estructurada el grado de conformidad con los controles establecidos en la norma ISO/IEC 27002. Este cuestionario se diseña con preguntas específicas orientadas a verificar si las políticas, procedimientos y medidas implementadas en el laboratorio cumplen con los estándares de seguridad física y lógica. Su aplicación facilita la obtención de información clara y objetiva, que posteriormente se traduce en indicadores de cumplimiento. Gracias a esta herramienta, es posible identificar fortalezas, detectar áreas críticas y proponer acciones correctivas que contribuyan a la mejora continua. Además, el cuestionario sirve como evidencia documental del proceso de auditoría, asegurando que la evaluación se realice bajo criterios uniformes y medibles.

A continuación, se detalla los cuestionarios y la metodología utilizadas, también de cual punto nos basamos para realizar cada pregunta:

**Tabla 13**

*Cuestionario de Requisito Según Normas ISO 27001 (Planificación).*

| **Cuestionario para el cumplimiento de requisito según normas ISO 27001 para el Laboratorio de Multimedios de la ULEAM** | | | | **C1 página 1-3** |
|---|---|---|---|---|
| **Requisito** | | **Preguntas** | **Cumplimiento** | **Observación** |
| **6. Planificación** | **6.1 Evaluación de riesgos** | ¿Se han identificado los riesgos físicos que pueden afectar la seguridad de la información en el laboratorio multimedia? | No Cumple | Se identificaron riesgos, pero no existía un proceso formal previo. |
| | | ¿Se ha realizado un análisis de impacto para determinar las consecuencias de los riesgos identificados? | No Cumple | No existía un análisis de impacto documentado antes de la auditoría. |
| | **6.1.3 Tratamiento de riesgos** | ¿Se han definido criterios para evaluar la probabilidad y el impacto de cada riesgo? | No Cumple | Se utilizaron criterios proporcionados por la auditoría. |
| | | ¿Existe un plan documentado para tratar los riesgos físicos detectados? | No Cumple | La auditoría propone un plan de contramedidas en anexos. |
| | | ¿Se han definido controles específicos para mitigar los riesgos más críticos? | No Cumple | No existen controles documentados ni implementados |
| | **6.2 Objetivos de seguridad de la información** | ¿Se han establecido objetivos claros para mejorar la seguridad física del laboratorio multimedia? | No Cumple | No existen objetivos de seguridad establecidos por la institución para el laboratorio |
| | | ¿Están alineados estos objetivos con la política institucional y los requisitos legales? | Si Cumple | |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por**: Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 08/10/2025 | | | **Firma:** | |

**Tabla 14**

*Cuestionario De Requisito Según Normas ISO 27002 (Controles Físicos).*

| **Cuestionario para el cumplimiento de requisito según normas ISO 27002 para el Laboratorio de Multimedia de la ULEAM** | | | | **C1 página 2-3** |
|---|---|---|---|---|
| **Requisito** | | **Preguntas** | **Cumplimiento** | **Observaciones** |
| **7. Controles Físicos** | **7.2 Control de entrada física** | ¿Existen mecanismos para controlar el acceso físico al laboratorio multimedia? | No Cumple | No hay controles de acceso; las puertas y ventanas no cuentan con cerraduras seguras. |
| | | ¿Se utilizan credenciales, tarjetas o sistemas biométricos para el ingreso? | No Cumple | No existe ningún sistema de identificación, registro o credencial para ingresar. |
| | | ¿Hay personal encargado de supervisar el acceso? | Si Cumple | El docente que está a cargo según el horario. |
| | **7.4 Supervisión de la seguridad física** | ¿El laboratorio cuenta con cámaras de video vigilancia instaladas? | No Cumple | No existe sistema de vigilancia. |
| | | ¿Se realiza monitoreo activo de las grabaciones? | No Cumple | No hay cámaras. |
| | | ¿Existe registro histórico de accesos y eventos? | No Cumple | No se lleva registro de ingreso al laboratorio. |
| | | ¿Se cuenta con sistemas contra incendios (extintores, alarmas)? | No Cumple | No hay extintores, ni alarmas. |
| | **7.5 Protección contra amenazas físicas y ambientales** | ¿Están alineados estos objetivos con la política institucional y los requisitos legales? | Si Cumple | |
| | | ¿Existen medidas para prevenir daños por inundaciones o fallos eléctricos? | No Cumple | No hay drenaje, canaletas, ni protección del cableado. |
| | | ¿Hay protocolos de respuesta ante desastres naturales? | Si Cumple | |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 08/10/2025 | | | **Firma:** | |

**Tabla 15**

*Cuestionario para el cumplimiento de requisito según metodología* PDCA.

| **Cuestionario para el cumplimiento de requisito según METODOLOGIA PDCA para el Laboratorio de Multimedia de la ULEAM** | | | | **C1 página 3-3** |
|---|---|---|---|---|
| **Requisitos** | | **Preguntas** | **Cumplimientos** | **Observaciones** |
| **Gestión de riesgos & PDCA – Identificación de activos** | **APO12 Gestión de riesgos** | ¿Existe un procedimiento documentado para gestionar riesgos físicos y tecnológicos en el laboratorio? | No Cumple | No existe un procedimiento formal, manual o política institucional. |
| | | ¿Se realizan evaluaciones periódicas de riesgos? | No Cumple | No hay evidencia de evaluaciones periódicas; la auditoría fue el primer diagnóstico formal realizado. |
| | | ¿Se asignan responsables para la mitigación de riesgos? | No Cumple | No hay personal asignado oficialmente como responsable de gestionar riesgos o activar medidas preventivas. |
| | **Identificación de activos** | ¿Se cuenta con un inventario actualizado de los activos físicos y tecnológicos del laboratorio multimedia? | No Cumple | No cuenta con inventarios. |
| | | ¿Se han clasificado los activos según su criticidad? | No Cumple | No existe una clasificación basada en criticidad, valor, impacto o confidencialidad. |
| | | ¿Se han identificado las amenazas que pueden afectar cada activo? | No Cumple | Las amenazas no fueron identificadas previamente. |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 08/10/2025 | | | **Firma:** | |

### 4.5.3 Análisis del entorno y riesgos en el laboratorio

El análisis del entorno del Laboratorio de Multimedia de la ULEAM permite comprender las condiciones físicas, operativas y organizacionales que influyen directamente en el nivel de seguridad del área. Este laboratorio constituye un espacio académico donde estudiantes y docentes acceden a equipos informáticos, software especializado y recursos digitales esenciales para el desarrollo de actividades educativas, por lo que su protección resulta fundamental para evitar interrupciones, pérdidas de información o afectaciones a los activos institucionales.

Al verlo desde el punto de vista de equipo físico, el laboratorio requiere de una revisión detallada de sus características estructurales como los accesos principales sin mecanismos de control avanzado, áreas que son potencialmente vulnerables a intrusiones de seguridad, ausencia de perímetros seguros y limitaciones en cuanto a la supervisión.

Este análisis preliminar evidencia que el laboratorio requiere de la implementación de controles de seguridad física que estén alineados con normas como la ISO/IEC 27001 e ISO/IEC 27002, además del soporte de diferentes marcos de gestión de riesgos como PDCA, todo por la oportunidad de reducir la vulnerabilidad del laboratorio y optimizar los procesos de control y protección integral de todos los activos institucionales.

Por tal motivo, se procede a describir cada elemento que ha sido evaluado y ponderado, los cuáles pueden ser útiles para elaborar una base de vulnerabilidades, oportunidades de mejora y diferentes acciones correctivas que permitan fortalecer la seguridad física del laboratorio.

#### 4.5.3.1 Interpretación General de los Cuestionarios.

De la revisión conjunta de los instrumentos aplicados conforme a las normas ISO 27001, ISO 27002 y la metodología PDCA, se advierte un panorama en el cual el Laboratorio Multimedia se halla desprovisto de los mecanismos formales que exige una adecuada gestión de seguridad. Las prácticas observadas no guardan relación con los principios de planificación, control y mejora continua que dichas normas establecen como fundamento indispensable para la protección de los activos institucionales, en el primer cuestionario se identificó que:

- No existía un proceso formal de identificación de riesgos.
- No se habían realizado análisis de impacto.
- No existían criterios documentados para evaluar probabilidad e impacto.
- No se dispone de un plan documentado de tratamiento de riesgos.
- No existían objetivos institucionales para mejorar la seguridad física.

Esto refleja que el laboratorio opera sin una estructura formal de gestión de seguridad, lo cual incrementa el riesgo y dificulta la implementación de acciones preventivas.

En el segundo cuestionario, se evidenció que:

- No hay ningún mecanismo de control de acceso físico.
- No existen cámaras de vigilancia ni supervisión del entorno.
- No se llevan registros de accesos o eventos.
- No hay medidas contra incendios (extintores, alarmas, señalización).
- Existen riesgos ambientales como filtraciones, cableado deteriorado y falta de drenaje.

- No existen protocolos para emergencias naturales o fallas eléctricas.

De acuerdo con la norma ISO/IEC 27002, estas condiciones representan vulnerabilidades críticas que pueden afectar la disponibilidad, integridad y seguridad de los activos tecnológicos.

os resultados muestran que el laboratorio no aplica el ciclo de mejora continua PDCA, debido a la ausencia total de documentación, control y seguimiento.

- Los principales hallazgos indican que:
- No existe un procedimiento para gestionar riesgos.
- No se realizan evaluaciones periódicas.
- No hay responsables designados para la mitigación.
- No hay inventario actualizado de activos.
- No existe clasificación de activos según criticidad.
- Las amenazas no habían sido identificadas previamente.

La ausencia de estos elementos impide que el laboratorio pueda mantener un sistema de gestión de seguridad estable, verificable y mejorable.

**Tabla 16**

*Cumplimiento De Políticas Y Requisitos De Seguridad ISO.*

| ÉSTANDAR | CUMPLIMIENTO | INCUMPLIMIENTO |
|---|---|---|
| **ISO 27001** | 14% | 86% |
| **ISO 27002** | 27% | 73% |

### 4.5.4 FASE III VERIFICAR.

#### 4.5.4.1 Introducción a los cuestionarios de riesgos físicos y lógicos

Como parte del proceso de auditoría informática orientada a la seguridad física del Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí, se diseñaron cuestionarios específicos para evaluar el nivel de exposición frente a riesgos críticos que pueden afectar la integridad de los equipos y la continuidad operativa. Estos cuestionarios abordan amenazas como robo de equipos, daños por manipulación inadecuada, incendios, inundaciones y ataques por malware, las cuales fueron identificadas durante el diagnóstico inicial como factores de alto impacto en la infraestructura tecnológica.

Los cuestionarios permitieron obtener información real sobre el estado actual del laboratorio, además identificar el tipo de prácticas realizadas por los usuarios y el análisis de las medidas preventivas. A partir de esta información, se logró identificar las vulnerabilidades y tomar datos de base para tomar medidas preventivas.

La temática de los cuestionarios se basó en riesgos prioritarios que pueden afectar la seguridad y disponibilidad de los activos tecnológicos en el laboratorio. Sobresalen riesgos como robos, incendios o inundaciones que son los que tienen mayor probabilidad y pueden provocar pérdidas considerables, por otro lado, están las amenazas lógicas, como el malware, que pueden llegar a generar daños en los equipos y perdida de información. Analizar esto permite plantear una propuesta que considere la protección física y la prevención de riesgos.

Claro que se basan en la norma ISO 27002, la cual establece controles para la gestión de la seguridad de la información tanto para personas, como en lo tecnológicos y lo físico. En este caso, se priorizan los controles del apartado 7 (seguridad física) y del apartado 8 (protección tecnológica), asegurando que las preguntas estén alineadas con estándares

internacionales y que los resultados permitan implementar medidas efectivas para la mejora continua.

#### *4.5.4.1.1 Cuestionario de riesgo:*

A continuación, se presentan los cuestionarios utilizados para evaluar los riesgos que pueden afectar la seguridad física y operativa del Laboratorio Multimedia de Idiomas de la ULEAM. El objetivo principal de la aplicación de los cuestionarios es detectar posibles amenazas que puedan poner en riesgo los activos tecnológicos del Laboratorio, evitar la pérdida de la información y dar continuidad académica.

En el cuestionario se contemplan posibles riesgos que han tenido antecedentes como lo son los robos, incendios, inundaciones, daños en los equipos y ataques de malware. Atreves del mismo nos dio una vista real de la situación actual por la que pasa el laboratorio y el tipo de prácticas que se llevan a cabo. Estos cuestionarios fueron aplicados al personal técnico, docente y administrativo, y se complementaron con investigación de campo y observación para obtener información más precisa del entorno.

Toda la información obtenida de su aplicación es un pilar para la construcción de la matriz de riesgos, ya que permite clasificar y priorizar las amenazas según su impacto y probabilidad, sacando de ahí las bases para tomar acciones preventivas que refuercen la seguridad física y lógica del laboratorio.

**Tabla 17**

*Cuestionario de Identificación (Robo).*

| CUESTIONARIO PARA IDENTIFICAR RIESGO ROBO | | | C2 Pág. 1 de 5 | |
|---|---|---|---|---|
| **Preguntas** | **Respuestas** | | **Observación** | **Riesgo** |
| | **Si** | **No** | | |
| 1 ¿Existen controles de acceso físico al laboratorio? | | X | | 0 |
| 2 ¿El laboratorio cuenta con cerraduras seguras en puertas y ventanas? | | X | | 0 |
| 3 ¿Se utiliza algún sistema de identificación para ingresar al laboratorio? | | X | | 0 |
| 4 ¿Hay cámaras de vigilancia funcionando en el área? | | X | | 0 |
| 5 ¿Se registran las entradas y salidas del personal? | | X | | 0 |
| 6 ¿El personal conoce las políticas de acceso? | X | | | 1 |
| 7 ¿Se restringe el acceso a personas no autorizadas? | | X | | 0 |
| 8 ¿Se controla el ingreso de equipos externos? | | X | | 0 |
| 9 ¿Se cuenta con un inventario actualizado de equipos? | X | | | 1 |
| 10 ¿Se realizan auditorías periódicas de los activos? | | X | | 0 |
| 11 ¿Existen protocolos ante intento de robo? | | X | | 1 |
| 12 ¿El laboratorio está ubicado en un área segura? | X | | | 1 |
| 13 ¿Se controla el acceso fuera del horario laboral? | | X | | 0 |
| 14 ¿Se cuenta con seguro contra robo? | X | | | 1 |
| 15 ¿Se revisan periódicamente los sistemas de seguridad? | X | | | 1 |
| 16 ¿Los cables están ordenados y accesibles desde zonas externas? | | X | | 0 |
| 17 ¿Las ventanas permiten ingreso desde el exterior? | X | | | 0 |
| 18 ¿Los escritorios están alineados y sin daños visibles? | X | | | 1 |
| 19 ¿Los equipos presentan faltantes de piezas o conexiones? | | X | | 1 |
| 20 ¿Se observan elementos ajenos al ambiente educativo en el laboratorio? | | X | | 1 |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 20-23/10/2025 | | | **Firma:** | |

**Tabla 18**

*Cuestionario de Identificación de Riesgo (Incendio).*

| **CUESTIONARIO PARA IDENTIFICAR IDENTIFICACIÓN DE INCENDIO** | | | | **C2 Pág. 2 de 5** |
|---|---|---|---|---|
| **INCENDIO** | | | | |
| | **Preguntas** | **Respuestas** | | **Observación** | **Riesgo** |
| | | **Si** | **No** | | |
| 1 | ¿El laboratorio cuenta con detectores de humo? | | X | No Hay | 2 |
| 2 | ¿Existen extintores en lugares estratégicos? | - | - | No Hay | 2 |
| 3 | ¿Los cables eléctricos presentan cortes, peladuras o signos de deterioro? | X | | | 0 |
| 4 | ¿Hay señalización de rutas de evacuación? | | X | | 0 |
| 5 | ¿Hay tomacorrientes sobrecargados? | | X | | 1 |
| 6 | ¿Hay carteles visibles con instrucciones ante incendios? | | X | | 0 |
| 7 | ¿Se almacenan papel, químicos u objetos inflamables junto a equipos? | | X | | 1 |
| 8 | ¿Las cortinas, muebles y pisos son de material resistente al fuego? | | X | | 0 |
| 9 | ¿Hay luces de emergencia con carga suficiente? | | X | | 0 |
| 10 | ¿Filtran líquidos del techo hacia instalaciones eléctricas? | X | | | 0 |
| 11 | ¿Están los pasillos y puertas libres de obstáculos? | X | | | 1 |
| 12 | ¿Hay botiquines de primeros auxilios accesibles y completos? | | X | | 0 |
| 13 | ¿Los cables de red y electricidad están diferenciados y ordenados? | | x | | 0 |
| 14 | ¿El tablero eléctrico principal tiene disyuntores y protecciones? | | X | | 0 |
| 15 | ¿Las paredes muestran humedad cerca de enchufes o cables? | X | | | 0 |
| 16 | ¿Hay personal responsable de seguridad contra incendios? | | X | | 0 |
| 17 | ¿Se dispone de un sistema automático de rociadores? | | X | | 0 |
| 18 | ¿La estructura del techo evita filtraciones sobre los equipos? | | X | | 0 |
| 19 | ¿Se revisa la temperatura de equipos críticos? | | x | | 0 |
| 20 | ¿Se cuenta con seguro contra incendios? | X | | | 1 |
| 21 | ¿Se dispone de un botiquín de primeros auxilios? | | x | | 0 |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 20-23/10/2025 | | | | **Firma:** | |

