UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR

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

AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DE SALAS DE DOCENTES EN ULEAM EXTENSIÓN EL CARMEN

ZAMBRANO BENALCÁZAR DAYANA MISHELLE

AUTORA:

A.S. MINAYA MACIAS RENELMO WLADIMIR, MG.

TUTOR

EL CARMEN, FEBRERO 2026

CERTIFICACIÓN DEL TUTOR

Uleam ELOY ALFARO DE MANABÍ	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 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 **ZAMBRANO BENALCÁZAR DAYANA MISHELLE**, legalmente matriculado/a en la carrera de Ingeniería en Tecnología de la Información, período académico 2025(1)-2025(2), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es "**AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DE SALAS DE DOCENTES EN ULEAM EXTENSIÓN EL CARMEN**".

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

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

El Carmen, 02 de Enero de 2026.

Lo certifico,

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

TRIBUNAL DE SUSTENTACIÓN

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:
AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DE SALAS DE DOCENTES EN ULEAM EXTENSIÓN EL CARMEN.

Modalidad:
Proyecto Integrador

Autor:
Zambrano Benalcázar Dayana Mishelle

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

Tribunal de Sustentación:

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

Fecha de Sustentación:
23 Febrero de 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: AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DE SALAS DE DOCENTES EN ULEAM EXTENSIÓN EL CARMEN, corresponde exclusivamente a: ZAMBRANO BENALCÁZAR DAYANA MISHELLE con CI. 2300698467, y los derechos patrimoniales de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí.

Zambrano Benalcázar Dayana Mishelle
C.I. 2300698467

DEDICATORIA

A moca y michi oreo ya que a pesar de la hora siempre se durmieron junto a mi computadora acompañándome.

A mis padres Daniel y Nancy Marcial Benalcázar, quienes, aunque hasta el día de mi graduación me preguntaran "¿De qué te gradúas?", siempre supieron brindarme su apoyo, amor y tiempo cada que lo necesito sin pedirme nada a cambio, por enseñarme el valor de la responsabilidad y no desampararme en este proceso, los amo.

A mis abuelos Edgar, Raúl, Gloria y Sara por siempre brindarme su bendición en cada paso, aunque para ellos siempre fue "mijita usted que le sabe, préstame este celular", nunca dejaron la ilusión de ver a un nieto titulado profesionalmente, deseo que no sea la primera ni la última vez que puedan decir este orgullo que solo ellos conocen.

A cada uno de los que me dedicaron su amor y amistad en todo este proceso quienes, aunque nunca los abrazaba entendían que les demostraba mi amor cocinándoles cada cosa que querían, con quienes hasta no hacer nada juntos era mejor que no hacer nada solos, espero que en cada perrito o gatito que encuentren y sepan que me lo hubiera querido robar se acuerden de mí y sientan que siempre estaré para ustedes.

Especialmente al hombre que a pesar de todo a estado conmigo, principalmente al momento de realizar esté proceso tan importante, gracias por haber confiado en mi incluso cuando yo no lo hacía, gracias por brindarme tu amor con mucha paciencia, aunque estuviese llorando, sin tu apoyo no hubiera sido emocionalmente posible para mí. Te amo Spanki.

Dayana

AGRADECIMIENTO

Expreso mi sincero agradecimiento a la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, por abrirme sus puertas y brindarme la oportunidad de alcanzar un título universitario, así como por proporcionar un entorno académico que fomenta el aprendizaje, la investigación y el desarrollo profesional.

De manera especial, agradezco a la **c**arrera de Tecnología de la Información y docentes que lo conforman, por los conocimientos impartidos a lo largo de mi formación, los cuales han sido fundamentales para el desarrollo de mis habilidades técnicas, analíticas y profesionales, preparándome para enfrentar los retos del ámbito laboral con responsabilidad y compromiso.

Mi reconocimiento y gratitud al Ing. Wladimir Minaya, tutor de la presente investigación, por su guía, paciencia y apoyo constante durante el desarrollo de este trabajo de titulación. Sus observaciones, correcciones y conocimientos fueron esenciales para fortalecer el contenido de la tesis y orientarme hacia un trabajo académico riguroso y de calidad.

Finalmente, agradezco profundamente a mi familia, por su apoyo incondicional, comprensión y motivación constante. Gracias por creer en mí, acompañarme en cada etapa de este camino y ser el pilar fundamental que me impulsó a no rendirme y a alcanzar esta meta profesional.

Dayana Z Benalcázar.

ÍNDICE DE CONTENIDOS

ÍNDICE TABLAS

ÍNDICE GRÁFICOS E ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación tuvo como objetivo realizar una auditoría informática para evaluar la seguridad física y lógica de los equipos ubicados en la sala de docentes de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, con el fin de identificar riesgos que afecten la confidencialidad, integridad y disponibilidad de la información institucional.

El problema identificado se relaciona con debilidades en los controles de acceso, la protección de los equipos y la gestión de la seguridad, lo que incrementa la exposición a robos, accesos no autorizados, amenazas informáticas y eventos ambientales.

La metodología empleada fue de tipo descriptiva, aplicando la metodología MAGERIT para el análisis y valoración de riesgos. Se utilizaron técnicas como la observación directa, encuestas y entrevistas al personal docente y técnico, considerando como referencia las normas ISO/IEC 27001, ISO/IEC 27002 y COBIT.

Como propuesta, se desarrolló un proceso de auditoría estructurado que permitió evaluar el cumplimiento de controles de seguridad y determinar vulnerabilidades existentes.

Los principales hallazgos evidenciaron deficiencias en el control de acceso físico, ausencia de sistemas de vigilancia, falta de medidas preventivas ante incendios e inundaciones, y debilidades en la protección contra malware y mantenimiento de equipos.

Se recomienda implementar un Manual de Buenas Prácticas orientado al fortalecimiento de controles, gestión de incidentes y capacitación del personal, a fin de reducir los riesgos identificados y mejorar la seguridad institucional.

ABSTRACT

This research aimed to conduct an IT audit to evaluate the physical and logical security of the equipment located in the teachers' room at Universidad Laica Eloy Alfaro de Manabí, El Carmen Extension, in order to identify risks affecting the confidentiality, integrity, and availability of institutional information.

The identified problem is related to weaknesses in access controls, equipment protection, and security management, which increase exposure to theft, unauthorized access, cyber threats, and environmental risks.

The methodology was descriptive in nature, applying the MAGERIT methodology for risk analysis and assessment. Data collection techniques included direct observation, surveys, and interviews with teaching and technical staff. The study also considered the guidelines of ISO/IEC 27001, ISO/IEC 27002, and COBIT as reference standards.

As a proposal, a structured audit process was developed to evaluate compliance with security controls and identify existing vulnerabilities.

The main findings revealed deficiencies in physical access control, lack of surveillance systems, absence of preventive measures against fire and flooding, and weaknesses in malware protection and equipment maintenance.

It is recommended to implement a Best Practices Manual focused on strengthening access controls, incident management, and staff training in order to reduce identified risks and improve institutional information security

CAPÍTULO 1

1 INTRODUCCIÓN

1.1 Introducción

La transformación digital ha incrementado significativamente la dependencia de las instituciones educativas respecto a los sistemas de información y recursos tecnológicos, convirtiendo a la seguridad informática en un elemento estratégico para garantizar la continuidad de los procesos académicos y administrativos. En este contexto, la protección de los activos tecnológicos, tanto físicos como lógicos, se vuelve fundamental para preservar la confidencialidad, integridad y disponibilidad de la información institucional.

Las universidades, al gestionar información académica, administrativa y personal de estudiantes y docentes, se encuentran expuestas a múltiples riesgos, tales como accesos no autorizados, robo de equipos, fallas técnicas, malware y amenazas ambientales. La ausencia de políticas formales, controles de acceso adecuados y procedimientos documentados puede incrementar la vulnerabilidad de los sistemas informáticos, afectando directamente el desempeño institucional y la calidad del servicio educativo.

En la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, las salas de docentes constituyen espacios estratégicos donde se desarrollan actividades académicas y administrativas apoyadas en el uso de equipos informáticos. Sin embargo, la falta de una evaluación sistemática de los controles de seguridad existentes genera incertidumbre respecto al nivel de protección de los activos tecnológicos y la gestión de los riesgos asociados.

Ante esta problemática, la presente investigación tiene como objetivo desarrollar una auditoría informática orientada a evaluar la seguridad de los equipos en las salas de docentes,

aplicando como marco de referencia la norma ISO/IEC 27001 para la verificación del cumplimiento de controles y la metodología MAGERIT para el análisis y valoración de riesgos. A través de esta evaluación, se busca identificar vulnerabilidades, determinar el nivel de riesgo existente y proponer acciones de mejora que fortalezcan la gestión de la seguridad de la información en la institución.

1.2 Presentación del tema.

Esta "AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DE SALAS DE DOCENTES EN ULEAM EXTENSIÓN EL CARMEN" está enfocada en los mecanismos de control de accesos, considerando aspectos como la identificación de vulnerabilidades, la evaluación de políticas y procedimientos, esencial para garantizar la protección de la infraestructura tecnológica, los datos confidenciales y la operatividad segura de los sistemas. Este tipo de auditoría no solo evalúa el acceso físico y lógico, sino que también considera la seguridad de las redes

1.3 Ubicación y contextualización de la problemática.

La Universidad Laica Eloy Alfaro de Manabí (ULEAM) fue creada legalmente el 13 de noviembre de 1985. Su fundación fue impulsada por un grupo de docentes y estudiantes, liderados por el Dr. Medardo Mora Solórzano, quien propuso convertir a Manta en una ciudad universitaria en febrero de 1981. La Ley de Creación fue publicada en el registro oficial 313, después de un proceso de dos años para su establecimiento, su matriz se encuentra en la ciudad de manta y dos años después de la creación se aprobó la creación de la extensión en el cantón más distante de la matriz, existiendo las carreras vinculadas a educación, agropecuaria y contabilidad.

La Extensión El Carmen de la Universidad Laica Eloy Alfaro de Manabí (Uleam) 4 de julio 1987, inicio sus actividades correspondientes dentro de esta institución. Con un enfoque de trabajo centrado en formar profesionales que sean competentes y también emprendedores apoyados desde lo académico, en la investigación, y la vinculación, que contribuyan así a una mejor en la calidad de vida de nuestra sociedad.

La seguridad de la información se ha convertido en un elemento fundamental para las instituciones de educación superior, ya que garantiza la protección de los activos tecnológicos y la continuidad de las actividades académicas y administrativas. En la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, los equipos informáticos ubicados en la sala de docentes constituyen recursos esenciales para el desarrollo de funciones académicas, administrativas y de investigación, por lo que su adecuada protección resulta indispensable.

1.4 Planteamiento del problema

1.4.1 Problematización

El principal inconveniente radica en la falta de seguridad en el acceso a las oficinas de la planta central de ULEAM El Carmen. Este problema abarca no solo el ingreso y salida del personal administrativo, sino también de los alumnos. Al ser un entorno expuesto, se vulnera tanto la información como los equipos, ya sean de uso personal de los docentes o las herramientas proporcionadas por la institución.

Dada la situación descrita, estas oficinas enfrentan riesgos significativos que requieren una evaluación detallada. En dicha evaluación, se valoran las vulnerabilidades dentro de las políticas aplicadas en estas áreas, las cuales demandan un mayor cuidado. Estas vulnerabilidades representan un riesgo tanto para la información personal del personal administrativo como para la de los estudiantes

1.4.2 Génesis del problema

La tecnología constituye un pilar fundamental para el desarrollo de un país, dado que el futuro está estrechamente vinculado a los avances tecnológicos. Esta verdad era especialmente evidente en situaciones nuevas, como con el uso de clases virtuales y el teletrabajo. Aquí, es particularmente la seguridad del equipo tecnológico lo que importa, porque un compromiso es perjudicial en todos los sectores laborales. Cuando se trata de instituciones públicas, a diferencia de las privadas, esto es mucho más común ya que las instituciones públicas son más propensas a enfrentar el riesgo de robo de equipos tecnológicos, amenazando así la eficacia de las medidas de seguridad existentes debido al libre acceso de personas a sus instalaciones, uno de los riesgos más comunes en este contexto sería la pérdida o daño de dispositivos por acceso no autorizado, externo o interno, de personas dentro de la organización, típicamente estudiantes o personal administrativo sin las licencias o permisos asociados. De manera similar, existe otra gran amenaza, la del uso inapropiado de los recursos tecnológicos, incluyendo el acceso a sitios no autorizados o la difusión de contenido ilegal, lo que representa un riesgo continuo de socavar la estructura de la institución.

1.4.3 Estado actual del problema

En la actualidad, uno de los factores que más afecta el funcionamiento de los equipos utilizados por el personal administrativo en las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen además del libre acceso de usuarios, son las condiciones climáticas. Estos factores ambientales comprometen la seguridad y el desempeño de los equipos tecnológicos, acelerando su deterioro y reduciendo significativamente su vida útil.

Por este problema, es primordial asegurar que se apliquen bien las normas para cuidar los bienes de tecnología. Pero, no tener una revisión de cómo se manejan los riesgos es un fallo grande. Esto pasa porque no se pueden revisar bien si las defensas y las correcciones se están

usando. Si no hay un proceso de revisión cierto, no se puede mirar si lo que se hace sirve para la seguridad. Tampoco se puede ver si cumple con lo que la entidad necesita para seguir trabajando

1.5 Diagrama causa – efecto del problema

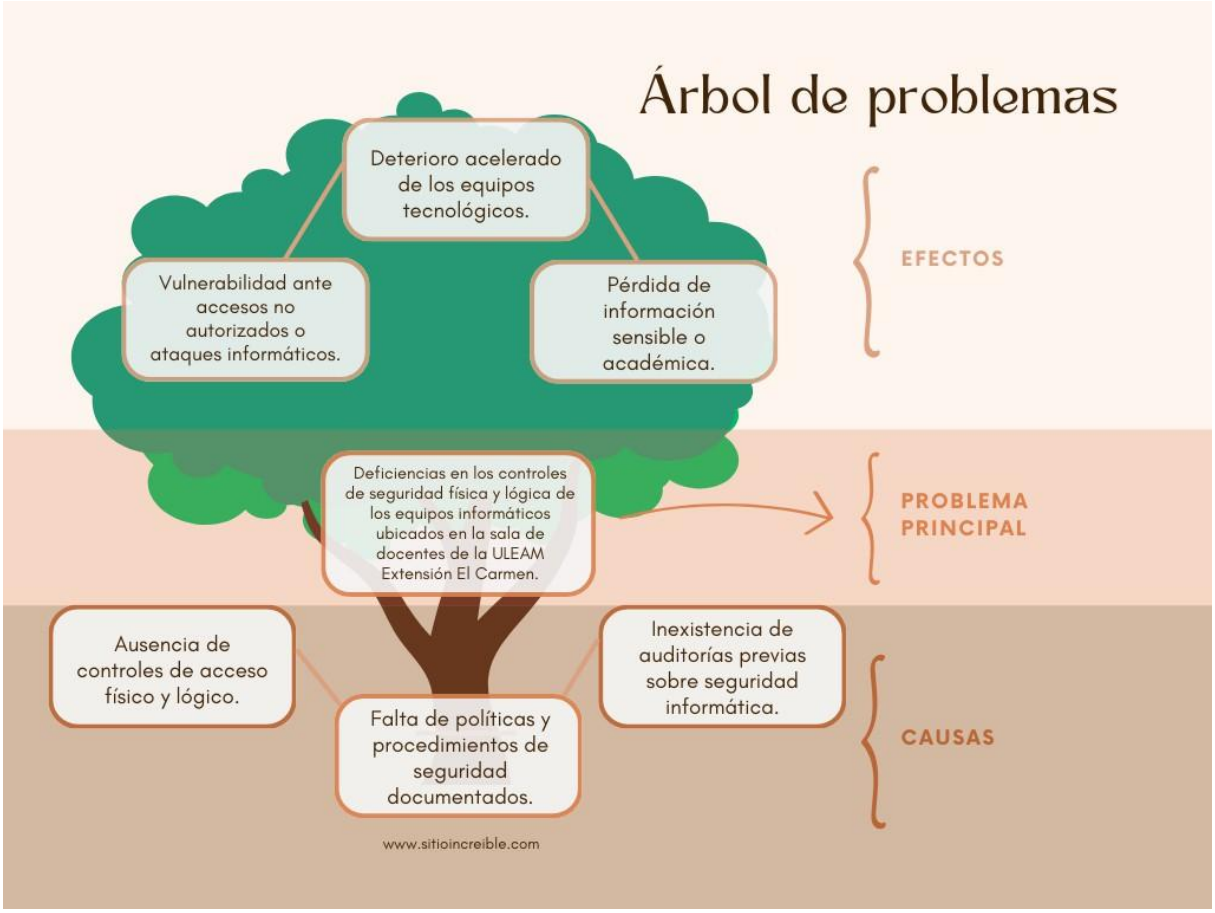


Figura 1 *Árbol de decisiones*

1.6 Objetivos

1.6.1 Objetivo general

Desarrollar una auditoría informática a la Seguridad de los equipos de salas de Docentes en Uleam Extensión El Carmen

1.6.2 Objetivos específicos.

- Describir las características de la problemática mediante un proceso estructurado para identificar los elementos a considerar en la solución
- Identificar antecedentes de investigaciones en fuentes de los últimos 5 años, bibliografías y variables.
- Identificar la existencia o no del problema mediante técnicas y métodos de investigación.
- Realizar una auditoría que evalúe los riesgos de seguridad de las salas de docentes aplicando las Normas y reglamentos elegidos.
- Proponer una solución con los resultados de la auditoría.

1.7 Justificación

La auditoría informática se ha convertido en un elemento esencial para garantizar la seguridad y el cumplimiento de normativas en diversas organizaciones, tanto en el ámbito educativo como empresarial. El objetivo principal es evaluar a fondo la configuración técnica, localizar vulnerabilidades y verificar que los sistemas electrónicos estén en sintonía con las leyes y regulaciones existentes. Está metodología no solo diagnostica el estado de los sistemas, sino que también define correctivas y preventivas que mantienen la integridad, disponibilidad y confidencialidad de los recursos de TI.

En la situación de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, específicamente en las salas docentes de está, no se ha realizado previamente una auditoría enfocada a la gestión de seguridad de los docentes, la ausencia de esta información nos deja claro que es esencial llevar a cabo un proceso de auditoría que sea objetivo para documentar el estado de los sistemas tecnológicos y los posibles riesgos, problemas de seguridad y posibles factores de amenaza para operar los sistemas.

Además, la gestión de la seguridad de TI te ayuda a anticipar riesgos debido a algunos eventos significativos, incluidos los eventos de desastres naturales, pérdidas de equipos o daños a la infraestructura, como tal, debe estar bajo ciertas regulaciones que mantengan en funcionamiento las instituciones, los resultados de una auditoría no se limitan únicamente a señalar fallas, sino que también permiten definir medidas efectivas que ayuden a evitar la repetición de incidentes y a mejorar la seguridad del entorno tecnológico. El impacto de la auditoría de TI no se refleja solo en el análisis técnico de los sistemas, sino también en la toma de decisiones estratégicas y en la gobernanza organizacional. Al contar con una visión integral de los sistemas de información, las instituciones pueden anticipar riesgos y responder oportunamente a los avances tecnológicos (Raya, 2019)

Además, la auditoría informática es fundamental para garantizar la transparencia y la rendición de cuentas, especialmente en entornos educativos donde la protección de datos personales y académicos es de suma importancia. La implementación de auditorías regulares contribuye a la creación de una cultura organizacional orientada a la mejora continua y al cumplimiento de estándares internacionales de seguridad de la información.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

La ULEAM extensión El Carmen mediante una auditoria basada en herramientas de investigación, por salas se obtendrá un resultado exacto el cual nos ayudará a crear el plan de mejora para así obtener un impacto tecnológico basado en la seguridad controlando el acceso físico y lógico, las normas, las políticas y creando un plan para afrontar los desastres naturales, lo cual ayudará a solucionar problemas actuales y estar preparados para problemas futuros.

No había reglas claras de protección. Los docentes en su mayoría no tenían conocimiento de estas, esto causó que datos que eran muy importantes se perdieran. Hablamos de notas de estudiantes y papeles del trabajo diario. Un examen se hizo en las escuelas públicas de Santo Domingo. Este mostró algo clave. Muchos programas para manejar notas no tienen defensas sólidas. Esto llevó a que se borraran muchos datos. Las razones fueron ataques o fallas que pasaron solas. (Calazacón Aguavil, 2021)

La adopción de tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, en los procesos de auditoría informática, permite una detección más eficiente y precisa de anomalías y patrones de riesgo. Estas herramientas avanzadas facilitan la identificación temprana de posibles brechas de seguridad y optimizan la asignación de recursos para su mitigación. Así mismo, la implementación de soluciones de virtualización y computación en la nube ha transformado la manera en que las instituciones gestionan sus infraestructuras tecnológicas. Estas tecnologías ofrecen mayor flexibilidad, escalabilidad y eficiencia en el uso de recursos, lo que se traduce en una mejora significativa en la resiliencia y continuidad operativa de los servicios educativos. (Reyes, 2023)

1.8.2 Impacto social

La implementación de planes de seguridad informática en instituciones educativas contribuye a la protección de datos personales y académicos, promoviendo una cultura de responsabilidad digital y fortaleciendo la confianza en el entorno institucional. Además, la educación en ciudadanía digital permite que estudiantes y docentes desarrollen competencias para el uso seguro y responsable de la tecnología, reduciendo riesgos asociados al manejo inadecuado de la información.

En la ULEAM Extensión El Carmen, el fortalecimiento de la seguridad informática impactará directamente en la comunidad universitaria, al garantizar la protección de notas, documentos académicos y datos personales. Asimismo, la implementación de buenas prácticas y capacitaciones permitirá que docentes y estudiantes comprendan la importancia del resguardo de la información, fomentando un entorno digital más seguro, confiable y responsable.

1.8.3 Impacto ecológico

Las buenas prácticas en el uso y mantenimiento de equipos informáticos permiten extender su vida útil, reducir el consumo energético y disminuir la generación de residuos electrónicos, los cuales representan un problema ambiental significativo debido a sus componentes contaminantes. Además, la implementación de estrategias tecnológicas sostenibles contribuye a optimizar recursos y reducir la huella de carbono asociada al uso de infraestructura digital.

En el contexto de la ULEAM Extensión El Carmen, la identificación de vulnerabilidades y la implementación de planes de mantenimiento preventivo contribuirán a prolongar la vida útil de los equipos ubicados en las salas de docentes, evitando reemplazos innecesarios y reduciendo la generación de desechos electrónicos. De esta manera, la auditoría no solo fortalecerá la seguridad tecnológica, sino que también promoverá una gestión responsable y sostenible de los recursos informáticos institucionales.

CAPÍTULO II:

2 MARCO TEÓRICO

2.1 Antecedentes históricos

La auditoría informática es un proceso sistemático que permite evaluar la eficacia y seguridad de los sistemas de información dentro de una organización. Su propósito principal es garantizar que estos sistemas cumplan con los estándares establecidos, protejan los activos informáticos y apoyen los objetivos organizacionales. Para lograrlo, se utilizan diversas metodologías y herramientas que facilitan la identificación de riesgos y la implementación de controles adecuados. (Arantes, 2023)

La auditoría informática ha crecido como una disciplina y herramienta para garantizar la integridad, confidencialidad y disponibilidad de la información, su importancia a crecido debido al aumento del uso de tecnologías de la información y la comunicación en los procesos académicos y administrativos. (Ramírez Coello, 2023)

En la Universidad Laica Eloy Alfaro de Manabí (ULEAM), se han desarrollado investigaciones que abordan la necesidad de implementar auditorías informáticas para fortalecer la seguridad de la información.

Por ejemplo, Ávila Cevallos (2019) realizó un estudio enfocado en evaluar el cumplimiento de las políticas de seguridad al compartir información por parte de los docentes, identificando vulnerabilidades en los sistemas informáticos institucionales.

La auditoría informática es un proceso que mantiene la integridad de los datos, cumple efectivamente los fines organizacionales y optimiza el uso de los recursos disponibles.

El auditor informático, dentro de su rol, evalúa y supervisa en momentos determinados los controles y procedimientos más complejos asociados a los sistemas computarizados. Para

ello, aplica métodos automatizados de auditoría, apoyándose en herramientas de software especializadas. En la actualidad, debido al nivel de complejidad de los sistemas, no siempre es viable realizar verificaciones manuales sobre los procesos que agrupan, calculan y clasifican grandes volúmenes de datos.

El auditor también tiene la responsabilidad de presentar informes a la alta dirección, en los cuales se analiza el diseño y la operación de los controles implementados, junto con la evaluación de la fiabilidad de la información generada por los sistemas, por lo tanto, el trabajo resulta ser importante para fortalecer la seguridad de la informática institucional y facilitar la toma de decisiones estratégicas basadas en información valida. Se conoce que, en Ecuador, el desarrollo de la auditoría informática se ha estado vinculando al fortalecimiento de la gobernanza tecnológica dentro de las instituciones públicas y privadas.

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Los mecanismos de seguridad de la infraestructura están orientados a proteger los diferentes recursos presentes en el sistema, tanto en su ver tiente material como en la de su explotación (esto es, la capa básica de software que habilita el uso de los recursos). A menudo, muchas de estas medidas están encaminadas a controlar el acceso (físico o lógico) a los diferentes recursos (de usuario, de servicio o de comunicaciones), de manera que todos los intentos fraudulentos para acceder a él sean detectados, controlados y filtrados, y se evite, dentro de lo posible, la propagación de los incidentes hacia el resto del sistema. (Raya, 2019)

La seguridad del sistema debe empezar por la protección física de los recursos contra accesos indebidos, riesgos naturales o el fallo de cualquiera de los so portes, sin olvidar que cada recurso de la infraestructura necesitará la protección adecuada de acuerdo con las características que posea y la función que realice.

Así mismo, Demera Zambrano (2023) implementó una auditoría informática basada en la metodología MAGERIT para identificar fallas y vulnerabilidades en los equipos de cómputo de los docentes de la ULEAM Extensión El Carmen, concluyendo que existe una falta de conocimiento sobre los riesgos asociados a la exposición de datos personales y la ausencia de medidas de protección adecuadas.

2.3 Normas ISO/IEC/27001

La norma ISO/IEC 27001 establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), basado en un enfoque de gestión de riesgos y en el ciclo de mejora continua que permita garantizar su seguridad, reducir los riesgos inherentes a su tratamiento, ahorrar costes orientando y complementando correctamente las medidas, garantizar la gestión activa de la seguridad y cumplir con la legislación vigente. Todo esto permitirá sustentar tanto la seguridad técnica como la jurídica de dicha información. Esto implica, además, que la seguridad de la información no es un resultado, sino un proceso iterativo ordenado en fases de planificación, implantación, verificación y actuación (PDCA, de la sigla en inglés de plan, do, check, act). Como se señala en la Ley general de protección de datos (LGPD) y en el Reglamento general de protección de datos (RGPD), el enfoque sobre los riesgos y la responsabilidad proactiva son los ejes principales para garantizar la seguridad de la información. ISO/IEC 27001 no se limita únicamente a controles tecnológicos, sino que integra aspectos organizacionales, humanos y técnicos. Esto implica que la seguridad de la información debe abordarse desde una perspectiva integral que incluya políticas institucionales, procedimientos documentados, formación del personal y controles físicos y lógicos, la norma se fundamenta en el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar) (Raya, Amadeus, & Albus, 2019)

2.3.1 Variable Independiente: Auditoria

Durante mucho tiempo, la auditoría ha sido relacionada con ideas equivocadas, como la creencia de que su finalidad es encontrar errores o señalar a los funcionarios. No obstante, este enfoque es limitado, ya que la auditoría ha evolucionado y actualmente abarca un análisis más amplio. En la actualidad, la auditoría de Tecnologías de la Información ocupa un lugar relevante dentro de las organizaciones modernas, debido a que la gestión de riesgos y la protección de la información se han convertido en factores clave para garantizar la sostenibilidad y el valor empresaria. (Reyes, 2023)

Cuando se habla de revisar cuentas, la gente a veces piensa mal del proceso. Piensan que la meta es solo buscar fallos en una empresa. Creen que se trata de señalar a los empleados, esta idea tiene algo de cierto. Pero la revisión va más allá de solo encontrar fallas o ver cosas raras en quienes son revisados. Con los años, la idea de auditoría cambió. Las áreas que nacen de ella también han crecido (Imbaquingo, y otros, 2020)

Poner en marcha un buen plan de revisión de tecnología es clave. Esto asegura que los datos de una empresa se mantengan correctos y secretos. Hoy, el negocio usa mucha información. Cuidar esos datos importantes es una forma buena de asegurar que la empresa dure. También da valor al negocio. En el campo de revisar la TI, se han hecho muchos intentos para resolver los problemas de ahora. Estos intentos incluyen usar ideas de inteligencia artificial (IA) en las revisiones de TI. Esto es ahora una gran opción para mejorar mucho el proceso de revisión. La IA ofrece muchas herramientas y formas de ver muchos datos. Puede hallar formas raras y hacer tareas que se repiten sin ayuda humana. Esto libera tiempo y dinero para hacer cosas más pensadas y de gran importancia (Reyes, 2023)

Además de su función tradicional de revisión financiera, la auditoría en el contexto actual cumple un papel estratégico dentro de la gobernanza organizacional. Según el Institute

of Internal Auditors (IIA), la auditoría interna proporciona aseguramiento y consultoría independiente y objetiva, diseñada para agregar valor y mejorar las operaciones de una organización, ayudando a cumplir sus objetivos mediante un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno corporativo (Institute of Internal Auditors, 2023)

En el ámbito de las Tecnologías de la Información, la auditoría informática se enfoca en evaluar la seguridad, disponibilidad, integridad y confidencialidad de los sistemas, garantizando que los recursos tecnológicos estén alineados con los objetivos institucionales y cumplan con las normativas vigentes. De acuerdo con ISACA (2019) la auditoría de TI permite identificar debilidades en la infraestructura tecnológica, evaluar controles automatizados y verificar el cumplimiento de estándares internacionales como ISO/IEC 27001.

