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 INGENIERIA EN TECNOLOGÍAS DE LA INFORMACIÓN

AUDITORÍA INFORMÁTICA DE SEGURIDAD FÍSICA DEL LABORATORIO DE COMPUTACIÓN DE LA UNIDAD EDUCATIVA "AMERICANO"

AUTORA

KAREN MISHELLE CEVALLOS BRAVO

TUTOR

ING. WLADIMIR MINAYA MACÍAS, MG.

EL CARMEN, ENERO 2025

CERTIFICACIÓN DEL TUTOR

CERTIFICACIÓN

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

Haber dirigido y revisado el trabajo de investigación, bajo la autoría de la estudiante **CEVALLOS BRAVO KAREN MISHELLE**, legalmente matriculada en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(1)-2024(2), cumpliendo el total de 384 horas, bajo la opción de titulación de proyecto integrador, cuyo tema del proyecto es "Auditoría Informática de Seguridad Física del Laboratorio de Computación de Unidad Educativa "Americano" ".

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

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

El Carmen, 06 de Enero del 2025.

Lo certifico,

Wladimir Minaya Macías, Mg.
Docente Tutor
Área: Sistemas

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

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 de seguridad física del laboratorio de computación de la unidad educativa "Americano".

Modalidad:
Proyector Integrador.

Autor:
Karen Mishelle Cevallos Bravo.

Tutor:
Ing. Wladimir Minaya Macías, Mg.

Tribunal de Sustentación:

- **Presidente:** Ing. Alex Mora Marcillo.
- **Miembro:** Ing. Raul Reascos Pinchao
- **Miembro:** Ing. Rocío Mendoza Villamar.

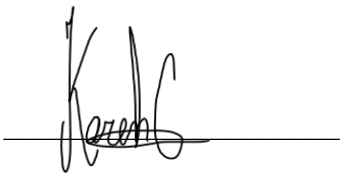
Fecha de Sustentación:
29 de Mayo del 2025

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, con el siguiente tema: "AUDITORÍA INFORMÁTICA DE SEGURIDAD FÍSICA DEL LABORATORIO DE COMPUTACIÓN DE LA UNIDAD EDUCATIVA AMERICANO", corresponde exclusivamente a: Karen Mishelle Cevallos Bravo con cédula de ciudadanía N° 2300698921, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.



Cevallos Bravo Karen Mishelle

C.I. 230069892-1

DEDICATORIA

Dedico mi tesis en primer lugar a Dios, quien me ha dado fuerzas en mi recorrido de vida, universitaria y personal. También se la dedico a mis padres por su invaluable apoyo, ejemplo de perseverancia y valores y por haberme brindado las herramientas necesarias para alcanzar este logro académico. Mis amigas porque son las personas por las que estoy hoy logrando mis sueños y siguiendo adelante a pesar de las dificultades de la vida. A mis docentes, cuyo compromiso, sabiduría y dedicación dejaron una huella imborrable en mi formación profesional. Y especialmente a mi novio cuyo apoyo fue fundamental en cada etapa de mi proceso para ser una persona capaz, por su guía, confianza y respaldo constante, elementos fundamentales para la culminación de este trabajo.

Con profundo respeto y gratitud, dedico este esfuerzo a todos ustedes.

Karen Cevallos

AGRADECIMIENTO

Agradezco a la Universidad Laica Eloy Alfaro de Manabí por el respaldo brindado, tanto en recursos, tiempo y espacio. Institución de alto estima para lograr mis metas logrando convertirme en profesional. A mis compañeros de estudio, quienes me acompañaron en esta etapa y colaboración. A mis amigos por ser un soporte emocional y compartir momentos de alegría y reflexión, a todas las personas que gracias a ellos hoy puedo dar mis agradecimientos por su apoyo y guía continua en mi formación como estudiante y persona; logrando ahora entrar a una nueva etapa de formación profesional y laboral.

Agradeciendo finalmente a mi tutor de tesis: Wladimir Minaya, a quien le expreso mi más sincera gratitud por su guía, paciencia y orientación durante el desarrollo de este trabajo. Su experiencia y dedicación fueron fundamentales para superar los desafíos que se presentaron en el camino.