**Tabla 19**

*Cuestionario de Identificación de Riesgo (Daño De Equipo).*

| CUESTIONARIO PARA IDENTIFICAR IDENTIFICACIÓN DE DAÑOS DE EQUIPO | | | | C2 Pág. 3 de 5 | |
|---|---|---|---|---|---|
| DAÑO DE EQUIPO | | | | | |
| | Preguntas | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿Se realiza mantenimiento preventivo a los equipos? | | X | | 0 |
| 2 | ¿Existen protocolos visibles para manipulación segura de equipos? | | X | | 0 |
| 3 | ¿Se capacita al personal estudiantil en uso adecuado de equipos? | | X | | 0 |
| 4 | ¿Se cuenta con manuales de operación visibles? | | X | | 0 |
| 5 | ¿Hay control de temperatura y humedad en el laboratorio? | | X | | 0 |
| 6 | ¿Se revisan periódicamente los equipos? | | X | | 0 |
| 7 | ¿Se documentan fallas y reparaciones? | | X | Se realizaba antiguamente. | 0 |
| 8 | ¿Se cuenta con seguro para equipos? | | X | | 0 |
| 9 | ¿El personal docente recibe capacitación sobre el uso adecuado del laboratorio? | | X | Se hizo al inicio, en la actualidad ya no se realiza | 0 |
| 10 | ¿Se controla el acceso a equipos delicados? | | X | | 0 |
| 11 | ¿Se evita el uso indebido de equipos? | | X | | 0 |
| 12 | ¿Hay protocolos visibles para desconexión segura? | | X | | 0 |
| 13 | ¿Se inspeccionan cables y conexiones? | | X | | 0 |
| 14 | ¿Se controla el polvo y limpieza del área? | | X | | 0 |
| 15 | ¿Se dispone de repuestos básicos? | | X | | 0 |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 20-23/10/2025 | | | | **Firma:** | |

**Tabla 20**

*Cuestionario de Identificación de Riesgo (Inundación).*

| CUESTIONARIO PARA IDENTIFICAR DE INUNDACIÓN | | | | C2 Pág. 4 de 5 | |
|---|---|---|---|---|---|
| | INUNDACIÓN | | | | |
| | Preguntas | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿El laboratorio está ubicado en zona segura contra inundaciones? | X | | | 1 |
| 2 | ¿El piso del laboratorio presenta acumulación de agua? | | X | | 1 |
| 3 | ¿Las puertas sellan correctamente al cerrar? | | X | | 0 |
| 4 | ¿Se drena el agua alrededor del edificio? | | X | | 0 |
| 5 | ¿El techo presenta filtraciones o manchas de humedad? | X | | | 0 |
| 6 | ¿Las ventanas cierran herméticamente? | | X | | 0 |
| 7 | ¿Los equipos están instalados sobre superficies elevadas? | X | | | 1 |
| 8 | ¿Se observan rastros de agua en paredes o esquinas? | X | | | 0 |
| 9 | ¿Los cables están protegidos del contacto con el piso? | | X | | 0 |
| 10 | ¿Hay estructuras externas que protejan del agua? | | X | | 0 |
| 11 | ¿Hay techos con materiales deteriorados? | X | | | 0 |
| 12 | ¿Se almacenan papeles o materiales absorbentes cerca del piso? | | X | | 1 |
| 13 | ¿Hay espacios despejados alrededor de las estaciones de trabajo? | X | | | 1 |
| 14 | ¿Los canalones están obstruidos con hojas o basura? | | X | No Hay | 2 |
| 15 | ¿Los techos cuentan con canaletas funcionales? | | X | | 0 |
| 16 | ¿Los interruptores eléctricos están por encima del nivel del piso? | X | | | 1 |
| 17 | ¿El entorno del edificio permite el drenaje natural del agua? | X | | | 1 |
| 18 | ¿Se observan medidas para proteger equipos durante lluvias? | | X | | 0 |
| 19 | ¿Hay materiales que impidan la evacuación del agua? | | X | | 1 |
| 20 | ¿Las instalaciones se revisan tras eventos de lluvia? | | X | | 0 |

| **Realizado Por:** | **Revisado Por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** | **Firma:** |
| 20-23/10/2025 | |

**Tabla 21**

*Cuestionario de Identificación de Riesgo (Malware).*

| CUESTIONARIO PARA IDENTIFICAR DE MALWARE<br>MALWARE | | | | C2<br>Pág. 5 de 5 |
|---|---|---|---|---|
| | **Preguntas** | **Respuestas** | | **Observación** | **Riesgo** |
| | | **Si** | **No** | | |
| 1 | ¿Se cuenta con software antivirus actualizado? | | X | | 0 |
| 2 | ¿Se realizan análisis periódicos de malware? | | X | | 0 |
| 3 | ¿Se capacita al personal en prevención de malware? | | X | | 0 |
| 4 | ¿Existen políticas visibles para instalación de software? | | X | | 0 |
| 5 | ¿Se controla el uso de dispositivos USB? | | X | | 0 |
| 6 | ¿Se aplican actualizaciones de seguridad en sistemas? | | X | | 0 |
| 7 | ¿Hay protocolos ante detección de malware? | | X | | 0 |
| 8 | ¿Se dispone de firewall activo? | | X | | 0 |
| 9 | ¿Se monitorean las conexiones de red? | | X | | 0 |
| 10 | ¿Se restringe el acceso a sitios web no seguros? | | X | | 0 |
| 11 | ¿Se realizan copias de seguridad periódicas? | | X | | 0 |
| 12 | ¿Se controla el uso de correos electrónicos sospechosos? | | X | | 0 |
| 13 | ¿Se aplican políticas de contraseñas seguras? | | X | | 0 |
| 14 | ¿Se verifica la integridad de archivos descargados? | | X | | 0 |
| 15 | ¿Se documentan incidentes de malware? | | X | | 0 |
| 16 | ¿Se cuenta con herramientas de análisis forense digital? | | X | | 0 |
| 17 | ¿Se restringe el acceso remoto no autorizado? | | X | | 0 |
| 18 | ¿Se aplican pruebas de penetración periódicas? | | X | | 0 |
| 19 | ¿Se controla el uso de software pirata? | | X | | 0 |
| 20 | ¿Se dispone de un plan de respuesta ante ataques? | | X | | 0 |
| **Realizado Por:**<br>Castro Alava Julexy Jamileth | | | | **Revisado Por:**<br>Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:**<br>20-23/10/2025 | | | | **Firma:** | |

#### *4.5.4.1.2 Recolección de datos*

El proceso de recolección de datos se hizo haciendo investigación de campo en la cual mediante observación se logró recolectar información valiosa sobre el entorno en el que se encuentran los equipos y el estado de seguridad real, para complementar y hacer más valiosa la información se hizo uso de técnicas como cuestionario, para a través de la experiencia se puedan identificar amenazas no vistas en primera instancia.

Los puntos clave a llevar una revisión fueron el acceso no permitido al laboratorio, condición física de la infraestructura, ubicación de los equipos y si se están cumpliendo las reglas de seguridad básica en el mismo. Por último, se tomó evidencias con fotografías, para respaldar los documentos y técnicas aplicadas.

El objetivo con el que se estipuló fue hacer la recolección de los datos mediante investigación de campo, para posteriormente realizar una identificación de riesgos que nos ayuda a crear nuestra matriz y dar niveles, que sean la bese de la auditoría.

**Figura 2**

*Techado del laboratorio.*

**Figura 3**

*Parte de la iluminación del techo.*

**Figura 4**

*Escritorio del laboratorio.*

**Figura 5**

*Muebles o Escritorios del laboratorio.*

**Figura 6**

Estructura Física del laboratorio.

**Figura 7**

*Ventanas y Ubicación de RAM.*

**Figura 8**

*Cableado*

**Figura 9**

*Cableado y Escritorios desalojados.*


**Figura 10**

*Puerta de ingreso*

#### 4.5.4.1.3 ***Identificación de Riesgo.***

Para identificar los riesgos, se llevó a cabo un análisis exhaustivo del entorno físico y operativo del laboratorio, considerando tanto las áreas más vulnerables como los activos críticos que podrían verse comprometidos. Este proceso incluyó la revisión de la infraestructura, sistemas de seguridad, condiciones ambientales y procedimientos internos. Se aplicaron cuestionarios y entrevistas dirigidas al personal técnico, docente y administrativo, con el objetivo de conocer las prácticas actuales, el nivel de conciencia sobre la seguridad y las posibles amenazas que enfrentan en su labor diaria.

La observación directa fue utilizada como complemento para la recolección de información, permitiendo identificar situaciones que podrían pasar inadvertidas, como accesos no controlados, almacenamiento incorrecto de los equipos y la ausencia de protocolos frente a eventos de emergencia. A través de esta combinación de metodología se lograron reconocer riesgos asociados al robo, incendios, daños en los equipos por problemas eléctricos, inundaciones y amenazas digitales como el malware.

Esta etapa resultó fundamental para establecer una lista clara y priorizada de riesgos, la cual sirvió como base para la valoración y jerarquización en fases posteriores del análisis. De esta manera, se garantizó que las decisiones futuras se sustentaran en información precisa y contextualizada, contribuyendo a la formulación de estrategias efectivas para la mitigación y control de riesgos.

**Tabla 22**

*Identificaciones de Riesgo (Robo, Incendio, Daño de Equipo, Inundación, Malware).*

| **Identificación de Riesgos** | **R1**<br>**Pág. 1 de 5** |
|---|---|

**Robo debido a:**

- No hay controles de acceso físico.
- No cuenta con cerraduras en puertas y ventanas.
- No hay sistema de identificación.
- No hay cámaras de vigilancia dentro del laboratorio.
- No hay control de ingreso mediante formularios o registros.
- No hay restricciones a personas que no pertenecen tanto a la universidad como a la carrera.
- No hay restricciones de equipos fuera del lugar.
- No se realizan auditorias periódicas.
- No se cuenta con protocolos ante intento de robo.
- No se controla el ingreso fuera del horario laboral.
- Los cables no están ordenados y son accesibles desde zonas internas.
- Las ventanas permiten ingreso desde el exterior.

| | |
|---|---|
| **Realizado por**: | **Revisado por:** |
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** | **Firma:** |
| 30/10/2025 | |

**Tabla 23**

*Identificaciones de Riesgo (Robo, Incendio, Daño de Equipo, Inundación, Malware)*

| Identificación de Riesgos | R1<br>Pág. 2 de 5 |
|---|---|

**Incendio debido a:**

- No hay extintores.
- Los cables eléctricos presentan signos de deterioro.
- Rutas de evacuación sin señalización.
- No hay carteles con instrucciones ante incendios.
- Ventanas con cortinas, muebles y pisos no resistentes al fuego.
- Luz de emergencia sin carga suficiente.
- Se filtra liquido a través del techo.
- No hay botequines de primeros auxilios accesibles y completos.
- Los cables de electricidad no se encuentran diferenciados ni ordenados.
- El tablero principal no cuenta con disyuntores ni protecciones.
- No hay persona responsable de la seguridad contra incendio.
- No hay sistema automático de rociadores.
- La estructura del techo no evita la filtración de agua sobre los equipos.

| **Realizado por**: | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**30/10/2025 | **Firma:** |

**Tabla 24**

*Identificaciones de Riesgo (Robo, Incendio, Daño de Equipo, Inundación, Malware)*

| **Identificación de Riesgos** | **R1**<br>**Pág. 3 de 5** |
|---|---|

**Daño de equipos debido a:**

- No se realiza mantenimiento preventivo a los equipos.
- No existen protocolos visibles para la manipulación de los equipos.
- No se capacita al personal estudiantil en el uso adecuado de los equipos.
- No se cuenta con manuales de operaciones visibles.
- No hay control sobre la temperatura del laboratorio.
- No se revisa periódicamente los equipos.
- No hay capacitación actualmente para los docentes que usan el laboratorio.
- Uso indebido de los equipos.
- No hay inspección de los cables.
- No hay señalización de limpieza alguna.
- No se cuenta con repuestos básicos.

| | |
|---|---|
| **Realizado por**: | **Revisado por:** |
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** 30/10/2025 | **Firma:** |

**Tabla 25**

*Identificaciones de Riesgo (Robo, Incendio, Daño de Equipo, Inundación, Malware)*

| Identificación de Riesgos | R1<br>Pág. 4 de 5 |
|---|---|

**Inundación debido a:**

- La puerta cuenta con un cerrojo defectuoso.
- Los cables no están protegidos por canaletas.
- Falta de drenaje de aguas lluvias en la universidad, se empoza.
- Goteras visibles en el techo lo que causa filtración.
- Ventanas con filtraciones pequeñas ante grandes aguaceros.
- Presencia de humedad en el cielo raso.
- Cables en contacto directo con el piso.
- Oxido y material deteriorado en el techo.
- Falta de altura al piso de los equipos.
- Revisión post lluvias no se hace regularmente.

| | |
|---|---|
| **Realizado por**: Castro Alava Julexy Jamileth | **Revisado por:** Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**30/10/2025 | **Firma:** |

**Tabla 26**

*Identificaciones de Riesgo (Robo, Incendio, Daño de Equipo, Inundación, Malware)*

| Identificación de Riesgos | R1<br>Pág. 5 de 5 |
|---|---|

**Malware debido a:**

- No cuenta con un antivirus completo, ni actualizado.
- No se hace informes de malware periódicas.
- No existen herramientas adecuadas para manejar los ataques malware.
- No hay un protocolo a seguir para instalar software.
- No se controla el uso de dispositivos USB.
- No se hacen las actualizaciones de software.
- No se encuentra activo el firewall en los dispositivos.
- No se lleva control de los movimientos en la red
- No hay un plan de copias de seguridad efectivo.
- No se usa contraseñas con niveles altos de seguridad.
- No se lleva un historial de accidentes de malware.
- No se controla el uso de software pirata en los equipos del laboratorio.
- No hay un plan de respuesta ante algún ataque.

| | |
|---|---|
| **Realizado por**: Castro Alava Julexy Jamileth | **Revisado por:** Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**30/10/2025 | **Firma:** |

#### *4.5.4.1.4 Valoración de Riesgo o Tabulación de Datos.*

Para este paso decidí organizar y analizar la información obtenida durante la recolección, con el propósito de identificar patrones y determinar el nivel de exposición a cada amenaza, fue por ello que se realizó este análisis en el cuestionario en el cual le asignamos el número que representa el riesgo en el área evaluada. Este proceso permite transformar los datos en indicadores claros, asignando valores que reflejen la frecuencia y el impacto potencial de los riesgos. La tabulación facilita la construcción de matrices y gráficos que apoyan la toma de decisiones, asegurando que las conclusiones se basen en evidencia objetiva y verificable.

Además, este paso constituye un puente entre la identificación inicial y la priorización de riesgos, ya que permite jerarquizar las amenazas según su nivel de criticidad, lo que fue clave para definir estrategias de mitigación efectivas en las fases posteriores.

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

**Tabla 27**

*Escala de Evaluación Sobre*

*Cumplimiento de Control*

| | |
|---|---|
| **SI** | **1** |
| **NO** | **0** |
| **NO APLICA** | **2** |

**Tabla 28**

*Valoración de Riesgo 1 (Robo, Incendio, Daño de Equipo, Inundación y Malware).*

| Valoración De Riesgos | R2<br>Pág. 1 de 3 |
|---|---|

| PROBABILIDAD DE ROBO | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 20 | 0 |
| **Total, Seguro** | 9 | 0 |
| **Total, Riesgo** | 11 | 0 |
| **Porcentaje Seguro** | 9*100/20= | 45 % |
| **Porcentaje Riesgo** | 11*100/20= | 55% |

| PROBABILIDAD DE INCENDIO | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 21 | 2 |
| **Total, Seguro** | 4 | 0 |
| **Total, Riesgo** | 15 | 0 |
| **Porcentaje Seguro** | 4*100/19= | 21% |
| **Porcentaje Riesgo** | 15*100/19= | 79% |

| **Realizado por:** | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** | **Firma:** |
| 10/11/2025 | |

**Tabla 29**

*Valoración de riesgos 2*

| Valoración de riesgos | R2<br>Pág. 2 de 3 |
|---|---|

| PROBABILIDAD DE DAÑO DE EQUIPO | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 15 | 0 |
| **Total, Seguro** | 0 | 0 |
| **Total, Riesgo** | 15 | 0 |
| **Porcentaje Seguro** | 0*100/15= | 0% |
| **Porcentaje Riesgo** | 15*100S/15= | 100% |

| PROBABILIDAD DE INUNDACIÓN | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 20 | 1 |
| **Total, Seguro** | 8 | 0 |
| **Total, Riesgo** | 11 | 0 |
| **Porcentaje Seguro** | 8*100/19= | 42% |
| **Porcentaje Riesgo** | 11*100/19= | 58% |

| **Realizado por:** | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** 10/11/2025 | **Firma:** |

**Tabla 30**

*Valoración de riesgos 3*

| Valoración de riesgos | | R2<br>Pág. 3 de 3 |
|---|---|---|
| **PROBABILIDAD DE MALWARE** | | |
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 20 | 0 |
| **Total, Seguro** | 0 | 0 |
| **Total, Riesgo** | 20 | 0 |
| **Porcentaje Seguro** | 0*100/20= | 0% |
| **Porcentaje Riesgo** | 20*100/2= | 100% |

| Riesgo | Porcentaje De Riesgo | Porcentaje De Seguridad |
|---|---|---|
| **Robo** | 55% | 45% |
| **Incendio** | 58% | 42% |
| **Daño de Equipo** | 100% | 0% |
| **Inundación** | 58% | 42% |
| **Malware** | 100% | 0% |

| | |
|---|---|
| **Realizado por:** | **Revisado por:** |
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**10/11/2025 | **Firma:** |

#### *4.5.4.1.5 Matriz de Riesgo.*

La matriz de riesgo también forma parte de nuestra Valoración de Riesgo, constituye una parte esencial dentro del proceso de valoración, ya que permite organizar y analizar los resultados obtenidos tras calcular los porcentajes de riesgo y seguridad identificados en el laboratorio. Este instrumento no solo facilita la representación visual de los riesgos, sino que también ayuda a comprender la relación entre la probabilidad de ocurrencia y el impacto que cada amenaza puede generar sobre los activos tecnológicos y la continuidad operativa.