Asimismo, la auditoría moderna adopta un enfoque basado en riesgos. Esto implica que los recursos de auditoría se concentran en aquellas áreas con mayor probabilidad de impacto negativo para la organización, según el enfoque basado en riesgos mejora la eficiencia del proceso de auditoría al priorizar controles críticos y reducir la exposición a amenazas significativas.

2.3.1.1 Funciones del auditor

Según la (EAE, 2023) la función principal de un auditor es el lograr analizar y evaluar los estados financieros, los controles internos y otra información económica relevante, con el fin de comprobar que los datos sean correctos y confiables, los auditores cumplen un papel importante en el mantenimiento generando confianza pública entre los mercados financieros, gracias a su trabajo, los auditores contribuyen a mantener la confianza pública en los mercados financieros, permitiendo que inversionistas, reguladores y otras partes interesadas cuenten con información confiable para la toma de decisiones.

Además de analizar estados financieros y controles internos, el auditor debe evaluar la eficacia de los sistemas de control implementados y verificar que estos funcionen conforme a las políticas establecidas. En auditoría de TI, esto incluye revisar:

- Configuración de usuarios y privilegios.
- Gestión de contraseñas.
- Registros de acceso (logs).
- Procedimientos de respaldo y recuperación.
- Políticas de seguridad institucional.

De acuerdo a esto el auditor de TI debe obtener evidencia suficiente y competente mediante pruebas sustantivas y pruebas de cumplimiento, con el fin de emitir una opinión objetiva sobre la confiabilidad de los sistemas evaluados.

Además, el auditor cumple una función asesora, ya que puede recomendar mejoras que optimicen procesos tecnológicos y fortalezcan la gobernanza digital.

2.3.1.2 Objetivos de un auditor

El propósito de un auditor es ofrecer una evaluación independiente de los estados financieros de una empresa, para ello se examinan los registros, los controles y otro tipo de información financiera para determinar su validez, integridad y cumplimiento de la ley, teniendo en cuenta que otro de los objetivos de auditor también se centra en garantizar que el estado contable de una empresa se elaboren en base a los principios contables generalmente aceptados (PCGA), todo esto les ayuda a garantizar que los estados financieros sean fáciles de comparar entre empresas, lo que es esencial para tomar decisiones de inversión informadas.

2.3.1.3 Cuál es el perfil de un auditor

Los auditores deben poseer la capacidad de analizar datos financieros complejos y comunicar sus hallazgos a las partes interesadas, tanto en el ámbito financiero como en otros aspectos, de manera clara y concisa. Además, es esencial que estén familiarizados con las normativas legales relacionadas con la contabilidad y sean capaces de recopilar información sobre la compra y venta de servicios o productos, así como sobre los fondos invertidos.

El perfil del auditor moderno requiere una combinación de conocimientos técnicos, capacidad analítica y comprensión del entorno tecnológico. En el caso de la auditoría informática, es indispensable que el profesional posea conocimientos en:

- Seguridad de redes.
- Sistemas operativos.
- Bases de datos.
- Gestión de riesgos.
- Normativas internacionales (ISO 27001, COBIT).

Según Whitman & Mattord (2021) el auditor de seguridad de la información debe comprender tanto los aspectos técnicos de los sistemas como los factores humanos que influyen en la seguridad organizacional, ya que muchos incidentes se originan por errores o negligencia del personal.

También es fundamental que el auditor tenga habilidades comunicativas sólidas, ya que debe presentar informes claros y técnicamente fundamentados a la alta dirección.

2.3.1.4 Habilidades y competencias que todo auditor debe tener

La auditoría se conoce como profesión la cual es considera importante para garantizar la transparencia y la confianza de una empresa, para lo cual se requiere un alto nivel de conocimientos técnicos, habilidades blandas, la capacidad de análisis y comunicativas que ayudan a desempeñar su papel de manera más efectiva, un auditor debe poseer una amplia gama de habilidades y competencias (EAE, 2023)

- **Conocimientos técnicos**

Estos conocimientos se consideran muy importantes ya que en esta profesión se debe poseer un buen conocimiento de las normas contables, las normas de información financiera y los procedimientos de auditoría.

- **Capacidad analítica**

La capacidad de saber realizar un buen análisis es una de las habilidades más importantes que debe poseer un auditor para realizar una auditoría de manera más efectiva, los auditores deben ser capaces de analizar una gran cantidad de datos financieros y contables para así poderlos convertir en información significativa para una empresa.

- **Independencia y objetividad**

Es fundamental en esta profesión, ya que deben asegurar la credibilidad y la integridad en el proceso de análisis, del mismo modo, se logra garantizar que la toma de decisiones empresariales sea información confiable y precisa, una auditoría debe realizarse sin interferencias externas y sin estar influenciado por factores que puedan afectar su juicio.

- **Conducta ética**

La conducta ética es fundamental para la profesión de auditoría ya que los auditores deben ser justos, honestos e imparciales en todas sus decisiones e interacciones. La conducta

ética incluye mantener la confidencialidad, evitar conflictos de intereses y evitar cualquier acción que pueda comprometer su integridad.

- **Gestión del tiempo**

La gestión de tiempo es una habilidad esencial para todo auditor, puesto que los auditores por lo general trabajan con plazos ajustados y deben ser capaces de administrar su tiempo de manera efectiva para cumplir con las fechas y completar las asignaciones de manera efectiva.

2.3.1.5 Auditoría informática y gobernanza de TI

La auditoría informática se vincula estrechamente con la gobernanza de Tecnologías de la Información. La gobernanza de TI asegura que los recursos tecnológicos apoyen la estrategia institucional y generen valor, mientras que la auditoría verifica que estos procesos se desarrollen de manera segura y eficiente.

El marco COBIT 2019, desarrollado por ISACA, establece principios y prácticas para la gobernanza y gestión de TI, proporcionando herramientas que fortalecen la función de auditoría y permiten evaluar el desempeño de los procesos tecnológicos (ISACA, 2019). Este marco enfatiza la importancia de la alineación estratégica, la entrega de valor y la gestión adecuada de riesgos tecnológicos.

En entornos universitarios, la gobernanza de TI es fundamental debido al manejo de información académica, administrativa y personal. La auditoría informática contribuye a verificar que los controles implementados sean adecuados para proteger dichos activos críticos.

2.3.1.6 Enfoque basado en riesgos en auditoría de TI

El enfoque basado en riesgos constituye uno de los pilares fundamentales de la auditoría moderna. Según ISO 31000:2018, actualizada y vigente como referencia internacional en gestión de riesgos, las organizaciones deben identificar, analizar y evaluar los riesgos antes de determinar las medidas de tratamiento adecuadas.

En auditoría informática, este enfoque implica:

- Identificar activos críticos.
- Analizar amenazas y vulnerabilidades.
- Evaluar probabilidad e impacto.
- Determinar el nivel de riesgo residual.
- Proponer controles mitigantes.

De acuerdo con ENISA (2021) la gestión sistemática del riesgo fortalece la resiliencia organizacional frente a amenazas cibernéticas, reduciendo el impacto de incidentes de seguridad.

Este enfoque se alinea directamente con metodologías como MAGERIT y con estándares como ISO/IEC 27001, lo que demuestra la coherencia teórica entre la variable independiente (auditoría) y el marco metodológico de la investigación.

2.3.2 Variable Dependiente: Control de accesos

Es un mecanismo que regula quién puede acceder a qué recursos dentro de un sistema. En el ámbito de la seguridad informática, los controles juegan un papel crucial en la protección de los activos de una organización. Estos controles son acciones y mecanismos diseñados para prevenir o reducir el impacto de eventos no deseados que puedan poner en riesgo dichos activos. Su objetivo principal es mitigar los efectos de amenazas o riesgos, asegurando que las operaciones se realicen conforme a los programas, órdenes y principios establecidos. (Pozo Hernandéz, Reascos Pinchao, & Minaya Macías, 2025)

- **Autenticación**: Verificación de identidad (por ejemplo, contraseñas, biometría).
- **Autorización**: Permisos asignados a usuarios o roles.
- **Auditoría**: Registro de accesos y actividades para su posterior revisión.

El control de accesos constituye uno de los pilares fundamentales dentro de la seguridad de la información, ya que permite garantizar que únicamente los usuarios autorizados puedan interactuar con los recursos tecnológicos de una organización. De acuerdo con **Whitman y Mattord (2021)**, el control de acceso es un conjunto de mecanismos técnicos y administrativos diseñados para regular el acceso a sistemas, aplicaciones, bases de datos y redes, asegurando el cumplimiento del principio de mínimo privilegio.

Asimismo, el estándar **ISO/IEC 27001:2022** establece que las organizaciones deben implementar políticas formales de control de acceso, incluyendo procedimientos para la gestión del ciclo de vida de las cuentas de usuario (creación, modificación, suspensión y eliminación). Esto reduce significativamente el riesgo de accesos no autorizados y filtraciones de información.

El control de accesos no solo se limita a restringir el ingreso, sino que también implica supervisar, registrar y analizar las actividades realizadas por los usuarios dentro del sistema, fortaleciendo así la trazabilidad y la rendición de cuentas.

2.3.2.1 Seguridad informática

Cuando se habla sobre el tema de la seguridad informática es importante saber cuáles son sus fundamentos es decir las definiciones las cuales forman parte de los principios para comprender en qué consisten, así como las formas variadas que existen de ataques, las técnicas de seguridad que se puedan aplicar y las normas aplicadas. (Ponce Ordóñez & Samaniego Mena, 2021) , es el conjunto de políticas, procedimientos y herramientas diseñadas para proteger los activos informáticos de una organización. La seguridad como su nombre lo menciona es una manera de resguardar algo, en este caso información importante de la institución, permite la libertad ante el peligro, con el objetivo de proteger contra ataques o robos premeditados

Para lograr un nivel suficiente de seguridad en la organización, es necesario implementar un sistema de varias capas, las cuales se encuentran conectadas estratégicamente con elementos comunes; por lo tanto, es responsabilidad de la organización asegurarse de que cuenta con estrategias adecuadamente planificadas y organizadas. Los pilares de la información se basan en la necesidad de que los datos sean más fiables y accesibles para conseguir el máximo rendimiento con el mínimo riesgo, por lo que si la información necesaria para la toma de decisiones cayera en manos equivocadas perdería su valor, provocando pérdida de maniobrabilidad y reputación, y perjuicios por el volumen de información disponible. (ENISA, 2021)

Según (Pozo Hernandéz, Reascos Pinchao, & Minaya Macías, 2025) La información es un activo valioso para las organizaciones, por lo que es necesario protegerla y garantizar su seguridad. Los principales objetivos de la seguridad informática incluyen:

Confidencialidad de datos: Garantizar que la información sea accesible únicamente para usuarios, dispositivos y procesos autorizados, también se debe asegurar que sólo el personal autorizado accede a la información que le corresponde utilizar según los recursos que necesarios en la realización de sus tareas, por lo tanto, se asegura la confidencialidad en la cual deben existir tres recursos: Autenticación de usuarios, gestión de privilegios, cifrado de información. (Peltier, 2020)

Integridad: Se refiere a la protección contra alteraciones, adiciones o destrucciones no autorizadas. Asegurar la integridad es esencial, especialmente cuando la información es valiosa y no debe perderse, o cuando los datos podrían ser modificados intencionalmente para engañar al receptor. Normalmente, la información se resguarda contra el borrado mediante métodos que garantizan la confidencialidad y la realización de copias de seguridad. Además, la integridad se verifica mediante técnicas de hashing para asegurar que no haya distorsiones.

Integridad de los datos: Protección contra cambios o manipulación no autorizada.

Disponibilidad: Garantizar el acceso oportuno y confiable a la información y a los 8 servicios de información. Las violaciones típicas de accesibilidad incluyen fallos de software/hardware y ataques de denegación de servicio distribuido (DDoS). El sistema de información se protege contra deficiencias eliminando sus causas y contra ataques DDoS bloqueando el tráfico no deseado

2.3.2.2 Seguridad Física/Hardware

Proteger los elementos físicos de cualquier daño, brinda una seguridad un poco más robusta, por eso es importante proteger los sistemas de energía ininterrumpida con (UPS),

corta fuegos, entre otros. Para conocer si el hardware es seguro hay que tomar atención a los problemas de vulnerabilidades en la fabricación, los dispositivos de entrada y salida de datos que permiten la navegación en la red. (Stallings & Brown, 2021)

La seguridad física es la primera barrera de protección dentro de una infraestructura tecnológica. Según ISO/IEC 27002:2022, las instalaciones que alojan equipos informáticos deben contar con controles de acceso físico, vigilancia, protección contra incendios, sistemas de energía ininterrumpida (UPS) y medidas de control ambiental.

La protección del hardware implica también:

- Control de ingreso a salas de servidores.
- Uso de cámaras de seguridad.
- Registros de visitantes.
- Protección contra sabotaje o robo.

De acuerdo a esto una falla en la seguridad física puede anular cualquier medida lógica implementada, ya que el acceso directo a los equipos permite la manipulación de información o la instalación de dispositivos maliciosos.

En el contexto universitario, la protección de laboratorios y salas docentes resulta fundamental para evitar daños o alteraciones en los equipos tecnológicos.

2.3.2.3 Seguridad Lógica/Software

Protege el software de amenaza que puede ser causado por una brecha u otras posibles vulnerabilidades que crean principios de seguridad de la información, como la confidencialidad, la integridad y la disponibilidad de datos. En el software, puede encontrar diferentes formas de romperlo, por ejemplo, de la implementación de errores, defectos en la fase de diseño, utilizando un desbordamiento de parachoques, falta de seguridad del código,

falta de errores espontáneos, entre otras cosas. Las amenazas son un acto que puede conducir a una violación del sistema, interrupción o corrupción utilizando vulnerabilidades conocidas o desconocidas. Podemos encontrar dos tipos de amenazas: amenazas inesperadas y conscientemente. (Von Solms & Van Niekerk, 2019)

Existen varias amenazas que debemos siempre tomar en cuenta, no solo la vulnerabilidad de ataques o robos, sino también los daños por desastres naturales, es decir que son amenazas accidentales conocidos como los desastres naturales como tormentas, inundaciones, incendios, cortes de energía, terremotos, entre otros. En la parte tecnológica este tipo de amenazas incluyen interrupciones por fallas que se presentan en los equipo, problemas como el software y otros problemas no planificados del sistema, la red o el usuario (CISCO, 2023) a pesar de que estas amenazas son casi imposibles de evitar, si es posible crear un plan el cual nos ayude a manejar estás situaciones y a estar prevenidos, también existen las amenazas deliberadas que se relacionan con estas interrupciones las cuales resultan de una vulnerabilidad del sistema, son el tipo de amenazas que se encuentran mediante los ataques de servicio que impactan la seguridad. (Otero, 2021)

2.3.2.4 Identificación y autenticación

Cuando desarrollamos medidas de seguridad, ya sea un mecanismo específico o infraestructura completa, identificación y la autenticación son los conceptos principales. La identificación es una declaración de lo que alguien

Si algo es y la confirmación determina si esta declaración es verdadera. Podemos ver que dichos procesos tienen lugar todos los días en una variedad de formas. Soltero un ejemplo muy común de identificación y aprobación puede encuentre el uso de la tarjeta de débito que requiere un número de identificación personal (pin). Cuando nos deslizamos sobre el mapa, la tira magnética confirmamos que somos una persona que figura en el mapa. En este punto hemos

dado ya nuestra identificación, pero nada más. Cuando se nos pide que ingresemos al pin de la rama con la tarjeta terminamos la parte de aprobación de la transacción con buena suerte.

Según Vega Briceño (2021) los métodos de identificación y autenticación actuales que se usan normalmente no siempre son de confianza, ya que su efectividad depende de la honestidad de quienes participan en este proceso, por ejemplo, en situaciones donde se requiere mostrar el documento de identificación personal para comprar ciertos productos que se necesita cierta edad, se da por hecho que la identificación es válida y refleja datos reales ya que ni existe una revisión previa haciendo qué este se vuelva un problema.

También dependemos de que la persona o el sistema que realiza la autenticación sea competente y capaz no solo de realizar el acto de autenticación, sino también de poder detectar actividades falsas o fraudulentas. Podemos utilizar varios métodos de identificación y autenticación, desde el simple uso de nombres de usuario y contraseñas, hasta tokens de hardware especialmente diseñados que sirven para establecer nuestra identidad de múltiples maneras.

2.3.2.5 Identificación

La identificación, como mencionamos en la sección anterior, es simplemente una afirmación de quiénes somos. Esto puede incluir quién afirmamos ser como persona, quién afirma que un sistema está a través de la red, quién es la parte de origen de un correo electrónico o transacciones similares. Es importante tener en cuenta que el proceso de identificación no se extiende más allá de este reclamo y no implica ningún tipo de verificación o validación de la identidad que reclamamos. Esa parte del proceso se conoce como autenticación y es una transacción separada (Parra, 2019). Seguridad de la información Quien decimos ser es un concepto tenue, en el mejor de los casos. Podemos identificarnos por nuestros nombres completos, versiones abreviadas de nuestros nombres, apodos, números de cuenta, nombres de usuario, tarjetas de identificación, huellas digitales, muestras de ADN y una enorme variedad

de otros métodos, desafortunadamente, existen varias excepciones, tales métodos de identificación no son únicos, e incluso algunos de los métodos de identificación supuestamente únicos, como la huella digital, pueden duplicarse en muchos casos.

2.3.2.6 Verificación de identidad

La verificación de identidad es un paso fuera de la identificación, pero todavía está un paso por debajo de la aprobación que discutiremos en la siguiente sección. Cuando se nos pide que mostremos una licencia de conducir, tarjeta de identificación, pasaporte, certificado de nacimiento u otro formulario de identificación similar, esto generalmente tiene el objetivo de verificar la identidad, no la aprobación. Este es el equivalente aproximado de alguien que reclama la identidad "Juan Pérez" nosotros preguntamos si la persona es realmente Juan Pérez y estamos contentos con un "Soy una reacción determinada" de una persona (además de un pequeño documento).

2.3.2.7 Autenticación

Según Madrid Parra & Guillén (2019) los servicios de autenticación y autorización son esenciales para restringir el acceso a recursos críticos en entornos digitales, lo cual también se aplica en infraestructuras educativas que utilizan redes compartidas por estudiantes, docentes y administrativos.

En términos de autenticación, hay varios métodos que podemos usar, y cada categoría se denomina factor. Dentro de cada factor, hay varios métodos posibles que podemos usar. Cuando intentamos autenticar un reclamo de identidad, cuantos más factores usemos, más positivos serán nuestros resultados. Los factores son algo que sabes, algo que eres, algo que tienes, algo que haces y dónde estás.

2.4 Fundamentación teórica de la metodología

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un marco de referencia desarrollado para identificar, analizar y gestionar los riesgos que afectan a los sistemas de información. Su enfoque se basa en la identificación de activos, amenazas, vulnerabilidades, impacto y probabilidad, permitiendo estimar el nivel de riesgo y definir medidas de tratamiento. Esta metodología adopta un enfoque sistemático orientado a la gestión de la seguridad de la información y es ampliamente utilizada en entornos institucionales para fortalecer los controles de seguridad. (CCN-CERT, 2019)

MAGERIT se fundamenta en un enfoque sistemático y metódico que facilita la toma de decisiones basada en el riesgo. Para ello, estructura el proceso en fases claramente definidas que incluyen: identificación de activos, valoración de activos, análisis de amenazas, determinación de vulnerabilidades, estimación de impacto, cálculo del riesgo y definición de medidas de tratamiento. Este proceso permite cuantificar o cualificar el nivel de riesgo, facilitando la priorización de acciones correctivas y preventivas.

Uno de los elementos más relevantes de la metodología es su modelo de activos, el cual no se limita únicamente a los equipos tecnológicos, sino que contempla información, servicios, aplicaciones, personal, instalaciones y recursos organizacionales. Esta visión integral permite comprender que la seguridad no depende exclusivamente del componente tecnológico, sino también de factores humanos y organizativos.

Asimismo, MAGERIT adopta una perspectiva alineada con estándares internacionales como ISO/IEC 27001, ya que promueve la gestión del riesgo como eje central de la seguridad de la información. En este sentido, la metodología no solo identifica riesgos, sino que también propone estrategias de tratamiento, tales como la mitigación, transferencia, aceptación o

eliminación del riesgo, fortaleciendo así el Sistema de Gestión de Seguridad de la Información (SGSI).

En el contexto de la presente investigación, la aplicación de MAGERIT permitió identificar los activos tecnológicos presentes en las salas de docentes, analizar amenazas como accesos no autorizados, fallas eléctricas, malware o desastres naturales, y estimar su impacto en la continuidad de los servicios académicos. De esta manera, la metodología facilitó la elaboración de un diagnóstico estructurado y fundamentado para proponer un plan de mejora orientado al fortalecimiento del control de accesos y la seguridad informática institucional.

2.4.1 Identificación de amenazas y vulnerabilidades

En el marco de la metodología MAGERIT, la identificación de amenazas y vulnerabilidades constituye una fase esencial del análisis de riesgos, ya que permite determinar qué eventos pueden afectar los activos de información y cuáles son las debilidades que podrían ser explotadas. La evaluación de vulnerabilidades implica el uso de técnicas como monitoreo, revisión de configuraciones, análisis de registros y herramientas automatizadas, con el objetivo de detectar fallos de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de los sistemas.

Los ataques a la seguridad pueden clasificarse en ataques pasivos y ataques activos. Los ataques pasivos buscan obtener información sin alterar el funcionamiento del sistema, como ocurre en la interceptación de datos o el análisis del tráfico de red. En cambio, los ataques activos implican la modificación, alteración o interrupción de los recursos del sistema, incluyendo la suplantación de identidad, la repetición de mensajes, la modificación de datos o la denegación de servicio.

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

El desarrollo del marco teórico ha permitido identificar y profundizar en los aspectos fundamentales que sustentan la relación entre la auditoría informática y la seguridad de los equipos tecnológicos en entornos universitarios, específicamente en las salas docentes de la ULEAM Extensión El Carmen.

En síntesis, la identificación de amenazas y vulnerabilidades, junto con la aplicación de técnicas de auditoría para la obtención de evidencia, constituye la base del análisis de riesgos dentro de la metodología MAGERIT. Estos elementos permiten estimar la probabilidad e impacto de los riesgos que pueden afectar los activos tecnológicos institucionales, considerando especialmente los principios de confidencialidad, integridad y disponibilidad. De esta manera, el proceso metodológico no solo facilita la detección de debilidades en los controles de seguridad, sino que también orienta la toma de decisiones para fortalecer el sistema de control de accesos y mejorar la protección de la información institucional.

Además, se observa que la auditoría de la computadora no está aislada, pero afecta la mejora de la seguridad física y lógica del equipo. Su implementación correcta le permite identificar debilidades, proponer soluciones técnicas, reducir los riesgos legales y operativos y fortalecer la confianza institucional en la gestión de la información. Finalmente, el análisis teórico respalda la necesidad de introducir una auditoría informática que se centre en los equipos tecnológicos en la capacitación de seguridad como una estrategia preventiva y correctiva basada en estándares internacionales y adaptada al contexto universitario.

CAPÍTULO III:

3 MARCO INVESTIGATIVO (DISEÑO METODOLÓGICO)

3.1 Introducción

En el presente capítulo se describe el diseño metodológico utilizado para el desarrollo de la investigación. Se detallan el tipo y enfoque de estudio, los métodos empleados, las técnicas e instrumentos de recolección de información, así como la población objeto de análisis. La metodología aplicada permitió evaluar el nivel de seguridad informática en las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen, mediante la verificación del cumplimiento de los controles establecidos en la norma ISO/IEC 27001 y la aplicación de la metodología MAGERIT para el análisis y valoración de riesgos. A través de este procedimiento se identificaron vulnerabilidades, amenazas y niveles de riesgo, con el propósito de proponer acciones de mejora orientadas al fortalecimiento de la gestión de la seguridad de la información institucional. (Hernández Sampieri & Mendoza, 2022)

3.2 Tipo de investigación

La investigación descriptiva busca especificar las características y propiedades de un fenómeno sin manipular variables, permitiendo detallar su comportamiento dentro de un contexto determinado, en la presente investigación fue de tipo descriptiva, ya que permitió analizar la situación actual de la seguridad informática en las salas de docentes sin alterar las condiciones existentes. Se identificaron debilidades en controles físicos y lógicos y se determinó el nivel de cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001. (Bernal, 2020)

Este estudio fue aplicado, ya que, este tipo de investigación tiene como finalidad resolver problemas prácticos mediante la aplicación del conocimiento científico, en este caso,

la investigación fue aplicada porque se diagnosticó la situación real de la institución y se propuso un plan de mejora orientado al fortalecimiento de la seguridad tecnológica, el diseño fue de campo, dado que la información se recolecto directamente en el lugar donde se presentó la problemática, a través de técnicas como la observación, encuestas y entrevistas dirigidas al personal docente, permitiendo obtener datos reales sobre las condiciones de seguridad tecnológica existentes.

Debido a que su finalidad es resolver un problema real y concreto relacionado con la seguridad informática en los equipos de las salas de docentes de la ULEAM Extensión El Carmen. A través de una auditoría informática, se busca diagnosticar la situación actual y proponer acciones correctivas para mejorar los niveles de protección tecnológica.

3.2.1 Investigación descriptiva

La investigación descriptiva tiene como finalidad detallar las características de un fenómeno o situación específica sin manipular variables, permitiendo identificar comportamientos, propiedades y condiciones dentro de un contexto determinado. (Hernández Sampieri & Mendoza, 2022)

En la presente investigación se utilizó el enfoque descriptivo para analizar el estado actual de los controles de acceso y las medidas de seguridad informática en las salas de docentes de la ULEAM Extensión El Carmen. Se describieron las condiciones existentes, identificando debilidades y riesgos sin alterar el entorno evaluado.

3.2.2 Investigación Bibliográfica

Se entiende por investigación bibliográfica a la etapa científica de la investigación donde se explora el uso y avance de la comunidad académica sobre un tema determinado, supone un conjunto de actividades encontradas como documentos relacionados con un tema o

un autor en específico, esto nos permite conocer el estado actual de lo que se está investigando. (URUGUAY, 2020)

En este trabajo se realizó una investigación bibliográfica mediante la revisión de normas como ISO/IEC 27001, la metodología MAGERIT y literatura especializada en auditoría de TI y control de accesos. Esta revisión permitió sustentar conceptualmente las variables y establecer el marco teórico del estudio.

3.2.3 Investigación cuantitativa

La investigación cuantitativa es un método estructurado que se basa en la recolección y análisis de datos numéricos para medir variables, cuantificar problemas, hacer predicciones, comprobar relaciones causales y establecer relaciones mediante procedimientos estadísticos, enfocados en medir fenómenos con objetividad. (Ñaupas, Valdivia, Palacios, & Romero, 2022)

En la presente investigación se aplicó un enfoque cuantitativo para medir el nivel de cumplimiento de los controles de seguridad en los equipos evaluados. Se utilizaron listas de verificación y encuestas estructuradas que permitieron obtener datos objetivos y cuantificables para el análisis de riesgos bajo la metodología MAGERIT.