A todos ustedes, muchas gracias.

Karen Cevallos

ÍNDICE GENERAL

PORTADA I

CERTIFICACIÓN DEL TUTOR III

TRIBUNAL DE SUSTENTACIÓN IV

DECLARACIÓN DE AUTORÍA V

DEDICATORIA VI

AGRADECIMIENTO VII

ÍNDICE GENERAL VIII

ÍNDICE DE TABLAS XV

ÍNDICE DE ILUSTRACIONES XVII

ÍNDICE DE ANEXOS XVIII

RESUMEN XIX

ABSTRACT XX

CAPÍTULO I 1

1 INTRODUCCIÓN 1

1.1 Introducción 1

1.2 Presentación del tema 2

1.3 Ubicación y contextualización de la problemática 2

1.4 Planteamiento del problema 2

1.4.1 Problematización 2

1.4.2 Génesis del problema 3

1.4.3 Estado actual del problema 4

1.5 Diagrama causa – efecto del problema 5

1.6 Objetivos 5

1.6.1 Objetivo general 5

1.6.2 Objetivos específicos 5

1.7 Justificación 6

1.8 Impactos esperados 6

1.8.1 Impacto tecnológico 6

1.8.2 Impacto social 7

1.8.3 Impacto ecológico 7

1.8.4 Impacto educativo y cultural 8

CAPÍTULO II 9

2 MARCO TEÓRICO 9

2.1 Antecedentes históricos 9

2.1.1 Diseño de una guía para la función de auditoría interna en las organizaciones de carácter empresarial de la ciudad de Sucre 10

2.1.2 Auditoría informática dentro de la empresa “Promaelec” de la ciudad de Quevedo, en tiempo de COVID-19 11

2.1.3 El rol de la auditoría informática en la era de la protección de datos personales en Ecuador 11

2.1.4 Estrategias de IA aplicada a la auditoria informática 11

2.1.5 Escalabilidad y Sostenibilidad en Implementaciones de Blockchain para Auditoría Informática: Retos y Soluciones Futuras 12

2.2 Definiciones conceptuales 12
2.2.1 Auditoría informática 12
2.2.1.1 Historia y evolución de la auditoría informática 14
2.2.1.2 Objetivos de la Auditoría Informática 14
2.2.1.3 Áreas de aplicación 15
2.2.1.4 Fases de la auditoría informática 16
2.2.1.5 Herramientas de auditoría informática 18
2.2.2 Seguridad física 19
2.2.2.1 Importancia de la Seguridad Física en Laboratorios de Computación 20
2.2.2.2 La auditoría de seguridad física 20
2.2.2.3 Fases de la auditoría de seguridad física 21
2.2.2.4 Herramientas y métodos utilizados 21
2.2.2.5 Beneficios de la auditoría de seguridad física en laboratorios de computo 22
2.2.2.6 Metodología MAGERIT 22
2.2.2.7 Objetivos de MAGERIT 23
2.2.2.8 Fase 1: Definición del Alcance 24
2.2.2.9 Fase 2: Identificación de Activos y Recursos 24
2.2.2.10 Fase 3: Identificación de Amenazas y Vulnerabilidades 25
2.2.2.11 Fase 4: Evaluación de Impactos 25
2.2.2.12 Fase 5: Evaluación de Probabilidades 25
2.2.2.13 Fase 6: Establecimiento de Medidas de Control 25

2.2.2.14 Fase 7: Monitorización y Revisión 26
2.2.2.15 Beneficios de Utilizar MAGERIT en Auditorías de Seguridad Física 26
2.3 Conclusiones del marco teórico 27
CAPÍTULO III 28
3 MARCO INVESTIGATIVO 28
3.1 Introducción 28
3.2 Tipos de investigación 28
3.2.1 Investigación de enfoque mixto 28
3.2.2 Investigación bibliográfica o documental 29
3.2.3 Investigación de campo 29
3.2.4 Investigación descriptiva 29
3.3 Métodos de investigación 30
3.3.1 Analítico – Sintético 30
3.4 Fuentes de información de datos 30
3.4.1 Fuentes primarias y secundarias 30
3.4.2 Fuente primaria: Entrevista 31
3.4.3 Fuente secundaria: Encuesta 31
3.5 Estrategia operacional para la recolección de datos 31
3.5.1 Población - Segmentación - Técnica de muestreo - Tamaño de la muestra 32
3.5.1.1 Población 32
3.5.1.2 Muestra 32