La matriz de riesgos fue elaborada a partir de los datos recopilados y analizados previamente, asignando valores que representan la frecuencia estimada de cada riesgo y el nivel de afectación que podría ocasionar. En este proceso, la probabilidad indica la posibilidad de que un evento ocurra, mientras que el impacto determina las consecuencias que tendría, permitiendo clasificar los riesgos en categorías como bajo, medio o alto para establecer prioridades de atención.

Este análisis permite contar con una visión estructurada del panorama de riesgos, facilitando la toma de decisiones estratégicas. La matriz sirve como apoyo para la asignación adecuada de recursos, la definición de acciones correctivas y la implementación de medidas preventivas, contribuyendo a mejorar la seguridad del laboratorio y a cumplir con los lineamientos establecidos en la norma ISO/IEC 27002.

**Tabla 31**

*Escala de Valoración Sobre el Nivel de Probabilidades de Riesgo*

| Nivel de aparición | | Nivel de riesgo |
|---|---|---|
| **1** | Mas bajo | 1% - 10% |
| **2** | | 11% - 30% |
| **3** | | 31% - 50% |
| **4** | | 51% - 75% |
| **5** | Mas alto | 76% - 100% |

**Tabla 32**

*Evaluación De Riesgos.*

| Riesgo | Impacto | Probabilidad | Valor de riesgo | |
|---|---|---|---|---|
| **Robo** | 3 | 4 | 12 | **Importante** |
| **Incendio** | 4 | 5 | 20 | **Muy Grave** |
| **Daño de equipos** | 3 | 5 | 15 | **Muy Grave** |
| **Inundación** | 2 | 4 | 8 | **Apreciable** |
| **Malware** | 5 | 5 | 25 | **Muy Grave** |

**Tabla 33**

*Matriz de Riesgo.*

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

zzz

**Tabla 34**

*Niveles de Riesgo*

| | |
|---|---|
| | **Riesgo muy grave**: Requiere medidas importantes preventivas urgentes |
| | **Riesgo importante:** Medidas preventivas obligatorias |
| | **Riesgo apreciable:** Estudiar económicamente si es necesario |
| | **Riesgo marginal:** Se vigilará, aunque no requiere medidas preventivas |

### 4.5.5 FASE IV (ACTUAR)

#### 4.5.5.1 Cálculo de Impacto.

El cálculo de impacto es una etapa crítica dentro del proceso de gestión de riesgos, ya que permite determinar la magnitud de las consecuencias que tendría la materialización de un riesgo sobre los activos del laboratorio. Este análisis no se limita únicamente a identificar la afectación física, sino que también considera aspectos operativos, económicos y de continuidad del servicio. El cálculo del impacto consiste en analizar las posibles consecuencias que puede generar un evento adverso, tales como la pérdida de información, daños en los equipos, interrupciones en las actividades académicas y los costos necesarios para la recuperación.

Para llevar a cabo esta evaluación se definió una escala numérica del 1 al 5, donde cada valor representa un nivel de severidad previamente establecido. Esta clasificación facilita la incorporación de los resultados en la matriz de riesgos; al combinar el impacto con la probabilidad de ocurrencia, se obtiene una visión clara del nivel de riesgo, lo que ayuda a priorizar las amenazas más críticas. De este modo, el cálculo de impacto se convierte en una herramienta clave para la toma de decisiones, la correcta asignación de recursos y la aplicación de acciones correctivas que aseguren la continuidad operativa del laboratorio y el cumplimiento de la norma ISO/IEC 27002.

**Tabla 35**

*Valor Sobre Cálculo de Impacto***.**

| Cálculo de Impacto | | | | R2<br>Pág. 1 de 1 |
|---|---|---|---|---|
| **Riesgo** | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Valor de impacto** |
| **Robo** | 1 | 4 | 3 | 8 |
| **Incendio** | 3 | 4 | 3 | 10 |
| **Daño de Equipos** | 1 | 3 | 3 | 7 |
| **Inundación** | 1 | 1 | 3 | 5 |
| **Malware** | 5 | 5 | 4 | 14 |

| Escala | Descripción |
|---|---|
| **1** | No afecta mayormente |
| **2** | Afecciones menores |
| **3** | Paralización de la actividad, corto tiempo |
| **4** | Afecciones mayores |
| **5** | Efecto catastrófico |

**Realizado por:** Castro Alava Julexy Jamileth

**Revisado por:** Minaya Macias Renelmo Wladimir, Mg.

**Fecha:** 15/11/2025

**Firma:**

# Capítulo V

# 5 Evaluación de resultados

## 5.1 Introducción

Este presente capitulo tiene como presente o finalidad la evaluación de resultados la cual constituye una etapa fundamental dentro del proceso de auditoría informática, ya que permite analizar y valorar la información obtenida durante la aplicación de los instrumentos de diagnóstico. En esta fase se interpretan los datos recolectados a través de cuestionarios, observaciones y análisis técnicos, con el objetivo de determinar el nivel de cumplimiento de los controles de seguridad física y tecnológica en el Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen.

A partir de los hallazgos obtenidos presenciamos las evidencias de la fortalezas y debilidades que existente en la infraestructura y en las prácticas de seguridad, así como también proporciona una base sólida para la formulación de recomendaciones orientadas a la mejora continua. La evaluación se realizó considerando los riesgos identificados, tales como robo de equipos, daños por manipulación, incidentes ambientales (incendios e inundaciones) y amenazas lógicas como infecciones por malware, los cuales fueron priorizados por su impacto en la disponibilidad y protección de los activos tecnológicos.

Los hallazgos los obtuvimos mediante cuestionarios y entrevista la cual le realizamos al encargado o coordinador de inglés de esta manera, la presente sección busca ofrecer una visión clara y objetiva del estado actual del laboratorio.

## 5.2 Presentación y monitoreo de resultados.

Con base en la información recolectada durante la auditoría informática, se procedió a la tabulación y análisis de los datos obtenidos mediante los cuestionarios aplicados y las observaciones realizadas en el Laboratorio Multimedia de Idiomas. Los resultados permitieron identificar el nivel de riesgo al que se encuentra expuesta la infraestructura tecnológica, considerando las principales amenazas evaluadas: robo, daño de equipos, incendio, inundación y malware.

Para facilitar la interpretación, los datos fueron representados mediante gráficos y tablas comparativas que muestran la proporción entre condiciones seguras y vulnerables en cada categoría analizada. Esta representación gráfica permite visualizar de manera clara las áreas críticas que requieren intervención inmediata, apoyando la toma de decisiones para la formulación de acciones correctivas y preventivas.

El monitoreo de resultados se orienta a garantizar que las medidas propuestas sean implementadas de manera efectiva y que contribuyan a la reducción del riesgo en el tiempo. Este seguimiento se realizó bajo el enfoque de mejora continua, utilizando indicadores que permitan evaluar el impacto de las acciones aplicadas y asegurar la sostenibilidad de la seguridad física y tecnológica del laboratorio.

### 5.2.1 Informe de Auditoría.

**Tipo De Auditoria:** Auditoria de seguridad física.

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

**Motivo:** Programa de titulación.

#### 5.2.1.1 Objetivos:

- Identificar los principales riesgos físicos que afectan la integridad de los activos informáticos del Laboratorio Multimedia.
- Evaluar el nivel actual de cumplimiento de las normas ISO/IEC 27001 e ISO/IEC 27002 relacionadas con la seguridad física y ambiental.

#### 5.2.1.2 Alcance:

El alcance de la auditoría comprende las actividades necesarias para evaluar el estado actual de la seguridad física en el laboratorio multimedia de idiomas, considerando tanto los riesgos identificados como las medidas implementadas para mitigarlos. Para ello, se establecen técnicas y procedimientos que permitan obtener información confiable mediante la aplicación de instrumentos y métodos adecuados. Estas acciones se orientan a la recopilación, análisis y valoración de datos, con el propósito de determinar el nivel de seguridad y proponer soluciones efectivas que reduzcan las vulnerabilidades detectadas.

Para ello se realizó:

- Técnicas y procedimientos.
- Elaborar cuestionario para analizar riesgos.
- Responder el cuestionario.
- Inspección de instalación para llenar cuestionario.
- Entrevista a encargado para llenar cuestionario.
- Analizar cuestionarios e identificar riesgos.
- Valoración de riesgos.
- Calcular nivel de seguridad.
- Elaborar plan de contramedida.

5.2.1.3 **Personal Relacionado**:

Encargado del laboratorio:

- Ing. Argenis Román.

## 5.3 Hallazgo:

Durante la ejecución de la auditoría se identificaron novedades en la infraestructura riesgos asociados a la seguridad física. Entre los principales hallazgos se encuentran:

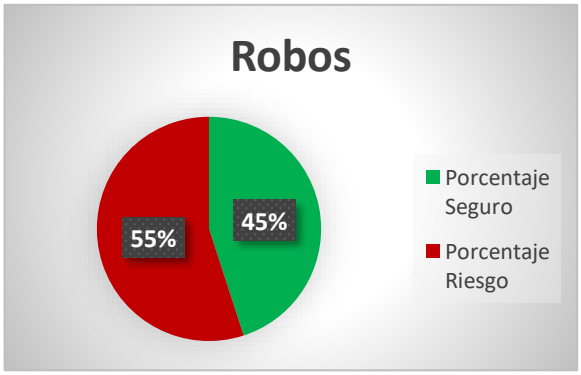
### 5.3.1 Interpretación General Del Riesgo

Una vez obtenidos los valores de probabilidad e impacto para cada riesgo identificado, se procedió a realizar la interpretación general con el objetivo de determinar el nivel de criticidad de las amenazas que pueden afectar la seguridad física y operativa del laboratorio. Esta etapa es fundamental porque permite transformar los datos numéricos en información estratégica, clasificando los riesgos en categorías como bajo, medio y alto, según su nivel de afectación y frecuencia estimada.

La interpretación general del riesgo constituye una herramienta importante para la toma de decisiones, ya que permite priorizar los riesgos más críticos y definir acciones orientadas a su mitigación. Mediante este análisis se identificaron los riesgos que requieren atención inmediata y los que pueden ser tratados con controles preventivos, lo que garantiza una adecuada asignación de recursos y la aplicación de acciones correctivas acordes a los estándares de seguridad de la norma ISO/IEC 27002.

**Tabla 36**

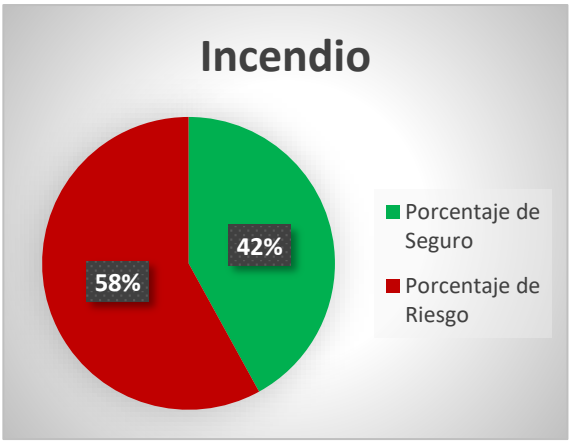
*Interpretación General de los Riesgos Encontrados (Robo, Incendio, Daño de Equipo, Inundación y Malware).*

| **Robos** | **Debido a:** |
|---|---|
|  | • No hay controles de acceso físico.<br>• No cuenta con cerraduras en puertas y ventanas.<br>• No hay sistema de identificación.<br>• No hay cámaras de vigilancia dentro del laboratorio.<br>• No hay restricciones a personas que no pertenecen tanto a la universidad como a la carrera.<br>• No se realizan auditorias periódicas. |

**Interpretación:**

El nivel de protección frente a robos en el Laboratorio Multimedia de Idiomas no es adecuado, ya que las medidas actuales resultan insuficientes para prevenir este tipo de incidentes. La ausencia de elementos esenciales como controles de acceso físico, cerraduras seguras en puertas y ventanas, cámaras de vigilancia y sistemas de identificación crea un entorno vulnerable que facilita el ingreso de personas no autorizadas.

**Incendio**



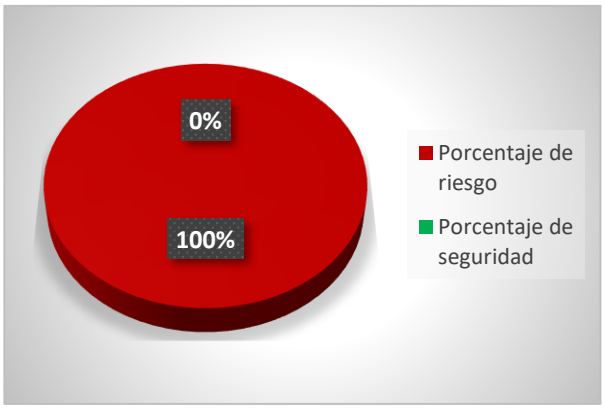

**Debido a:**

- No hay extintores.
- Los cables eléctricos presentan signos de deterioro.
- Ventanas con cortinas, muebles y pisos Zno resistentes al fuego.
- Se filtra liquido a través del techo.
- Los cables de electricidad no se encuentran diferenciados ni ordenados.
- No se cuenta con un botequín de primeros auxilios.

**Interpretación:**

El nivel de seguridad frente a incendios es bajo, lo que evidencia una alta exposición a este tipo de amenaza. La ausencia de equipos y recursos básicos, como extintores, señalización de rutas de evacuación, carteles de instrucciones y botiquines accesibles, limita la capacidad de respuesta ante una emergencia. Está situación demanda la implementación inmediata de medidas preventivas y correctivas, tanto a nivel estructural como operativo, para salvaguardar la integridad de las personas, los bienes y la continuidad de las actividades en el laboratorio.

**Daño de equipos.**



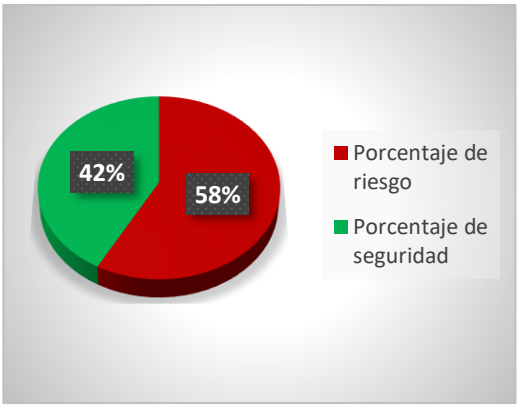

**Debido a:**

- No se realiza mantenimiento preventivo a los equipos.
- No existen protocolos visibles para la manipulación de los equipos.
- No se capacita al personal estudiantil en el uso adecuado de los equipos.
- No se cuenta con manuales de operaciones visibles.
- No hay control sobre la temperatura del laboratorio.
- No se revisa periódicamente los equipos.

**Interpretación:**

El nivel de seguridad en relación con el daño a los equipos es elevado ya que no corre muchos riesgos. Pero la falta de cuidados básicos, como el control de temperatura, el uso indebido de equipos, y la falta de limpieza causan daño en los equipos. Aunque el riesgo actual es moderado, resulta necesario implementar mejoras preventivas, como sistemas de drenaje adecuados y medidas de protección para los equipos, con el fin de garantizar una protección más robusta a futuro.

**Inundación**



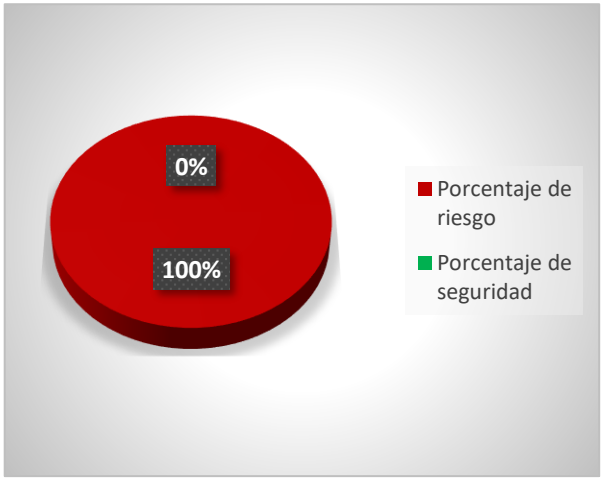

**Debido a:**

- La puerta no cierra correctamente.
- No existe canaletas.
- No hay drenaje alrededor del edificio.
- Presencia de filtración o manchas de agua en el techo.
- Las ventanas cuentan sin cierre emergentes.
- Los cables no están protegidos en el piso.

**Interpretación:**

El nivel de seguridad frente a inundaciones es aceptable, aunque persisten ciertos factores que podrían generar incidentes en caso de lluvias intensas. Aunque el riesgo actual es moderado, resulta necesario implementar mejoras preventivas, como sistemas de drenaje adecuados y medidas de protección para los equipos, con el fin de garantizar una protección más robusta a futuro.