3.3 Fuentes de información de datos

Según Ñaupas et al. (2022) las fuentes de información pueden clasificarse en primarias, cuando los datos se obtienen directamente del objeto de estudio, y secundarias, cuando provienen de documentos o investigaciones previas.

En esta investigación se utilizaron fuentes primarias como entrevistas realizadas al responsable del área informática y encuestas aplicadas a los docentes. También se emplearon fuentes secundarias como documentos institucionales, bibliografía especializada y la norma

ISO/IEC 27001, las cuales sirvieron de base teórica para fundamentar el análisis y las recomendaciones propuestas.

3.3.1 Fuentes primarias –Entrevista

Las fuentes primarias son aquellas que proporcionan información directa y original obtenida por el investigador mediante técnicas como entrevistas, encuestas u observación, permitiendo recolectar datos de primera mano sobre el fenómeno estudiado. (Hernández Sampieri & Mendoza, 2022)

En la presente investigación se utilizó como fuente primaria una entrevista dirigida al laboratorista, el Ing. Jean Carlos Cuje, responsable de los equipos tecnológicos de la institución. A través de esta técnica se obtuvo información directa sobre el estado de la seguridad informática, el manejo de los equipos y las necesidades existentes en el área tecnológica. Las preguntas se diseñaron en coherencia con los objetivos del estudio y en complemento con la encuesta aplicada a los docentes, permitiendo contrastar la información obtenida.

3.3.2 Fuente secundaria-Encuesta

Las fuentes secundarias también incluyen instrumentos estructurados como encuestas, que permiten recopilar datos específicos directamente de los sujetos involucrados en la investigación, facilitando la medición de variables y el análisis cuantitativo de resultados. (Arias, 2021)

En este trabajo se aplicó una encuesta a los docentes de la Sede El Carmen de la Universidad Laica Eloy Alfaro de Manabí con el propósito de recolectar información sobre su percepción y conocimiento respecto a la seguridad informática y el cumplimiento de políticas institucionales. Los datos obtenidos permitieron identificar posibles debilidades en la

aplicación de controles de acceso y sirvieron como insumo para el análisis de riesgos bajo la metodología MAGERIT.

3.4 Estrategia operacional para la recolección de datos

3.4.1 Población

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

Se aplico un muestreo no probabilístico intencional, considerando a los todos los docentes de la institución para actividades académicas y administrativas. Debido a las limitaciones de tiempo y recursos, el tamaño de la muestra se planteó con un mínimo de 50 docentes encuestados en una población de 70 pertenecientes, lo cual permitió obtener una visión representativa del estado de los equipos y de la seguridad informática.

3.4.2 Tamaño de la muestra

Según Gutiérrez (2022) muestra es un subconjunto representativo de la población seleccionado para facilitar el estudio, permitiendo obtener resultados válidos sin necesidad de analizar a todos los integrantes del universo.

El análisis se logró gracias a la respuesta de 50 docentes de la institución situados en las diferentes áreas de la institución, dándonos así resultados más concretos utilizando una muestra discrecional.

3.4.3 Análisis de las herramientas de recolección de datos a utilizar

3.4.3.1 Encuesta

Destinada a los docentes, con el objetivo de recopilar información cuantitativa sobre el estado de los equipos, frecuencia de fallas, accesos, mantenimientos y percepciones sobre la seguridad informática.

3.4.3.2 Entrevista - Observación / Otras

Dirigida a personal técnico del área de soporte o responsables de TIC, para obtener información cualitativa y más detallada respecto a la gestión, políticas de seguridad y respuesta ante incidentes.

Observación directa: aplicada en las salas docentes, permitirá verificar las condiciones físicas de los equipos, la existencia de medidas de seguridad y las prácticas de uso

3.4.3.3 Estructura de lo(s) instrumento(s) de recolección de datos aplicados

- La encuesta contiene preguntas cerradas de selección múltiple.
- La entrevista es semiestructurada, con preguntas abiertas que buscan profundizar en la experiencia del personal técnico sobre la gestión de la seguridad informática.
- La observación sigue una lista de verificación basada en controles de seguridad física y lógica (ej. contraseñas, antivirus, estado físico de los equipos, accesos restringidos).

3.4.4 Plan de recolección de datos

- Diseño de instrumentos (encuestas y entrevistas).
- Aplicación en el periodo académico 2025-1 con la participación de docentes y personal técnico de la ULEAM Extensión El Carmen.
- Registrar y organizar datos para posteriores análisis estadísticos y cualitativos.

3.5 Análisis y presentación de resultados

La encuesta, la entrevista y la observación proporcionan datos sobre los estudiantes, lo que te permite triangular los resultados: Por ejemplo, aquí se implementa:

• Causa. Las deficiencias en el mantenimiento preventivo del equipo de aula causan fallas repetidas y afectan la continuidad del trabajo académico.

• Pregunta relacionada de la encuesta. ¿Con qué frecuencia se realiza el mantenimiento del equipo de laboratorio?

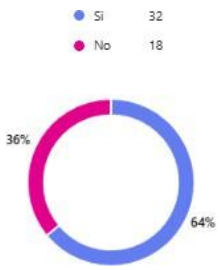
• Una pregunta comparable de la entrevista: ¿Cuál es el procedimiento a seguir en el área técnica si el personal docente tiene errores repetidos?

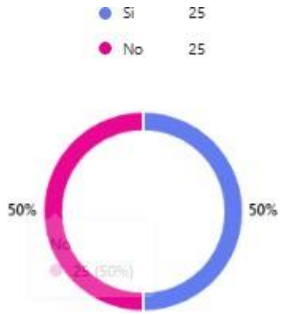
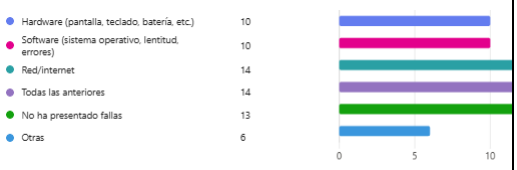
• Un ejemplo de análisis potencial o investigación hipotética (aún por analizar):

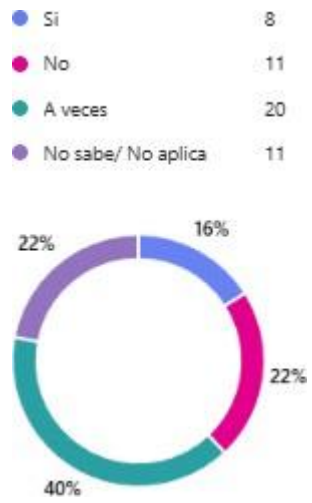
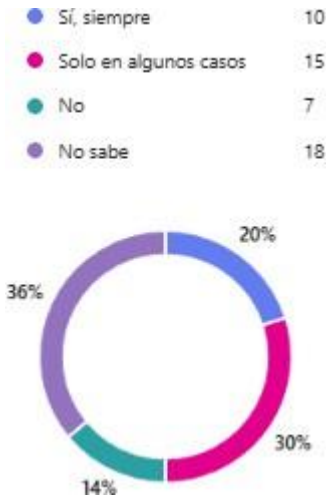
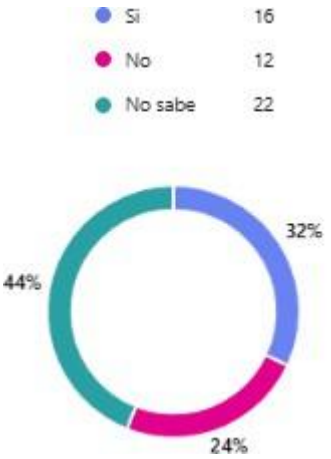
Si los profesores encuestados indican que el mantenimiento es infrecuente o inexistente, y el personal técnico en la entrevista confirma que los recursos son limitados para prevenir daños, se confirma que hay una brecha crítica en el plan de mantenimiento que representa un riesgo para la disponibilidad del equipo.

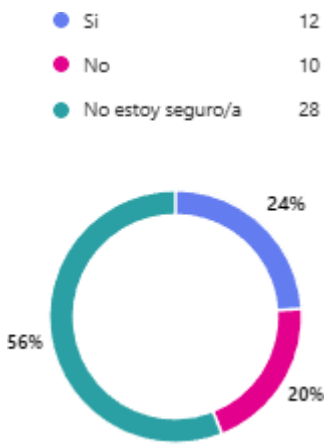
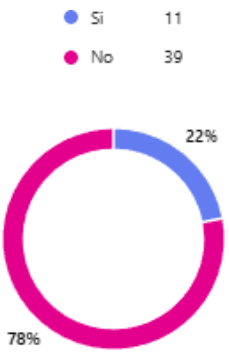
3.5.1 Tabulación y análisis de los datos

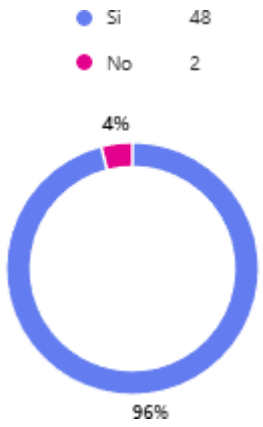
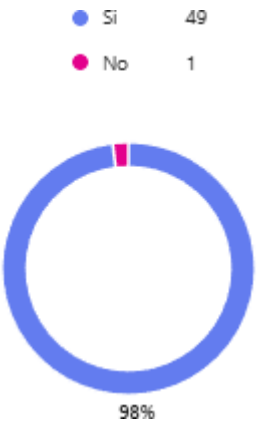
Tabla 1 *Resultado del método de investigación*

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
1. ¿Cuál es su rol dentro de la universidad?		A pesar de ser orientado a sala docentes, se pudo identificar la existencia de personal administrativo como coordinadores dentro de la población.
2. ¿En qué carrera o departamento trabaja usted?		La mayor parte de docentes que participaron en esta encuesta son del área TI/SW
3. ¿Posee actualmente un equipo informático asignado por la institución?		Se pudo identificar que existe un alto porcentaje de docentes los cuales no disponen de un equipo.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
4. ¿Con qué frecuencia utiliza su equipo informático institucional?		Existe una gran cantidad de docentes que no les dan uso a sus equipos de manera diaria.
5. ¿Su computadora asignada ha presentado fallas recientemente?		Podemos identificar que existen equipos los cuales no están funcionales al 100%, lo que quiere decir que existe una falta de mantenimiento.
6. ¿Qué tipo de fallas ha presentado el equipo? (Puede marcar más de una)		En la mayoría de equipos podemos identificar que existe una falta de mantenimiento tanto externo como interno.
7. ¿Con qué frecuencia considera que debería realizarse mantenimiento preventivo a estos equipos?		Existe una falta de capacitación a docentes sobre el mantenimiento de sus equipos.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
8. ¿Cuándo se presenta un daño, el área técnica responde a tiempo?		Se observa que hay una deficiencia clara en cuanto a las políticas de seguridad en los equipos.
9. ¿Se reemplazan piezas o componentes dañados por parte de la universidad?		Se analiza que existe una falta de compromiso bastante alarmante por parte del área técnica en cuanto a la resolución de un daño de equipos.
10. ¿El equipo asignado cuenta con mecanismos de seguridad (contraseña, cifrado, antivirus, etc.)?		A pesar de existir una gran población de docentes a los que se les asignado un equipo, se puede identificar que estos no conocen la seguridad informática de este.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
11. ¿Sabe si existe una política institucional sobre el uso seguro de los equipos?		Hay una falta clara de conocimiento sobre la política, se necesita una auditoria para mitigar estos riesgos.
12. ¿Quién tiene acceso físico al equipo asignado cuando usted no lo utiliza?		Existe un alto porcentaje de respuestas negativas, al no saber que personas tienen acceso a un equipo esta representa un riesgo.
13. ¿Alguna vez ha detectado accesos no autorizados a su equipo?		A pesar de que la mayoría de respuestas son positivas, el porcentaje negativo es alarmante ya que, aunque sea mínimo quiere decir que existe un fallo de seguridad que podría convertirse en un problema legal a futuro.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
14. ¿Considera que es necesario implementar controles más estrictos sobre el acceso a los equipos?		Existe una mínima cantidad de docentes que no conocen una política clara, se puede solucionar con una audiencia para mitigar.
15. ¿Cree que la universidad debería implementar herramientas de monitoreo y auditoría para los equipos docentes?		Está claro que, a pesar de tener una deficiencia de información en ciertas áreas, cada docente es consciente de lo importante que es darles el uso correcto a los equipos de la institución.

3.5.2 Presentación y descripción de los resultados obtenidos

3.6.2.1 Entrevista al encargado

Tabla 2 *Resultado Instrumento Entrevista*

Preguntas	Respuestas	Interpretación
1. ¿Cuál es su cargo y cuáles son sus principales responsabilidades en relación con los equipos informáticos de la universidad?	Mi función dentro de la institución es administrar y dar mantenimiento a los equipos informáticos asignados al personal docente, brindar soporte técnico ante fallas de hardware, software y red, y colaborar en la aplicación de medidas básicas de seguridad de la información.	El laboratorista indicó que su trabajo consistía en administrar y dar mantenimiento a los equipos, brindar soporte técnico y aplicar medidas básicas de seguridad. El mantenimiento preventivo no se hacía de forma regular, sino solo cuando los equipos presentaban fallas.
2.Actualmente, ¿la universidad lleva un registro actualizado donde se pueda ver qué equipos están asignados a cada docente?	En la institución dispone de lo que es un inventario para los equipos informáticos; sin embargo, este registro no se lo mantiene actualizado en todo momento, el problema surge por la rotación constante de los equipos y por la falta de un sistema que automatice su gestión.	Se encontró que existe un inventario de los equipos, pero no siempre está actualizado debido a la rotación de dispositivos y la falta de un sistema automatizado. Los equipos se asignan según disponibilidad y necesidades de los docentes.
3.Al momento de entregar un equipo a un docente, ¿en qué cosas se fijan o qué se toma en cuenta para hacer esa asignación	La asignación de los equipos se realiza de acuerdo con la disponibilidad institucional y las necesidades académicas, priorizando a los docentes que utilizan los equipos de forma permanente para sus actividades educativas y administrativas.	La asignación de equipos se realiza según la disponibilidad institucional y las necesidades académicas de los docentes, priorizando a quienes usan los equipos de manera constante. Esto indica que la institución intenta cubrir las necesidades, aunque sin un control formal detallado.

Preguntas	Respuestas	Interpretación
4. ¿Cada cuánto tiempo se les da mantenimiento a los equipos que se usan en la institución?	El mantenimiento preventivo no se ejecuta con una periodicidad definida, ya que generalmente se realiza cuando los equipos presentan fallas o disminuyen su rendimiento, principalmente por limitaciones de tiempo y recursos.	El mantenimiento preventivo no se realiza de manera periódica, sino que se hace principalmente cuando los equipos presentan fallas o bajo rendimiento. Esto refleja que la gestión del mantenimiento es reactiva más que preventiva.
5.Según su experiencia, ¿qué problemas o fallas son los que más se repiten en los equipos que usan los docentes?	Entre las fallas más comunes de los equipos se puede encontrar los problemas de software y la baja velocidad del sistema, a todo esto, se suman la aparición de malware, el deterioro de piezas físicas y los inconvenientes en la conectividad de red.	Entre las fallas más comunes se encuentran problemas de software, lentitud del sistema, malware, deterioro físico de los dispositivos y problemas de conectividad. Esto muestra que los equipos enfrentan riesgos tanto físicos como lógicos que afectan su desempeño.
6.Cuando un docente reporta que un equipo está dañado, ¿qué es lo que normalmente hace el área técnica para atender ese caso?	Ante el reporte de un daño, se lleva a cabo una revisión del equipo para de esta manera poder definir si el problema puede resolverse dentro de la institución o si se debe cambiar algún componente, a pesar de todo esto, el proceso puede verse afectado por la disponibilidad de repuestos y por la gestión administrativa necesaria.	Cuando un docente reporta un equipo dañado, el área técnica realiza una revisión para determinar si puede repararse internamente o si se debe cambiar algún componente. Sin embargo, este proceso puede retrasarse por la falta de repuestos o recursos disponibles.

Preguntas	Respuestas	Interpretación
7.En su opinión, ¿el tiempo que se tarda el área técnica en responder a las fallas es el correcto?	Los equipos no siempre reciben solución de una manera inmediata en todos los casos, ya que el tiempo de la respuesta está marcado por la cantidad de trabajo que tengas en el área técnica y por los recursos que se encuentren disponibles.	El tiempo de respuesta del área técnica no siempre es inmediato, ya que depende de la cantidad de trabajo pendiente y de los recursos disponibles. Esto indica que algunas fallas pueden tardar en resolverse, afectando la continuidad de las actividades académicas.
8. ¿La universidad cuenta actualmente con políticas o normativas relacionadas con el uso seguro y adecuado de los equipos informáticos?	Aunque existen las normas generales sobre el uso de los equipos informáticos, no todos los docentes las manejan o las ponen en práctica de manera correctamente dentro de la institución.	Aunque existen normas generales sobre el uso de los equipos, no todos los docentes las conocen o las aplican correctamente. Esto refleja una falta de concientización y seguimiento sobre la política de seguridad informática.
9. ¿Qué medidas de seguridad lógica se aplican en los equipos, como por ejemplo antivirus, uso de contraseñas, actualizaciones del sistema o control del software instalado?	Las medidas de seguridad en los equipos incluyen contraseñas de acceso y software antivirus, pero no en todos los casos se puede asegurar una actualización continua ni un control adecuado de las aplicaciones que se instalan	Los equipos cuentan con antivirus y contraseñas, pero no siempre se asegura la actualización continua ni el control del software instalado. Esto indica que las medidas de seguridad son básicas y necesitan fortalecerse para proteger mejor la información.
10. ¿Cómo se controla el acceso físico a los equipos informáticos cuando los docentes no se encuentran presentes en las salas?	El acceso físico a los equipos no siempre se encuentra controlado, especialmente cuando estos se ubican en espacios compartidos, lo que permite que puedan ser manipulados por personas no autorizadas.	El acceso físico a los equipos no siempre está controlado, sobre todo cuando se encuentran en espacios compartidos. Esto permite que personas no autorizadas puedan manipular los dispositivos, generando un riesgo de seguridad.

Preguntas	Respuestas	Interpretación
11. ¿Se han detectado incidentes relacionados con accesos no autorizados, pérdida de información o malware en los equipos docentes?	Los incidentes más comunes reportados incluyen infecciones de lo que son malware y de accesos no autorizados, que en su mayoría surgen o se deben al uso de dispositivos de almacenamiento externos y a la descarga de archivos provenientes de fuentes poco seguras o confiables.	Los incidentes más frecuentes incluyen infecciones por malware y accesos no autorizados, generalmente causados por dispositivos externos o descargas de fuentes no confiables. Esto evidencia la necesidad de controles más estrictos y concienciación en los usuarios.
12. ¿La institución realiza respaldos periódicos de la información que se encuentra almacenada en los equipos informáticos?	No existe un proceso sistemático para realizar las copias de seguridad, por lo que en la mayoría de los casos son los mismos docentes quienes deben encargarse de realizarlas en sus propios equipos.	No existe un proceso sistemático de copias de seguridad, por lo que los docentes deben encargarse de realizar sus propios respaldos. Esto aumenta el riesgo de pérdida de información importante.
13. ¿Existen procedimientos definidos para el reemplazo de equipos o componentes dañados?	El reemplazo de equipos o componentes dañados se efectúa únicamente cuando el daño es considerable y existe disponibilidad presupuestaria, lo que provoca que algunos equipos continúen en uso aun presentando fallas.	El reemplazo de equipos o componentes dañados solo se realiza cuando el daño es grave y hay disponibilidad presupuestaria, por lo que algunos equipos continúan en uso aun presentando fallas. Esto afecta la eficiencia y seguridad de los equipos.

Preguntas	Respuestas	Interpretación
14. ¿El personal docente recibe capacitación sobre el uso adecuado y seguro de los equipos informáticos?	No se realizan capacitaciones periódicas al personal docente sobre el uso adecuado y seguro de los equipos informáticos, limitándose únicamente a indicaciones básicas al momento de la entrega del equipo.	No se realizan capacitaciones periódicas sobre el uso seguro de los equipos; los docentes reciben solo indicaciones básicas al momento de la entrega. Esto limita la comprensión de las buenas prácticas de seguridad.
15.Desde su experiencia, ¿qué riesgos considera más críticos en relación con la seguridad de los equipos informáticos de los docentes?	Considero que los riesgos más críticos a los que están expuestos los equipos informáticos son el robo, la pérdida de información, el daño físico de los dispositivos y las infecciones por malware.	El entrevistado considera que los riesgos más críticos son el robo, la pérdida de información, el daño físico de los equipos y las infecciones por malware. Esto evidencia la vulnerabilidad de los equipos y la necesidad de controles más estrictos.
16. ¿Cree usted que es necesario implementar controles más estrictos de acceso y monitoreo sobre los equipos informáticos?	Desde mi punto de vista, es necesario implementar controles más estrictos de acceso físico y lógico, así como herramientas de monitoreo, políticas claras de uso y programas de capacitación, con el fin de fortalecer la seguridad de los equipos informáticos institucionales.	Se considera necesario implementar controles más estrictos de acceso físico y lógico, junto con herramientas de monitoreo, políticas claras y programas de capacitación. Esto permitiría fortalecer la seguridad de los equipos en la institución.

Preguntas	Respuestas	Interpretación
17. ¿Qué mejoras recomendaría para fortalecer la seguridad física y lógica de los equipos informáticos institucionales?	Mi función dentro de la institución es administrar y dar mantenimiento a los equipos informáticos asignados al personal docente, brindar soporte técnico ante fallas de hardware, software y red, y colaborar en la aplicación de medidas básicas de seguridad de la información.	Entre las mejoras recomendadas están la aplicación de políticas claras, mayor control de acceso, monitoreo constante, actualizaciones periódicas y capacitación a los docentes. Esto refleja la necesidad de un enfoque integral para proteger los equipos y la información institucional.

3.5.3 Informe final del análisis de los datos.

El informe final del análisis de los datos se elaboró a partir de la información recopilada mediante la aplicación de encuestas al personal docente, entrevistas al encargado de los equipos informáticos y la observación directa realizada en la sala de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen.

Juntar estos medios sirvió para conseguir información real y buena. Hablamos del estado de las máquinas. Esto incluye el cuidado lógico, real y de uso del personal que enseña. Los hallazgos mostraron fallos grandes. Esto pasó en el modo de cuidar el acceso físico. El sitio de los maestros no tiene formas claras. Estas formas deben limitar quién puede entrar. Solo gente lista debería pasar. También se notó que faltan listas de entrada y salida. Faltan cámaras. Faltan modos fijos para prevenir o actuar si roban algo, el riesgo de pérdida o sustracción de las computadoras aumenta debido a la falta de medidas adecuadas.

Según la investigación hablando de los daños a los equipos, los resultados reflejan que el mantenimiento preventivo no se lleva a cabo de forma regular, ya que solo se realiza cuando se presenta alguna falla debido a la falta de conocimiento, así mismo se logró identificar que

no existe un manual, ni registros técnicos dentro del tiempo recomendado, lo que provoca un deterioro más rápido de los equipos informáticos.

La falta de capacitación para el personal docente aumenta las posibilidades de infección por software malicioso y la pérdida de información.

El análisis general de los datos demuestra que, debido a los múltiples problemas que existen en la seguridad informática, la sala de docentes presenta niveles de riesgo de medio a alto, siendo las amenazas más relevantes como los robos, daños a los equipos y malware por la falta de un correcto mantenimiento del lugar, los resultados serán una base importante para la propuesta de mejora que ayudara a fortalecer los controles de acceso, protegerá los equipos, y sensibilizará al personal docente, garantizando así la seguridad de la información y mantendrá la continuidad de las actividades académicas de una manera más sana.

Causa del problema 1: Insuficientes controles de acceso y protección de los equipos informáticos

Resultado de la encuesta:

Los docentes manifestaron que no existen controles de acceso físico adecuados en la sala de docentes, evidenciando la ausencia de registros de ingreso, sistemas de identificación y vigilancia permanente. Asimismo, una parte significativa indicó desconocer políticas institucionales claras relacionadas con la protección de los equipos asignados, lo que incrementa el riesgo de robo o uso no autorizado.

Resultado de la entrevista:

El responsable de los equipos confirmó que actualmente no se dispone de sistemas formales de control de acceso, ni de cámaras de vigilancia específicas para la sala de docentes. Además, señaló que el control del uso de los equipos se basa principalmente en la confianza y responsabilidad del personal, sin mecanismos documentados que regulen el ingreso o salida de equipos informáticos.

Interpretación:

La información obtenida tanto en la encuesta como en la entrevista coincide en señalar la inexistencia de controles físicos y administrativos adecuados para la protección de los equipos informáticos. Esta concordancia valida la existencia de un riesgo significativo de robo o uso indebido de los activos tecnológicos, evidenciando la necesidad de implementar controles de acceso más estrictos y políticas institucionales formales.

Causa del problema 2: Falta de mantenimiento preventivo y gestión de daños de equipos

Resultado de la encuesta:

Los resultados reflejan que los equipos asignados a los docentes presentan fallas recurrentes y que el mantenimiento preventivo no se realiza de manera periódica. Asimismo, varios docentes indicaron que las respuestas del área técnica no siempre son oportunas y que no existe claridad sobre los procedimientos para el reemplazo de componentes dañados.

Resultado de la entrevista:

El encargado de los equipos señaló que el mantenimiento se realiza principalmente de forma correctiva, cuando los equipos ya presentan fallas. También indicó que no existe un cronograma establecido de mantenimiento preventivo ni un registro formal de reparaciones y reemplazos realizados.

Interpretación:

Ambas fuentes coinciden en que la gestión de mantenimiento es reactiva y carece de planificación. Esta situación incrementa el riesgo de daño de equipos, reduce su vida útil y afecta la continuidad de las actividades académicas, confirmando la necesidad de establecer protocolos formales de mantenimiento preventivo y registro técnico.

Causa del problema 3: Debilidades en la seguridad lógica y prevención de malware

Resultado de la encuesta:

Los docentes indicaron que no reciben capacitación periódica sobre seguridad informática y prevención de malware. Además, se evidenció el desconocimiento sobre políticas de instalación de software, uso de dispositivos USB y procedimientos ante incidentes de seguridad.

Resultado de la entrevista:

El encargado ayudo a la confirmación que no existe una intervención formal en la que se utilice una capacitación en seguridad informática, ni protocolos documentados para la respuesta ante incidentes de malware. También señaló limitaciones en el monitoreo de la red y en la aplicación de controles de seguridad avanzados.

Interpretación:

La coincidencia entre ambos instrumentos confirma una vulnerabilidad elevada frente a amenazas de malware, derivada de la falta de capacitación, políticas claras y mecanismos de respuesta ante incidentes. Esto valida la necesidad de implementar controles técnicos y programas de concienciación dirigidos al personal docente.

A partir de la triangulación de los datos se encontró en la encuesta y la entrevista, que se logró confirmar la presencia de debilidades importantes en la seguridad informática de la sala de docentes, relacionadas con aspectos estructurales, técnicos y de organización. La consistencia entre ambas fuentes respalda la validez de los resultados obtenidos y sirve como base para plantear medidas correctivas orientadas a reducir riesgos, fortalecer la protección de los equipos y mantener la operatividad institucional.

CAPÍTULO IV:

4 MARCO PROPOSITIVO (ELABORACIÓN DE LA PROPUESTA)

El presente capítulo desarrolla la propuesta de implementación derivada del proceso de auditoría informática aplicado a la seguridad de los equipos tecnológicos de las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen. La propuesta tiene como finalidad fortalecer la protección de los equipos de cómputo institucionales, así como optimizar los controles de acceso, el mantenimiento preventivo y las prácticas de uso seguro de los recursos tecnológicos. Desde la perspectiva del daño al equipo, los datos obtenidos indican que el mantenimiento preventivo no se realiza periódicamente y se limita principalmente a intervenciones correctivas cuando el equipo presenta fallas.

la planificación de la auditoría, orientada a la verificación del cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001, se evidenció que la institución no cuenta con manuales de operación ni procedimientos documentados para el manejo adecuado de los equipos informáticos. Asimismo, no existen registros formales relacionados con fallas técnicas o incidencias, lo que refleja debilidades en la gestión de activos y en la documentación de controles internos exigidos por la normativa. Esta situación ha generado un uso inadecuado de los recursos tecnológicos y un desgaste progresivo del equipamiento entregado a los docentes, evidenciando un nivel de cumplimiento parcial en los controles asociados a la administración y mantenimiento de los activos de información.