3.5.2 Análisis de las herramientas de recolección de datos a utilizar 34
3.5.2.1 Encuesta - Entrevista 34
3.5.2.2 Estructura de los instrumentos de recolección de datos aplicados 34
3.5.3 Plan de recolección de datos 35
3.6 Análisis y presentación de resultados 35
3.6.1 Tabulación y análisis de los datos de las encuestas realizadas 35
3.6.2 Presentación y análisis de datos de las entrevistas realizadas 38
3.6.3 Presentación y descripción de los resultados obtenidos 41
3.6.4 Informe final del análisis de los datos 42
CAPÍTULO IV 43
4 MARCO PROPOSITIVO 43
4.1 Introducción 43
4.2 Objetivos 44
4.3 Descripción de la propuesta 44
4.4 Determinación de recursos 46
4.4.1 Humanos 46
4.4.2 Tecnológicos 47
4.4.3 Económicos 48
4.5 Etapas del desarrollo de la propuesta 49
4.5.1 Antecedentes 49
4.5.1.1 Datos informativos 50

4.5.1.2 Misión 51
4.5.1.3 Visión 51
4.5.2 Organigrama de la institución 52
4.5.2.1 Programa de auditoria informática 52
4.5.2.2 Planificación 53
4.5.2.3 Normas de seguridad 54
4.5.2.4 Metodología Magerit 54
4.5.2.5 Gráfico de las fases de la metodología Magerit 55
4.5.2.6 Aplicación de metodología Magerit 56
4.5.2.7 Definición y valoración de activos 56
4.5.2.8 Identificación de amenazas 58
4.5.2.9 Diseño de instrumento para analizar riesgos 60
4.5.2.10 Aplicación de instrumentos 65
4.5.2.11 Tabulación 66
4.5.3 Análisis de resultados 72
5 Hallazgos 76
6 Nivel de Riesgo de Robo 77
7 Nivel de Riesgo de Inundación 79
8 Nivel de Riesgo de Daño de Equipos 80
9 Nivel de Riesgo de Incendio 82
10 Nivel de Riesgo de Malware 83

10.1.1 Guía de buenas prácticas informáticas para la seguridad física 84

11 EVALUACIÓN DE RESULTADOS 86

11.1 Introducción 86

11.2 Resultado de auditoria 87

11.2.1.1 Guía de buenas prácticas 89

11.2.1.2 Propuesta de Política de sanciones por infracciones de seguridad informática en la Unidad Educativa 96

11.2.1.3 Sanciones 98

11.2.1.4 Propuestas de temas de capacitación para los usuarios del laboratorio sobre buenas prácticas informáticas y seguridad 100