**Malware**




**Debido a:**

- No se cuenta con software antivirus actualizado.
- No se realiza análisis periódicos de malware.
- No se capacita al personal en prevención de malware.
- No existen políticas visibles para la instalación de software.
- No se controla el uso de dispositivo USB.
- No se aplica actualizaciones de seguridad en sistemas.

**Interpretación:**

El nivel de protección frente a amenazas de malware en el Laboratorio Multimedia de Idiomas es extremadamente bajo, ya que las medidas actuales resultan insuficientes para prevenir, detectar y responder ante este tipo de incidentes. La ausencia de controles críticos como software antivirus actualizado, análisis periódicos, políticas de instalación segura y monitoreo de conexiones de red crea un entorno altamente vulnerable a infecciones y ataques.

### 5.3.2 Identificación De Riesgos En Robos:

- No hay controles de acceso físico.
- No cuenta con cerraduras en puertas y ventanas.
- No hay sistema de identificación.
- No hay cámaras de vigilancia dentro del laboratorio.
- No hay control de ingreso mediante formularios o registros.
- No hay restricciones a personas que no pertenecen tanto a la universidad como a la carrera.
- No hay restricciones de equipos fuera del lugar.
- No se realizan auditorias periódicas.
- No se cuenta con protocolos ante intento de robo.
- No se controla el ingreso fuera del horario laboral.
- Los cables no están ordenados y son accesibles desde zonas internas.
- Las ventanas permiten ingreso desde el exterior.

### 5.3.3 Identificación De Riesgos En Incendio:

- No hay extintores.
- Los cables eléctricos presentan signos de deterioro.
- Rutas de evacuación sin señalización.
- No hay carteles con instrucciones ante incendios.
- Ventanas con cortinas, muebles y pisos no resistentes al fuego.
- Luz de emergencia sin carga suficiente.
- Se filtra liquido a través del techo.
- No hay botequines de primeros auxilios accesibles y completos.
- Los cables de electricidad no se encuentran diferenciados ni ordenados.

- El tablero principal no cuenta con disyuntores ni protecciones.
- No hay persona responsable de la seguridad contra incendio.
- No hay sistema automático de rociadores.
- La estructura del techo no evita la filtración de agua sobre los equipos.
- No se revisa la temperatura de los equipos.
- No se cuenta con un botequín de primeros auxilios.

### 5.3.4 Identificación De Riesgos En Daños de Equipo:

- No se realiza mantenimiento preventivo a los equipos.
- No existen protocolos visibles para la manipulación de los equipos.
- No se capacita al personal estudiantil en el uso adecuado de los equipos.
- No se cuenta con manuales de operaciones visibles.
- No hay control sobre la temperatura del laboratorio.
- No se revisa periódicamente los equipos.
- No hay capacitación actualmente para los docentes que usan el laboratorio.
- Uso indebido de los equipos.
- No hay inspección de los cables.
- No hay señalización de limpieza alguna.
- No se cuenta con repuestos básicos.

### 5.3.5 Identificación De Riesgos En Inundación:

- La puerta no cierra correctamente.
- No existe canaletas.
- No hay drenaje alrededor del edificio.
- Presencia de filtración o manchas de agua en el techo.
- Las ventanas cuentan sin cierre emergentes.

- Presencia de humedad.
- Los cables no están protegidos en el piso.
- No hay estructuras externas que protejan del agua.
- Presencia de material deteriorado en el techo.
- Falta de presencia para los equipos durante la lluvia.
- Las instalaciones no se revisan tras la lluvia.

### 5.3.6 Identificación De Riesgos En Malware:

- No se cuenta con software antivirus actualizado.
- No se realiza análisis periódicos de malware.
- No se capacita al personal en prevención de malware.
- No existen políticas visibles para la instalación de software.
- No se controla el uso de dispositivo USB.
- No se aplica actualizaciones de seguridad en sistemas.
- No hay protocolos ante la detección de malware.
- No se dispone de firewall activo.
- No se monitoreo las conexiones de red.
- No se realiza copias de seguridad.
- No se controla el uso de correo electrónicos sospechosos.
- No se aplican políticas de contraseñas seguras.
- No se verifica la integridad de archivos descargables.
- No se documentan con incidentes de malware.
- No se restringe el acceso remoto autorizado.
- No se aplica pruebas de penetración periódicas.
- No se controla el uso de software pirata.

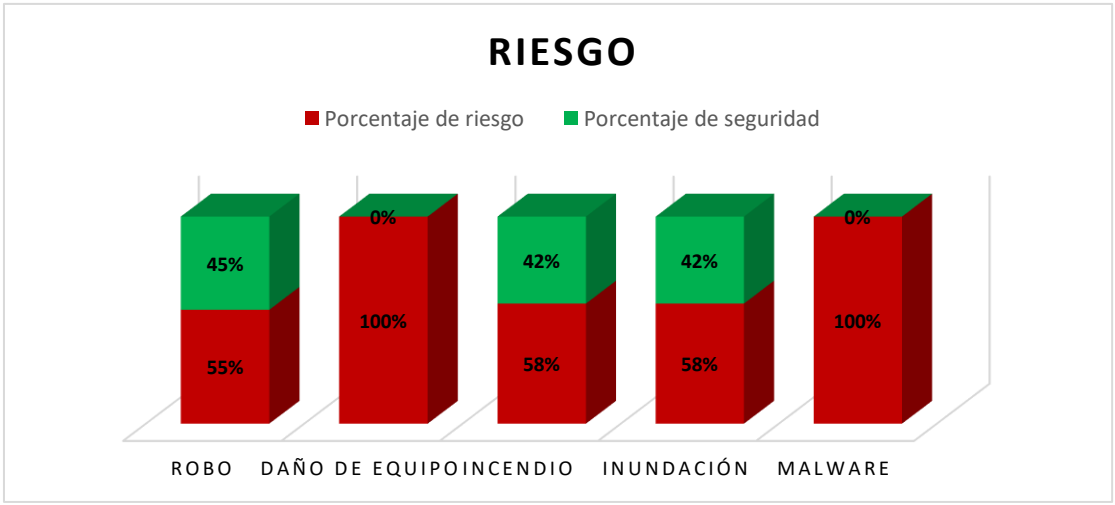
- No se dispone de un plan de respuestas ante ataque.

## 5.4 Interpretación Objetiva.

### 5.4.1 Gráfica General de Seguridad y Riesgo.

**Figura 11**

*Gráfica de Seguridad y Riesgos Encontrados.*




**Interpretación.**

El resultado del análisis de riesgos muestra que el Laboratorio de inglés es propenso a riesgos en varias de las categorías evaluadas. Entre los riesgos que tomaron más relevancia son el malware y el daño de equipos, las cuales reflejan un nivel de riesgo muy alto debido a la falta de salvaguardas y correctivos a esos riesgos. En conclusión, no se usan las medidas básicas que debe tener un laboratorio como antivirus actualizados, protocolos de instalación o prohibición de inserción de periféricos, lo que expone completamente a los equipos a posibles ataques y pérdida de información.

En cuanto al robo, el riesgo también es elevado, reflejando la falta de mecanismos de seguridad física como cerraduras seguras, cámaras de vigilancia, sistemas de identificación

y registros de acceso. Esta situación facilita el ingreso no autorizado y aumenta la probabilidad de sustracción de equipos.

Respecto a incendio e inundación, aunque el nivel de riesgo es menor en comparación con malware y daño de equipos, sigue siendo considerable. La ausencia de protocolos de emergencia, señalización adecuada y equipos de respuesta rápida incrementa la vulnerabilidad ante eventos ambientales que podrían afectar la continuidad operativa del laboratorio.

### 5.4.2 Gráfico General.

A continuación, se mostrará el resultado general de riesgo y seguridad con el que cuenta el laboratorio:

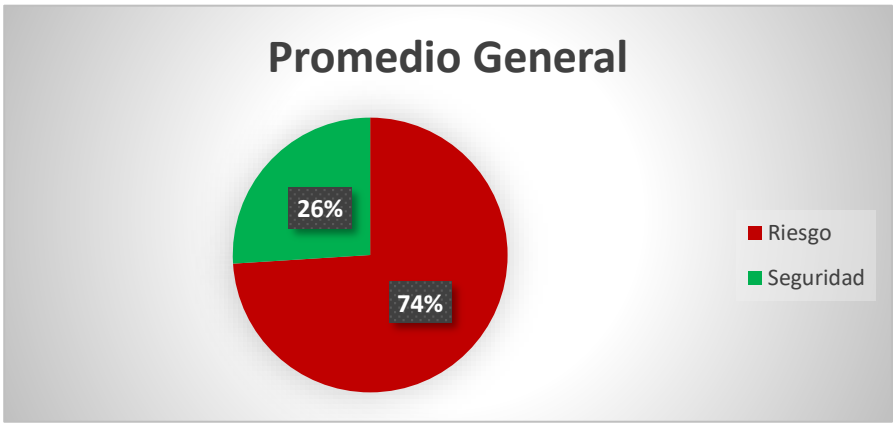
**Tabla 37**

*Porcentaje General de Riesgo y Seguridad*

| Riesgo | Porcentaje De Riesgo | Porcentaje De Seguridad |
|---|---|---|
| **Robo** | 55% | 45% |
| **Incendio** | 58% | 42% |
| **Daño de Equipo** | 100% | 0% |
| **Inundación** | 58% | 42% |
| **Malware** | 100% | 0% |
| **TOTAL** | **74%** | **26%** |

**Figura 12**

*Gráfica General de Riesgo y Seguridad*




**Interpretación.**

El análisis global refleja que el nivel de riesgo supera ampliamente al nivel de seguridad en el laboratorio multimedia de idiomas. Esto evidencia una alta vulnerabilidad frente a las amenazas evaluadas, lo que puede comprometer la continuidad operativa y la protección de los recursos tecnológicos y físicos.

En términos generales, la situación requiere acciones inmediatas para reducir el riesgo, fortaleciendo las medidas de seguridad física y lógica, así como la implementación de planes de contingencia. El objetivo debe ser equilibrar los porcentajes para garantizar un entorno seguro y confiable.

## 5.5 Opinión.

Una vez finalizada la auditoría se pudo identificar que el laboratorio de cómputo en la ULEAM Ext. El Carmen se puedo observar que está expuesto a los siguientes riesgos:

**Tabla 38**

*Opinión y Nivel de Riesgo*.

| Riesgo | Valor De Riesgo | Nivel De Riesgo |
|---|---|---|
| **Robo** | 55% | Riesgo Importante |
| **Incendio** | 58% | Riesgo Importante |
| **Daño de Equipo** | 100% | Muy Grave |
| **Inundación** | 58% | Riesgo Importante |
| **Malware** | 100% | Muy Grave |

Con los resultados obtenidos se pudo clasificar por el nivel de riesgo a cada una de las amenazas siendo malware y daño de equipos los riesgos muy graves y los de mayor peligro, seguidos por inundación e incendios con un riego importante y por último el ribo con el menor porcentaje de riesgo, pero con riesgo importante igualmente. Cada riesgo fue valorado considerando su impacto y probabilidad, generando una calificación numérica que permitió establecer su nivel de criticidad.

## 5.6 Conclusión y Recomendaciones.

### 5.6.1 Conclusión.

Con ayuda de la auditoria física realizada en el Laboratorio de Inglés se pudo cumplir con los objetivos planteados en un inicio en el programa de auditoría, se pudo detectar los principales riesgos que generan más peligro en el laboratorio y se puedo detectar que había medidas que estaban mal direccionadas y dejaban brechas en la seguridad y producían por ejemplo fallas eléctricas y daños irreversibles en los equipos.

De igual manera se alineo todo a las normas ISO 27001 y 27002, para gestionar de mejor manera la seguridad física y ambiental, donde se hizo evidente la fata de controles de prevención en el laboratorio tanto así que el nivel de riesgo dio un 74% frente a un 26% que

dio en seguridad, que refleja lo mal gestionado que se encuentra actualmente el mismo, por lo que pasa de ser una necesidad critica el aumentar las salvaguardas a los equipos y además proteger lo lógico mediante un plan de contramedidas que reduzca los riesgos identificados.

### 5.6.2 Recomendaciones.

Para fortalecer la seguridad del laboratorio y reducir el riesgo de robos, es fundamental implementar medidas que refuercen tanto la protección física como el control de accesos. Estas acciones deben orientarse a limitar las oportunidades de ingreso no autorizado, proteger los equipos y monitorear constantemente las instalaciones. A continuación, se presentan recomendaciones clave que contribuirán a crear un entorno más seguro y confiable para resguardar los recursos y garantizar la continuidad de las actividades.

Para poder mitigar los riesgos encontrados en los hallazgos, recomendamos usar el manual de contramedida el cual se encuentra en el Anexo B, en este se registra las medidas a utilizar y responder ante el daño físico de la infraestructura.

# Capítulo VI

# 6 Conclusiones y recomendaciones

## 6.1 Conclusiones

- La auditoría informática aplicada a la seguridad física, permitió cumplir con el objetivo general del estudio al analizar de forma integral el estado actual de la seguridad del laboratorio. A partir de esta evaluación, se identificaron factores que afectan directamente la protección del entorno, evidenciándose debilidades importantes como deficiencias en los controles de acceso, ausencia de sistemas de monitoreo permanente, falta de protocolos formalizados y condiciones inadecuadas de la infraestructura física, lo que incrementa los riesgos sobre la integridad y disponibilidad de los activos informáticos.
- El desarrollo del marco conceptual que abarca la auditoría de seguridad informática sirvió como sustento teórico para el proceso de evaluación, que permitió interpretar y aplicar adecuadamente las contramedidas a los riesgos según la situación actual del laboratorio. Asimismo, la auditoría realizada con siguiendo la guía puesta por las normas ISO 27002 y 27001 y mediante instrumentos de recolección de datos como encuestas, entrevistas, observación directa e investigación de campo, permitió determinar un bajo nivel de cumplimiento de buenas prácticas de seguridad física, revelando los riesgos que más impacto generan y en los cuales hay que poner plena atención.
- Con base en los resultados obtenidos, se elaboró una propuesta de mejora orientada a reducir los riesgos identificados, mediante la implementación de acciones correctivas y preventivas alineadas con las recomendaciones de la norma, contribuyendo a una gestión más eficiente de la seguridad física.

## 6.2 Recomendaciones

- Se recomienda diseñar un plan completo de contingencia orientado a tomar medidas preventivas y manejar de mejor manera los riesgos y así estar preparados ante accidentes que no están previstos y tener tiempos de respuesta más cortos y que los usuarios conozcan como actuar ante estas situaciones. Por ello el manual debe llevar planes de respuesta ante incidentes, procedimientos de recuperación y la definición de responsabilidades.
- Además, se recomienda reforzar tomar acciones en el control de acceso al laboratorio que está muy vulnerable a terceros, haciendo uso de sistemas de identificación biométrica para mayor eficiencia y evitando el gasto en tarjetas o quemar tiempo con contraseñas, para así llevar registros de ingreso y salida, de ser posible sumar colocación de cámaras de video vigilancia, asegurando un monitoreo constante y protección de los equipos.
- La última recomendación se trata de bajar el nivel de riego en el laboratorio ya que el nivel actual es muy alto con respecto a la seguridad brindada, pues lo mejor sería tener mayor seguridad que riesgos, para así crear un ambiente más seguro para los estudiantes y docentes.

# Bibliografía


Acevedo Juárez, H. (2020). *Integrando COBIT, ITIL e ISO 27001 como parte del gobierno de TI. Magazcitum.*

Aguilar Rivera, K. (2021). Auditoría de seguridad física y lógica en laboratorios de informática universitarios. *Repositorio Institucional UNACH.* Obtenido de Repositorio Institucional UNACH.

Albarrán Trujillo, S. E., Pérez Merlos, J. C., Salgado Gallegos, M., & Valero Conzuelo, L. L. (23 de Enero de 2019). *Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares* .

Alcívar Rivas, M. J. (22 de Enero de 2024). *Auditoría informática en seguridad física de los equipos informáticos en el Distrito de Educación 13D05 El Carmen.* Obtenido de Repsoitorio ULEAM: https://repositorio.uleam.edu.ec/handle/123456789/7392

Angamarca, L. (Junio de 2023). *Estrategias de auditoría informática en la era de la transformación digital.*

Bruce, C. (2025). Auditoría de sistemas de información para la seguridad y eficiencia organizacional. En *Experior, Vol. 4 Núm. 1*.

Buenaño, J., Cedeño, M., & Zambrano, L. (2021). Diseño e implementación de un sistema de control de acceso biométrico para laboratorios de informática. En U. T. Manabí.

Calder, A., & Watkins, S. (2019). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* Kogan Page.

Cárdenas Paredes, L. (2021). Auditoría informática para el fortalecimiento de la seguridad en redes de datos en la empresa Netcom S.A. En *Universidad Técnica del Norte (Ecuador).*

Cedeño, L., & Morales, V. (2023). Auditoría informática en entornos híbridos y distribuidos. *Revista Tecnológica Avanzada*, 10(1), 18–30.

Chirou, Á., & Laprovittera , C. (2024). *Blog.* Obtenido de Guía completa de las norma ISO 27001 vs 27002: https://achirou.com/

Contreras Alqui, J. (2024). Auditoría de sistemas informáticos y redes en la empresa de servicios tecnológicos TecnoRed S.A. En *Universidad Técnica de Ambato (Ecuador).*

Delgado, J., & Cedeño, R. (2023). Herramientas tecnológicas para el fortalecimiento del control interno. *Revista Ecuatoriana de Innovación Tecnológica*, 8(1), 59–72.

Enriquez Bastidas, H. P. (2024). Diseño del sistema de continuidad de negocio a través de la norma ISO 22301- 2019 para la empresa ModArte. En U. T. NORTE. Ibarra-Ecuador.