En relación con el riesgo de inundación, y conforme a los controles de seguridad física y ambiental establecidos en ISO/IEC 27001, se identificaron condiciones que podrían afectar la disponibilidad de los equipos, tales como la presencia de humedad en determinadas áreas, la

ubicación de equipos a nivel del piso y la ausencia de medidas preventivas durante la temporada de lluvias. En la Fase 2 de ejecución de la auditoría, mediante la aplicación de la metodología MAGERIT, estas condiciones fueron analizadas como amenazas ambientales que impactan directamente la disponibilidad de los activos tecnológicos. Aunque el nivel de riesgo no fue clasificado como alto, se determinó la necesidad de gestionarlo adecuadamente para prevenir daños acumulativos a largo plazo y reducir la probabilidad de afectaciones futuras.

Respecto al riesgo de malware, se identificó que la institución carece de lineamientos formales en materia de seguridad informática, políticas para el uso de dispositivos externos, procedimientos de respaldo de información y protocolos de respuesta ante incidentes. Si bien existen medidas básicas como el uso de contraseñas y software antivirus, la limitada formación del personal docente incrementa la probabilidad de incidentes asociados a amenazas informáticas. Bajo el enfoque de la metodología MAGERIT, este escenario fue evaluado considerando la probabilidad de ocurrencia y el impacto sobre la confidencialidad, integridad y disponibilidad de la información, determinándose la necesidad de fortalecer los controles técnicos, documentar políticas de seguridad y establecer programas de capacitación continua.

La propuesta se sustenta en los resultados del diagnóstico situacional y del análisis de riesgos, utilizando como herramientas encuestas, entrevistas y observación directa. Los hallazgos muestran debilidades en políticas, controles técnicos y procedimientos, por lo que la propuesta se basa en estándares internacionales como ISO/IEC 27001, ISO/IEC 27002, COBIT y MAGERIT, enfocados en la gestión de riesgos y la mejora continua.

Este capítulo tiene como objetivo presentar una descripción exhaustiva de los requisitos de recursos, etapas de implementación, controles de seguridad identificados y enfoques de evaluación para reforzar la seguridad del equipo técnico en las aulas, basándose en la integridad, confidencialidad y disponibilidad de la información, y la continuidad operativa de

las actividades académicas. Además, se revisará la estructura organizativa, las responsabilidades asignadas, el cronograma de ejecución y los instrumentos de verificación del cumplimiento de los controles. Finalmente, como una propuesta basada en el escrutinio continuo de los hallazgos y la adaptación de las medidas de seguridad a las necesidades reales de la Extensión El Carmen de ULEAM, se introduce una filosofía de mejora continua.

El proceso de auditoría informática, que se llevó a cabo minuciosamente en las salas de estudio de la Universidad Laica Eloy Alfaro de Manabí, Ampliación El Carmen, identificó diversas deficiencias en la aplicación de controles de seguridad, mantenimiento preventivo, políticas de acceso y gestión de los equipos tecnológicos de las instituciones.

Durante el desarrollo de la investigación se utilizaron varios tipos de recursos, los cuales fueron de suma importancia ya que ayudaron a garantizar la validez y confiabilidad de los resultados, entre ellos se destacan que los recursos humanos fueron aquellos que brindaron mayor información ya que se contó con su participación activa tanto de los docentes como del personal técnico responsable.

El recurso tecnológico también jugó un papel importante, ya que se utilizaron equipos de cómputo, software ofimático y herramientas digitales para la elaboración de documentos, procesamiento estadístico de las investigaciones y sistematización de los resultados obtenidos. Estas herramientas permitieron la recopilación y organización precisa de información que contribuye a un análisis más detallado de las condiciones de seguridad.

Por otro punto en cuanto a lo financiero se logró cubrir los gastos relacionados con lo básico de los materiales del dispositivo utilizado en la fase de recolección y análisis de datos. Esta disciplina fiscal también fue fundamental para proteger un registro transparente de los costos de gastos asociados con la investigación.

Se utilizaron herramientas más formales, como encuestas a los profesores sobre que herramientas utilizan en las instalaciones, entrevistas semiestructuradas y observaciones directas del entorno físico y lógico de las instalaciones para obtener datos relevantes e identificar los riesgos de TI existentes. , estas herramientas fueron desarrolladas tomando en cuenta los lineamientos de las normas ISO/IEC 27001 y los marcos de auditoría COBIT y MAGERIT, lo que permitió una evaluación del nivel de cumplimiento y protección de la información de las instituciones.

Los datos recopilados fueron estructurados y tabulados con la ayuda de Microsoft Excel, lo que nos facilitó la organización de los datos y la creación de los gráficos estadísticos representativos, esto se realizó a través de la sistematización para poder visualizar de una manera más clara el nivel de riesgo, las brechas de la seguridad existentes y el grado de vulnerabilidad al que está expuesto el equipo tecnológico de las aulas de la Extensión ULEAM El Carmen, en resumen, este análisis el cual se llevó a cabo es la base para las recomendaciones de propuestas de mejora, las cuales pueden servir para fortalecer la seguridad de la información, y así mejorar el uso de la tecnología y establecer una norma que sirva para la prevención de estos problemas, logrando evitarlos o si existen como saber mitigarlos.

Durante el proceso de auditoría informática realizado en las salas docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, se logró obtener la identificación de varios problemas relacionados con la seguridad, mantenimiento y manejo de los equipos tecnológicos, los resultados de las encuestas a docentes indican un grado elevado de vulnerabilidad debido a la falta de controles técnicos adecuados y a la falta de políticas institucionales claras en materia de seguridad informática.

En primer lugar, se observó que la máquina presentaba errores repetidos como lentitud, daños en los periféricos (incluido teclado, batería) y problemas de conexión con la red

institucional. Pese a estos incidentes, la mayoría del personal docente indicó que no se brinda atención técnica a tiempo, lo que afecta el normal desarrollo de las actividades académicas. Asimismo, una parte considerable de los empleados entrevistados indicó que las piezas o componentes dañados del equipo no son reemplazados, lo que agrava las deficiencias técnicas y reduce su vida útil.

En algunas ocasiones los docentes indicaron que los equipos no fueron utilizados por largas temporadas dejando pasar el tiempo por falta de mantenimiento preventivo o correctivo. Por otro lado, otro aspecto importante demostrado es por la falta de mecanismos de seguridad como contraseñas seguras, cifrado de información o software antivirus actualizado, frente a esta situación se logra observar que aumenta la exposición de los dispositivos a accesos no autorizados, malware y pérdida de información institucional importante.

En cuanto a la seguridad física y el acceso a las salas, no se aplicó una política estándar, se conoció que la mayor parte de docentes no conoces la existencia de una política sobre quién puede usar el equipo en ausencia de ellos o el ingreso a su cubículo sin presencia de autoridades, algunas respuestas también demostraron que existen computadoras que en ocasiones puedan llegar a permanecer encendidas o suspendidas durante períodos cortos, lo que pone en riesgo la seguridad de la información tanto personal del docente como académica poniendo su integridad en peligro y también el estado físico de los dispositivos en caso de ingreso a dispositivos no autorizados, se diseñó e implementó un plan de mejora para la seguridad informática, con un enfoque en el equipo de cómputo utilizado en las salas de docentes, para así evitar fallos técnicos, controlar el acceso no autorizado de alumnos y asegurar el uso adecuado de los recursos tecnológicos.

Este plan contempla acciones como:

- Establecimiento de políticas básicas de uso y seguridad de los equipos docentes.

- Implementación de un cronograma de mantenimiento preventivo.
- Definición de procedimientos ante fallas técnicas recurrentes.
- Refuerzo de controles de acceso físico y lógico a los equipos.
- Concienciación del personal docente sobre buenas prácticas de seguridad informática.

Finalmente, los resultados muestran una falta de cultura organizacional en la seguridad informática, pues la mayoría de los docentes desconocen que existen normas o protocolos internos para el uso y protección de los equipos, sin embargo aún existe una falta clara de información a muchas áreas de docentes, así mismo se logró analizar que existe la ausencia de auditorías enfocadas a este tipo de problemas provocando un entorno poco seguro, donde las buenas prácticas tecnológicas dependen casi por completo del criterio personal de cada uno y no de reglas claras.

En general, los resultados reflejan que hace falta mejorar de forma urgente las políticas de mantenimiento, el control de acceso y la seguridad informática en la Extensión de la ULEAM en El Carmen, implementar controles más claros, herramientas de seguimiento y capacitaciones constantes permitiría cerrar las brechas existentes y asegurar la correcta protección de los recursos tecnológico

4.1 Determinación de recursos

4.1.1 Humanos

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 de mejora de la seguridad de los equipos tecnológicos de las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen.

Este recurso fue importante, ya que permitió la recopilación de la información, la cual se determinó ser más confiable mediante el aporte del soporte técnicos, experiencias y el apoyo de los instrumentos de recolección de datos. Las personas involucradas en el análisis se incluyeron a todos los docentes para analizar si todos utilizan un equipo informático, la participación de estos permitió la identificación de las principales vulnerabilidades existentes, la evaluación del cumplimiento de los controles de seguridad y la construcción de un diagnóstico que sirvió como base para el desarrollo de la propuesta destinada a fortalecer la seguridad informática en las salas de enseñanza.

Tabla 3 *Recursos humanos*

CANTIDAD	RECURSOS	FUNCIÓN	ACTIVIDAS
1	Ing. Wladimir Minaya	Tutor del proyecto de titulación	Colaboradora de brindar orientación al estudiante en su proceso de proyecto de titulación.
1	Ing. Jean Carlos	Director de la institución educativa y encargado de los equipos de computó	Colaborador del Permiso de la realización del trabajo de titulación y así mismo colaborador con la entrevista realizada en la institución.
50	Docentes ULEAM	Docentes de la institución educativa y participantes de la auditoría	Colaboradores de la realización del proceso de la encuesta.
1	Dayana Zambrano	Auditora	Como Auditor pude identificó falta de política y controles de seguridad en la institución educativa.

4.1.2 Tecnológicos

Los recursos tecnológicos corresponden al conjunto de equipos y herramientas digitales que hicieron posible la ejecución del proceso de auditoría informática y el análisis de la seguridad de los equipos tecnológicos. Los recursos disponibles fueron necesarios para la recopilación de evidencia obtenida, se analizó y preparo la documentación relacionada con la presente investigación de estudio, se utilizó una computadora personal asignada para el auditor, dispositivos de almacenamiento, programas de office y hojas de cálculo para la organización de los resultados, así como herramientas digitales para la redacción del informe final, dichas herramientas tecnológicas facilitaron la identificación de errores, riesgos y así mismo facilito la gestión de la seguridad de la información, además de apoyar la preparación de informes y propuestas basadas en estándares internacionales.

Tabla 4 *Recursos tecnológicos*

CANTIDAD	RECURSOS
1	Portátil Dell AMD RADEON Ryzen 5 de 8 GB de memoria Ram
1	Memoria RAM 8 GB expandible
1	Celular Honor x8B, almacenamiento interno 512gb y 8 de ram

4.1.3 Económicos

Los recursos económicos comprenden los costos asociados al desarrollo de la auditoría informática y a la implementación de la propuesta de mejora de la seguridad de los equipos tecnológicos. Estos costos están relacionados principalmente con la operación y mantenimiento

de los equipos de cómputo, adquisición de materiales de apoyo, uso de herramientas tecnológicas y elaboración de documentación e informes.

A pesar de que ciertos recursos fueron proporcionados por la institución, los valores económicos corresponden a una estimación del uso de los recursos a lo largo del proceso de investigación, considerando tanto su uso directo como indirecto. Esta identificación de costos permitió evaluar la viabilidad de la propuesta y garantizar que las acciones planteadas sean realistas y sostenibles para la ULEAM Extensión El Carmen

Tabla 5 *Recursos Económicos*

CANTIDAD	DESCRIPCIÓN	PRECIO UNITARIO	SUBTOTAL
1	Portatil Dell AMD Ryzen 5	$570	$570
1	Ram 8Gb	$30	$30
1	Celular Honor x8B	$230	$230
		Total	$830

4.2 Etapas de acción para el desarrollo de la propuesta (software)

4.2.1 Fase 1 Planificar

Durante la esta fase correspondiente a la planificación de la auditoría, se realizó la revisión del cumplimiento de los requisitos establecidos en la norma ISO/IEC 27001, específicamente aquellos relacionados con la gestión de políticas de seguridad, controles físicos y protección frente a amenazas informáticas. Como resultado del análisis documental y

de la inspección directa, se evidenció que la institución no dispone de manuales formales de operación ni de procedimientos documentados para el uso y mantenimiento de los equipos informáticos. Asimismo, no existen registros estructurados sobre fallas técnicas o incidencias reportadas, lo cual representa un incumplimiento parcial de los controles asociados a la gestión de activos y a la documentación de políticas de seguridad de la información. Esta situación ha generado un uso inadecuado de los recursos tecnológicos y un desgaste progresivo del equipamiento asignado a los docentes.

En relación con la seguridad física y ambiental, y conforme a los controles establecidos por la norma ISO/IEC 27001, se identificaron condiciones que podrían afectar la disponibilidad de los activos tecnológicos, tales como la presencia de humedad en determinadas áreas, la ubicación de equipos directamente a nivel del piso y la ausencia de medidas preventivas durante la temporada de lluvias. Desde el enfoque de la metodología MAGERIT, estas condiciones fueron clasificadas como amenazas ambientales que impactan la disponibilidad de los activos, con una probabilidad media y un impacto moderado. Aunque el nivel de riesgo no fue considerado crítico, se determinó la necesidad de implementar medidas preventivas para evitar daños acumulativos a largo plazo y reducir la exposición a incidentes físicos.

4.2.1.1 Programa de Auditoría

Tabla 6 *Programa de Auditoría*

Programa de auditoría informática para la gestión de seguridad de la información en la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen		
Objetivo • Evaluar el nivel de cumplimiento de normas y política de seguridad en los cubículos docentes Universidad Laica Eloy Alfaro de Manabí extensión EL Carmen según la norma ISO 27001. • Identificar los posibles riegos de seguridad informática a los que está expuesto.		
Técnica y procedimiento		
	Referencia a papel de trabajo	**Fecha**
1. Revisar las normas ISO 27001	4.4.1.2	00/08/2025
2. Diseño de instrumento según ISO 27001 para evaluar cumplimento de controles y política de la institución en el área informática	4.4.1.3	00/08/2025
3. Elaborar instrumentos para evaluar riesgos	4.5.2.1.1	03/06/2024 10/06/2024
4. Entrevista a laboratorista de la institución.	4.5.3.1	10/06/2024
5. Entrevistar de los instrumentos al encargado de la institución.	4.5.3.1	10/06/2024
6. Tabulación de datos	4.5.3.2	27/06/2024
Elaborado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir	
Fecha:	**Firma**:	

4.2.1.2 Revisión de IS0 27001

La **ISO/IEC 27001** es la norma internacional que establece los requisitos para implementar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información (SGSI)**. La revisión de esta norma dentro de una auditoría tiene como objetivo verificar que la organización cumple con los estándares de seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos.

Objetivos de la revisión de ISO 27001:

1. **Evaluar la conformidad** del SGSI con los requisitos de la norma.
2. **Identificar deficiencias o brechas** en los controles de seguridad implementados.
3. **Proponer mejoras** en los procesos, políticas y procedimientos de seguridad de la información.

Proceso de revisión:

- **Revisión documental:** Se analiza la política de seguridad, procedimientos, registros de auditorías internas, análisis de riesgos y plan de tratamiento de riesgos.
- **Entrevistas y cuestionarios:** Se recaban evidencias del cumplimiento de los controles a través de entrevistas con responsables de procesos y encuestas a usuarios clave.
- **Inspección de controles:** Se verifica la implementación de lo física y lo técnica de los controles.
- **Reporte de hallazgos:** Se documentan las observaciones, no conformidades y recomendaciones para la mejora continua del SGSI.

La revisión periódica de ISO 27001 permite fortalecer la cultura de seguridad de la información, reducir los riesgos y permite garantizar que los activos de la información estén protegidos conforme a los estándares internacionales que son reconocidos.

A continuación, un cuadro comparativo de las diferentes ISO:

Tabla 7 *Modelo Iso (Fases)*

Norma ISO	**Descripción**	**Objetivo**	**Enfoque Principal**
ISO/IEC 27001	Norma internacional que especifica los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).	Proteger la confidencialidad, integridad y disponibilidad de la información mediante un SGSI efectivo.	Gestión de riesgos, implementación de controles, mejora continua.
ISO/IEC 27002	Norma que reúne un conjunto de buenas prácticas orientadas a la aplicación de controles de seguridad de la información dentro de las organizaciones.	Proporcionar directrices para seleccionar, implementar y gestionar controles de seguridad.	Controles técnicos, físicos y organizativos de seguridad.
ISO/IEC 27005	Estándar que establece lineamientos para identificar, analizar y gestionar los riesgos relacionados con la seguridad de la información.	Identificar, evaluar y tratar riesgos de seguridad de manera sistemática.	Gestión de riesgos, análisis y tratamiento de amenazas.
ISO/IEC 27017	Guía para controles de seguridad en servicios en la nube.	Mejorar la seguridad de la información en entornos de computación en la nube.	Controles específicos para proveedores y usuarios de la nube.
ISO/IEC 27018	Código de buenas prácticas para protección de datos personales en la nube.	Proteger la información personal identificable (PII) en servicios en la nube.	Privacidad, confidencialidad y control de datos personales.

Norma ISO	Descripción	Objetivo	Enfoque Principal
ISO 22301	Norma de gestión de continuidad del negocio.	Garantizar que la organización pueda continuar operaciones críticas ante interrupciones.	Planificación de continuidad, análisis de impacto y recuperación ante desastres.

Descripción de las normas ISO 27001:

Aspecto	Descripción
Nombre de la norma	ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información (SGSI)
Objetivo	Proteger la confidencialidad, integridad y disponibilidad de la información mediante la implementación de un SGSI basado en la gestión de riesgos.
Alcance	Aplicable a cualquier tipo de organización, independientemente de su tamaño o sector, que maneje información sensible.
Estructura	Basada en el ciclo **Planificar-Hacer-Verificar-Actuar (PDCA)** para la mejora continua. Incluye políticas, procesos, controles y registros.
Principales requisitos	Contexto de la organización y liderazgo- Planificación y evaluación de riesgos- Implementación de controles de seguridad- Monitoreo, auditoría y revisión del SGSI- Mejora continua
Beneficios	Reducción de riesgos de seguridad de la información- Cumplimiento legal y regulatorio- Confianza de clientes y partes interesadas- Mejor gestión de incidentes y continuidad del negocio

Aspecto	Descripción
Controles clave	Control de accesos- Seguridad física y ambiental- Gestión de incidentes- Seguridad en comunicaciones y operaciones- Gestión de proveedores y terceros

4.2.1.3 Fase 2 Ejecución

Esta es correspondiente a la ejecución de la auditoría, se aplicó la metodología MAGERIT para la identificación de activos, amenazas, vulnerabilidades y estimación del nivel de riesgo asociado. En cuanto al riesgo de malware, se evidenció la ausencia de lineamientos formales en materia de seguridad informática, uso de dispositivos externos, políticas de respaldo de información y protocolos de respuesta ante incidentes. Si bien la institución cuenta con medidas básicas como el uso de contraseñas y software antivirus, la limitada capacitación del personal docente incrementa la probabilidad de incidentes relacionados con ingeniería social o ejecución de software malicioso. Bajo el enfoque de MAGERIT, este escenario fue evaluado considerando la probabilidad de ocurrencia y el impacto sobre la confidencialidad e integridad de la información, determinándose un nivel de riesgo significativo que requiere acciones de mitigación mediante políticas formales, capacitación y fortalecimiento de controles técnicos.

De esta manera, la integración de la norma ISO/IEC 27001 como marco de cumplimiento y de la metodología MAGERIT como herramienta de análisis de riesgos permitió realizar una evaluación estructurada, identificando brechas en los controles de seguridad y estableciendo prioridades de mejora para fortalecer la protección de los activos informáticos institucionales.

La auditoría inicial fue la primera fase formal del proceso encaminado a obtener una visión clara y estructurada del estado actual de la seguridad informática en los centros de cómputo y oficinas administrativas de la ULEAM, Extensión El Carmen. En esta etapa se realizó un reconocimiento preliminar del entorno técnico y organizacional, que permitió identificar los activos involucrados, los procesos críticos y los mecanismos de control existentes.

La actividad inició con las entrevistas exploratorias al personal responsable del área de tecnologías de la información que sirvieron para recopilar la información sobre la infraestructura tecnológica, las políticas internas, prácticas de acceso y el uso de equipos. Esta información nos permitió definir el alcance de la auditoría y de establecer criterios de evaluación que se ajusten a las necesidades institucionales.

Luego se realizó una inspección física de lo que es el área de auditoría, se observó así de manera directa las condiciones de operación, dispositivos instalados, puntos de acceso físico, disposición del cableado, presencia de mecanismos de control (incluyendo cerraduras, registros, cámaras) y el estado general de los equipos.

Durante esta fase se revisó la documentación institucional relacionada con la seguridad, incluidas instrucciones de acceso, registros de mantenimiento, inventarios de activos y protocolos operativos. Toda esta información permitió crear una línea de base del desempeño actual de los sistemas, condición esencial para realizar mayores comparaciones e identificar la brecha entre la situación real y la situación deseada. La primera auditoría proporcionó en general el insumo básico para la adecuada planificación de las etapas posteriores y la correcta aplicación de las herramientas de análisis de riesgos.

4.2.1.4 Ejecución

La fase de implementación implicó la aplicación directa de los métodos y herramientas definidos en la planificación. Durante esta fase se desarrollaron actividades operativas con el objetivo de recopilar documentación suficiente y adecuada para evaluar los controles de seguridad existentes.

La investigación de información detallada se realizó mediante listas basadas en estándares de seguridad como ISO/IEC 27001 e ISO/IEC 27002 además, se utilizó la encuesta dirigida al personal administrativo, seguido de esto se realizaron comprobaciones como comprobar las configuraciones de seguridad de los equipos, comprobar los permisos de los usuarios, revisar las copias de seguridad y analizar la integridad física de los sistemas. Durante la ejecución se registraron todas las violaciones descubiertas, así como los hallazgos que pudieran representar riesgos a la integridad, disponibilidad o confidencialidad de los activos tecnológicos.

Cada hallazgo que fue documentado con la evidencia fotográfica, las descripciones técnicas y la ubicación exacta siguiendo así las buenas prácticas de auditoría informática. La información recopilada en esta etapa constituye la base para un mayor análisis de riesgos y la formulación de recomendaciones para fortalecer la seguridad institucional.

4.2.2 Análisis del Contexto

El análisis del contexto tuvo como finalidad identificar las condiciones internas y externas que influyen directa o indirectamente en la seguridad informática de la institución. Este examen consideró factores tecnológicos, organizacionales, ambientales y humanos que determinan el nivel de exposición a amenazas.

Se realizo una evaluación del entorno físico donde se encuentran ubicados los equipos, tomando en cuenta también la ventilación, la seguridad del área, el control de humedad y los

riesgos de ingresos no autorizados, además, se logró llegar a un análisis de la estructura organizacional del área, incluyendo los niveles de responsabilidad, los procesos aplicados y el nivel de seguridad, en el nivel tecnológico, se evaluó a los equipos utilizados, el sistema de autenticaciones seguras, la existencia de copias de seguridad o respaldos, las actualizaciones de software y las configuraciones de red, en cuanto al factor humano, se observó las buenas prácticas de contraseñas seguras, los accesos de los usuarios, el manejo de dispositivos y el cumplimiento de las normativas internas. También se tomaron en cuenta factores externos, como las amenazas prevalentes en el ámbito educativo, los riesgos de ciberataques en instituciones públicas y las normas legales sobre protección de datos. Este análisis resultó ser un insumo clave en la evaluación de riesgos al ayudar a identificar el nivel de exposición y la capacidad de la institución para responder a incidentes.

Tabla 8 *Cuestionario de Cumplimiento normas ISO*

Cuestionario para cumplimiento de requisitos Según normas ISO			C1 Pag 1 de 5
REQUISITOS	PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
4.1Comprensión de la Organización y su Contexto	1. ¿Existen objetivos definidos para el sistema de seguridad informática relacionados con el control de accesos físico y lógico?	0	
	2 ¿Se e ha revisado cómo están por dentro las instalaciones, para ver si todo eso influye en el control de accesos?	0	
	3 ¿Se han identificado problemas externos, como personas que ingresan sin permiso?	1	
	4. ¿Se dispone de un análisis previo de vulnerabilidades para determinar riesgos asociados a los accesos?	2	
4.4 Gestión del Control de Accesos	1. ¿Existe una política institucional vigente para el control de accesos?	0	
	4. ¿Existen medidas de autenticación adicional (MFA) para equipos o áreas críticas?	2	
	5. ¿Se implementan controles físicos como cerraduras, cámaras o tarjetas electrónicas?	0	
	6. ¿Se registra el ingreso y salida del personal a los centros de cómputo?	0	
	7. ¿Se revisan periódicamente los permisos y perfiles de acceso?	0	
Elaborado por: Zambrano Benalcázar Dayana Mishelle		**Revisado por:** Ing. Minaya Macias Renelmo Wladimir	
Fecha:		**Firma**:	

Tabla 9 *Cuestionario de requisitos Acceso Lógico*

Cuestionario para cumplimiento de requisitos				C1 Pag 2 de 5
	REQUISITOS	PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
	5.1 Control de Acceso Lógico	1. ¿Los equipos cuentan con autenticación obligatoria mediante usuario y contraseña?	1	
		2. ¿Se establecen reglas para la complejidad, longitud y caducidad de contraseñas?	0	
		3. ¿Existe un registro de todos los usuarios con acceso a los equipos institucionales?	0	
		4. ¿Se eliminan oportunamente los accesos de usuarios inactivos o desvinculados?	2	
		5. ¿Se restringe el acceso administrativo únicamente al personal autorizado?	0	
		6. ¿Se monitorean intentos fallidos de acceso?	2	

Elaborado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma**:

Tabla 10 *Cuestionario requisitos Control de Accesos Físicos*

Cuestionario para cumplimiento de requisitos			C1 Pag 3 de 5	
REQUISITOS			PREGUNTAS	REQUISITOS
	5.2 Control de Acceso Físico	1. ¿Las salas de cómputo y oficinas cuentan con cerraduras seguras y funcionamiento adecuado?	0	
		2. ¿Se dispone de cámaras o sistemas de vigilancia en áreas donde existen equipos críticos?	0	
		3. ¿Las ventanas, puertas y accesos secundarios presentan condiciones de seguridad apropiadas?	0	
		4. ¿Se dispone actualmente de un listado actualizado de las llaves, tarjetas de acceso y permisos físicos que se utilizan en la institución?	0	
	5.3 Gestión de Usuarios	1. ¿Se ha establecido algún proceso para registrar por primera vez a los usuarios que acceden al sistema?	2	
		2. ¿Se verifica la identidad del usuario antes de otorgar accesos?	1	
		3. ¿Se realiza revisión periódica de roles y privilegios asignados a cada usuario?	0	
		4. ¿Se documentan solicitudes de modificación o eliminación de usuarios?	0	
		5. ¿Los usuarios reciben capacitación sobre políticas de acceso y uso de equipos?	0	
Elaborado por: Zambrano Benalcázar Dayana Mishelle			**Revisado por:** Ing. Minaya Macias Renelmo Wladimir	
Fecha:			**Firma**:	

Tabla 11 *Cuestionario cumplimiento Gestión de riesgos*

Cuestiomario para cumplimiento de controles				C1 Pag 4 de 5
	REQUISITOS	PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
	6.2 Gestión de Riesgos	1. ¿Se ha realizado un análisis de riesgos específico para control de accesos?	0	
		2. ¿Se han detectado situaciones como robos, uso indebido de los equipos, ingresos sin autorización o pérdida de información?	1	
		3. ¿Se revisan aspectos como el uso de contraseñas poco seguras, permisos mal otorgados o problemas en la seguridad física del área?	0	
		4. ¿Los riesgos se clasifican por probabilidad e impacto?	0	
		5. ¿Se han definido medidas preventivas y correctivas ante los riesgos identificados?	0	
	6.3 Medidas de Protección y Monitoreo	1. ¿Se realizan copias de seguridad de información institucional?	0	
		2. ¿Se aplican actualizaciones de software y parches de seguridad de forma regular?	0	
		3. ¿Existe monitoreo continuo del uso de los equipos y accesos?	0	
		5. ¿Se aplican controles para evitar que usuarios autorizados conecten dispositivos externos?	0 no	
		6. ¿Se cuenta con antivirus, firewall u otras herramien protección activas?	1 tas de	

Elaborado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma**:

Tabla 12 *Cuestionario control de registros*

Cuestionario para cumplimiento de controles				C1 Pag 5 de 5
REQUISITOS		PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
		1. ¿Existe un procedimiento documentado para reportar incidentes de acceso no autorizado?	1	
		2. ¿El personal conoce los canales para reportar incidentes?	0	
		3. ¿Se lleva un registro de incidentes relacionados con accesos indebidos o intentos de intrusión?	0	
		4. ¿Se analizan las causas de los incidentes para evitar recurrencia?	0	
Elaborado por: Zambrano Benalcázar Dayana Mishelle			**Revisado por:** Ing. Minaya Macias Renelmo Wladimir	
Fecha:			**Firma**:	

4.2.2.1 Ejecución de los cuestionarios para analizar riesgos

Una vez diseñados los cuestionarios basados en las normas de seguridad informática aplicables, se procedió a su aplicación en los centros de cómputo y oficinas administrativas de la ULEAM, Extensión El Carmen. Esta actividad se llevó a cabo con la participación del personal administrativo, usuarios frecuentes de los equipos institucionales y responsables del área de Tecnologías de la Información.