11.2.2 Informe final del análisis de los datos 102

11.2.3 Recomendación de auditoria 103

CAPÍTULO VI 104

12 CONCLUSIONES Y RECOMENDACIONES 104

12.1 Conclusiones 104

12.2 Recomendaciones 105

BIBLIOGRAFÍA 107

13 Bibliografía 107

ANEXOS 111

GLOSARIO DE TÉRMINOS 118

ÍNDICE DE TABLAS

Tabla 1 Estrategia operacional para la recolección de datos 32

Tabla 2 Tabulación y análisis de los datos de las encuestas realizadas 38

Tabla 3 Presentación y análisis de datos de las entrevistas realizadas 41

Tabla 4 Recursos humanos 46

Tabla 5 Recursos tecnológicos.....47

Tabla 6 Recursos económicos.....48

Tabla 7 Datos informativos de la institución 51

Tabla 8 Programa de auditoria informática (planificación).....53

Tabla 9 Valoración de activos.....56

Tabla 10 Definición y valoración de activos 57

Tabla 11 Identificación de amenazas.....58

Tabla 12 Cuestionarios para identificar riesgos (Robo) 60

Tabla 13Cuestionarios para identificar riesgos (Incendio) 61

Tabla 14 Cuestionarios para identificar riesgos (Inundación) 62

Tabla 15 Cuestionarios para identificar riesgos (Malware).....63

Tabla 16 Cuestionarios para identificar riesgos (Daños a equipos).....64

Tabla 17 Cuestionarios para identificar riesgos (Robo) 67

Tabla 18 Cuestionarios para identificar riesgos (Incendio) 68

Tabla 19 Cuestionarios para identificar riesgos (Inundación). 69

Tabla 20 Cuestionarios para identificar riesgos (Malware). 70

Tabla 21 Cuestionarios para identificar riesgos (Daños a equipos). 71

Tabla 22 Valoración de impacto 73

Tabla 25 Nivel de Riesgo de Robo 78

Tabla 26 Nivel de Riesgo de Inundación 80

Tabla 27 Nivel de Riesgo de Daño de Equipos 81

Tabla 28 Nivel de Riesgo de Incendio 83

Tabla 29 Nivel de Riesgo de Malware 84

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Diagrama de causa - efecto del problema 5

Ilustración 2 Organigrama de la institución 52

Ilustración 3 Calculo del impacto 59

Ilustración 4 Matriz de riesgo 72

Ilustración 5 Valoración de riesgo del cuestionario 73

Ilustración 6 Gravedad de impacto 74

Ilustración 8 Matriz de riesgo Leyenda 76

Ilustración 9 Nivel de seguridad general 76

Ilustración 10 Portada de guía 89

Ilustración 11 Introducción de la guía 90

Ilustración 12 Objetivo de la guía 90

Ilustración 13 Definiciones de la guía 91

Ilustración 14 Normativas de seguridad para el uso de los laboratorios de computación 92

Ilustración 15 Riesgo de robo e incendio 93

Ilustración 16 Riesgo de daño de equipos e inundación 94

Ilustración 17 Riesgo de malware 95

Ilustración 18 Propuesta de política de sanciones por infracciones de seguridad 97

Ilustración 19 Sanciones 98

Ilustración 20 Procedimiento de aplicación 99

Ilustración 21 Propuestas de temas de capacitación para los usuarios del laboratorio 101

ÍNDICE DE ANEXOS

Anexo A: Aprobación del tema 111

Anexo B: Certificado de análisis Compilatio 112

Anexo C: Certificado de la empresa 113

Anexo D: Fotografías.....114

Anexo E: Evidencia de aplicación de encuestas y entrevista 116

RESUMEN

Este trabajo de investigación se centra en una auditoría informática de seguridad física realizada en el laboratorio de computación de la Unidad Educativa Americano. El propósito principal fue analizar el nivel de seguridad física del laboratorio y verificar si cumple con las normativas necesarias para proteger sus recursos tecnológicos. Para ello, se identificaron los problemas existentes mediante encuestas y entrevistas realizadas a los docentes y autoridades de la institución.

La metodología utilizada fue MAGERIT, que facilitó tareas clave como la identificación de activos y amenazas, el análisis y tabulación de riesgos, y la elaboración de una matriz de riesgos. Analizando parámetros para medir el nivel de riesgos, los cuales fueron incendio, robo, malware, inundación y daño de equipos, identificando así posibles vulnerabilidades en cuyos aspectos se obtuvo cierto porcentaje de riesgos, en base a los resultados obtenidos se organizó la información para mitigar estos riesgos en cada una de las áreas evaluadas

Con base en este análisis, se desarrolló un informe de auditoría junto con una manual de recomendaciones prácticas. Estas recomendaciones incluyen estrategias específicas para reforzar la seguridad física del laboratorio, minimizar riesgos y garantizar la protección de los recursos tecnológicos de la institución.

ABSTRACT

This research focuses on a physical security IT audit conducted in the computer laboratory of the "Americano" Educational Unit. The main purpose was to analyze the laboratory's physical security level and verify compliance with the necessary regulations to protect its technological resources. To achieve this, existing issues were identified through surveys and interviews conducted with teachers and the institution's authorities.