Estradas Rodríguez, L. J., & Paéz Arévalo, Y. P. (2021). *¿Cómo integra COBIT 4.1 el estándar ISO 27001 para obtener un gobierno de seguridad de la información?*

Fajardo, T., & Ramos, L. (2022). Gobernabilidad institucional y control interno en entornos universitarios. *Revista de Gestión Académica y Tecnología*, 7(2), 18–30.

Flores Konja, J. V. (2024). LA AUDITORÍA INFORMÁTICA: CONCEPTOS Y METODOLOGÍA OPERATIVA.

Fuela Echeverría, J. G. (2022). Sistema de control de acceso biométrico con notificación en tiempo real mediante Telegram y Raspberry Pi. En U. P. Salesiana..

García, T., Ramos, E., & Vargas, M. (2023). Buenas prácticas en auditoría informática según ISO/IEC y COBIT. *Journal of IT Governance*, 5(1), 12–25.

Group, E. (2023). *ISOTools.* Obtenido de Seguridad física y del entorno en ISO 27002: https://www.isotools.us/2023/06/06/seguridad-fisica-y-del-entorno-en-iso-27002/

Group, E. (04 de Septiembre de 2025). *BLOG ESPECIALIZADO EN CIBERSEGURIDAD.* Obtenido de MG SSI – Controles físicos en la norma ISO/IEC 27001:2022: https://www.pmg-ssi.com/2025/09/que-es-y-para-que-sirve-la-norma-iso-27002/

Guzmán, J., & Rivera, D. (2021). Control interno aplicado a sistemas de gestión académica. *Revista de Tecnología y Seguridad*, 10(2), 22–36.

Hernández, R., Morales, L., & Pérez, J. (2021). *Fundamentos modernos de seguridad física en entornos tecnológicos.* Journal of Security Management, 15(2), 45–60.

Hernández, R., Morales , L., & Pérez, J. (2020). *Fundamentos modernos de seguridad física en entornos tecnológicos.* Journal of Security Management, 15(2), 45-60.

Herrera, P., & Molina, F. (2022). Perspectiva multidisciplinaria de la auditoría informática. *Revista Iberoamericana de Auditoría Digital*, 6(3), 44–59.

Holloway, D. (06 de Agosto de 2025). *ISMS-ONLINE.* Obtenido de La guía definitiva para ISO 27002: https://es.isms.online/iso-27002/

Horna Vallejos, C. (2020). NTP-ISO 22301: 2020 Seguridad y resiliencia. Sistemas de gestión de continuidad del negocio. En S. d. Requisitos. Lima-Perú.

Inglés, B. A. (2014). *EF Standard English Test*. Obtenido de https://www.britishacademiadeingles.com/blog/que-es-el-nivel-de-ingles-b1-explicado/

International, A. (2019). *ANSI/ASIS Physical Security Standard.* ASIS International.

ISACA. (2020). *COBIT 2019 Framework: Governance and Management Objectives.* ISACA.

ISO. (2022). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls.* International Organization for Standardization.

ISOtools. (2022). *GROUP, ESGINOVA.* Obtenido de Controles físicos en ISO/IEC 27002:2022.: https://www.isotools.us/2022/08/26/controles-fisicos-en-iso-iec-270022022-te-lo-contamos-todo/

Lahm , P., Oye, E., & Micah, L. (2024). AI in risk assessment and disaster preparedness for building structures. ResearchGate.

Lopez, A. (2021-2022). *Studocu.* Obtenido de Guía ISO/IEC 27002:2022 - Controles de Seguridad Informática.

Mejías Macías, J. (2020). *Metodología para auditorías de ciberseguridad [Trabajo de fin de grado, Universidad de Valladolid]*. Obtenido de UVaDoc Repositorio.

Mena, J., & Villacrés, A. (2023). Auditoría tecnológica en laboratorios educativos: Una revisión de prácticas. *Revista Científica de Educación y Tecnología*, 8(2), 21–34.

Mendoza, D., & Jaramillo, F. (2021). Seguridad y control de equipos en laboratorios académicos. *Revista Científica de Tecnología Aplicada*, 9(3), 36–50.

Moncayo Ronquillo, K. C., & Llerena Izquierda, J. F. (2021). SEGURIDADES DE LA INFORMACIÓN BASES DE DATOS DISTRIBUIDAS: UN MAPEO SISTEMÁTICO. En U. P. GUAYAQUIL. Guayaquil-Ecuador.

Morales, L., & Ibarra, M. (2023). Auditoría informática en instituciones educativas: Aplicación y desafíos. *Revista de Tecnología Universitaria*, 8(2), 33–48.

Morán Arellano, A. S. (2020). *Auditoria informática utilizando el marco de referencia COBIT 2019 caso de estudio: departamento de TI de la Congregación de Hermanas Dominicas de la Inmaculada Concepción.* Obtenido de REPOSITORIO INSTITUCIONAL UNIVERSIDAD CENTAL DEL ECUADOR: https://www.dspace.uce.edu.ec/entities/publication/4c5cbcb4-a10f-47f4-b4b0-1a561940364c

Morán Arellano, A. S. (2022). *Auditoria informática utilizando el marco de referencia COBIT 2019 caso de estudio: departamento de TI de la Congregación de Hermanas Dominicas de la Inmaculada Concepción, para el año 2020.* Obtenido de http://www.dspace.uce.edu.ec/handle/25000/25827

Muñoz, A., & Cedeño, S. (2020). Aplicación del modelo COSO en entornos universitarios. *Revista de Auditoría y Administración Pública*, 4(3), 41–56.

Narváez Guerrón, J. P. (24 de Abril de 2024). *Análisis de la seguridad informática basado en la norma ISO/IEC 27002:2022 y NIST 800-61 para el área de operaciones y servicios del Gobierno Provincial de Imbabura.* Obtenido de Repositorio UTN: https://repositorio.utn.edu.ec/handle/123456789/15944

Navarrete, L., & Córdova, H. (2023). Implementación de controles internos basados en ISO/IEC 27001. *Revista Iberoamericana de Sistemas Seguros*, 9(1), 15–30.

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Revision 5).* National Institute of Standards and Technology.

Ochoa Caicedo, D. (2020). *Evaluación de la infraestructura tecnológica bajo estándares ISO 27001 en universidades públicas del Ecuador.* Obtenido de REPOSITORIO INSTITUCIONAL: http://www.dspace.uce.edu.ec/handle/25000/21545

Ormachea Montes, J. (2023). *Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional [Tesis doctoral, CAEN].* Obtenido de Repositorio Institucional CAEN.

Patricio Robalino, A., Yanza Chávez, W. G., & Montoya Lunavictoria, J. K. (26 de Agosto de 2022). Auditoría Informática. Riobamba.

Pérez, D., & León, S. (2022). Evaluación de la infraestructura digital universitaria mediante auditoría informática. *Revista Científica de Sistemas*, 6(3), 50–63.

QUIMIS SANCHEZ, A., & BARRETO TOALA, A. G. (22 de Julio de 2021). *AUDITORIA INFORMÁTICA APLICANDO METODOLOGÍA COBIT EN LOS LABORATORIOS DE COMPUTO DE LA FACULTAD DE CIENCIAS TÉCNICAS DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANAB.* Obtenido de Repositorio Digital UNESUM.

Rivas, J., & Gómez, C. (2024). Enfoques proactivos en la auditoría de tecnologías de la información. *Revista de Innovación y Gestión de Riesgos*, 9(1), 70–85.

Rivera Páez, S. (2021). Fuerzas militares, asistencia humanitaria y respuesta a desastres ocasionados por fenómenos naturales. En ResearchGate.

Romero Payano, G. O. (2021). *Implementación de una metodología de gestión de riesgos de ciberseguridad para una empresa minera.* Obtenido de Repositorio Institucional UTP.

Silva Martínez, K. M. (Enero de 2020). *Desarrollo de una metodología para la auditoría en informática.* Obtenido de Repositorio Institucional UNAM.

Silva Martinez, K. M. (2020). *Desarrollo de una metodología para la auditoría en informática [Tesis de licenciatura, UNAM].* Obtenido de Repositorio UNAM.

Solano Maza, L. O., Farías Gonsález, M. J., Fernández Pereira, M. D., & Porras Fernández, M. I. (2024). Uso de herramientas y tecnologías emergentes en la enseñanza de la educación superior. Prohominum vol.6 no.1 Villa de Cura.

Tenorio Ordoñez, I. J. (2024). Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001. En *Universidad Nacional de Chimborazo.* Riobamba, Ecuador.

Tenorio Ordoñez, I. J. (07 de Enero de 2025). *Auditoría informática de seguridad física en el área de redes en la Universidad.* Obtenido de Repositorio General UNACH: http://dspace.unach.edu.ec/handle/51000/14470

Torres, K., & Benítez, D. (2022). Automatización de procesos en auditoría informática. *Revista de Ingeniería Computacional*, 11(2), 70–83.

Torres, P., & Méndez, A. (2021). Fundamentos del control interno informático. *Revista Científica de Auditoría Digital*, 6(2), 65–78.

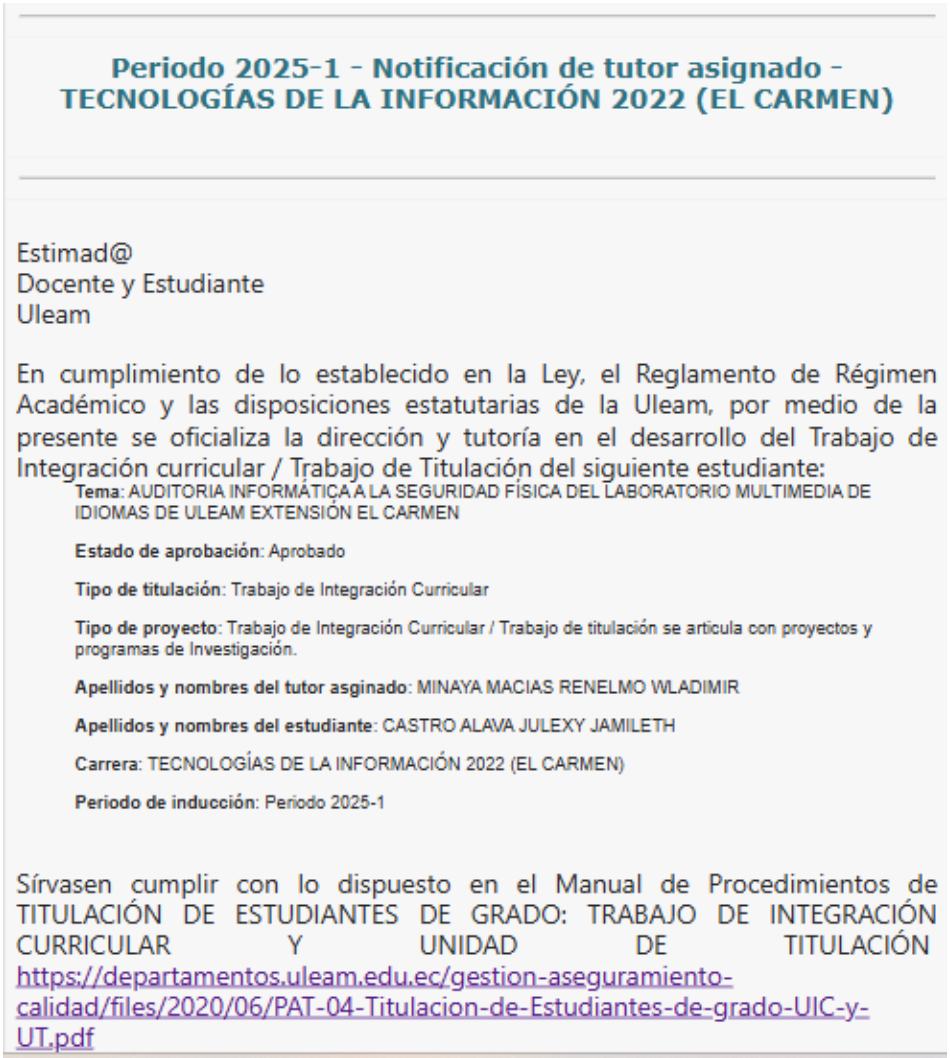
Zamora, R., & Delgado, H. (2021). Aplicación de normas internacionales en auditoría de TI. *Revista de Control Tecnológico*, 7(1), 19–34.

# Anexos

## Anexo A. Aprobación de tema

### Figura 13

*Aceptación de tema de Titulación.*



**Periodo 2025-1 - 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 INFORMÁTICA A LA SEGURIDAD FÍSICA DEL LABORATORIO MULTIMEDIA DE IDIOMAS DE ULEAM 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**: MINAYA MACIAS RENELMO WLADIMIR

**Apellidos y nombres del estudiante**: CASTRO ALAVA JULEXY JAMILETH

**Carrera**: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

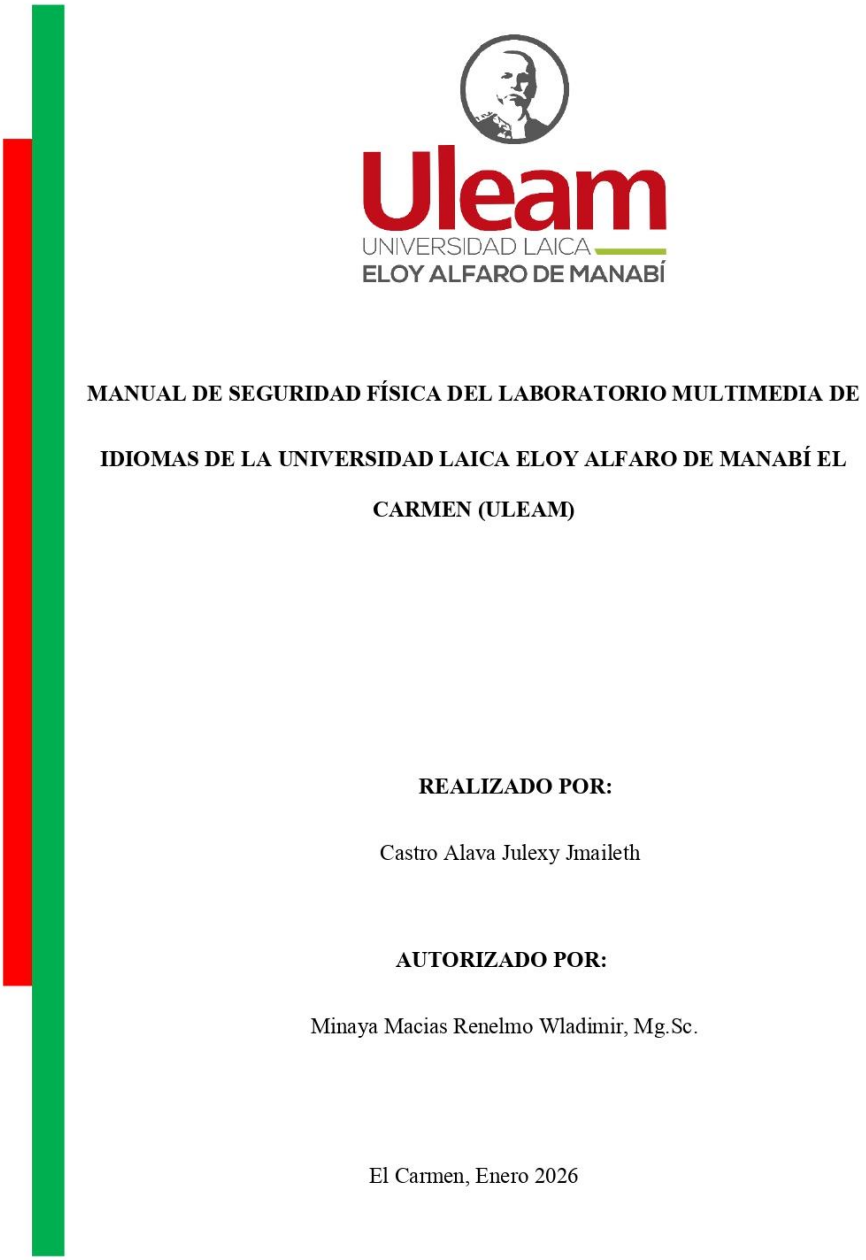
**Periodo de inducción**: Periodo 2025-1

Sírvasen cumplir con lo dispuesto en el Manual de Procedimientos de TITULACIÓN DE ESTUDIANTES DE GRADO: TRABAJO DE INTEGRACIÓN CURRICULAR Y UNIDAD DE TITULACIÓN https://departamentos.uleam.edu.ec/gestion-aseguramiento-calidad/files/2020/06/PAT-04-Titulacion-de-Estudiantes-de-grado-UIC-y-UT.pdf

## Anexo B. Manual de Contingencia.

**Figura 14**

*Manual de Contingencia*



**Índice**

**Manual De Políticas Sobre La Seguridad**

**Introducción**

La seguridad física y operativa de los laboratorios tecnológicos es fundamental para garantizar la continuidad de las actividades académicas y administrativas en las instituciones de educación superior. Estos espacios son esenciales para el aprendizaje práctico, por lo que incidentes como accesos no autorizados, robos, fallas eléctricas, daños en los equipos o factores ambientales pueden afectar la disponibilidad de los recursos tecnológicos y el normal desarrollo de las clases.

En respuesta a esta situación, la elaboración de un Manual de Contingencia se plantea como una medida preventiva orientada a mitigar los riesgos identificados durante la Auditoría Informática de la seguridad física del Laboratorio Multimedia de Idiomas de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. Los hallazgos evidencian debilidades en los controles físicos, operativos y organizativos, lo que hace necesaria la definición de políticas, procedimientos y acciones claras para reducir la probabilidad de incidentes y minimizar su impacto.