Los cuestionarios se aplicaron de manera presencial mediante entrevistas directas y observación asistida. Esto permitió que cada interrogante fuera interpretada correctamente por los participantes, asegurando la fidelidad de la información recopilada. Además, durante la

ejecución, se aclararon dudas sobre los controles implementados, la gestión de accesos, el uso de contraseñas y las prácticas operativas que podrían afectar la seguridad del entorno.

La aplicación de los cuestionarios permitió identificar el nivel de cumplimiento de los requisitos de seguridad informática y detectar posibles brechas relacionadas con el acceso físico y lógico a los equipos tecnológicos. Asimismo, se obtuvo información clave sobre percepciones, hábitos y comportamientos de los usuarios, lo cual constituyó un insumo fundamental para el proceso de análisis de riesgos.

Tabla 13 *Cuestionario de Identificación (Robo).*

CUESTIONARIO PARA IDENTIFICAR RIESGO				C2 Pág. 1 de 5	
ROBO					
Preguntas		Respuestas		Observación	Riesgo
		Si	No		
1	¿La sala de docentes cuenta con un control de acceso físico que limite el ingreso únicamente a personal autorizado?		X		0
2	¿Las puertas de acceso a la sala de docentes permanecen cerradas cuando no se encuentran en uso?	X			1
3	¿Las cerraduras de las puertas de la sala de docentes se encuentran en buen estado y funcionamiento?		X		0
4	¿Las ventanas de la sala de docentes cuentan con sistemas de seguridad que impidan el acceso desde el exterior?		X		0
5	¿Existe un responsable designado para el control de llaves de la sala de docentes?		X		0
6	¿Se controla el acceso de personas externas a la sala de docentes?		X		0
7	¿La sala de docentes cuenta con algún sistema de vigilancia (cámaras, guardias u otro medio)?		X		0
8	¿Los sistemas de vigilancia, en caso de existir, se encuentran operativos?		X	No tienen	0
9	¿Se restringe el acceso a la sala de docentes fuera del horario laboral?	X			1
10	¿Existe un registro de ingreso y salida del personal que accede a la sala de docentes?		X		0
11	¿Se cuenta con un inventario actualizado de los equipos informáticos ubicados en la sala de docentes?		X		0
12	¿Los equipos informáticos se encuentran correctamente identificados como propiedad institucional?	X			1
13	¿Se controla la salida de equipos informáticos de la sala de docentes?		X		0
14	¿Se han reportado intentos de robo o pérdida de equipos informáticos en la sala de docentes?	X			1
15	¿Existen procedimientos definidos ante la pérdida o robo de equipos informáticos?	X			1
16	¿El personal docente conoce las normas institucionales relacionadas con la prevención de robos?		X	Mínimamente	0
17	¿Se realizan inspecciones periódicas para verificar la presencia de todos los equipos informáticos?		X		0
18	¿La ubicación de la sala de docentes facilita el control y vigilancia del área?		X		0
19	¿La sala de docentes cuenta con iluminación adecuada para prevenir actos delictivos?	X			1
20	¿Se considera que los controles actuales son suficientes para prevenir el robo de equipos informáticos?		X		0
Realizado Por: Zambrano Benalcázar Dayana Mishelle				**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:				**Firma:**	

Tabla 14 *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	¿La sala de docentes cuenta con detectores de humo?		X	No hay	2
2	¿Existen extintores en lugares visibles y accesibles?		X	No hay	2
3	¿Los extintores se encuentran vigentes y señalizados?		X		1
4	¿Hay señalización visible de rutas de evacuación?		X		0
5	¿Existen carteles con instrucciones ante incendios?		X		1
6	¿Los tomacorrientes se encuentran sobrecargados?		X		0
7	¿Los cables eléctricos presentan cortes o deterioro?	X			1
8	¿Los cables eléctricos están protegidos adecuadamente?		X		0
9	¿Se almacenan objetos inflamables junto a equipos informáticos?		X		0
10	¿Las cortinas y muebles son de material resistente al fuego?		X		1
11	¿La sala cuenta con iluminación de emergencia funcional?	X			1
12	¿El tablero eléctrico dispone de protecciones?		X		0
13	¿Se observan filtraciones de agua cerca de instalaciones eléctricas?	X			0
14	¿Las paredes presentan humedad cerca de enchufes o cableado?	X			1
15	¿Los cables eléctricos y de red están ordenados y diferenciados?	X			1
16	¿La estructura del techo evita filtraciones sobre los equipos?		X		0
17	¿Los pasillos y puertas se encuentran libres de obstáculos?	X			0
18	¿Existe personal responsable de seguridad contra incendios?		X		0
19	¿Se revisa periódicamente la temperatura de los equipos?		X		0
20	¿Se dispone de un botiquín de primeros auxilios?		X		0
Realizado Por: Zambrano Benalcázar Dayana Mishelle				**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:				**Firma:**	

Tabla 15 *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		1
2	¿Existen protocolos para manipulación segura de equipos?	X			1
3	¿El personal docente recibe capacitación sobre el uso adecuado de los equipos?		X		1
4	¿La institución cuenta con manuales de operación de los equipos informáticos?		X		1
5	¿Se controla la temperatura del área donde se ubican los equipos?	X			0
6	¿Se controla la humedad en la sala de docentes?		X		0
7	¿Se revisa periódicamente el estado físico de los equipos?		X		1
8	¿Se documentan las fallas técnicas y reparaciones realizadas?		X		1
9	¿La institución cuenta con seguro para los equipos informáticos?	X			1
10	¿Existen políticas para el reemplazo de equipos dañados?	X			1
11	¿Se controla el acceso a equipos considerados críticos o delicados?		X		0
12	¿Se evita el uso indebido o no autorizado de los equipos?		X		1
13	¿Existen protocolos para la desconexión segura de los equipos?	X			1
14	¿Se inspeccionan periódicamente los cables eléctricos y de red?		X		0
15	¿Los cables y conexiones se encuentran en buen estado?		X		1
Realizado Por: Zambrano Benalcázar Dayana Mishelle				**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:				**Firma:**	

Tabla 16 *Cuestionario de Identificación de Riesgo (Inundación).*

CUESTIONARIO PARA IDENTIFICAR DE INUNDACIÓN				**C2** **Pág. 4 de 5**	
INUNDACIÓN					
Preguntas		**Respuestas**		**Observación**	**Riesgo**
		Si	**No**		
1	¿La sala de docentes se encuentra ubicada en una zona con bajo riesgo de inundación?	X			1
2	¿El piso de la sala de docentes presenta acumulación de agua durante la temporada de lluvias?	X			1
3	¿Las puertas de la sala de docentes sellan correctamente al momento de cerrarse?		X		1
4	¿Existen sistemas de drenaje funcionales alrededor del edificio?		X		1
5	¿El techo de la sala de docentes presenta filtraciones o signos de humedad?	X			1
6	¿Las ventanas de la sala de docentes cierran de forma hermética?		X		1
7	¿Los equipos informáticos se encuentran ubicados sobre superficies elevadas?	X			1
8	¿Se observan rastros de humedad en paredes o esquinas del área?	X			1
9	¿Los cables eléctricos y de red se encuentran protegidos del contacto con el piso?		X		1
10	¿La sala de docentes cuenta con protección externa frente al ingreso de agua?		X		1
11	¿La estructura del techo se encuentra en buen estado?		X		1
12	¿Los documentos y materiales se almacenan fuera del nivel del piso?	X			2
13	¿El área dispone de espacios despejados para la evacuación del agua?		X		1
14	¿Las canaletas y canalones se mantienen libres de obstrucciones?		X		1
15	¿Las canaletas del techo funcionan adecuadamente?		X		1
16	¿Los interruptores eléctricos están ubicados por encima del nivel del piso?	X			2
17	¿El entorno del edificio permite un drenaje natural del agua?		X		1
18	¿Se aplican medidas preventivas durante lluvias intensas?		X		1
19	¿Existen obstáculos que impidan la evacuación del agua?		X		1
20	¿Las instalaciones se revisan después de eventos de lluvia?		X		1
Realizado Por: Zambrano Benalcázar Dayana Mishelle				**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:				**Firma:**	

Tabla 17 *Cuestionario de Identificación de Riesgo (Malware).*

CUESTIONARIO PARA IDENTIFICAR DE MALWARE				C2 Pág. 5 de 5	
MALWARE					
Preguntas		**Respuestas**		**Observación**	**Riesgo**
		Si	**No**		
1	¿Los equipos informáticos cuentan con software antivirus actualizado?		X		1
2	¿Se realizan análisis periódicos para la detección de malware?		X		1
3	¿El personal docente recibe capacitación sobre prevención de malware?		X		1
4	¿Existen políticas institucionales para la instalación de software?	X			1
5	¿Se controla el uso de dispositivos de almacenamiento externo (USB)?		X		1
6	¿Se aplican actualizaciones de seguridad en los sistemas operativos?		X		1
7	¿Existen protocolos definidos ante la detección de malware?	X			1
8	¿La red cuenta con un firewall activo y configurado adecuadamente?	X			1
9	¿Se monitorean las conexiones de red de los equipos?		X		0
10	¿Se restringe el acceso a sitios web considerados no seguros?		X		1
11	¿Se realizan copias de seguridad periódicas de la información?		X		0
12	¿Se controla el uso de correos electrónicos sospechosos?		X		1
13	¿Se aplican políticas de contraseñas seguras?		X		1
14	¿Se verifica la integridad de los archivos descargados?		X		1
15	¿Se documentan los incidentes relacionados con malware?		X		1
16	¿Se dispone de herramientas básicas para análisis forense digital?		X		1
17	¿Se restringe el acceso remoto no autorizado a los equipos?		X		1
18	¿Se realizan pruebas de seguridad o vulnerabilidad periódicas?		X		1
19	¿Se controla el uso de software no autorizado o pirata?		X		1
20	¿La institución dispone de un plan de respuesta ante ataques de malware?	X			1
Realizado Por: Zambrano Benalcázar Dayana Mishelle				**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:				**Firma:**	

4.2.2.2 Recolección de datos

La recolección de datos se llevó a cabo mediante visitas programadas a las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, con el propósito de obtener información directa, relevante y confiable sobre el estado actual de la seguridad informática y física de los equipos tecnológicos asignados al personal docente. Esta fase constituyó un elemento fundamental dentro del proceso de auditoría, ya que permitió recopilar evidencia real sobre las condiciones en las que se encuentran los activos informáticos y los controles de seguridad existentes.

Para el desarrollo de esta etapa se aplicaron instrumentos de recolección de datos previamente diseñados y validados, tales como encuestas estructuradas dirigidas al personal docente, entrevistas semiestructuradas a los responsables del área tecnológica y observaciones directas del entorno físico. Estos instrumentos permitieron identificar riesgos asociados al acceso no autorizado, robos, daños físicos, incendios, inundaciones y amenazas lógicas como la presencia de malware, así como evaluar el cumplimiento de políticas, procedimientos y buenas prácticas de seguridad informática.

A través de la observación directa se logró una verificación más clara del estado de la infraestructura física, los controles de acceso, la ubicación del equipo, las condiciones ambientales y las medidas de protección existentes en las salas de docentes, también se reunió información sobre el conocimiento del personal a través de encuestas y entrevistas. En esta etapa, el objetivo era reunir información objetiva y verificable para utilizar en el desarrollo de un análisis técnico coherente y consistente con los estándares internacionales; los objetivos principales siendo ISO/IEC 27001, ISO/IEC 27002, COBIT y MAGERIT, la información obtenida permitió la identificación de vulnerabilidades, la evaluación de riesgos y sugerencias para mejorar la seguridad informática, asegurando la confidencialidad, integridad y disponibilidad de la información institucional.

Figura 2 *Techo sala docente*

Figura 3 *Rac*

Figura 4 *No cuentan con extintores*

Figura 5 *Ruta de salida*

Figura 6 *Paredes en mal estado*

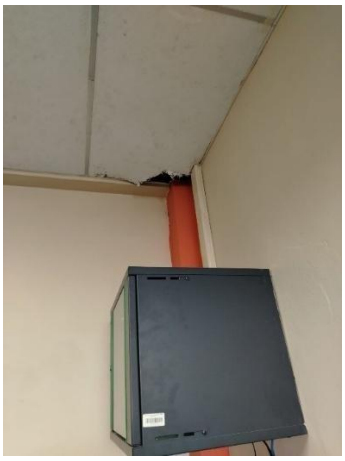


Figura 7 *Techo en mal estado*

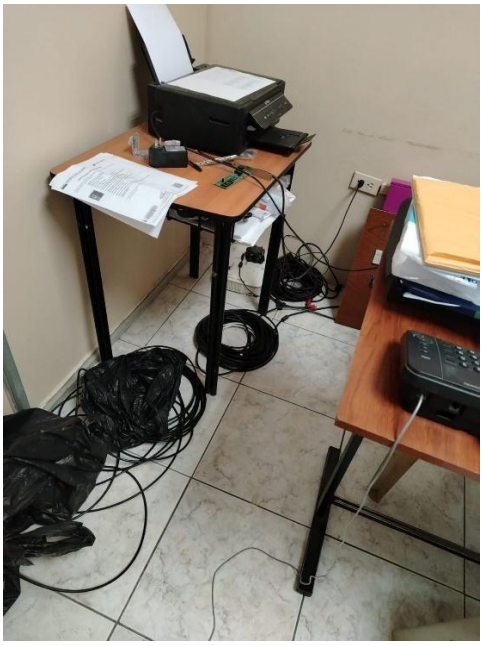


Figura 8 Obstrucción de cables

Figura 9 *Enchufes en mal estado*

Figura 10 *Filtraciones de Agua*

Figura 11 *Cubículos sin implementos*

4.2.2.3 Aplicación de análisis de riesgo

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

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

débiles, falta de supervisión de accesos, carencia de cerraduras seguras o inexistencia de registros de ingreso.

Tabla 18 Identificación de riesgos

Identificación de Riesgos	**R1** **Pág. 1 de 4**
Robo debido a: • La inexistencia de controles de acceso físico que limiten el ingreso únicamente a personal autorizado. • El deficiente estado y funcionamiento de las cerraduras de las puertas de la sala de docentes. • La ausencia de sistemas de seguridad en las ventanas que impidan el acceso desde el exterior. • La falta de un responsable designado para el control y administración de llaves. • La ausencia de controles para el ingreso de personas externas a la sala de docentes. • La sala no cuenta con un sistema de vigilancia, como son las cámaras o el personal de seguridad asignado. • Los medios de vigilancia presentes en ciertos lugares no cumplen su función de manera adecuada, ya que su operación no es constante. • No existen registros formales que permitan llevar un control sobre el ingreso y salida del personal en la sala. • No se dispone de un inventario actualizado de los equipos informáticos asignados a la sala de docentes. • No se cuenta con un control efectivo sobre la salida o préstamo de equipos informáticos. • El personal docente no conoce claramente las normas institucionales relacionadas con la prevención de robos. • La ausencia de inspecciones periódicas para verificar la integridad y presencia de los equipos informáticos. • La ubicación de la sala de docentes que dificulta el control y la vigilancia del área. • La percepción de insuficiencia de los controles actuales para prevenir el robo de equipos informáticos.	
Realizado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma:**

Incendio debido a:

- La inexistencia de detectores de humo en la sala de docentes.
- La ausencia de extintores en lugares visibles y accesibles.
- La falta de extintores vigentes y debidamente señalizados.
- La inexistencia de señalización de rutas de evacuación.
- La ausencia de carteles con instrucciones ante incendios.
- La falta de protección adecuada en los cables eléctricos.
- El uso de mobiliario que no garantiza resistencia al fuego.
- No se ha designado a una persona responsable de la seguridad y prevención de incendios en la sala de docentes.
- No se realizan revisiones periódicas de la temperatura de los equipos informáticos.
- El área no cuenta con botiquines de primeros auxilios para atender emergencias.

Daño de equipos debido a:

- No se ejecuta un mantenimiento preventivo regular a los equipos informáticos.
- No existen protocolos o lineamientos definidos claramente para la manipulación segura de los equipos.
- No se ha capacitación al personal docente sobre el uso correcto y adecuado de los equipos otorgados.
- La carencia de manuales de operación de los equipos informáticos.
- La falta de revisiones periódicas del estado físico de los equipos informáticos.
- La ausencia de documentación de las fallas técnicas y reparaciones realizadas.
- La inexistencia de los seguros para los equipos informáticos.
- La ausencia de políticas para el reemplazo de equipos dañados.
- La falta de control sobre el uso indebido o no autorizado de los equipos.
- La inexistencia de protocolos para la desconexión segura de los equipos.
- El deficiente estado de cables y conexiones eléctricas y de red.

Realizado por:	**Revisado por:**
Zambrano Benalcázar Dayana Mishelle	Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma:**

<table>
<tr><th>Identificación de Riesgos</th><th>R1
Pág. 4 de 4</th></tr>
<tr><td colspan="2">

Malware debido a:

- La inexistencia de software antivirus actualizado en los equipos.
- La ausencia de análisis periódicos para la detección de malware.
- La falta de capacitación al personal docente sobre prevención de malware.
- La inexistencia de políticas institucionales para la instalación de software.
- La falta de un control claro sobre el uso de dispositivos de almacenamiento externo, como memorias USB.
- Los sistemas operativos no reciben actualizaciones de seguridad de forma regular.
- No se cuenta con procedimientos definidos para actuar cuando se detecta malware.
- No existe un firewall activo o este no se encuentra correctamente configurado.
- No se realiza un seguimiento del tráfico ni de las conexiones de red.
- No se efectúan copias de seguridad periódicas de la información almacenada.
- No se aplican controles para identificar o prevenir el uso de correos electrónicos sospechosos.
- La falta de documentación de incidentes relacionados con malware.
- La ausencia de herramientas de análisis forense digital.
- La inexistencia de un plan de respuesta ante ataques de malware.

</td></tr>
<tr><td>Realizado por:
Zambrano Benalcázar Dayana Mishelle</td><td>Revisado por:
Ing. Minaya Macias Renelmo Wladimir</td></tr>
<tr><td>Fecha:</td><td>Firma:</td></tr>
</table>

Inundación debido a:

- El piso de la sala de docentes presenta acumulación de agua durante la temporada de lluvias.
- Las puertas de la sala de docentes no sellan correctamente al momento de cerrarse.
- No existen sistemas de drenaje funcionales alrededor del edificio.
- El techo de la sala de docentes presenta filtraciones o signos de humedad.
- Las ventanas de la sala de docentes no cierran de forma hermética.
- Los cables eléctricos y de red no se encuentran protegidos del contacto con el piso.
- La sala de docentes no cuenta con protección externa frente al ingreso de agua.
- La estructura del techo no se encuentra en óptimas condiciones.
- Los documentos y materiales frecuentemente se colocan directamente en el piso, lo que aumenta el riesgo de que se dañen cuando entra agua.
- El espacio no consta de áreas despejadas que puedan facilitar la extracción del agua en caso de una inundación.
- Las canaletas y canalones no se les realiza limpieza con frecuencia, por lo que se tapan con facilidad.
- Las canaletas del techo presentan fallas y no pueden cumplir correctamente su función.
- Durante las lluvias torrenciales no se aplican acciones preventivas para evitar acumulaciones de agua.
- Se observan objetos que impiden que el agua fluya o se evacúe adecuadamente.
- Después de eventos de lluvia no se realizan inspecciones para verificar el estado de las instalaciones.

Realizado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma:**

4.2.2.4 Tabulación de análisis de riesgos

Una vez obtenida la información del análisis de riesgos, se procedió a la tabulación y organización de los datos recopilados, cada uno de los riesgo identificados se los fue registrando en una matriz que permitió visualizar de una mejor manera, más clara y ordenada la relación entre amenazas, vulnerabilidades y activos, este proceso facilitó la comparación entre riesgos, destacando así a aquellos con una mayor relevancia para la seguridad institucional, de igual forma la tabulación permitió obtener una visión cuantitativa y cualitativa del estado actual de la seguridad en las salas docentes y administrativas, sirviendo así de ayuda para priorizar las acciones y medidas correctivas.

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 19 *Evaluación y cumplimiento*

SI	**1**
NO	**0**
NO APLICA	**2**

Tabla 20 *Valoración ISO*

Requisito	Evaluadas	Cumple	No cumple	% Cumplimiento	% Brecha
4.1 Contexto	3	1	2	33%	67%
4.4 Gestión Control	4	0	4	0%	100%
5.1 Acceso Lógico	4	1	3	25%	75%
5.2 Acceso Físico	4	0	4	0%	100%
5.3 Gestión Usuarios	4	1	3	25%	75%
6.2 Gestión Riesgos	5	1	4	20%	80%
6.3 Protección	5	1	4	20%	80%
Gestión Incidentes	4	1	3	25%	75%
TOTAL GENERAL	**33**	**6**	**27**	**18%**	**82%**

Tabla 21 *% Nivel de Madurez del Sistema*

% Cumplimiento	Nivel de Madurez
0% – 20%	Inicial / Crítico
21% – 40%	Básico
41% – 60%	Intermedio
61% – 80%	Aceptable
81% – 100%	Óptimo

El análisis del cuestionario aplicado evidenció un cumplimiento general del 18% respecto a los requisitos evaluados relacionados con el control de accesos conforme a los lineamientos de la norma ISO 27001. Los resultados reflejan una brecha del 82%, indicando un nivel crítico de deficiencia en la gestión de seguridad, especialmente en los controles físicos, gestión de riesgos y formalización documental. Esta situación incrementa significativamente la probabilidad de materialización de amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Tabla 22 *Valoración de riesgos*

Valoración de riesgos	**R2** **Pág. 1 de 3**

PROBABILIDAD DE ROBO		
	Total	**No Aplica**
Total, De Campo Evaluados	20	0
Total, Seguro	6	0
Total, Riesgo	14	0
Porcentaje Seguro	6*100/20=	30 %
Porcentaje Riesgo	14*100/20=	70%

Realizado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir.
Fecha:	**Fecha:**

PROBABILIDAD DE INCENDIO		
	Total	**No Aplica**
Total, De Campo Evaluados	20	0
Total, Seguro	10	0
Total, Riesgo	10	0
Porcentaje Seguro	10*100/20=	50%
Porcentaje Riesgo	10*100/20=	50%

PROBABILIDAD DE DAÑO DE EQUIPO		
	Total	**No Aplica**
Total, De Campo Evaluados	15	0
Total, Seguro	4	0
Total, Riesgo	11	0
Porcentaje Seguro	4*100/15=	27%
Porcentaje Riesgo	11*100/15=	73%

PROBABILIDAD DE INUNDACIÓN		
	Total	**No Aplica**
Total, De Campo Evaluados	20	1
Total, Seguro	5	0
Total, Riesgo	15	0
Porcentaje Seguro	5*100/20=	25%
Porcentaje Riesgo	15*100/20=	75%

Realizado por: Castro Alava Julexy Jamileth	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Fecha:**

Valoración de riesgos	R2 Pág. 3 de 3

PROBABILIDAD DE MALWARE		
	Total	**No Aplica**
Total, De Campo Evaluados	20	0
Total, Seguro	2	0
Total, Riesgo	18	0
Porcentaje Seguro	2*100/20=	10 %
Porcentaje Riesgo	18*100/20=	90%

Realizado por:	**Revisado por:**
Zambrano Benalcázar Dayana Mishelle	Ing. Minaya Macias Renelmo Wladimir.
Fecha:	**Fecha:**

4.2.2.5 Impacto de análisis de riesgos

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

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

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

se establecieron cuáles son las prioridades y se definieron las acciones de mejora acordes a la realidad de la institución.

4.2.2.6 Valoración de riesgos

La valoración de riesgos consistió en la asignación de un nivel de riesgo resultante a partir de la combinación de la probabilidad y el impacto identificados en las etapas anteriores. Para ello, se empleó una escala que permitió clasificar los riesgos en categorías:

- **Muy Bajo**
- **Apreciable**
- **Muy Alto**

Esta valoración facilitó la identificación de los riesgos más críticos relacionados con el control de accesos y permitió establecer prioridades en la implementación de medidas de corrección y prevención. Además, la valoración proporcionó una guía objetiva para la toma de decisiones, orientando a la institución hacia el fortalecimiento de sus controles de seguridad física y lógica.

Tabla 23 *Escala de probabilidades*

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%

4.2.2.7 Matriz de Riesgo

Con base en la valoración realizada, se elaboró una matriz de riesgos que integró la probabilidad y el impacto para cada riesgo identificado. La matriz permitió representar

visualmente el nivel de criticidad de los riesgos, clasificándolos en zonas de atención inmediata, moderada o mínima.

Tabla 24 *Clasificación riesgos*

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

La matriz incluyó:

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

Tabla 25 *Evaluación de riesgos*

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

4.2.2.8 Procesos (Ejemplo: estudio de factibilidad)

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

Lo primero que se realizó fue revisar si la institución cuenta con la infraestructura necesaria para poder implementar las mejoras en los sistemas de control, como son el uso de tarjetas electrónicas, la biometría o la autenticación en dos pasos, después de esto se analizó si el personal y los procesos actuales permitirían aplicar estos cambios sin mostrar mayores complicaciones, considerando la capacitación y adaptación del personal involucrado, con lo que respecta al aspecto económico, se tuvo en cuenta los costos que estaban relacionados con la compra de los equipos, su mantenimiento y la capacitación requerida, por último, a nivel institucional se realizó una evaluación para ver si existen las condiciones organizativas requeridas para poder adoptar los nuevos protocolos de seguridad y ponerlos en práctica de forma correcta.

Tabla 26 *Calculo de impacto*

Cálculo de Impacto	R2 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	2	3	6
Inundación	1	1	3	5
Malware	4	4	3	11

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:**
Zambrano Benalcázar Dayana Mishelle	Minaya Macias Renelmo Wladimir, Mg.
Fecha:	**Firma:**

Durante la auditoría se evaluaron los controles establecidos en la norma ISO/IEC 27001 relacionados con seguridad física, gestión de activos y protección contra amenazas informáticas. En relación con los controles de seguridad física y control de acceso, se determinó un nivel de cumplimiento bajo, debido a la inexistencia de controles formales de acceso, sistemas de vigilancia, registros de ingreso y mecanismos de identificación del personal autorizado, lo cual incumple los lineamientos asociados a la protección de áreas seguras.

Respecto al control relacionado con la protección contra incendios y seguridad ambiental, se evidenció un cumplimiento parcial, dado que la institución no dispone de detectores de humo, extintores funcionales ni señalización adecuada, lo que refleja debilidades en la prevención y respuesta ante emergencias físicas.

En cuanto al control de gestión y mantenimiento de activos, se determinó un nivel de cumplimiento bajo, debido a la ausencia de mantenimiento preventivo periódico, protocolos de manipulación segura, documentación de fallas técnicas y políticas de reemplazo de equipos, lo cual incrementa la probabilidad de deterioro prematuro de los activos tecnológicos.

En relación con los controles de seguridad ambiental vinculados a la protección contra desastres naturales, se identificó un cumplimiento parcial, considerando que no existen medidas preventivas ante lluvias intensas, sellado adecuado de puertas y ventanas, ni inspecciones posteriores a eventos climáticos.