The methodology used was MAGERIT, which facilitated key tasks such as identifying assets and threats, analyzing and tabulating risks, and creating a risk matrix. Parameters were analyzed to measure risk levels, including fire, theft, malware, flooding, and equipment damage. This process identified possible vulnerabilities, assigning a percentage to each risk. Based on the results, the information was organized to mitigate these risks in each of the evaluated areas.

Based on this analysis, an audit report was developed along with a practical recommendations manual. These recommendations include specific strategies to strengthen the physical security of the laboratory, minimize risks, and ensure the protection of the institution's technological resources.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

A lo largo del tiempo, las auditorías informáticas han adquirido una posición de gran importancia para cualquier empresa o institución. Esto no es sorprendente, dado el gran número de beneficios que aportan. Todo esto se debe a los diversos resultados derivados de la evolución constante de las auditorías informáticas, sustentada en el conocimiento acumulado por los auditores. En este contexto, la auditoría informática plantea una práctica minuciosa en la evaluación de la información de los sistemas informáticos con el fin de garantizar la exactitud y mejorar la utilidad de los usuarios, a la vez que verifica la autenticidad, integridad y calidad de la información (Angamarca, Estrategias de auditoría informática en la era de la transformación digital, 2021).

Reflejando la importancia de las auditorias informáticas las cuales se posicionan como una herramienta clave para evaluar y garantizar la eficacia, eficiencia y seguridad de los sistemas de información. Esta disciplina permite identificar vulnerabilidades, establecer controles y diseñar estrategias que mitiguen riesgos potenciales, alineando los procesos tecnológicos con los objetivos organizacionales y las normativas vigentes. Tomando en cuenta la importancia de las auditorias informativas, las organizaciones especificando a Ecuador deben considerar la auditoría informática como una herramienta estratégica dentro de su gobierno corporativo y gestión de riesgos.

Los departamentos de TI y las unidades de auditoría interna desempeñan un papel clave en la identificación de deficiencias y la implementación de controles que garanticen la integridad, disponibilidad y confidencialidad de la información. La auditoría informática en este nivel busca no solo la protección de los sistemas de información, sino también la alineación de las tecnologías con los objetivos empresariales, optimizando los recursos tecnológicos y asegurando la eficiencia operativa. Siguiendo esta línea de pensamiento, el presente trabajo se puede observar él porque es importante realizar auditorías informáticas en organizaciones que cuentan con áreas informáticas, en este caso es importante realizar una auditoria en los componentes del laboratorio de computación de la Unidad Educativa Americano para la identificación de riesgos en la infraestructura y a su vez poder evitar posibles vulnerabilidades.

1.2 Presentación del tema

Auditoría informática de seguridad física del laboratorio de computación de la UNIDAD EDUCATIVA "AMERICANO".

1.3 Ubicación y contextualización de la problemática

La Unidad Educativa Americano fundada en el año 1981 Escuela de Educación regular y sostenimiento particular laico, con jurisdicción Hispana, es una institución que ofrece aprendizajes de modalidad presencial de jornada matutina y nivel educativo de inicial, educación básica y bachillerato contando así con una cantidad aproximada a 174 estudiantes. Se encuentra situada en la provincia de Manabí, cantón El Carmen en la Av. Chone y Santa Ana en la zona 4 de manera geográfica, actualmente, cuenta con 18 colaboradores que trabajan bajo un enfoque orientado a la educación.

1.4 Planteamiento del problema

1.4.1 Problematización

Esta investigación consistió en una auditoría informática realizada en la unidad educativa Americano, localizada en el cantón El Carmen, Manabí. Gracias a un convenio firmado, se autorizó la ejecución de la auditoría en el Distrito durante el año 2024. Es preciso mencionar que la incorporación de la tecnología se ha transformado de la manera en que las organizaciones actuales operan, mejorando su eficiencia y productividad. Sin embargo, la ausencia de medidas adecuadas para reducir y controlar los riesgos que podrían afectar la seguridad física de los equipos informáticos representa una preocupación importante. Con el objetivo de abordar estos riesgos en el Distrito, se pretende desarrollar un conjunto de directrices que garanticen la protección de dichos equipos.