El manual se estructura con base en los hallazgos detectados, relacionando los riesgos con las medidas de control y contingencia propuestas, e incorpora buenas prácticas de seguridad física apoyadas en las normas ISO/IEC 27001 y 27002, el marco COBIT y la metodología MAGERIT, adaptadas al contexto institucional, con el fin de proteger los activos tecnológicos y asegurar la continuidad académica del laboratorio.

**Objetivo.**

Establecer un plan de contingencia que permita prevenir, mitigar y responder de manera oportuna ante incidentes físicos, ambientales y tecnológicos que puedan afectar al Laboratorio Multimedia de Idiomas de la ULEAM, El Carmen, garantizando la continuidad de las actividades académicas mediante la aplicación de procedimientos claros, la asignación de responsabilidades, la reducción de los riesgos identificados en la auditoría informática y la adopción de buenas prácticas de seguridad institucional.

**Alcance.**

El presente Manual de Contingencia tiene como alcance establecer y orientar lineamientos y procedimientos que permitan actuar de forma preventiva y organizada ante la ocurrencia de incidentes que puedan afectar la seguridad física, ambiental y tecnológica del laboratorio.

Este manual aplica a todo el personal que tenga acceso o responsabilidad sobre el laboratorio, incluyendo autoridades institucionales, personal técnico, docentes y estudiantes usuarios del espacio, quienes deberán cumplir los procedimientos establecidos para prevenir, reportar y responder ante situaciones de emergencia o contingencia.

El alcance del manual incluye la gestión de riesgos asociados a:

- Accesos no autorizados y robos de equipos.
- Daños físicos a los equipos informáticos por mal uso o falta de mantenimiento.
- Incendios ocasionados por fallas eléctricas o factores humanos.

**Continuidad operativa**: Capacidad de la institución para mantener sus actividades académicas y administrativas ante la ocurrencia de incidentes o eventos adversos.

**Buenas prácticas**: Acciones y comportamientos recomendados que permiten el uso responsable, seguro y eficiente de los recursos tecnológicos institucionales.

**Responsable.**

Los responsables de la aplicación y cumplimiento del presente Manual de Contingencia son:

- Encargado de la materia de English.
- Personal técnico del laboratorio.
- Estudiante que toman la materia.

**Responsabilidad del usuario.**

- El personal docente y estudiantil se compromete a:
- Mantener limpia la instalación.
- Cumplir las normas y políticas establecidas en el presente manual.
- Reportar de forma inmediata cualquier incidente, daño o irregularidad detectada.

**Política de Seguridad.**

**Políticas de Control de Acceso Físico**

- Permitir el acceso únicamente a personal autorizado.
- Mantener puertas y accesos cerrados cuando el laboratorio no esté en uso.

- Inundaciones o afectaciones por filtraciones de agua y eventos climáticos.
- Amenazas tecnológicas como infecciones por malware o uso inadecuado de los sistemas.

Asimismo, el manual contempla acciones de prevención, respuesta inmediata y recuperación, con el fin de garantizar la continuidad de las actividades académicas, la protección de los activos tecnológicos y la reducción del impacto de los riesgos identificados durante la auditoría informática realizada al laboratorio.

**Definición.**

Para una mejor comprensión del presente manual, se establecen las siguientes definiciones:

**Auditoría informática:** Proceso sistemático de evaluación que permite analizar la seguridad, el control y el uso adecuado de los recursos tecnológicos, con el objetivo de identificar riesgos, vulnerabilidades y proponer mejoras.

**Seguridad física**: Protección de los equipos, instalaciones y personas frente a amenazas como robos, incendios, inundaciones u otros eventos que puedan causar daños materiales o interrupciones operativas.

**Riesgo:** Probabilidad de que una amenaza se materialice y genere un impacto negativo sobre los activos informáticos, afectando la continuidad de las actividades institucionales.

**Vulnerabilidad:** Debilidad existente en los controles físicos o administrativos que puede ser aprovechada por una amenaza, incrementando el nivel de riesgo.

- Llevar un registro continuo de las personas que ingresan al laboratorio el cual permitirá llevar un mejor control de los accesos.

**Política de Prevención de Robos.**

Con base a los hallazgos que se ha identificado durante este proceso, se plantea la implementación de las siguientes políticas de prevención la cual esta orientada a fortalecer la seguridad física del laboratorio mediante medidas permitan reducir los riesgos identificados y de esta manera poder mejorar el resguardo de los recursos institucionales.

Para ello se recomienda lo siguiente:

- Instalar rejas metálicas en las ventanas.
- Colocar señalización de acceso restringido al ingresar al laboratorio.
- Instalar cámaras de seguridad en puntos estratégicos.
- Revisar y proteger los cables accesibles desde el exterior.
- Implementar un sistema de control de acceso con registros o formularios para estudiantes y visitantes.
- Reforzar las puertas e instalar cerraduras de alta seguridad.
- Implementar un sistema de registro de visitantes y control de acceso.

**Política de Prevención de Incendios.**

Durante el desarrollo de la auditoría informática se detectaron diversos riesgos relacionados con la posibilidad de incendios en el Laboratorio Multimedia de Idiomas, originados principalmente por deficiencias en las instalaciones eléctricas, el uso excesivo de tomas de energía y la falta de equipos adecuados para la protección contra incendios.

Estas condiciones constituyen una amenaza importante para la seguridad del espacio, la protección de los equipos informáticos y la continuidad normal de las actividades académicas.

Para ello se recomienda lo siguiente:

- Instalar extintores de polvo para electricidad en puntos visibles y accesibles, con mantenimiento regular.
- Señalizar rutas de evacuación y colocar carteles con instrucciones ante emergencias.
- Colocar carteles con instrucciones de seguridad contra incendios.
- Verificar el funcionamiento de luces de emergencia.
- Dotar al laboratorio de botiquines de primeros auxilios completos y accesibles.
- Reemplazar cableado dañado y evitar sobrecargas eléctricas.
- Reparar humedades en paredes y techos, especialmente cerca de enchufes.

**Política de Prevenir Inundación.**

Durante la auditoria se pudo identificar riesgos asociados a factores ambientales que podrían afectar la seguridad física del laboratorio. La presencia de estos riesgos representa amenazas directas, es por ello que se establece las siguientes políticas:

- Instalar canaletas y drenajes alrededor del edificio.
- Reparar techos y sellar ventanas para evitar filtraciones.
- Instalar sensores de humedad o detectores para el flujo de agua.

**Política para Prevenir Daño de Equipos.**

Durante la auditoría informática se identificaron riesgos relacionados con el deterioro y daño de los equipos informáticos del Laboratorio Multimedia de Idiomas, ocasionados principalmente por el uso inadecuado de los recursos, la falta de mantenimiento preventivo, las condiciones ambientales poco controladas y la ausencia de procedimientos claros para la manipulación de los equipos.

Para ello se recomienda seguir las siguientes políticas:

- Establecer rutinas de revisión y mantenimiento preventivo de equipos.
- Crear y difundir un formulario digital o físico para reportar daños.

**Política para Prevenir Malware.**

Durante la auditoría informática se identificaron riesgos relacionados con la presencia del deterioro de los equipos, estas situaciones pueden comprometer la integridad de la información y el correcto funcionamiento de los equipos, por lo que se establece una política orientada a prevenir infecciones de malware y evitar que estos se deterioren.

Para ello se recomienda lo siguiente:

- Instalar y mantener actualizado un software antivirus en todos los equipos.
- Habilitar actualizaciones automáticas del sistema operativo y software.
- Implementar política o implemento de limpieza
- Implementar políticas de uso responsable de internet y supervisión de navegación.
- Realizar copias de seguridad periódicas en medios físicos y seguros.

- Supervisar el uso de internet mediante filtros o monitoreo de red.

**Mecanismos de Seguimiento**

Con el fin de garantizar la efectividad de las políticas de seguridad y las buenas prácticas establecidas, se implementan los siguientes mecanismos de seguimiento:

**Registro y análisis de incidentes de seguridad**: Se efectuará de manera continua, documentando eventos relacionados con robos, daños, malware, incendios o inundaciones.

**Capacitación y sensibilización**: Se programará anualmente para reforzar las buenas prácticas y el uso seguro de los recursos tecnológicos.

**Revisión del manual**: Se realizará una vez al año, ajustando las medidas según los resultados obtenidos en evaluaciones y auditorías internas.

**Figura 15**

*Entrevista al Coordinador de Ingles.*

## Anexo C. Instrumento entrevista

**UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ**

**Encuesta Dirigida A:** Ing. Argenis Román.

**Objetivo:** El objetivo de esta entrevista es recopilar su opinión y expectativa sobre las la seguridad física del laboratorio. Esta información ayudará a obtener los resultados requeridos.

**1. ¿Cuál es su cargo actual dentro de la universidad y desde cuándo lo desempeña?**

Me desempeño como docente de la carrera de la Educación Básica, además soy responsable de en la extensión desde el 2014.

**2. Desde su experiencia, ¿con qué frecuencia se presentan fallas o problemas técnicos en los equipos del laboratorio?**

El laboratorio de English fue utilizado por la carrera de Idiomas en la extensión el cual funciono aproximadamente en el año 2015.

**3. ¿Considera que el laboratorio es seguro?**

Parcialmente seguro, ya que cuenta con una puerta que resguardaba los equipos del laboratorio. No obstante, existía la posibilidad de que alguien ingresara por las ventanas laterales.

**4. ¿Considera que el laboratorio está preparado para enfrentar desastres naturales como inundaciones o incendios? ¿Qué medidas existen actualmente?**

No cumple con las condiciones ante eventos como lo es el incendio.

**5. ¿Cree que sería beneficioso implementar sistemas de control de acceso biométrico o videovigilancia? ¿Por qué?**

Si, ya que al no contar con seguro se vuelve viable para el robo, o la perdida de objetos.

**6. ¿Considera que el laboratorio cuenta con medidas adecuadas de seguridad física, como cerraduras, cámaras o controles de acceso? ¿Por qué?**

No el laboratorio no cuenta con ninguna medida de seguridad.

**7. ¿Se brinda capacitación o información al personal y usuarios sobre normas de seguridad física en el laboratorio? ¿Con qué frecuencia?**

Al principio si se realizaba capacitación y se realizó manuales los cuales estaban pegados en la pared, para que sean observados y leído siempre que se utilizaba el laboratorio, actualmente ya no se realiza.

**8. ¿Ha ocurrido algún incidente relacionado con robos, humedad o polvo? ¿Cómo se ha gestionado?**

De robo no, de polvo si ya que no se realiza limpieza en esta área entonces los muebles y equipos son afectados.

**9. ¿Cómo evalúa el estado actual de la infraestructura del laboratorio (puertas, ventanas, techos, etc.) en relación con las normas técnicas de mantenimiento?**

El laboratorio es disfuncional, como se ha señalado anteriormente; su estado no es el más adecuado y su infraestructura tampoco resulta apropiada para que los estudiantes reciban clases.

**10. ¿Con qué frecuencia se realiza mantenimiento a los equipos? ¿Existe un cronograma establecido o se hace de forma reactiva?**

Actualmente no se cuenta con mantenimiento en los equipos, pero, cuando funcionaban, si se les realizaba de manera periódica.

**11. ¿Ha tenido conocimiento de accesos no autorizados al laboratorio? ¿Cómo se ha manejado esa situación?**

Si, ha habido ocasiones en la cual se ha tenido ingreso de estudiantes que no pertenecen o que no toman la materia.

**12. ¿Cuál es el estado general de los equipos tecnológicos del laboratorio? ¿Están todos operativos o hay algunos fuera de servicio?**

No están, están en desuso, ya que cumplieron su vida útil.

**13. ¿Considera útil realizar auditorías periódicas para evaluar la seguridad física del laboratorio?**

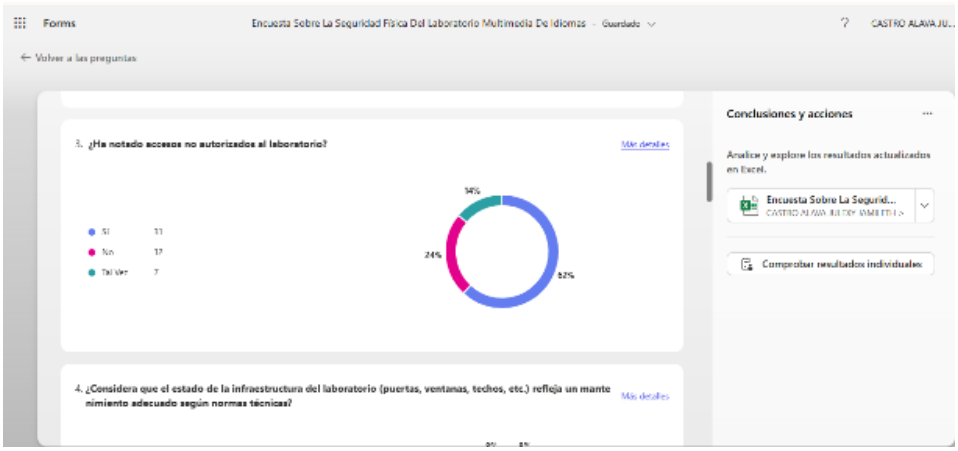
Por supuesto, si hubiera la manera de contar con un nuevo laboratorio si nos gustaría que tuviera con auditorías periódicas para evitar posibles daños.

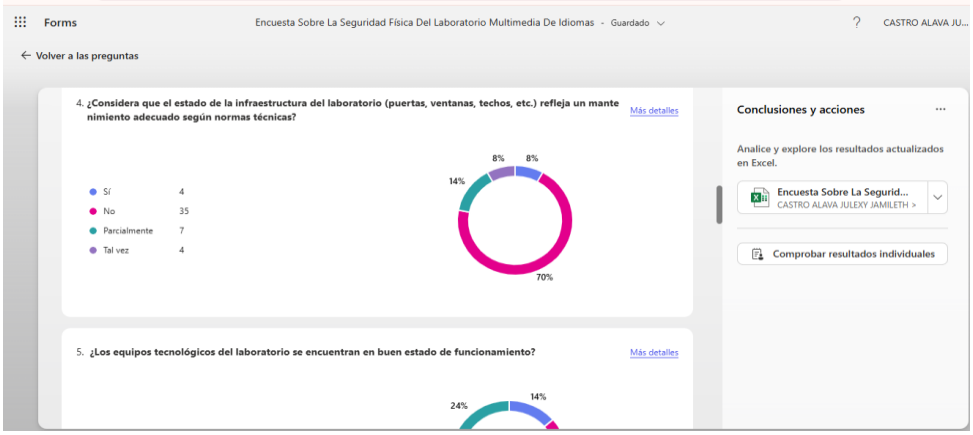
FIRMA

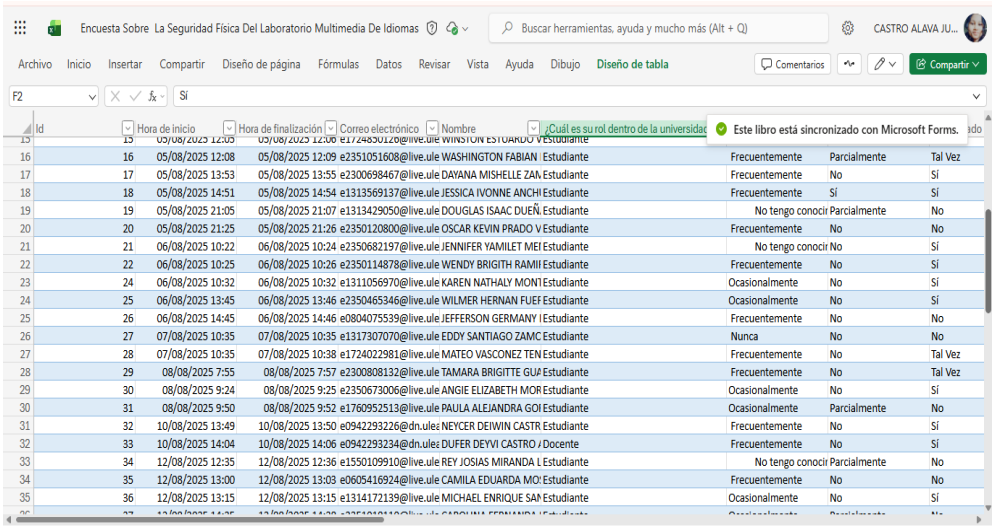
## Anexo D. Instrumento encuesta

## Figura 16

Encuesta a estudiantes



## Anexo E. Fotografías

**Figura 17**

*Entrevista al Coordinador de Ingles.*

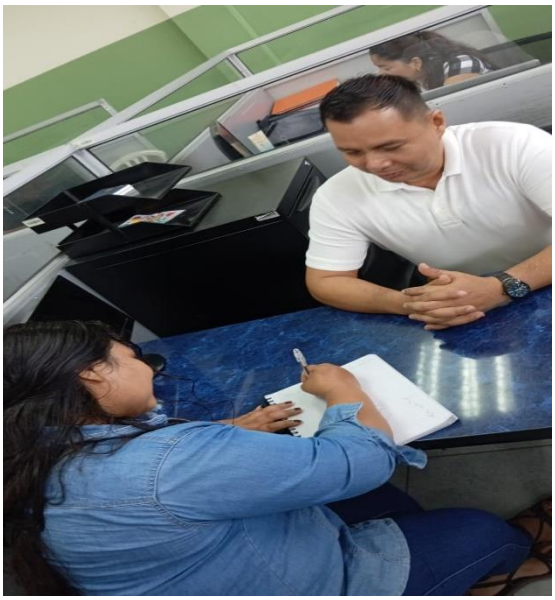
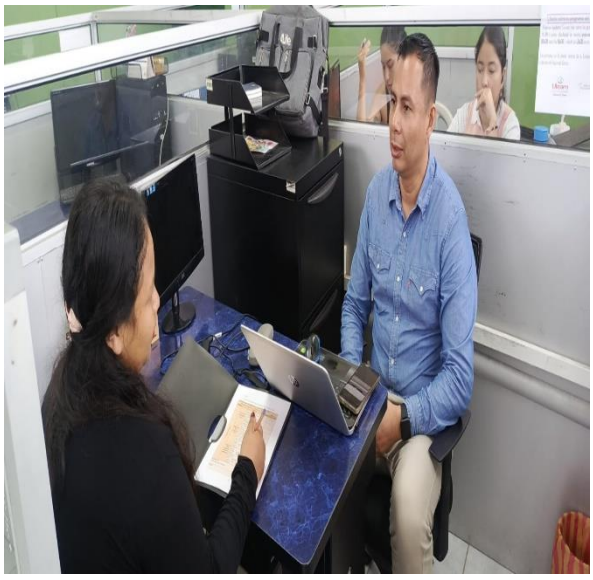