Finalmente, respecto a los controles asociados a la protección contra software malicioso y seguridad lógica, se determinó un nivel de cumplimiento bajo, debido a la inexistencia de políticas formales de seguridad informática, falta de análisis periódicos de malware, ausencia de copias de seguridad estructuradas y carencia de un plan de respuesta ante incidentes.

CAPÍTULO V:

5 EVALUACIÓN DE RESULTADOS

Tipo de Auditoría: Auditoría de Seguridad Informática

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

Objetivos:

- Evaluar el nivel de cumplimiento de normas y política de seguridad en cubículos docentes Universidad Laica Eloy Alfaro de Manabí extensión EL Carmen según la norma ISO 27001.
- Identificar los posibles riegos de seguridad informática a los que está expuesto.

Introducción

El presente capítulo tiene como finalidad presentar la propuesta de mejora derivada de los resultados obtenidos durante la auditoría informática aplicada a la seguridad de los equipos en las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen. La propuesta se fundamenta en los análisis de riesgos realizado en el capítulo anterior, el cual permitió identificar debilidades significativas en los controles de seguridad física, lógica y organizacional que protegen los activos informáticos institucionales.

A partir de los hallazgos obtenidos mediante la aplicación de cuestionarios, observación directa y entrevistas al personal responsable, se plantea un conjunto de acciones orientadas a fortalecer la seguridad de los equipos asignados a los docentes, reducir la probabilidad de incidentes como robos, incendios, daños por fallas técnicas, inundaciones y ataques de malware, así como mejorar la gestión institucional de la seguridad informática.

5.1 Objetivo de la propuesta

Diseñar una propuesta de mejora orientada a fortalecer la seguridad informática de los equipos ubicados en las salas de docentes de la ULEAM Extensión El Carmen, mediante la aplicación de controles físicos, lógicos y administrativos, basados en normativas y buenas prácticas de seguridad de la información, con el fin de reducir los riesgos identificados durante la auditoría informática.

5.1.1 Alcance de la propuesta

La propuesta está dirigida específicamente a las salas de docentes de la ULEAM Extensión El Carmen e involucra a los equipos informáticos asignados al personal docente, los controles de acceso físico, las políticas institucionales de uso de equipos, los mecanismos de protección contra amenazas físicas y lógicas, así como los procesos de mantenimiento, monitoreo y respuesta ante incidentes de seguridad informática.

5.2 Presentación y monitoreo de resultados

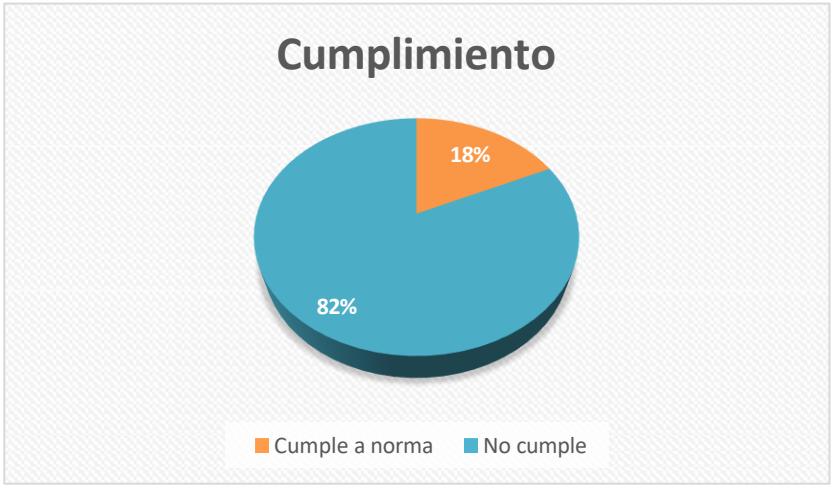
Con base en la información recolectada durante la auditoría informática, se procedió a la tabulación y análisis de los datos obtenidos a través de los instrumentos aplicados. Los resultados permitieron determinar el nivel de riesgo al que están expuestos los equipos informáticos de las salas de docentes, considerando las principales amenazas evaluadas: robo, incendio, daño de equipos, inundación y malware.

Los datos obtenidos fueron representados mediante gráficos de barras, los cuales permiten visualizar de manera clara y comprensible la proporción de condiciones seguras frente a aquellas consideradas de riesgo dentro de cada categoría analizada. Esta representación gráfica facilita la interpretación de los resultados y apoya la toma de decisiones para la formulación de acciones correctivas.

5.3 HALLAZGOS

Una vez obtenidos los valores de probabilidad e impacto, se procedió a realizar la interpretación general del riesgo de robo, con el propósito de determinar el nivel de criticidad de esta amenaza en las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen. Este análisis permitió priorizar los riesgos más relevantes y establecer una base técnica para la toma de decisiones orientadas a la implementación de medidas correctivas y preventivas que fortalezcan la seguridad de los activos informáticos institucionales.

Tabla 27 *Interpretación general cumplimientos ISO 27001*

Evaluación de cumplimientos de requisitos ISO 27001

Tomando en consideración el análisis del cumplimiento de los requisitos evaluados conforme a la norma ISO 27001 en relación con el control de accesos, se determinó un nivel general de cumplimiento del 18%, evidenciando una brecha del 82%. Los resultados reflejan un nivel crítico de madurez en la gestión de seguridad de la información.

4.1 Comprensión de la organización y su contexto

Interpretación: En el requisito correspondiente a la comprensión de la organización y su contexto se evidencia un bajo nivel de cumplimiento lo que refleja que no se encuentran claramente definidos todos los elementos necesarios para una adecuada gestión de seguridad de la información. Esto indica un nivel de madurez bajo en la identificación estructurada de factores internos y externos que influyen en el control de accesos. Las principales causas identificadas son: • No existe documentación formal sobre análisis del contexto organizacional. • No se han identificado de manera estructurada las partes interesadas. • No se dispone de un análisis completo de vulnerabilidades relacionadas con accesos físicos y lógicos.

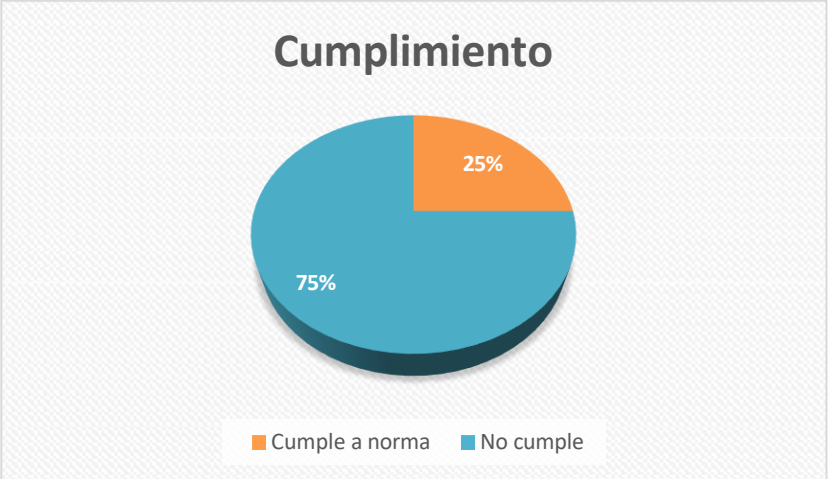
4.4 Gestión del Control de Accesos

Interpretación: En este requisito se evidencia un incumplimiento total muy bajo, lo cual representa un nivel crítico de madurez en la gestión formal del control de accesos. La ausencia de políticas documentadas y mecanismos estructurados de autenticación demuestra debilidades significativas en la protección de los activos tecnológicos institucionales.

Las causas principales son:

- No existe una política formal vigente sobre control de accesos.
- No se aplican medidas adicionales de autenticación en áreas críticas.
- No se registran formalmente los ingresos y salidas del personal.

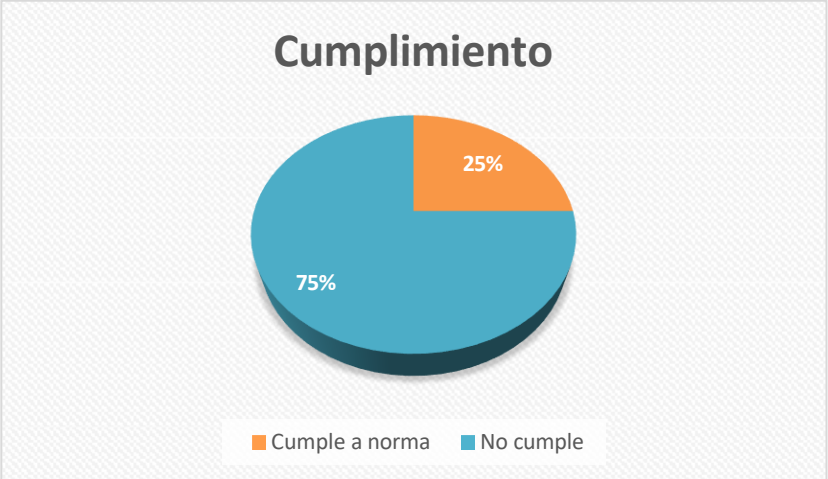
5.1 Control de Acceso Lógico



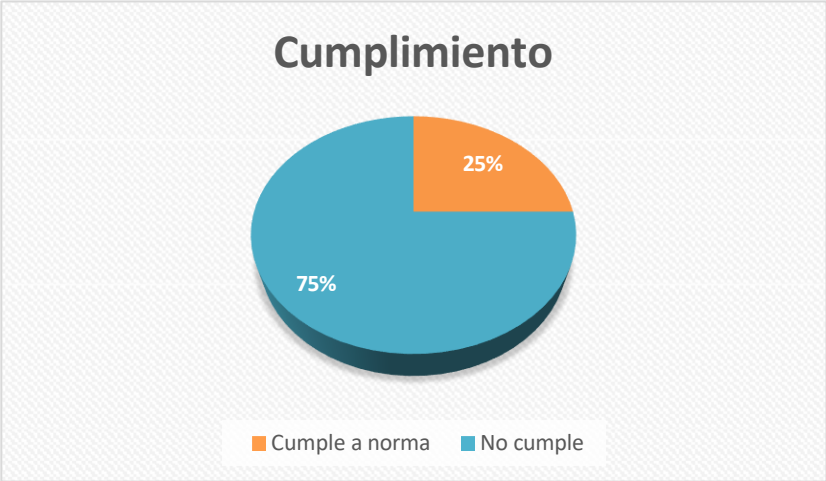
Interpretación: El nivel de cumplimiento indica que existen algunos controles básicos implementados, como el uso de usuario y contraseña, sin embargo, no se gestionan adecuadamente los requisitos de seguridad relacionados con la administración de accesos lógicos.

Las principales causas son:

- No se establecen políticas de complejidad de contraseñas documentadas.
- No existe monitoreo constante de intentos fallidos de acceso.
- No se eliminan oportunamente los accesos de usuarios inactivos.

5.2 Control de Acceso Físico

Interpretación: El análisis refleja un incumplimiento total en el control de acceso físico, lo que evidencia una brecha crítica en la protección de las instalaciones donde se encuentran los activos tecnológicos. Las causas identificadas incluyen: • Ausencia de controles físicos adecuados (cerraduras reforzadas, control electrónico). • No existe registro actualizado de llaves o permisos físicos. • No se dispone de sistemas de vigilancia en áreas críticas

5.3 Gestión de Usuarios



Interpretación: Se observa un nivel bajo de cumplimiento en la gestión de usuarios. Aunque existen prácticas básicas, no se encuentran formalizadas ni documentadas bajo un procedimiento institucional.

Las principales causas son:

- No se documentan solicitudes de creación o eliminación de usuarios.
- No se realiza revisión periódica de privilegios.
- No se capacita formalmente a los usuarios en políticas de acceso.

6.2 Gestión de Riesgos

Interpretación: El requisito presenta un bajo nivel de cumplimiento, evidenciando que no existe una gestión formal y documentada de riesgos asociados al control de accesos.

Las causas principales son:

- No se realiza análisis formal de riesgos bajo metodología estructurada (como MAGERIT).
- No se documentan los riesgos identificados.
- No se clasifican riesgos por probabilidad e impacto.

6.3 Medidas de Protección y Monitoreo

Interpretación: Existe un cumplimiento mínimo en la implementación de medidas de protección, lo que demuestra que, aunque se aplican algunas acciones básicas, no se encuentran formalizadas dentro de un sistema de gestión.

Las causas identificadas son:

- No existe monitoreo continuo documentado.
- No se aplican controles formales para dispositivos externos.
- No se gestionan actualizaciones de seguridad bajo procedimiento establecido

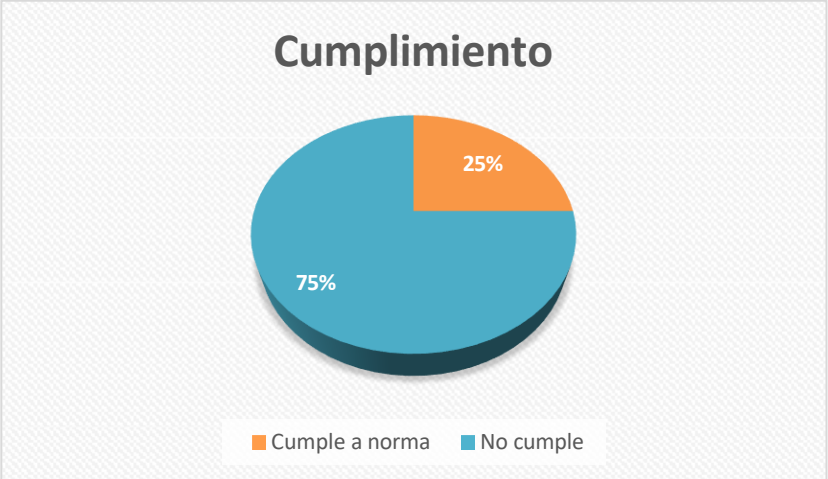
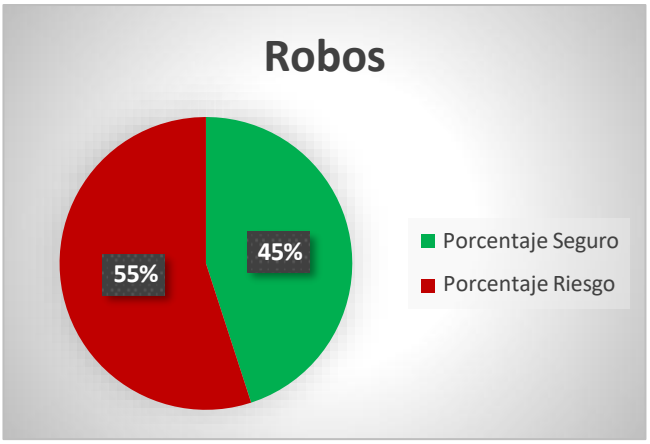
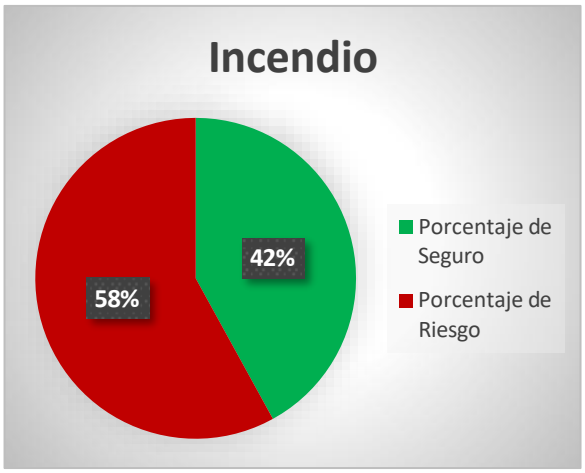
Gestión de Incidentes

Interpretación: El cumplimiento es bajo, lo que evidencia que la institución no cuenta con un procedimiento estructurado para la gestión de incidentes relacionados con accesos no autorizados. Las causas principales son: • No existe procedimiento documentado de reporte de incidentes. • No se lleva registro formal de incidentes. • No se realiza análisis de causas para evitar recurrencia.

Tabla 28 *Interpretación general*

<table>
<tr>
<td>Robos
 
</td>
<td>Debido a:
• La inexistencia de controles de acceso físico.
• La falta de seguridad en puertas y ventanas.
• La nula presencia de sistemas para la identificación
• La carencia de cámaras de vigilancia.
• La falta de registros de ingreso y salida del personal.
• Las condiciones estructurales que facilitan el ingreso desde el exterior.</td>
</tr>
<tr>
<td colspan="2">Interpretación:

El análisis realizado evidencia que el riesgo de robo presenta un nivel alto de este, debido a la elevada probabilidad de ocurrencia y al impacto significativo que tendría la pérdida de equipos informáticos en las actividades académicas y administrativas. La ausencia de controles de acceso físico, sistemas de vigilancia, registros de ingreso y procedimientos formales de prevención incrementa la exposición de las salas de docentes a accesos no autorizados.</td>
</tr>
</table>

Incendio



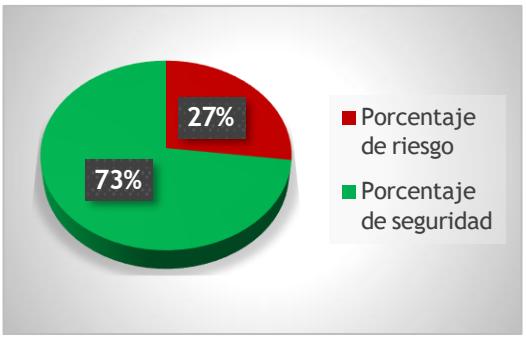
Debido a:

- La ausencia de detectores de humo y extintores funcionales.
- La falta de señalización y carteles informativos ante incendios.
- La inexistencia de responsables designados para la seguridad contra incendios.
- La sala carece de controles que regulen la temperatura de los equipos.
- No se cuenta con botiquines de primeros auxilios disponibles en el área.

Interpretación:

Se identificó que el riesgo de incendio es de un **nivel medio**, debido a la falta de acciones básicas de prevención y respuesta, la inexistencia de detectores de humo, extintores señalizados, rutas de evacuación y de un personal encargado de la seguridad contra incendios eleva la probabilidad de daños los materiales y compromete la seguridad del personal docente.

Daño de equipos.



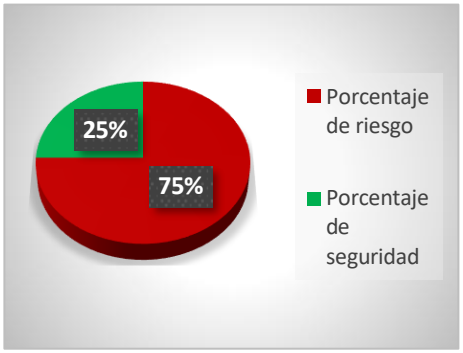
Debido a:

- La falta de un mantenimiento preventivo periódico.
- La ausencia de los protocolos para lo que es manipulación segura de los equipos.
- La falta de las capacitaciones al personal docente.
- La carencia de los manuales de operación.
- La falta de documentación de las fallas y las reparaciones.
- La inexistencia de seguros y políticas de reemplazo de equipos.

Interpretación:

Los resultados nos evidencian que el riesgo de daño en los equipos informáticos es considerablemente alto, esto surge por lo que es la ausencia del mantenimiento preventivo, los protocolos de seguridad en la manipulación y la capacitación al personal docente, dichos problemas afectan la durabilidad de los equipos y pueden ocasionar pérdidas económicas para la institución.

Inundación



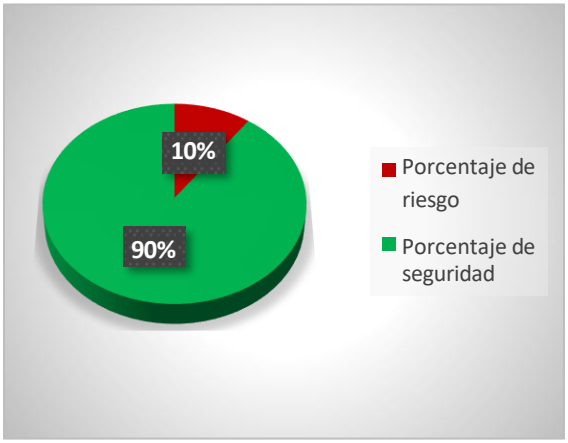
Debido a:

- Con la llegada de las lluvias, el sitio presenta acumulación de agua.
- Las puertas y ventanas no cuentan con un sellado adecuado.
- Los drenajes no están operativos o presentan fallas.
- Se colocan los documentos sobre el piso en lugar de ubicarlos en un sitio adecuado.
- No existe un control o inspección luego de las lluvias.
- No existen precauciones establecidas para enfrentar lluvias fuertes.

Interpretación:

Los resultados señalan que el riesgo de inundación tiene un alto nivel de riesgo, por lo que, a ocasionado daños en la infraestructura física gracias a la ausencia de las medidas preventivas ante eventos climáticos, por ello la acumulación de agua, la falta de drenajes y el almacenamiento inapropiado de materiales.

Malware



Debido a:

- La inexistencia de software antivirus actualizado.
- La falta de análisis periódicos de malware.
- La ausencia de políticas de seguridad informática.
- El uso no controlado de dispositivos externos.
- La inexistencia de copias de seguridad periódicas.
- La falta de un plan de respuesta ante incidentes de seguridad.

Interpretación:

En el siguiente análisis se logra evidenciar que el riesgo de malware presenta un alto nivel de inseguridad, debido a la alta probabilidad de que ocurra ataques maliciosos, ya que no existe un control en el uso de las computadoras, la ausencia de controles lógicos, políticas de seguridad, antivirus actualizado y planes de respuesta lo cual incrementa de manera visible la exposición de los equipos a amenazas informáticas.

5.4 Interpretación objetiva

Gráfico general de seguridad

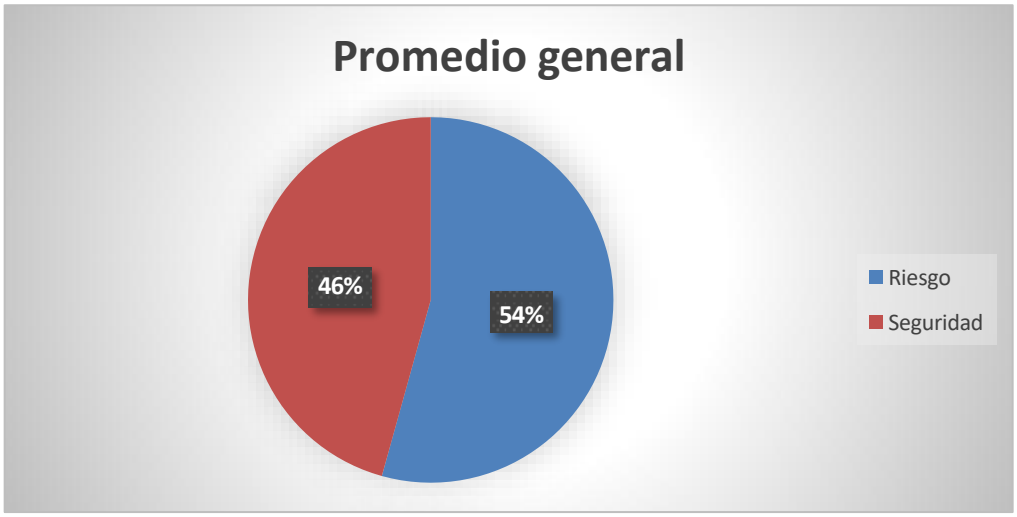


Figura 12 *Gráfico general*

El gráfico evidencia que, de manera general, el nivel de riesgo supera al nivel de seguridad en varias de las áreas evaluadas, lo que refleja debilidades en los controles de seguridad implementados en las salas de docentes. Las amenazas relacionadas con malware, robo e incendio se presentan como las más críticas, debido a la limitada aplicación de controles preventivos y correctivos.

Gráfico general de riesgos

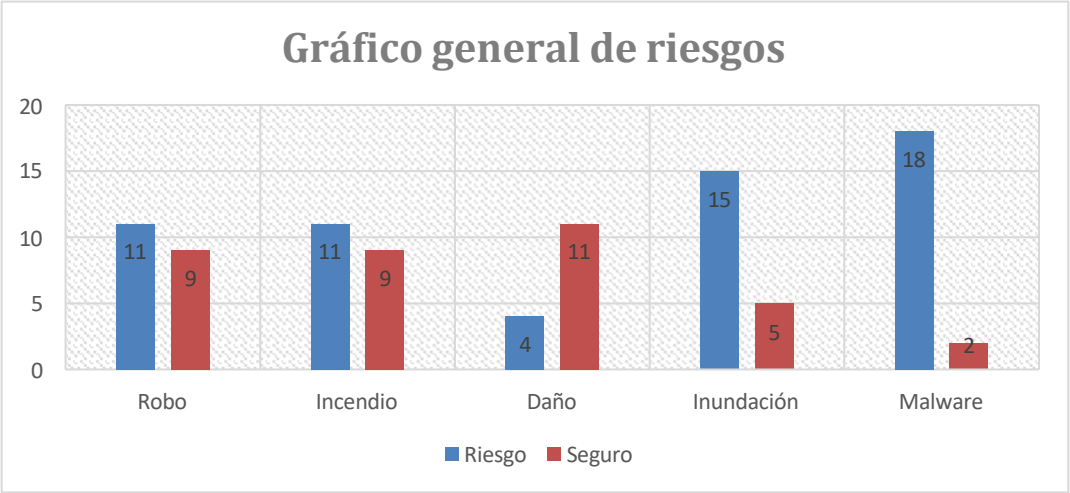


Figura 13 *Grafico de riesgo y seguridad*

El gráfico general de riesgos muestra una comparación entre el nivel de seguridad existente y el nivel de riesgo presente en la seguridad de los equipos informáticos de las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen. Se analizan cinco áreas críticas: robo, incendio, daño de equipos, inundación y malware.

Los resultados evidencian que, en la mayoría de las áreas evaluadas, el nivel de riesgo supera al nivel de seguridad, lo que refleja deficiencias en los controles físicos, lógicos y administrativos actualmente implementados. Los casos más importantes estarán en la amenaza de malware e incendio, donde la protección que ya ha recibido es limitada e ineficaz contra las amenazas identificadas. De manera similar, aunque los riesgos de daño al equipo e inundaciones han mejorado en términos de seguridad, continúan existiendo algunos defectos en los que el equipo informático podría verse potencialmente comprometido. En pocas palabras, el gráfico demuestra una exposición aguda al riesgo que justifica la necesidad de aumentar la seguridad informática mediante la aplicación de controles adecuados, políticas institucionales y acciones preventivas que minimicen las exposiciones identificadas en las salas de profesores.

5.5 Opinión de la Auditoría

Como resultado del proceso de auditoría realizado bajo los lineamientos de la norma ISO/IEC 27001 y la metodología MAGERIT, se concluye que la institución presenta debilidades significativas en la gestión de la seguridad de la información y en la administración de sus activos tecnológicos.

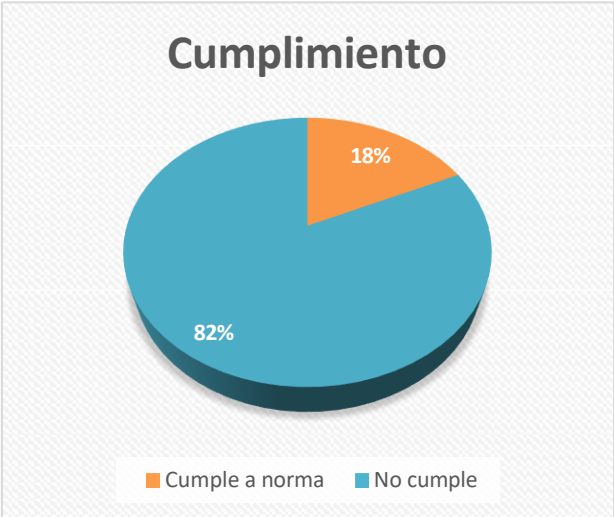


Figura 14 *Nivel de seguridad*

El bajo porcentaje de cumplimiento refleja la inexistencia de un Sistema de Gestión de Seguridad de la Información formalmente implementado. Asimismo, los riesgos identificados muestran una exposición considerable ante amenazas tanto tecnológicas como ambientales, que podrían afectar la disponibilidad, integridad y confidencialidad de la información institucional.

En consecuencia, el nivel general de madurez en materia de seguridad informática puede considerarse básico, requiriendo la implementación urgente de políticas formales, documentación estructurada, controles preventivos y un proceso continuo de gestión de riesgos alineado con estándares internacionales.

Tabla 29 *Riesgos identificados y nivel en ISO*

Nº	Riesgo Identificado	Activo Afectado	Nivel de Riesgo
1	Acceso no autorizado a equipos informáticos	Equipos tecnológicos	Alto
2	Pérdida de información por fallas eléctricas	Servidores y computadoras	Alto
3	Infección por malware	Sistemas informáticos	Medio
4	Uso indebido de credenciales	Cuentas de usuario	Alto
5	Ausencia de registro de incidentes	Información institucional	Medio
6	Ingreso físico no controlado a laboratorios	Infraestructura física	Alto

5.6 Recomendaciones de la Auditoría

Con base en los hallazgos identificados, se recomienda la implementación de un Manual de Buenas Prácticas en Seguridad Informática, detallado en el Anexo B, el cual establece lineamientos claros para el uso adecuado de los equipos informáticos, la gestión de respaldos, el manejo de dispositivos externos, la prevención de malware y la respuesta ante incidentes. Asimismo, se sugiere formalizar políticas de seguridad documentadas, establecer registros de mantenimiento y fallas técnicas, fortalecer los controles físicos en áreas vulnerables a humedad o inundaciones, y desarrollar programas de capacitación periódica dirigidos al personal docente. La aplicación de estas recomendaciones permitirá reducir los niveles de riesgo identificados y mejorar progresivamente el nivel de cumplimiento de los controles establecidos en la norma ISO/IEC 27001.

CAPÍTULO VI:

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

La auditoría de seguridad informática realizada mediante la aplicación de la metodología MAGERIT, junto con el uso de encuestas y entrevistas dirigidas al personal docente y al responsable de los equipos informáticos, permitió obtener un diagnóstico claro y detallado sobre el estado de la seguridad física y lógica de los equipos institucionales asignados a la sala de docentes, los resultados evidenciaron la existencia de debilidades bastante significativas que afectan a la protección de los activos tecnológicos y la continuidad de las actividades académicas y administrativas.

Este análisis permitió la identificación de los riesgos críticos relacionados con el robo de información, la presencia de malware y la posibilidad de incendios, los cuales representan una amenaza directa, asimismo, se detectaron riesgos de nivel medio asociados al daño de equipos y a eventos de inundación, los cuales, aunque presentan menor probabilidad, pueden generar impactos relevantes en la operatividad y en los costos de reposición de los activos tecnológicos.

Los resultados demuestran que gran parte de los riesgos identificados no solo provienen de factores externos, sino también de la ausencia de controles adecuados, la falta de procedimientos formales, el uso inadecuado de los equipos y la escasa capacitación del personal en temas de seguridad informática, esto resalta la importancia de establecer una cultura de seguridad dentro de la institución y medidas preventivas más robustas. Por último, el desarrollo de una propuesta para un manual de mejores prácticas (Anexo B), respaldado por las directrices de la metodología MAGERIT, proporciona una herramienta fundamental para la mejora continua de la seguridad de la información. Una implementación efectiva de esto dará

a la institución una guía estructurada para la gestión de riesgos, la asignación de responsabilidades, la priorización de acciones correctivas y el fortalecimiento de la protección del equipo informático institucional.

6.2 Recomendaciones

- Implementar el Manual de Buenas Prácticas de Seguridad Informática propuesto, orientado al uso adecuado de los equipos informáticos asignados a los docentes, con el fin de cumplir el objetivo de fortalecer la seguridad física y lógica de los activos institucionales y reducir los riesgos identificados durante la auditoría.
- Implementar un proceso formal para poder controlar el acceso físico a la sala de docentes, siguiendo lo señalado en el manual, donde se le apliquen métodos de identificación del personal autorizado, los registros de entrada y salida, y los límites de acceso fuera del horario laboral, con el fin de poder reducir riesgos de robo y de ingresos no permitidos.
- Implementar lo que es un sistema de inventario institucional y de etiquetado para los equipos informáticos, siguiendo lo que se describe en el manual de buenas prácticas, con el fin de poder optimizar la gestión de los activos, permitir un mejor control del estado de los equipos y ayudar a identificar rápidamente pérdidas o posibles sustracciones.
- Designar a un encargado que supervise y controle los equipos informáticos de la sala de docentes, revisando que se cumplan los procedimientos, coordinando el mantenimiento, registrando incidentes y asegurando la correcta aplicación de las políticas descritas en el manual.
- Reforzar la seguridad lógica de los equipos siguiendo lo indicado en el manual, usando lo que son el antivirus actualizado, las contraseñas seguras, las copias de seguridad

periódicas y controlando la instalación de software, para reducir riesgos de malware y pérdida de información.

7 BIBLIOGRAFÍA

Alles, M. (2021). *Data analytics in auditing. Journal of Emerging Technologies in Accounting.*

Arantes, S. C. (2023). *Auditoría de Seguridad Informática: Curso Práctico.* Colombia: Ediciones de la U (Colombia) / Ra-Ma Editorial (España).

Arias, F. G. (2021). *l proyecto de investigación: Introducción a la metodología científica (7.ª ed.).* Episteme.

ÁVILA CEVALLOS, A. A. (2019). *AUDITORÍA INFORMÁTICA DE SEGURIDAD LÓGICA PARA INFORMACIÓN DE DOCENTES "UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ" INGENIERA EN SISTEMAS.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/2071

Bernal, C. (2020). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales (4ª ed.).* Pearson.

Botha, J., & Solms, R. (2020). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Calazacón Aguavil, G. L. (2021). *La seguridad informática en sistemas de gestión académica y educativa de las unidades educativas fiscales del cantón Santo Domingo.*

CCN-CERT, C. (2019). *MAGERIT versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información.* Espana: Gobierno de Espana.

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

CISCO. (2023). *Cisco Cybersecurity Threat Trends Report. Cisco Systems.*

Demera Zambrano, A. L. (2023). *Auditoría informática para prevención de ataques informáticos aplicado a los docentes de la Universidad "Laica Eloy Alfaro de Manabí" extensión el Carmen.* Obtenido de https://repositorio.uleam.edu.ec/handle/123456789/4593?

EAE. (18 de 09 de 2023). *Business School Madrid*. Obtenido de EAE Madrid: https://www.eaemadrid.com/es/blog/perfil-funciones-competencias-auditor

ENISA. (2021). *Cybersecurity risk management framework.*

ENISA. (2021). *ENISA Threat Landscape Report 2021.* European Union.: European Union Agency for Cybersecurity.

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

Hall, J. A. (2021). *Information Technology Auditing and Assurance (5th ed.).* Cengage Learning.

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

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., Torre, J. D., & Jesús, J. (2020). *Análisis de las principales dificultades en la auditoría informática.* Argentina: Risti.

Institute of Internal Auditors. (2023). *International Professional Practices Framework (IPPF).*

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

ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.* International Organization for Standardization.

Labadze, I., Grigolia, R., & Machaidze, G. (2019). *Gestión de la seguridad informática en entornos educativos.* Academic Press.

Linder, D. Z. (2023). *Auditoría informática para prevención de ataques informáticos aplicado a los docentes de la universidad "Laica Eloy Alfaro de Manabí" extensión el carmen.* Obtenido de https://es.scribd.com/document/683819785/Uleam-Infor-0117

Madrid Parra, A., & Guillén, E. (2019). *Servicios de autenticación y autorización orientados a internet de las cosas.* Bogotá: Telemática, 17(2), 42–51.

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2022). *Metodología de la investigación cuantitativa, cualitativa y redacción de tesis.Ediciones de la U.*

Otero, A. (2021). *Information Technology Control and Audit.* CRC Press.

Peltier, T. (2020). *Information Security Policies, Procedures, and Standards. Auerbach Publications.*

Ponce Ordóñez, J. A., & Samaniego Mena, E. A. (2021). *Fundamentos de seguridad informática.* Guayaquil-Ecuador: Grupo Compás.

Pozo Hernandéz, C. G., Reascos Pinchao, R. S., & Minaya Macías, R. W. (2025). *Fundamentos de seguridad informática y ciberseguridad.* El Carmen, Manabí, Ecuador: GESICAP. 77 pp. .

Ramírez Coello, N. B. (2023). *Auditoría informática en la seguridad de la información según la ISO 27001 en empresas comerciales de El Carmen.*

Raya, A. A. (2019). *Fundamentos de seguridad informática.* Barcelona: FUOC.

Raya, Amadeus, & Albus. (2019). *Seguridad y auditoría de la información.* Barcelona: FUOC.

Reyes, A. (2023). *Estrategias de IA aplicada a la auditoria informática.* Buenos Aires,Argentina: Technology Rain Journal.

Ridder H, G. (2019). *The theory contribution of case study research designs.* Business Research, 12(2), 281–305.

Stallings, S., & Brown, L. (2021). *Information Technology Control and Audit.* CRC Press.

Stallings, W. (2021). *FUNDAMENTOS DE SEGURIDAD EN REDES.* Madrid: PEARSON.

URUGUAY, U. D. (2020). *ELABORACIÓN Y PRESENTACIÓN DE TRABAJOS ACADÉMICOS.* Montevideo : Creative Commons Atribución-No Comercial-Compartir Igual 4.0 Unported.

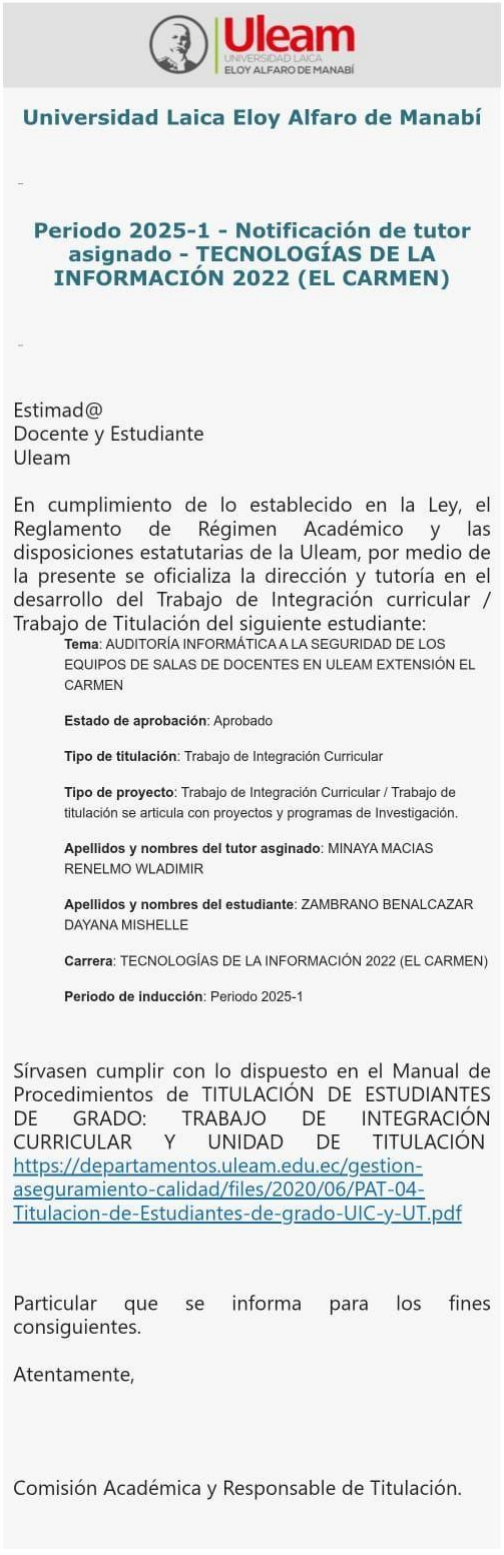
Vega Briceño , E. (2021). *SEGURIDAD DE LA INFORMACIÓN.* Zamora: Editorial Área de Innovación y Desarrollo,S.L.

Von Solms, R., & Van Niekerk, J. (2019). *From information security to cybersecurity.* Computers & Security, 38, 97–102.

Whitman, M., & Mattord, H. (2021). *Principles of Information Security.* Cengage Learning.

8 ANEXOS

Anexo A *Aprobación de tema*



Universidad Laica Eloy Alfaro de Manabí

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: AUDITORÍA INFORMÁTICA A LA SEGURIDAD DE LOS EQUIPOS DE SALAS DE DOCENTES EN 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: ZAMBRANO BENALCAZAR DAYANA MISHELLE

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

Particular que se informa para los fines consiguientes.

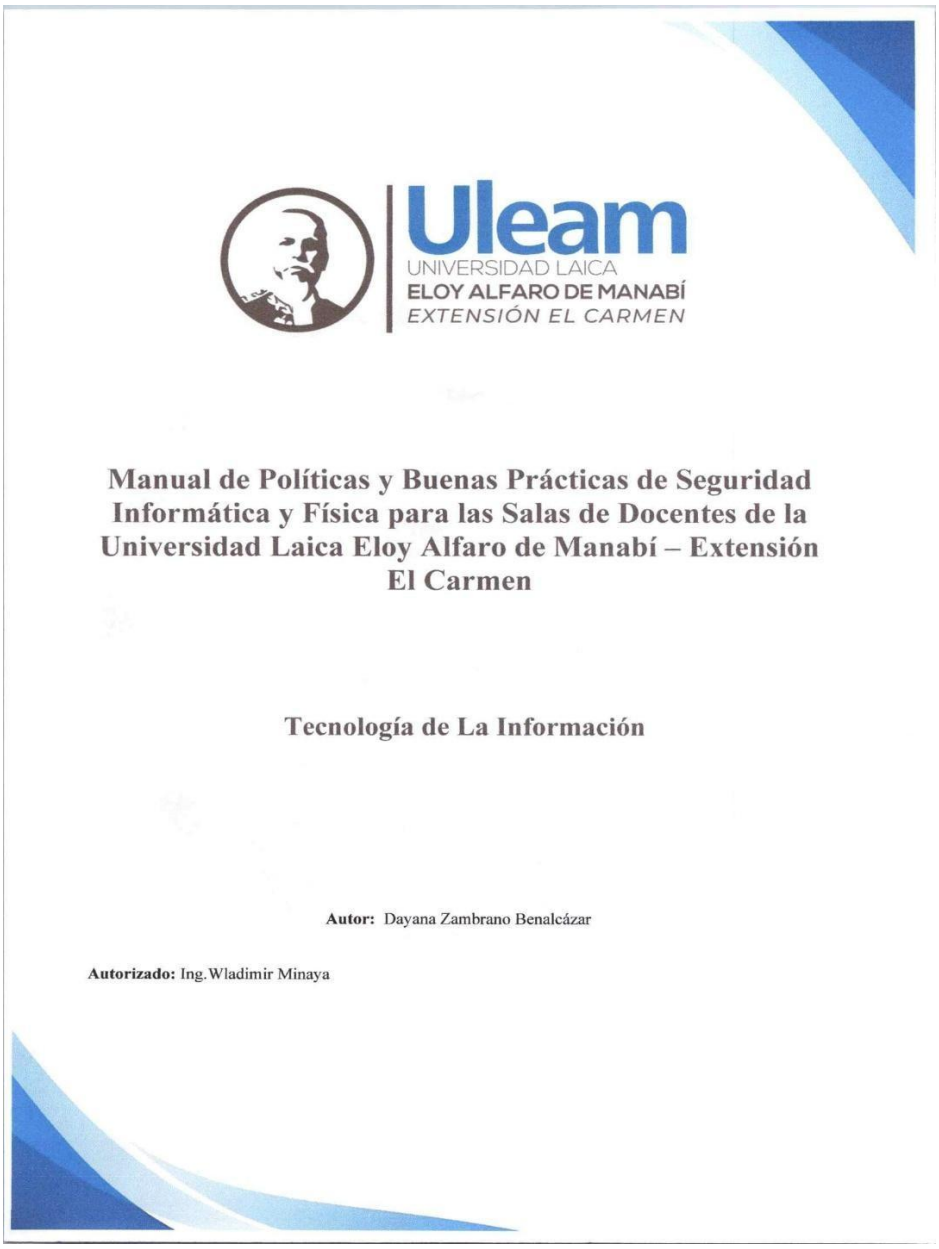
Atentamente,

Comisión Académica y Responsable de Titulación.

Figura 15 *Aprobación de tema*

Anexo B Manual

Figura 16 *Manual*



Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ
EXTENSIÓN EL CARMEN

Manual de Políticas y Buenas Prácticas de Seguridad Informática y Física para las Salas de Docentes de la Universidad Laica Eloy Alfaro de Manabí – Extensión El Carmen

Tecnología de La Información

Autor: Dayana Zambrano Benalcázar

Autorizado: Ing. Wladimir Minaya

INDICE

1. Introducción

El presente manual surge como resultado del proceso de auditoría informática aplicado en las salas de docentes de la Universidad Laica Eloy Alfaro de Manabí, Extensión El Carmen. Su finalidad es establecer políticas y buenas prácticas orientadas a prevenir riesgos físicos y lógicos que puedan afectar la seguridad de los equipos informáticos, la información institucional y la continuidad de las actividades académicas.

2. Objetivos

2.1. Objetivo general

Establecer políticas y buenas prácticas que permitan fortalecer la seguridad física y lógica de las salas de docentes, minimizando riesgos como robos, incendios, inundaciones, daños de equipos y malware.

2.2. *Objetivos específicos*

- Regular el acceso a las salas de docentes
- Prevenir incidentes de robo y daño de equipos
- Establecer medidas de protección ante desastres naturales
- Promover el uso seguro de los equipos informáticos
- Fortalecer la cultura de seguridad institucional

3. Alcance

Este manual aplica a todas las salas de docentes de la ULEAM Extensión El Carmen y está dirigido a docentes, personal técnico y autoridades que tengan acceso o responsabilidad sobre los equipos informáticos institucionales.

4. Definición

En este proceso sistemático de evaluación que permitirá analizar la seguridad, el control y el uso adecuado de los recursos tecnológicos, con el objetivo de identificar riesgos, vulnerabilidades y proponer mejoras.

Seguridad informática: Conjunto de medidas técnicas, físicas y administrativas destinadas a proteger los equipos informáticos, la información y los servicios, garantizando su confidencialidad, integridad y disponibilidad.

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 cause un impacto negativo sobre los activos informáticos, afectando la continuidad de las actividades institucionales.

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

5. Responsables

- Autoridades institucionales
- *Personal técnico*
- Docentes usuarios de los equipos

5.1. Responsabilidad del usuario

Compromiso del personal docente y técnico de utilizar los equipos informáticos de forma adecuada, cumpliendo las normas y reportando cualquier incidente.

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

Mantenimiento preventivo: Conjunto de actividades planificadas destinadas a conservar los equipos informáticos en condiciones óptimas de funcionamiento y prevenir fallas técnicas.

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

6. Políticas de seguridad

6.1. Políticas de Control de Acceso Físico

- Acceso solo a personal autorizado
- Mantener puertas cerradas
- Registro de ingreso cuando sea necesario

6.2. Política de Prevención de Robos

- Inventario actualizado de equipos
- Identificación de equipos como propiedad institucional
- Reporte inmediato de pérdidas

6.3. Política de Prevención de Incendios

- Uso correcto de tomacorrientes
- Prohibición de materiales inflamables
- Señalización básica y extintores

6.4. Política de Prevención de Inundaciones

- Protección de equipos ante lluvias
- Elevación de equipos cuando sea posible
- Revisión de filtraciones

6.5. Política de Prevención contra Malware

- Uso obligatorio de antivirus
- Prohibición de software no autorizado
- Uso responsable de USB y correos electrónicos

6.6. Política de Responsabilidad del Usuario

- Cuidado del equipo asignado
- Uso solo para fines institucionales
- Reporte de incidentes

7. Controles para prevenir riesgos

Riesgo	Descripción	Medidas de prevención
Robo	Pérdida de equipos por acceso no autorizado	Control de acceso, inventarios, vigilancia
Daño de equipos	Fallas por mal uso o falta de mantenimiento	Mantenimiento preventivo, capacitación
Incendio	Daños por cortocircuitos	Revisión eléctrica, extintores
Inundación	Daños por filtraciones de agua	Drenajes, revisión de techos
Malware	Infección por software malicioso	Antivirus, políticas de uso

8. Mecanismos de seguimiento

Con el fin de garantizar la efectividad de las políticas de seguridad y buenas prácticas propuestas para las salas de docentes, se establecen los siguientes mecanismos de seguimiento, indicando su periodicidad correspondiente:

Evaluación del cumplimiento de las políticas de uso: Se desarrollará **semestralmente**, mediante observaciones, encuestas y entrevistas al personal docente y técnico.

Registro y análisis de incidentes de seguridad: Se efectuará **de forma continua**, documentando cualquier evento relacionado con robos, daños, malware, incendios o inundaciones.

Capacitación y sensibilización al personal docente: Se programará **anualmente**, reforzando las buenas prácticas y el uso seguro de los recursos tecnológicos.

Revisión general del plan de seguridad y buenas prácticas: Se realizará **una vez al año**, ajustando las medidas según los resultados obtenidos en las evaluaciones y auditorías internas.

Anexo C Cuestionarios para identificar riesgos y requisitos

Figura 17 *Cuestionarios*

CUESTIONARIO PARA IDENTIFICAR RIESGO				C2 Pág. 1 de 5	
ROBO					
Preguntas		Respuestas		Observación	Riesgo
		Si	No		
1	¿La sala de docentes cuenta con un control de acceso físico que limite el ingreso únicamente a personal autorizado?		X		0
2	¿Las puertas de acceso a la sala de docentes permanecen cerradas cuando no se encuentran en uso?	X			1
3	¿Las cerraduras de las puertas de la sala de docentes se encuentran en buen estado y funcionamiento?		X		0
4	¿Las ventanas de la sala de docentes cuentan con sistemas de seguridad que impidan el acceso desde el exterior?		X		0
5	¿Existe un responsable designado para el control de llaves de la sala de docentes?		X		0
6	¿Se controla el acceso de personas externas a la sala de docentes?		X		0
7	¿La sala de docentes cuenta con algún sistema de vigilancia (cámaras, guardias u otro medio)?		X		0
8	¿Los sistemas de vigilancia, en caso de existir, se encuentran operativos?		X	No tienen	0
9	¿Se restringe el acceso a la sala de docentes fuera del horario laboral?	X			1
10	¿Existe un registro de ingreso y salida del personal que accede a la sala de docentes?		X		0
11	¿Se cuenta con un inventario actualizado de los equipos informáticos ubicados en la sala de docentes?		X		0
12	¿Los equipos informáticos se encuentran correctamente identificados como propiedad institucional?	X			1
13	¿Se controla la salida de equipos informáticos de la sala de docentes?		X		0
14	¿Se han reportado intentos de robo o pérdida de equipos informáticos en la sala de docentes?	X			1
15	¿Existen procedimientos definidos ante la pérdida o robo de equipos informáticos?	X			1
16	¿El personal docente conoce las normas institucionales relacionadas con la prevención de robos?		X	Minimamente	0
17	¿Se realizan inspecciones periódicas para verificar la presencia de todos los equipos informáticos?		X		0
18	¿La ubicación de la sala de docentes facilita el control y vigilancia del área?		X		0
19	¿La sala de docentes cuenta con iluminación adecuada para prevenir actos delictivos?	X			1
20	¿Se considera que los controles actuales son suficientes para prevenir el robo de equipos informáticos?		X		0
Realizado Por: Zambrano Benalcázar Dayana Mishelle				**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo	
Fecha:				**Firma:**	

CUESTIONARIO PARA IDENTIFICAR IDENTIFICACIÓN DE INCENDIO				C2 Pág. 2 de 5	
INCENDIO					
	Preguntas	Respuestas		Observación	Riesgo
		Si	No		
1	¿La sala de docentes cuenta con detectores de humo?		X	No hay	2
2	¿Existen extintores en lugares visibles y accesibles?		X	No hay	2
3	¿Los extintores se encuentran vigentes y señalizados?		X		1
4	¿Hay señalización visible de rutas de evacuación?		X		0
5	¿Existen carteles con instrucciones ante incendios?		X		1
6	¿Los tomacorrientes se encuentran sobrecargados?		X		0
7	¿Los cables eléctricos presentan cortes o deterioro?	X			1
8	¿Los cables eléctricos están protegidos adecuadamente?		X		0
9	¿Se almacenan objetos inflamables junto a equipos informáticos?		X		0
10	¿Las cortinas y muebles son de material resistente al fuego?		X		1
11	¿La sala cuenta con iluminación de emergencia funcional?	X			1
12	¿El tablero eléctrico dispone de protecciones?		X		0
13	¿Se observan filtraciones de agua cerca de instalaciones eléctricas?	X			0
14	¿Las paredes presentan humedad cerca de enchufes o cableado?	X			1
15	¿Los cables eléctricos y de red están ordenados y diferenciados?	X			1
16	¿La estructura del techo evita filtraciones sobre los equipos?		X		0
17	¿Los pasillos y puertas se encuentran libres de obstáculos?	X			0
18	¿Existe personal responsable de seguridad contra incendios?		X		0
19	¿Se revisa periódicamente la temperatura de los equipos?		X		0
20	¿Se dispone de un botiquín de primeros auxilios?		X		0
Realizado Por: Zambrano Benalcázar Dayana Mishelle		**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo			
Fecha:		**Firma:**			

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		1
2	¿Existen protocolos para manipulación segura de equipos?	X			1
3	¿El personal docente recibe capacitación sobre el uso adecuado de los equipos?		X		1
4	¿La institución cuenta con manuales de operación de los equipos informáticos?		X		1
5	¿Se controla la temperatura del área donde se ubican los equipos?	X			0
6	¿Se controla la humedad en la sala de docentes?		X		0
7	¿Se revisa periódicamente el estado físico de los equipos?		X		1
8	¿Se documentan las fallas técnicas y reparaciones realizadas?		X		1
9	¿La institución cuenta con seguro para los equipos informáticos?	X			1
10	¿Existen políticas para el reemplazo de equipos dañados?	X			1
11	¿Se controla el acceso a equipos considerados críticos o delicados?		X		0
12	¿Se evita el uso indebido o no autorizado de los equipos?		X		1
13	¿Existen protocolos para la desconexión segura de los equipos?	X			1
14	¿Se inspeccionan periódicamente los cables eléctricos y de red?		X		0
15	¿Los cables y conexiones se encuentran en buen estado?		X		1
Realizado Por: Zambrano Benalcázar Dayana Mishelle		**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo			
Fecha:		**Firma:**			

CUESTIONARIO PARA IDENTIFICAR DE INUNDACIÓN				C2 Pág. 4 de 5	
INUNDACIÓN					
Preguntas		Respuestas		Observación	Riesgo
		Si	No		
1	¿La sala de docentes se encuentra ubicada en una zona con bajo riesgo de inundación?	X			1
2	¿El piso de la sala de docentes presenta acumulación de agua durante la temporada de lluvias?	X			1
3	¿Las puertas de la sala de docentes sellan correctamente al momento de cerrarse?		X		1
4	¿Existen sistemas de drenaje funcionales alrededor del edificio?		X		1
5	¿El techo de la sala de docentes presenta filtraciones o signos de humedad?	X			1
6	¿Las ventanas de la sala de docentes cierran de forma hermética?		X		1
7	¿Los equipos informáticos se encuentran ubicados sobre superficies elevadas?	X			1
8	¿Se observan rastros de humedad en paredes o esquinas del área?	X			1
9	¿Los cables eléctricos y de red se encuentran protegidos del contacto con el piso?		X		1
10	¿La sala de docentes cuenta con protección externa frente al ingreso de agua?		X		1
11	¿La estructura del techo se encuentra en buen estado?		X		1
12	¿Los documentos y materiales se almacenan fuera del nivel del piso?	X			2
13	¿El área dispone de espacios despejados para la evacuación del agua?		X		1
14	¿Las canaletas y canalones se mantienen libres de obstrucciones?		X		1
15	¿Las canaletas del techo funcionan adecuadamente?		X		1
16	¿Los interruptores eléctricos están ubicados por encima del nivel del piso?	X			2
17	¿El entorno del edificio permite un drenaje natural del agua?		X		1
18	¿Se aplican medidas preventivas durante lluvias intensas?		X		1
19	¿Existen obstáculos que impidan la evacuación del agua?		X		1
20	¿Las instalaciones se revisan después de eventos de lluvia?		X		1
Realizado Por: Zambrano Benalcázar Dayana Mishelle		**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo			
Fecha:		**Firma:** 			