**Figura 18**

*Entrevista ala Coordinador de Ingles para responder a Cuestionarios*



## Anexo F. Programa de auditoria

## Figura 19

*Programa de auditoria*

**Tabla 1**

*Programa de Auditoría*

| **Programa de auditoría informática a la seguridad física del laboratorio multimedia de idiomas universidad laica Eloy Alfaro De Manabí El Carmen (ULEAM).** | | |
|---|---|---|
| **Objetivos**<br>1. Identificar los principales riesgos físicos que afectan la integridad de los activos informáticos del Laboratorio Multimedia.<br>2. Evaluar el nivel actual de cumplimiento de las normas ISO/IEC 27001 e ISO/IEC 27002 relacionadas con la seguridad física y ambiental. | | |
| **Técnicas y procedimientos** | **Referencia a papel de trabajo** | **Fecha** |
| 4.5.2.1 Elaborar cuestionario de Requisitos según Normas ISO 27001 | C1 | 08/10/2025 |
| 4.5.4.1 Elaborar Cuestionarios de Identificación de Riesgos | C2 | 20/10/2025 |
| 4.5.4.1 Responder el cuestionario | C2 | 23/10/2025 |
| 4.5.4.1 Entrevista a encargado para llenar cuestionario. | C1 | 23/10/2025 |
| 4.5.4.1.3 Identificación de Riesgo. | R1 | 30/10/2025 |
| 4.5.4.1.4 Valoración de riesgo | R2 | 10/11/2025 |
| 4.5.5.1 Calcular impacto | R3 | 15/11/2025 |
| 5.4.1 Calcular nivel de seguridad | | 18/11/2025 |
| Elaborar plan de contramedida | | 28/01/2026 |
| **Elaborado por:**<br>• Castro Alava Julexy Jamileth | **Revisado por:**<br>Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:**<br>06/10/2025 | **Firma**: | |

**Anexo G. cuestionario *norma ISO 27001***

**Figura 20**

*Cuestionario norma ISO 27001 parte 1*

**Tabla 13**

*Cuestionario de Requisito Según Normas ISO 27001 (Planificación).*

| **Cuestionario para el cumplimiento de requisito según normas ISO 27001 para el Laboratorio de Multimedios de la ULEAM** | | | | **C1 página 1-3** |
|---|---|---|---|---|
| **Requisito** | | **Preguntas** | **Cumplimiento** | **Observación** |
| **6. Planificación** | **6.1 Evaluación de riesgos** | ¿Se han identificado los riesgos físicos que pueden afectar la seguridad de la información en el laboratorio multimedia? | No Cumple | Se identificaron riesgos, pero no existía un proceso formal previo. |
| | | ¿Se ha realizado un análisis de impacto para determinar las consecuencias de los riesgos identificados? | No Cumple | No existía un análisis de impacto documentado antes de la auditoría. |
| | **6.1.3 Tratamiento de riesgos** | ¿Se han definido criterios para evaluar la probabilidad y el impacto de cada riesgo? | No Cumple | Se utilizaron criterios proporcionados por la auditoría. |
| | | ¿Existe un plan documentado para tratar los riesgos físicos detectados? | No Cumple | La auditoría propone un plan de contramedidas en anexos. |
| | | ¿Se han definido controles específicos para mitigar los riesgos más críticos? | No Cumple | No existen controles documentados ni implementados |
| | **6.2 Objetivos de seguridad de la información** | ¿Se han establecido objetivos claros para mejorar la seguridad física del laboratorio multimedia? | No Cumple | No existen objetivos de seguridad establecidos por la institución para el laboratorio |
| | | ¿Están alineados estos objetivos con la política institucional y los requisitos legales? | Si Cumple | |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 08/10/2025 | | | **Firma:** | |

**Figura 21**

*Cuestionario norma ISO 27001 parte 2*

**Tabla 14**

*Cuestionario De Requisito Según Normas ISO 27002 (Controles Físicos).*

| **Cuestionario para el cumplimiento de requisito según normas ISO 27002 para el Laboratorio de Multimedia de la ULEAM** | | | | **C1 página 2-3** |
|---|---|---|---|---|
| **Requisito** | | **Preguntas** | **Cumplimiento** | **Observaciones** |
| **7. Controles Físicos** | **7.2 Control de entrada física** | ¿Existen mecanismos para controlar el acceso físico al laboratorio multimedia? | No Cumple | No hay controles de acceso; las puertas y ventanas no cuentan con cerraduras seguras. |
| | | ¿Se utilizan credenciales, tarjetas o sistemas biométricos para el ingreso? | No Cumple | No existe ningún sistema de identificación, registro o credencial para ingresar. |
| | | ¿Hay personal encargado de supervisar el acceso? | Si Cumple | El docente que está a cargo según el horario. |
| | **7.4 Supervisión de la seguridad física** | ¿El laboratorio cuenta con cámaras de video vigilancia instaladas? | No Cumple | No existe sistema de vigilancia. |
| | | ¿Se realiza monitoreo activo de las grabaciones? | No Cumple | No hay cámaras. |
| | | ¿Existe registro histórico de accesos y eventos? | No Cumple | No se lleva registro de ingreso al laboratorio. |
| | | ¿Se cuenta con sistemas contra incendios (extintores, alarmas)? | No Cumple | No hay extintores, ni alarmas. |
| | **7.5 Protección contra amenazas físicas y ambientales** | ¿Están alineados estos objetivos con la política institucional y los requisitos legales? | Si Cumple | |
| | | ¿Existen medidas para prevenir daños por inundaciones o fallos eléctricos? | No Cumple | No hay drenaje, canaletas, ni protección del cableado. |
| | | ¿Hay protocolos de respuesta ante desastres naturales? | Si Cumple | |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 08/10/2025 | | | **Firma:** | |

**Figura 22**

*Cuestionario norma ISO 27001 parte 3*

**Tabla 15**

*Cuestionario para el cumplimiento de requisito según metodología* PDCA.

| **Cuestionario para el cumplimiento de requisito según METODOLOGIA PDCA para el Laboratorio de Multimedia de la ULEAM** | | | | **C1 página 3-3** |
|---|---|---|---|---|
| **Requisitos** | | **Preguntas** | **Cumplimientos** | **Observaciones** |
| **Gestión de riesgos & PDCA – Identificación de activos** | **APO12 Gestión de riesgos** | ¿Existe un procedimiento documentado para gestionar riesgos físicos y tecnológicos en el laboratorio? | No Cumple | No existe un procedimiento formal, manual o política institucional. |
| | | ¿Se realizan evaluaciones periódicas de riesgos? | No Cumple | No hay evidencia de evaluaciones periódicas; la auditoría fue el primer diagnóstico formal realizado. |
| | | ¿Se asignan responsables para la mitigación de riesgos? | No Cumple | No hay personal asignado oficialmente como responsable de gestionar riesgos o activar medidas preventivas. |
| | **Identificación de activos** | ¿Se cuenta con un inventario actualizado de los activos físicos y tecnológicos del laboratorio multimedia? | No Cumple | No cuenta con inventarios. |
| | | ¿Se han clasificado los activos según su criticidad? | No Cumple | No existe una clasificación basada en criticidad, valor, impacto o confidencialidad. |
| | | ¿Se han identificado las amenazas que pueden afectar cada activo? | No Cumple | Las amenazas no fueron identificadas previamente. |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 08/10/2025 | | | **Firma:** | |

## Anexo H. Identificación de riesgos

## Figura 23

*Cuestionario de identificación de riesgos*

**Tabla 2**

*Cuestionario de Identificación (Robo).*

| CUESTIONARIO PARA IDENTIFICAR RIESGO | | | | C2<br>Pág. 1 de 5 | |
|---|---|---|---|---|---|
| ROBO | | | | | |
| Preguntas | | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿Existen controles de acceso físico al laboratorio? | | X | | 0 |
| 2 | ¿El laboratorio cuenta con cerraduras seguras en puertas y ventanas? | | X | | 0 |
| 3 | ¿Se utiliza algún sistema de identificación para ingresar al laboratorio? | | X | | 0 |
| 4 | ¿Hay cámaras de vigilancia funcionando en el área? | | X | | 0 |
| 5 | ¿Se registran las entradas y salidas del personal? | | X | | 0 |
| 6 | ¿El personal conoce las políticas de acceso? | X | | | 1 |
| 7 | ¿Se restringe el acceso a personas no autorizadas? | | X | | 0 |
| 8 | ¿Se controla el ingreso de equipos externos? | | X | | 0 |
| 9 | ¿Se cuenta con un inventario actualizado de equipos? | X | | | 1 |
| 10 | ¿Se realizan auditorías periódicas de los activos? | | X | | 0 |
| 11 | ¿Existen protocolos ante intento de robo? | | X | | 1 |
| 12 | ¿El laboratorio está ubicado en un área segura? | X | | | 1 |
| 13 | ¿Se controla el acceso fuera del horario laboral? | | X | | 0 |
| 14 | ¿Se cuenta con seguro contra robo? | X | | | 1 |
| 15 | ¿Se revisan periódicamente los sistemas de seguridad? | X | | | 1 |
| 16 | ¿Los cables están ordenados y accesibles desde zonas externas? | | X | | 0 |
| 17 | ¿Las ventanas permiten ingreso desde el exterior? | X | | | 0 |
| 18 | ¿Los escritorios están alineados y sin daños visibles? | X | | | 1 |
| 19 | ¿Los equipos presentan faltantes de piezas o conexiones? | | X | | 1 |
| 20 | ¿Se observan elementos ajenos al ambiente educativo en el laboratorio? | | X | | 1 |
| **Realizado Por:**<br>Castro Alava Julexy Jamileth | | | | **Revisado Por:**<br>Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:**<br>20-23/10/2025 | | | | **Firma:** | |

**Figura 24**

*Cuestionario de identificación de riesgos parte 2*

| CUESTIONARIO PARA IDENTIFICAR IDENTIFICACIÓN DE INCENDIO | | | | C2 Pág. 2 de 5 | |
|---|---|---|---|---|---|
| INCENDIO | | | | | |
| Preguntas | | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿El laboratorio cuenta con detectores de humo? | | X | No Hay | 2 |
| 2 | ¿Existen extintores en lugares estratégicos? | - | - | No Hay | 2 |
| 3 | ¿Los cables eléctricos presentan cortes, peladuras o signos de deterioro? | X | | | 0 |
| 4 | ¿Hay señalización de rutas de evacuación? | | X | | 0 |
| 5 | ¿Hay tomacorrientes sobrecargados? | | X | | 1 |
| 6 | ¿Hay carteles visibles con instrucciones ante incendios? | | X | | 0 |
| 7 | ¿Se almacenan papel, químicos u objetos inflamables junto a equipos? | | X | | 1 |
| 8 | ¿Las cortinas, muebles y pisos son de material resistente al fuego? | | X | | 0 |
| 9 | ¿Hay luces de emergencia con carga suficiente? | | X | | 0 |
| 10 | ¿Filtran líquidos del techo hacia instalaciones eléctricas? | X | | | 0 |
| 11 | ¿Están los pasillos y puertas libres de obstáculos? | X | | | 1 |
| 12 | ¿Hay botiquines de primeros auxilios accesibles y completos? | | X | | 0 |
| 13 | ¿Los cables de red y electricidad están diferenciados y ordenados? | | x | | 0 |
| 14 | ¿El tablero eléctrico principal tiene disyuntores y protecciones? | | X | | 0 |
| 15 | ¿Las paredes muestran humedad cerca de enchufes o cables? | X | | | 0 |
| 16 | ¿Hay personal responsable de seguridad contra incendios? | | X | | 0 |
| 17 | ¿Se dispone de un sistema automático de rociadores? | | X | | 0 |
| 18 | ¿La estructura del techo evita filtraciones sobre los equipos? | | X | | 0 |
| 19 | ¿Se revisa la temperatura de equipos críticos? | | x | | 0 |
| 20 | ¿Se cuenta con seguro contra incendios? | X | | | 1 |
| 21 | ¿Se dispone de un botiquín de primeros auxilios? | | x | | 0 |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 20-23/10/2025 | | | | **Firma:**  | |

**Figura 25**

*Cuestionario de identificación de riesgos parte 3*

| CUESTIONARIO PARA IDENTIFICAR IDENTIFICACIÓN DE DAÑOS DE EQUIPO | | | | C2 Pág. 3 de 5 | |
|---|---|---|---|---|---|
| DAÑO DE EQUIPO | | | | | |
| Preguntas | | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿Se realiza mantenimiento preventivo a los equipos? | | X | | 0 |
| 2 | ¿Existen protocolos visibles para manipulación segura de equipos? | | X | | 0 |
| 3 | ¿Se capacita al personal estudiantil en uso adecuado de equipos? | | X | | 0 |
| 4 | ¿Se cuenta con manuales de operación visibles? | | X | | 0 |
| 5 | ¿Hay control de temperatura y humedad en el laboratorio? | | X | | 0 |
| 6 | ¿Se revisan periódicamente los equipos? | | X | | 0 |
| 7 | ¿Se documentan fallas y reparaciones? | | X | Se realizaba antiguamente. | 0 |
| 8 | ¿Se cuenta con seguro para equipos? | | X | | 0 |
| 9 | ¿El personal docente recibe capacitación sobre el uso adecuado del laboratorio? | | X | Se hizo al inicio, en la actualidad ya no se realiza | 0 |
| 10 | ¿Se controla el acceso a equipos delicados? | | X | | 0 |
| 11 | ¿Se evita el uso indebido de equipos? | | X | | 0 |
| 12 | ¿Hay protocolos visibles para desconexión segura? | | X | | 0 |
| 13 | ¿Se inspeccionan cables y conexiones? | | X | | 0 |
| 14 | ¿Se controla el polvo y limpieza del área? | | X | | 0 |
| 15 | ¿Se dispone de repuestos básicos? | | X | | 0 |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 20-23/10/2025 | | | | **Firma:** | |

**Figura 26**

*Cuestionario de identificación de riesgos parte 3*

| CUESTIONARIO PARA IDENTIFICAR DE INUNDACIÓN | | | | C2 Pág. 4 de 5 | |
|---|---|---|---|---|---|
| INUNDACIÓN | | | | | |
| Preguntas | | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿El laboratorio está ubicado en zona segura contra inundaciones? | X | | | 1 |
| 2 | ¿El piso del laboratorio presenta acumulación de agua? | | X | | 1 |
| 3 | ¿Las puertas sellan correctamente al cerrar? | | X | | 0 |
| 4 | ¿Se drena el agua alrededor del edificio? | | X | | 0 |
| 5 | ¿El techo presenta filtraciones o manchas de humedad? | X | | | 0 |
| 6 | ¿Las ventanas cierran herméticamente? | | X | | 0 |
| 7 | ¿Los equipos están instalados sobre superficies elevadas? | X | | | 1 |
| 8 | ¿Se observan rastros de agua en paredes o esquinas? | X | | | 0 |
| 9 | ¿Los cables están protegidos del contacto con el piso? | | X | | 0 |
| 10 | ¿Hay estructuras externas que protejan del agua? | | X | | 0 |
| 11 | ¿Hay techos con materiales deteriorados? | X | | | 0 |
| 12 | ¿Se almacenan papeles o materiales absorbentes cerca del piso? | | X | | 1 |
| 13 | ¿Hay espacios despejados alrededor de las estaciones de trabajo? | X | | | 1 |
| 14 | ¿Los canalones están obstruidos con hojas o basura? | | X | No Hay | 2 |
| 15 | ¿Los techos cuentan con canaletas funcionales? | | X | | 0 |
| 16 | ¿Los interruptores eléctricos están por encima del nivel del piso? | X | | | 1 |
| 17 | ¿El entorno del edificio permite el drenaje natural del agua? | X | | | 1 |
| 18 | ¿Se observan medidas para proteger equipos durante lluvias? | | X | | 0 |
| 19 | ¿Hay materiales que impidan la evacuación del agua? | | X | | 1 |
| 20 | ¿Las instalaciones se revisan tras eventos de lluvia? | | X | | 0 |
| **Realizado Por:** Castro Alava Julexy Jamileth | | | | **Revisado Por:** Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:** 20-23/10/2025 | | | | **Firma:** | |

**Figura 27**

*Cuestionario de identificación de riesgos parte 3*

| CUESTIONARIO PARA IDENTIFICAR DE MALWARE | | | | C2<br>Pág. 5 de 5 | |
|---|---|---|---|---|---|
| MALWARE | | | | | |
| Preguntas | | Respuestas | | Observación | Riesgo |
| | | Si | No | | |
| 1 | ¿Se cuenta con software antivirus actualizado? | | X | | 0 |
| 2 | ¿Se realizan análisis periódicos de malware? | | X | | 0 |
| 3 | ¿Se capacita al personal en prevención de malware? | | X | | 0 |
| 4 | ¿Existen políticas visibles para instalación de software? | | X | | 0 |
| 5 | ¿Se controla el uso de dispositivos USB? | | X | | 0 |
| 6 | ¿Se aplican actualizaciones de seguridad en sistemas? | | X | | 0 |
| 7 | ¿Hay protocolos ante detección de malware? | | X | | 0 |
| 8 | ¿Se dispone de firewall activo? | | X | | 0 |
| 9 | ¿Se monitorean las conexiones de red? | | X | | 0 |
| 10 | ¿Se restringe el acceso a sitios web no seguros? | | X | | 0 |
| 11 | ¿Se realizan copias de seguridad periódicas? | | X | | 0 |
| 12 | ¿Se controla el uso de correos electrónicos sospechosos? | | X | | 0 |
| 13 | ¿Se aplican políticas de contraseñas seguras? | | X | | 0 |
| 14 | ¿Se verifica la integridad de archivos descargados? | | X | | 0 |
| 15 | ¿Se documentan incidentes de malware? | | X | | 0 |
| 16 | ¿Se cuenta con herramientas de análisis forense digital? | | X | | 0 |
| 17 | ¿Se restringe el acceso remoto no autorizado? | | X | | 0 |
| 18 | ¿Se aplican pruebas de penetración periódicas? | | X | | 0 |
| 19 | ¿Se controla el uso de software pirata? | | X | | 0 |
| 20 | ¿Se dispone de un plan de respuesta ante ataques? | | X | | 0 |
| **Realizado Por:**<br>Castro Alava Julexy Jamileth | | | | **Revisado Por:**<br>Minaya Macias Renelmo Wladimir, Mg. | |
| **Fecha:**<br>20-23/10/2025 | | | | **Firma:** | |

**Figura 28**

*Cuestionario de identificación de riesgos parte 4*

| **Identificación de Riesgos** | **R1**<br>**Pág. 1 de 5** |
|---|---|
| **Robo debido a:**<br>• No hay controles de acceso físico.<br>• No cuenta con cerraduras en puertas y ventanas.<br>• No hay sistema de identificación.<br>• No hay cámaras de vigilancia dentro del laboratorio.<br>• No hay control de ingreso mediante formularios o registros.<br>• No hay restricciones a personas que no pertenecen tanto a la universidad como a la carrera.<br>• No hay restricciones de equipos fuera del lugar.<br>• No se realizan auditorias periódicas.<br>• No se cuenta con protocolos ante intento de robo.<br>• No se controla el ingreso fuera del horario laboral.<br>• Los cables no están ordenados y son accesibles desde zonas internas.<br>• Las ventanas permiten ingreso desde el exterior. | |
| **Realizado por**:<br>Castro Alava Julexy Jamileth | **Revisado por:**<br>Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>30/10/2025 | **Firma:** |

**Figura 29**

*Cuestionario de identificación de riesgos parte 5*

| **Identificación de Riesgos** | **R1**<br>**Pág. 2 de 5** |
|---|---|
| **Incendio debido a:**<br>• No hay extintores.<br>• Los cables eléctricos presentan signos de deterioro.<br>• Rutas de evacuación sin señalización.<br>• No hay carteles con instrucciones ante incendios.<br>• Ventanas con cortinas, muebles y pisos no resistentes al fuego.<br>• Luz de emergencia sin carga suficiente.<br>• Se filtra liquido a través del techo.<br>• No hay botequines de primeros auxilios accesibles y completos.<br>• Los cables de electricidad no se encuentran diferenciados ni ordenados.<br>• El tablero principal no cuenta con disyuntores ni protecciones.<br>• No hay persona responsable de la seguridad contra incendio.<br>• No hay sistema automático de rociadores.<br>• La estructura del techo no evita la filtración de agua sobre los equipos.<br>• No se revisa la temperatura de los equipos.<br>• No se cuenta con un botequín de primeros auxilios. | |
| **Realizado por**:<br>Castro Alava Julexy Jamileth | **Revisado por:**<br>Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>30/10/2025 | **Firma:** |

**Figura 30**

*Cuestionario de identificación de riesgos parte 6*

| **Identificación de Riesgos** | **R1**<br>**Pág. 3 de 5** |
|---|---|

**Daño de equipos debido a:**

- No se realiza mantenimiento preventivo a los equipos.
- No existen protocolos visibles para la manipulación de los equipos.
- No se capacita al personal estudiantil en el uso adecuado de los equipos.
- No se cuenta con manuales de operaciones visibles.
- No hay control sobre la temperatura del laboratorio.
- No se revisa periódicamente los equipos.
- No hay capacitación actualmente para los docentes que usan el laboratorio.
- Uso indebido de los equipos.
- No hay inspección de los cables.
- No hay señalización de limpieza alguna.
- No se cuenta con repuestos básicos.

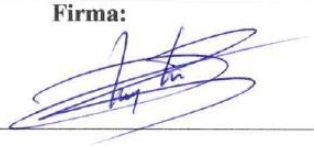
| **Realizado por**: | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>30/10/2025 | **Firma:**  |

**Figura 31**

*Cuestionario de identificación de riesgos parte 7*

| **Identificación de Riesgos** | **R1**<br>**Pág. 4 de 5** |
|---|---|
| **Inundación debido a:**<br>• La puerta cuenta con un cerrojo defectuoso.<br>• Los cables no están protegidos por canaletas.<br>• Falta de drenaje de aguas lluvias en la universidad, se empoza.<br>• Goteras visibles en el techo lo que causa filtración.<br>• Ventanas con filtraciones pequeñas ante grandes aguaceros.<br>• Presencia de humedad en el cielo raso.<br>• Cables en contacto directo con el piso.<br>• Oxido y material deteriorado en el techo.<br>• Falta de altura al piso de los equipos.<br>• Revisión post lluvias no se hace regularmente. | |
| **Realizado por**:<br>Castro Alava Julexy Jamileth | **Revisado por:**<br>Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>30/10/2025 | **Firma:** |

**Figura 32**

*Cuestionario de identificación de riesgos parte 8*

| **Identificación de Riesgos** | **R1**<br>**Pág. 5 de 5** |
|---|---|
| **Malware debido a:**<br>• No cuenta con un antivirus completo, ni actualizado.<br>• No se hace informes de malware periódicas.<br>• No existen herramientas adecuadas para manejar los ataques malware.<br>• No hay un protocolo a seguir para instalar software.<br>• No se controla el uso de dispositivos USB.<br>• No se hacen las actualizaciones de software.<br>• No se encuentra activo el firewall en los dispositivos.<br>• No se lleva control de los movimientos en la red<br>• No hay un plan de copias de seguridad efectivo.<br>• No se usa contraseñas con niveles altos de seguridad.<br>• No se lleva un historial de accidentes de malware.<br>• No se controla el uso de software pirata en los equipos del laboratorio.<br>• No hay un plan de respuesta ante algún ataque. | |
| **Realizado por**:<br>Castro Alava Julexy Jamileth | **Revisado por:**<br>Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>30/10/2025 | **Firma:** |

**Figura 33**

*Valoración de riesgos 1*

| Valoración De Riesgos | R2<br>Pág. 1 de 3 |
|---|---|

| PROBABILIDAD DE ROBO | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 20 | 0 |
| **Total, Seguro** | 9 | 0 |
| **Total, Riesgo** | 11 | 0 |
| **Porcentaje Seguro** | 9*100/20= | 45 % |
| **Porcentaje Riesgo** | 11*100/20= | 55% |

| PROBABILIDAD DE INCENDIO | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 21 | 2 |
| **Total, Seguro** | 4 | 0 |
| **Total, Riesgo** | 15 | 0 |
| **Porcentaje Seguro** | 4*100/19= | 21% |
| **Porcentaje Riesgo** | 15*100/19= | 79% |

| **Realizado por:** | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:**<br>10/11/2025 | **Firma:** |

**Figura 34**

*Valoración de riesgos 2*

| Valoración de riesgos | R2<br>Pág. 2 de 3 |
|---|---|

| PROBABILIDAD DE DAÑO DE EQUIPO | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 15 | 0 |
| **Total, Seguro** | 0 | 0 |
| **Total, Riesgo** | 15 | 0 |
| **Porcentaje Seguro** | 0*100/15= | 0% |
| **Porcentaje Riesgo** | 15*100/15= | 100% |

| PROBABILIDAD DE INUNDACIÓN | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 20 | 1 |
| **Total, Seguro** | 8 | 0 |
| **Total, Riesgo** | 11 | 0 |
| **Porcentaje Seguro** | 8*100/19= | 42% |
| **Porcentaje Riesgo** | 11*100/19= | 58% |

| **Realizado por:** | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** | **Firma:** |
| 10/11/2025 |  |

**Figura 35**

*Valoración de riesgos 3*

| Valoración de riesgos | R2<br>Pág. 3 de 3 |
|---|---|

| PROBABILIDAD DE MALWARE | | |
|---|---|---|
| | **Total** | **No Aplica** |
| **Total, De Campo Evaluados** | 20 | 0 |
| **Total, Seguro** | 0 | 0 |
| **Total, Riesgo** | 20 | 0 |
| **Porcentaje Seguro** | 0*100/20= | 0% |
| **Porcentaje Riesgo** | 20*100/2= | 100% |

| Riesgo | Porcentaje De Riesgo | Porcentaje De Seguridad |
|---|---|---|
| **Robo** | 55% | 45% |
| **Incendio** | 58% | 42% |
| **Daño de Equipo** | 100% | 0% |
| **Inundación** | 58% | 42% |
| **Malware** | 100% | 0% |

| **Realizado por:** | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** | **Firma:** |
| 10/11/2025 |  |

## Anexo I. Cálculo de impacto

**Figura 37**

*Cálculo de impacto*

| Cálculo de Impacto | R2<br>Pág. 1 de 1 |
|---|---|

| Riesgo | Confidencialidad | Integridad | Disponibilidad | Valor de impacto |
|---|---|---|---|---|
| **Robo** | 1 | 4 | 3 | 8 |
| **Incendio** | 3 | 4 | 3 | 10 |
| **Daño de Equipos** | 1 | 3 | 3 | 7 |
| **Inundación** | 1 | 1 | 3 | 5 |
| **Malware** | 5 | 5 | 4 | 14 |

| Escala | Descripción |
|---|---|
| **1** | No afecta mayormente |
| **2** | Afecciones menores |
| **3** | Paralización de la actividad, corto tiempo |
| **4** | Afecciones mayores |
| **5** | Efecto catastrófico |

| **Realizado por:** | **Revisado por:** |
|---|---|
| Castro Alava Julexy Jamileth | Minaya Macias Renelmo Wladimir, Mg. |
| **Fecha:** 15/11/2025 | **Firma:** |

## Anexo J. Certificado de coincidencia académica

### Figura 36

*Certificado Antiplagio*

CERTIFICADO DE ANÁLISIS
*magister*

AUDITORIA INFORMÁTICA JULEXI CASTRO COMPILATIO V3

4% Textos sospechosos

1% Similitudes
0% similitudes entre comillas
< 1% entre las fuentes mencionadas
3% Idiomas no reconocidos
10% Textos potencialmente generados por la IA (ignorado)

**Nombre del documento:** AUDITORIA INFORMÁTICA JULEXI CASTRO COMPILATIO V3.docx
**ID del documento:** b020f981fdcb8a3052cb438e37ec5c0ca0c631b6
**Tamaño del documento original:** 11,92 MB

**Depositante:** RENELMO MINAYA MACIAS
**Fecha de depósito:** 9/2/2026
**Tipo de carga:** interface
**fecha de fin de análisis:** 9/2/2026

**Número de palabras:** 22.197
**Número de caracteres:** 151.879

Ubicación de las similitudes en el documento:

**Fuentes principales detectadas**

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | tesis_Wendy_Ramirez.docx \| tesis_Wendy_Ramirez<br>Viene de de mi grupo<br>3 fuentes similares | < 1% | | Palabras idénticas: < 1% palabras) |
| 2 | repositorio.uleam.edu.ec<br>https://repositorio.uleam.edu.ec/bitstream/123456789/9095/1/ULEAM-TEC.INF-105.pdf<br>3 fuentes similares | < 1% | | Palabras idénticas: < 1% palabras) |
| 3 | definicion.de \| Directrices - Qué es, definición y concepto<br>https://definicion.de/directrices/ | < 1% | | Palabras idénticas: < 1% (66 palabras) |
| 4 | www.academia.edu \| (PDF) Memorias Científicas III Jornada Científica Internacio...<br>https://www.academia.edu/102049090/Memorias_Cientificas_III_Jornada_Cientifica_Internaci...<br>3 fuentes similares | < 1% | | Palabras idénticas: < 1% (77 palabras) |
| 5 | respuestasrapidas.com.mx \| Qué son las preguntas directrices de una investiga...<br>https://respuestasrapidas.com.mx/que-son-las-preguntas-directrices-de-una-investigacion/ | < 1% | | Palabras idénticas: < 1% (76 palabras) |

**Fuentes con similitudes fortuitas**

| Nº | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | repositorio.uleam.edu.ec<br>https://repositorio.uleam.edu.ec/bitstream/123456789/749671/ULEAM-TEC.INF-049.pdf | < 1% | | Palabras idénticas: < 1% (32 palabras) |
| 2 | doi.org \| Auditoría de Tecnologías de la Información Enfoques, Herramientas y N...<br>https://doi.org/10.70577/ey597m50/academia.editorial/2025 | < 1% | | Palabras idénticas: < 1% (36 palabras) |
| 3 | dspace.unach.edu.ec \| Repositorio Digital UNACH: Auditoría informática de segu...<br>http://dspace.unach.edu.ec/handle/51000/14470 | < 1% | | Palabras idénticas: < 1% (34 palabras) |
| 4 | es.ame-jumelle.com \| Significado De Idoneo [ 2023 ]<br>https://es.ame-jumelle.com/webstories/significado-de-idoneo/ | < 1% | | Palabras idénticas: < 1% (28 palabras) |
| 5 | JOSUE PEÑAFIEL.docx \| JOSUE PEÑAFIEL<br>Viene de de mi biblioteca | < 1% | | Palabras idénticas: < 1% (23 palabras) |

**Fuentes mencionadas (sin similitudes detectadas)** Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://achirou.com/
2 https://www.isotools.us/2023/06/06/seguridad-fisica-y-del-entorno-en-iso-27002/
3 https://www.pmg-ssi.com/2025/09/que-es-y-para-que-sirve-la-norma-iso-27002/
4 https://es.isms.online/iso-27002/
5 https://www.britishacademiadeingles.com/blog/que-es-el-nivel-de-ingles-b1-explicado/

# Glosario

***C***

**Controles Preventivos:**

Los controles preventivos son medidas diseñadas para identificar y minimizar riesgos antes de que ocurran, garantizando la protección en diferentes entornos, como la seguridad alimentaria o la ciberseguridad.

***E***

**Escaneo de Iris:**

es una tecnología que utiliza luz infrarroja para capturar los patrones únicos del ojo humano y almacenarlos para identificar a las personas con un margen de error casi nulo, similar a la huella digital.

**Estructurado:**

Que tiene buenas bases, que tiene buena estructura o buena disposición. Quiere decir quiere decir ordenado, organizado, armado, construido, configurado, preparado.

***D***

**Datos Sistemáticos:**

Conjuntos de información recopilados, organizados y analizados siguiendo un método estricto, ordenado y predefinido para asegurar fiabilidad, precisión y objetividad.

**Directrices:**

Una norma o una instrucción que se tiene en cuenta para realizar una cosa. También se trata de aquello que fija cómo se producirá algo. Las directrices, por lo tanto, sientan las bases para el desarrollo de una actividad o de un proyecto.

***G***

**Gestionar Riesgos:**

La gestión de riesgos es el proceso de identificar, evaluar y minimizar el impacto del riesgo. En otras palabras, es una forma de que las organizaciones identifiquen los peligros y amenazas potenciales y tomen medidas para eliminar o reducir las posibilidades de que ocurran.

## *I*

**Idóneo:**

Se emplea para calificar a aquello que resulta conveniente para algo. El término puede referirse a una persona, un objeto o una situación.

**Infraestructura:**

Se define como un sistema físico básico de una empresa, región o nación y suele implicar la producción o procesos de producción.

**Inalterables:**

Se utiliza para calificar lo que no puede alterarse o que nunca se altera. Alude a modificar la forma o la esencia de algo.

## *S*

**Sistema Biométrico:**

Es un sistema que permite identificar la identidad de una persona utilizando características físicas únicas como el iris.

## *M*

**Metodologías Operativas:**

Es un método analítico que permite resolver problemas y tomar mejores decisiones.

**Monitoreo:**

Es el proceso continuo mediante el cual se valora la eficiencia y la eficacia de un proyecto mediante la identificación de sus logros y debilidades.

## *R*

**Recopilación:**

Proceso de seleccionar diversas cosas, especialmente usado con información o datos, en un solo conjunto.

**Restringir:**

Limitar algo a menores cantidades, ya sea físicos, de numérico, tiempo o derechos.