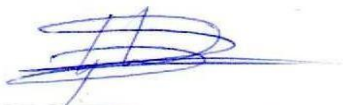
CUESTIONARIO PARA IDENTIFICAR DE INUNDACIÓN				C2 Pág. 4 de 5	
INUNDACIÓN					
Preguntas		Respuestas		Observación	Riesgo
		Si	No		
1	¿La sala de docentes se encuentra ubicada en una zona con bajo riesgo de inundación?	X			1
2	¿El piso de la sala de docentes presenta acumulación de agua durante la temporada de lluvias?	X			1
3	¿Las puertas de la sala de docentes sellan correctamente al momento de cerrarse?		X		1
4	¿Existen sistemas de drenaje funcionales alrededor del edificio?		X		1
5	¿El techo de la sala de docentes presenta filtraciones o signos de humedad?	X			1
6	¿Las ventanas de la sala de docentes cierran de forma hermética?		X		1
7	¿Los equipos informáticos se encuentran ubicados sobre superficies elevadas?	X			1
8	¿Se observan rastros de humedad en paredes o esquinas del área?	X			1
9	¿Los cables eléctricos y de red se encuentran protegidos del contacto con el piso?		X		1
10	¿La sala de docentes cuenta con protección externa frente al ingreso de agua?		X		1
11	¿La estructura del techo se encuentra en buen estado?		X		1
12	¿Los documentos y materiales se almacenan fuera del nivel del piso?	X			2
13	¿El área dispone de espacios despejados para la evacuación del agua?		X		1
14	¿Las canaletas y canalones se mantienen libres de obstrucciones?		X		1
15	¿Las canaletas del techo funcionan adecuadamente?		X		1
16	¿Los interruptores eléctricos están ubicados por encima del nivel del piso?	X			2
17	¿El entorno del edificio permite un drenaje natural del agua?		X		1
18	¿Se aplican medidas preventivas durante lluvias intensas?		X		1
19	¿Existen obstáculos que impidan la evacuación del agua?		X		1
20	¿Las instalaciones se revisan después de eventos de lluvia?		X		1
Realizado Por: Zambrano Benalcázar Dayana Mishelle			**Revisado Por:** Ing. Minaya Macias Wladimir Renelmo		
Fecha:			**Firma:**		

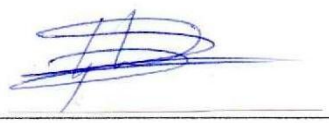
o

Figura 18 *Cuestionario de requisitos*

Cuestionario para cumplimiento de requisitos Según normas ISO			C1 Pag 1 de 5
REQUISITOS	PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
4.1Comprensión de la Organización y su Contexto	1. ¿Existen objetivos definidos para el sistema de seguridad informática relacionados con el control de accesos físico y lógico?	0	
	2 ¿Se e ha revisado cómo están por dentro las instalaciones, para ver si todo eso influye en el control de accesos?	0	
	3 ¿Se han identificado problemas externos, como personas que ingresan sin permiso?	1	
	4. ¿Se dispone de un análisis previo de vulnerabilidades para determinar riesgos asociados a los accesos?	2	
4.4 Gestión del Control de Accesos	1. ¿Existe una política institucional vigente para el control de accesos?	0	
	4. ¿Existen medidas de autenticación adicional (MFA) para equipos o áreas críticas?	2	
	5. ¿Se implementan controles físicos como cerraduras, cámaras o tarjetas electrónicas?	0	
	6. ¿Se registra el ingreso y salida del personal a los centros de cómputo?	0	
	7. ¿Se revisan periódicamente los permisos y perfiles de acceso?	0	
Elaborado por: Zambrano Benalcázar Dayana Mishelle		**Revisado por:** Ing. Minaya Macias Renelmo Wladimir	
Fecha:		**Firma:**	

Cuestionario para cumplimiento de requisitos				C1 Pag 2 de 5
	REQUISITOS	PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
	5.1 Control de Acceso Lógico	1. ¿Los equipos cuentan con autenticación obligatoria mediante usuario y contraseña?	1	
		2. ¿Se establecen reglas para la complejidad, longitud y caducidad de contraseñas?	0	
		3. ¿Existe un registro de todos los usuarios con acceso a los equipos institucionales?	0	
		4. ¿Se eliminan oportunamente los accesos de usuarios inactivos o desvinculados?	2	
		5. ¿Se restringe el acceso administrativo únicamente al personal autorizado?	0	
		6. ¿Se monitorean intentos fallidos de acceso?	2	

Elaborado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma:** 

Cuestionario para cumplimiento de requisitos			C1 Pag 3 de 5	
REQUISITOS			PREGUNTAS	REQUISITOS
	5.2 Control de Acceso Físico	1. ¿Las salas de cómputo y oficinas cuentan con cerraduras seguras y funcionamiento adecuado?	0	
		2. ¿Se dispone de cámaras o sistemas de vigilancia en áreas donde existen equipos críticos?	0	
		3. ¿Las ventanas, puertas y accesos secundarios presentan condiciones de seguridad apropiadas?	0	
		4. ¿Se dispone actualmente de un listado actualizado de las llaves, tarjetas de acceso y permisos físicos que se utilizan en la institución?	0	
	5.3 Gestión de Usuarios	1. ¿Se ha establecido algún proceso para registrar por primera vez a los usuarios que acceden al sistema?	2	
		2. ¿Se verifica la identidad del usuario antes de otorgar accesos?	1	
		3. ¿Se realiza revisión periódica de roles y privilegios asignados a cada usuario?	0	
		4. ¿Se documentan solicitudes de modificación o eliminación de usuarios?	0	
		5. ¿Los usuarios reciben capacitación sob políticas de acceso y uso de equipos?	0	
Elaborado por: Zambrano Benalcázar Dayana Mishelle			**Revisado por:** Ing. Minaya Macías Renelmo Wladimir	
Fecha:			**Firma:** 	

Cuestionario para cumplimiento de controles				CI Pag 4 de 5
	REQUISITOS	PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
	6.2 Gestión de Riesgos	1. ¿Se ha realizado un análisis de riesgos específico para control de accesos?	0	
		2. ¿Se han detectado situaciones como robos, uso indebido de los equipos, ingresos sin autorización o pérdida de información?	1	
		3. ¿Se revisan aspectos como el uso de contraseñas poco seguras, permisos mal otorgados o problemas en la seguridad física del área?	0	
		4. ¿Los riesgos se clasifican por probabilidad e impacto?	0	
		5. ¿Se han definido medidas preventivas y correctivas ante los riesgos identificados?	0	
	6.3 Medidas de Protección y Monitoreo	1. ¿Se realizan copias de seguridad de información institucional?	0	
		2. ¿Se aplican actualizaciones de software y parches de seguridad de forma regular?	0	
		3. ¿Existe monitoreo continuo del uso de los equipos y accesos?	0	
		5. ¿Se aplican controles para evitar que usuarios no autorizados conecten dispositivos externos?	0	
		6. ¿Se cuenta con antivirus, firewall u otras herramientas de protección activas?	1	

Elaborado por: Zambrano Benalcázar Dayana Mishelle	**Revisado por:** Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma**

Cuestionario para cumplimiento de controles				C1 Pag 5 de 5
REQUISITOS		PREGUNTAS	CUMPLIMIENTO	OBSERVACIÓN
		1. ¿Existe un procedimiento documentado para reportar incidentes de acceso no autorizado?	1	
		2. ¿El personal conoce los canales para reportar incidentes?	0	
		3. ¿Se lleva un registro de incidentes relacionados con accesos indebidos o intentos de intrusión?	0	
		4. ¿Se analizan las causas de los incidentes para evitar recurrencia?	0	

Elaborado por:	**Revisado por:**
Zambrano Benalcázar Dayana Mishelle	Ing. Minaya Macias Renelmo Wladimir
Fecha:	**Firma:**

Anexo D Fotografías

Figura 19

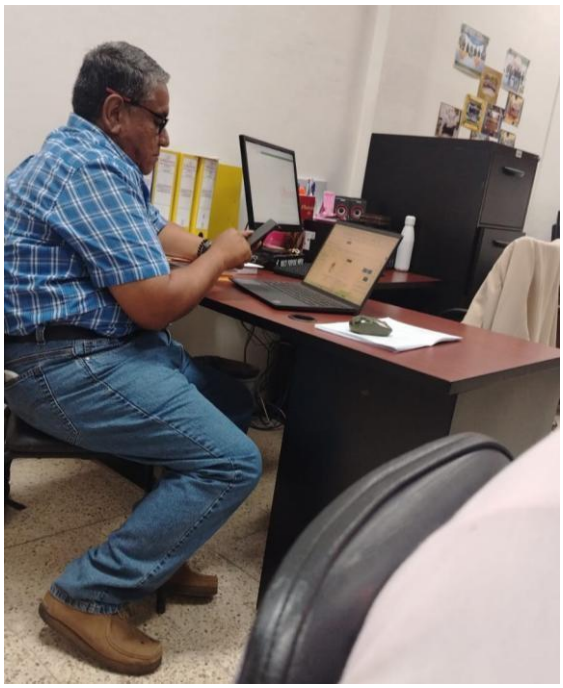


Figura 20

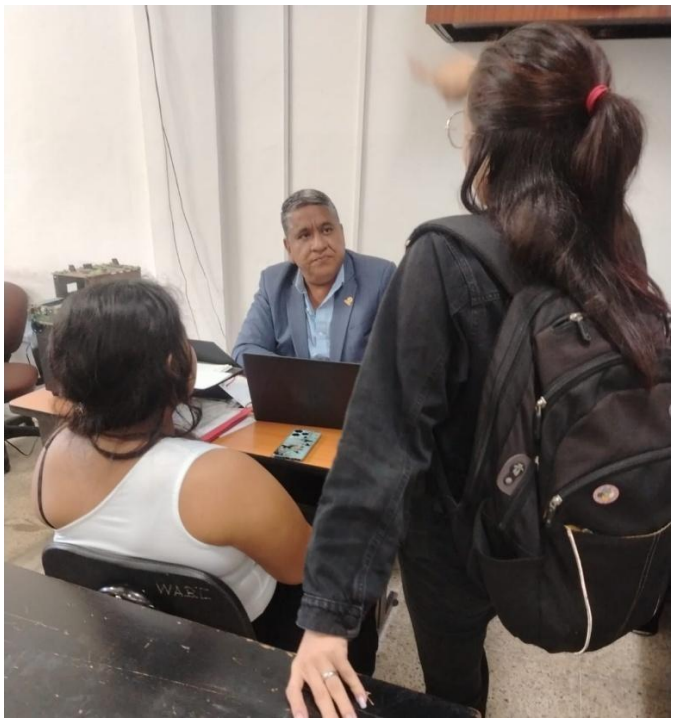
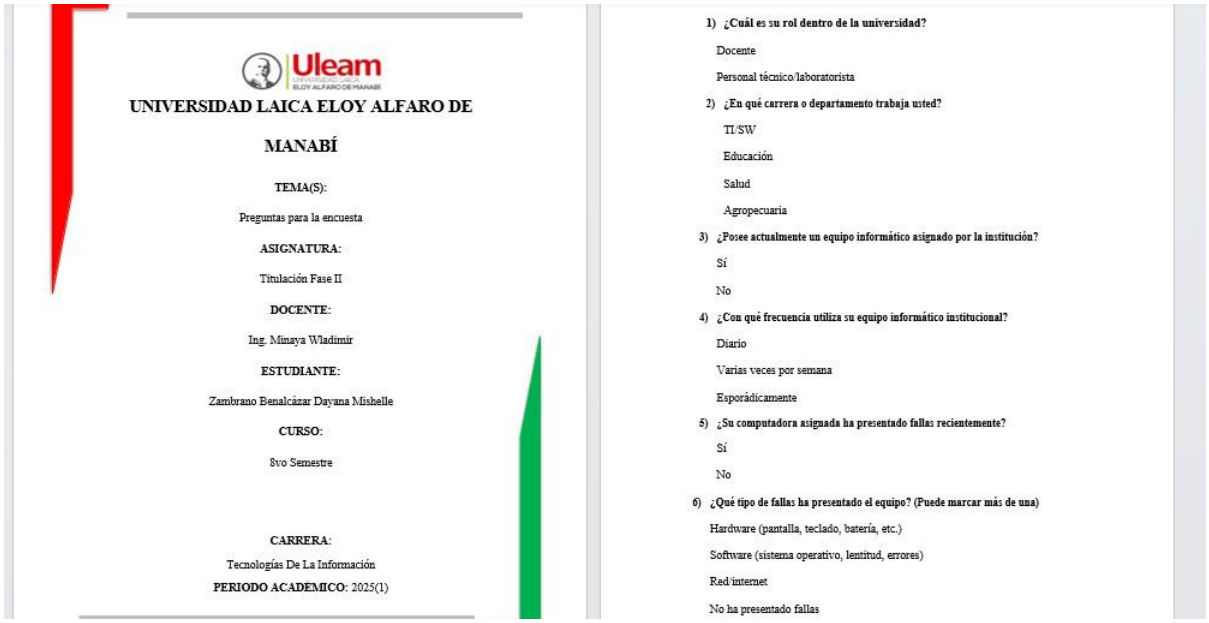


Figura 21

Anexo E Elaboración de encuestas

Figura 22



UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

TEMA(S):

Preguntas para la encuesta

ASIGNATURA:

Titulación Fase II

DOCENTE:

Ing. Minaya Wladimir

ESTUDIANTE:

Zambrano Benalcázar Dayana Mishelle

CURSO:

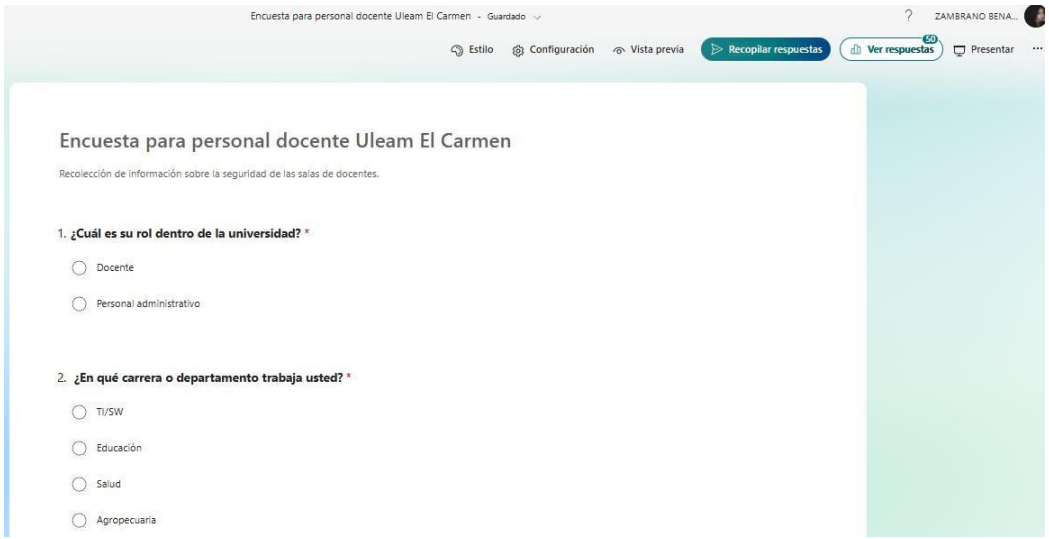
8vo Semestre

CARRERA:

Tecnologías De La Información

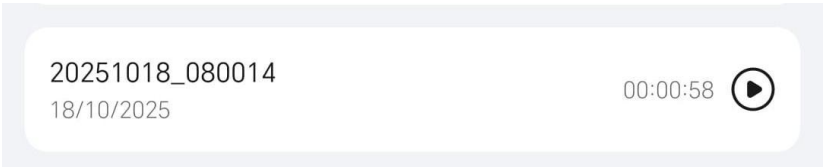
PERIODO ACADEMICO: 2025(1)

1) **¿Cuál es su rol dentro de la universidad?**
   - Docente
   - Personal técnico/laboratorista
2) **¿En qué carrera o departamento trabaja usted?**
   - TI/SW
   - Educación
   - Salud
   - Agropecuaria
3) **¿Posee actualmente un equipo informático asignado por la institución?**
   - Sí
   - No
4) **¿Con qué frecuencia utiliza su equipo informático institucional?**
   - Diario
   - Varias veces por semana
   - Esporádicamente
5) **¿Su computadora asignada ha presentado fallas recientemente?**
   - Sí
   - No
6) **¿Qué tipo de fallas ha presentado el equipo? (Puede marcar más de una)**
   - Hardware (pantalla, teclado, batería, etc.)
   - Software (sistema operativo, lentitud, errores)
   - Red/internet
   - No ha presentado fallas



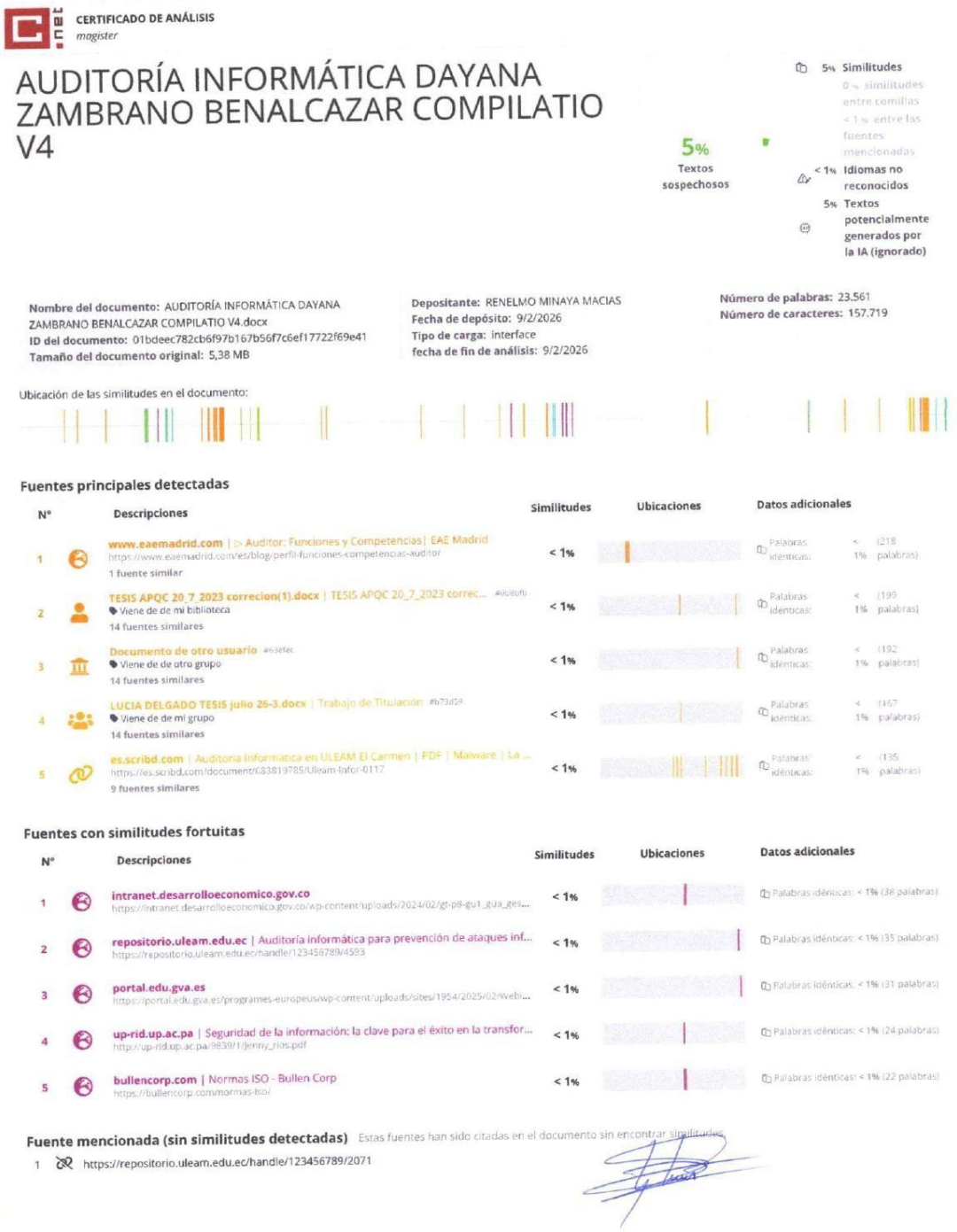
Entrevista / Mediante grabación de voz

1. ¿Cuál es su cargo y cuáles son sus principales responsabilidades en relación con los equipos informáticos de la universidad?
2. Actualmente, ¿la universidad lleva un registro actualizado donde se pueda ver qué equipos están asignados a cada docente?
3. Al momento de entregar un equipo a un docente, ¿en qué cosas se fijan o qué se toma en cuenta para hacer esa asignación
4. ¿Cada cuánto tiempo se les da mantenimiento a los equipos que se usan en la institución?
5. Según su experiencia, ¿qué problemas o fallas son los que más se repiten en los equipos que usan los docentes?
6. Cuando un docente reporta que un equipo está dañado, ¿qué es lo que normalmente hace el área técnica para atender ese caso?
7. En su opinión, ¿el tiempo que se tarda el área técnica en responder a las fallas es el correcto?
8. ¿La universidad cuenta actualmente con políticas o normativas relacionadas con el uso seguro y adecuado de los equipos informáticos?
9. ¿Qué medidas de seguridad lógica se aplican en los equipos, como por ejemplo antivirus, uso de contraseñas, actualizaciones del sistema o control del software instalado?
10. ¿Cómo se controla el acceso físico a los equipos informáticos cuando los docentes no se encuentran presentes en las salas?
11. ¿Se han detectado incidentes relacionados con accesos no autorizados, pérdida de información o malware en los equipos docentes?
12. ¡La institución realiza respaldos periódicos de la información que se encuentra almacenada en los equipos informáticos?
13. ¿Existen procedimientos definidos para el reemplazo de equipos o componentes dañados?
14. ¿El personal docente recibe capacitación sobre el uso adecuado y seguro de los equipos informáticos?
15. Desde su experiencia, ¿qué riesgos considera más críticos en relación con la seguridad de los equipos informáticos de los docentes?
16. ¿Cree usted que es necesario implementar controles más estrictos de acceso y monitoreo sobre los equipos informáticos?
17. ¿Qué mejoras recomendaría para fortalecer la seguridad física y lógica de los equipos informáticos institucionales?



Anexo F Certificado de coincidencia académica (emitido por tutor del sistema anti plagio)

Figura 23



CERTIFICADO DE ANÁLISIS
magister

AUDITORÍA INFORMÁTICA DAYANA ZAMBRANO BENALCAZAR COMPILATIO V4

5% Textos sospechosos

5% Similitudes
0 % similitudes entre comillas
< 1 % entre las fuentes mencionadas
< 1% Idiomas no reconocidos
5% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: AUDITORÍA INFORMÁTICA DAYANA ZAMBRANO BENALCAZAR COMPILATIO V4.docx
ID del documento: 01bdeec782cb6f97b167b56f7c6ef17722f69e41
Tamaño del documento original: 5,38 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: 23.561
Número de caracteres: 157.719

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.eaemadrid.com | ▷ Auditor: Funciones y Competencias | EAE Madrid https://www.eaemadrid.com/es/blog/perfil-funciones-competencias-auditor 1 fuente similar	< 1%		Palabras idénticas: < 1% (218 palabras)
2	TESIS APQC 20_7_2023 correcion(1).docx | TESIS APQC 20_7_2023 correc... Viene de de mi biblioteca 14 fuentes similares	< 1%		Palabras idénticas: < 1% (199 palabras)
3	Documento de otro usuario Viene de de otro grupo 14 fuentes similares	< 1%		Palabras idénticas: < 1% (192 palabras)
4	LUCIA DELGADO TESIS julio 26-3.docx | Trabajo de Titulación Viene de de mi grupo 14 fuentes similares	< 1%		Palabras idénticas: < 1% (167 palabras)
5	es.scribd.com | Auditoria Informatica en ULEAM El Carmen | PDF | Malware | La ... https://es.scribd.com/document/683819785/Uleam-Iafor-0117 9 fuentes similares	< 1%		Palabras idénticas: < 1% (135 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	intranet.desarrolloeconomico.gov.co https://intranet.desarrolloeconomico.gov.co/wp-content/uploads/2024/02/gt-p8-gu1_guia_ges...	< 1%		Palabras idénticas: < 1% (38 palabras)
2	repositorio.uleam.edu.ec | Auditoría informática para prevención de ataques inf... https://repositorio.uleam.edu.ec/handle/123456789/4593	< 1%		Palabras idénticas: < 1% (35 palabras)
3	portal.edu.gva.es https://portal.edu.gva.es/programes-europeus/wp-content/uploads/sites/1954/2025/02/Webi...	< 1%		Palabras idénticas: < 1% (31 palabras)
4	up-rid.up.ac.pa | Seguridad de la información: la clave para el éxito en la transfor... http://up-rid.up.ac.pa/9839/1/Jenny_rios.pdf	< 1%		Palabras idénticas: < 1% (24 palabras)
5	bullencorp.com | Normas ISO - Bullen Corp https://bullencorp.com/normas-iso/	< 1%		Palabras idénticas: < 1% (22 palabras)

Fuente mencionada (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes

1 https://repositorio.uleam.edu.ec/handle/123456789/2071

9 GLOSARIO

Activo: Elemento de valor para la institución, como equipos informáticos, información, software o infraestructura, que debe ser protegido frente a amenazas que puedan afectar su funcionamiento o disponibilidad.

Auditoría de Seguridad Informática: Proceso sistemático que permite evaluar el estado de la seguridad física y lógica de los sistemas de información, con el fin de identificar riesgos, vulnerabilidades y proponer medidas de mejora.

Confidencialidad: Principio de la seguridad de la información que garantiza que los datos solo sean accesibles por personas autorizadas, evitando divulgaciones no permitidas.

Control de Acceso: Conjunto de mecanismos físicos o lógicos que restringen el ingreso a instalaciones, equipos o sistemas únicamente a usuarios autorizados.

Disponibilidad: Propiedad que asegura que los sistemas, equipos e información estén accesibles y operativos cuando sean requeridos por los usuarios autorizados.

Equipo Informático: Conjunto de dispositivos tecnológicos como computadoras, laptops, periféricos y componentes de red utilizados para el desarrollo de actividades académicas y administrativas.

Firewall: Sistema de seguridad que controla y filtra el tráfico de red, permitiendo o bloqueando conexiones según reglas establecidas para prevenir accesos no autorizados.

Gestión de Riesgos: Proceso mediante el cual se identifican, analizan y evalúan los riesgos que pueden afectar a los activos, con el objetivo de aplicar controles que reduzcan su impacto.

Impacto: Consecuencia o efecto que puede generar la materialización de una amenaza sobre un activo, afectando la continuidad operativa, la información o los recursos institucionales.

Incendio: Amenaza física que puede ocasionar daños severos a equipos informáticos, infraestructura y documentación, generando pérdidas económicas y operativas.

Inundación: Riesgo físico asociado a la acumulación de agua por lluvias, filtraciones o fallas estructurales, que puede afectar equipos eléctricos y tecnológicos.

Integridad: Principio de seguridad que garantiza que la información se mantenga completa, correcta y sin modificaciones no autorizadas durante su almacenamiento o transmisión.

Inventario de Equipos: Registro detallado de los equipos informáticos institucionales, que permite su control, seguimiento, mantenimiento y verificación de existencia.

Malware: Software malicioso diseñado para dañar, alterar o acceder de forma no autorizada a sistemas informáticos, comprometiendo la seguridad de la información.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, utilizada para identificar amenazas, vulnerabilidades y valorar riesgos de manera estructurada.

Mantenimiento Preventivo: Conjunto de actividades programadas destinadas a conservar los equipos informáticos en buen estado, evitando fallas técnicas y prolongando su vida útil.

Políticas de Seguridad: Normas y lineamientos establecidos por la institución para regular el uso adecuado de los recursos tecnológicos y proteger la información.

Probabilidad: Nivel de posibilidad de que una amenaza se materialice y afecte un activo, considerando las condiciones actuales de seguridad y control.

Riesgo: Resultado de la combinación entre la probabilidad de ocurrencia de una amenaza y el impacto que esta puede generar sobre un activo.

Robo: Amenaza física que consiste en la sustracción no autorizada de equipos informáticos o activos institucionales, afectando la operatividad y la seguridad.

Sala de Docentes: Espacio institucional destinado al uso del personal docente, donde se ubican equipos informáticos y documentación que requieren medidas de seguridad adecuadas.

Seguridad Física: Conjunto de medidas destinadas a proteger instalaciones, equipos y personas frente a amenazas como robos, incendios o desastres naturales.

Seguridad Lógica: Medidas de protección aplicadas a los sistemas informáticos, como contraseñas, antivirus y políticas de acceso, para evitar ataques digitales y pérdida de información.

Vulnerabilidad: Debilidad o falla en los controles de seguridad que puede ser aprovechada por una amenaza para afectar un activo institucional.