En este sentido, resulta crucial llevar a cabo una auditoría para identificar y prevenir posibles vulnerabilidades dentro de las instalaciones, lo que permitirá tomar las necesarias para asegurar la integridad física del equipo informático. Si algún equipo sufre daños, las

consecuencias podrían ser graves tanto para la continuidad de los servicios como para las personas que dependen de ellos.

1.4.2 Génesis del problema

La tecnología actualmente es indispensable para la ejecución de profesiones y el avance inmenso de la sociedad, tanto en el ámbito familiar como en el profesional. Este avance ha transformado la dinámica educativa, incrementando la dependencia de herramientas tecnológicas en los procesos de enseñanza y aprendizaje. Esta creciente dependencia ha provocado un aumento significativo en la cantidad y el valor de los equipos tecnológicos utilizados en los laboratorios de computación, convirtiéndolos en activos esenciales para el funcionamiento de las instituciones educativas.

A pesar de su relevancia, es evidente que, en muchos casos, incluyendo el de la Unidad Educativa Americano, existe una notable falta de conciencia por parte de los usuarios sobre la importancia de la seguridad física en el cuidado de estos recursos. La ausencia de políticas y procedimientos claros relacionados con la protección de estos activos tecnológicos aumenta la vulnerabilidad frente a riesgos como robos, daños accidentales, mal uso y desgaste prematuro de los equipos. Esta deficiencia no solo afecta la operatividad del laboratorio, sino que también compromete la calidad educativa.

Por lo tanto, resulta fundamental la realización de una auditoría informática enfocada en la seguridad física, la cual permita identificar las deficiencias actuales y establecer un plan de acción para superarlas. Este proceso no solo garantizará la protección de los equipos, sino que también contribuirá a la sostenibilidad de los recursos tecnológicos, asegurando que estos sigan desempeñando su papel esencial en la formación académica. Asimismo, la auditoría ofrecerá información clave para desarrollar estrategias educativas que promuevan una cultura de responsabilidad y cuidado hacia los recursos tecnológicos, fomentando un entorno más seguro y eficiente dentro de la comunidad educativa.

1.4.3 Estado actual del problema

Con el objetivo de satisfacer las necesidades de la Unidad Educativa Americano, ubicada en el cantón El Carmen, se propone realizar una auditoría informática enfocada en la seguridad física de los componentes informáticos del laboratorio de cómputo de la institución. Esta iniciativa surge a partir de la identificación de riesgos potenciales y la falta de medidas efectivas para garantizar la protección de los recursos tecnológicos.

La solicitud formal para realizar la auditoría fue aprobada por el rector de la institución, permitiendo así un análisis exhaustivo de los riesgos asociados a la seguridad física del laboratorio. Entre los principales problemas detectados se encuentran la insuficiencia de una adecuada planificación y gestión de los equipos informáticos, la falta de espacio en las áreas de laboratorios, la ausencia de medidas preventivas ante desastres naturales, la manipulación inadecuada de los componentes tecnológicos, la incorrecta instalación de los cables, y deficiencias en los sistemas de seguridad que dejan vulnerables los equipos.

Para abordar estas problemáticas, se utilizará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), que permitirá realizar una identificación precisa de los riesgos, evaluar su impacto y proponer acciones correctivas que fortalezcan la seguridad física del laboratorio. La información requerida para llevar a cabo este análisis será recopilada a través de las fuentes institucionales disponibles, como la secretaría de la institución, garantizando un enfoque riguroso y basado en datos.

El propósito final de la auditoría es no solo identificar y mitigar los riesgos, sino también establecer una base sólida para la gestión futura de los activos tecnológicos. Esto incluye el diseño e implementación de protocolos claros para la protección de los equipos, la capacitación del personal en medidas de seguridad, y la creación de un entorno educativo más seguro y eficiente. Así, se garantizará la continuidad operativa y la protección de los recursos tecnológicos, promoviendo un entorno de aprendizaje seguro y sostenible para la comunidad educativa.

1.5 Diagrama causa – efecto del problema

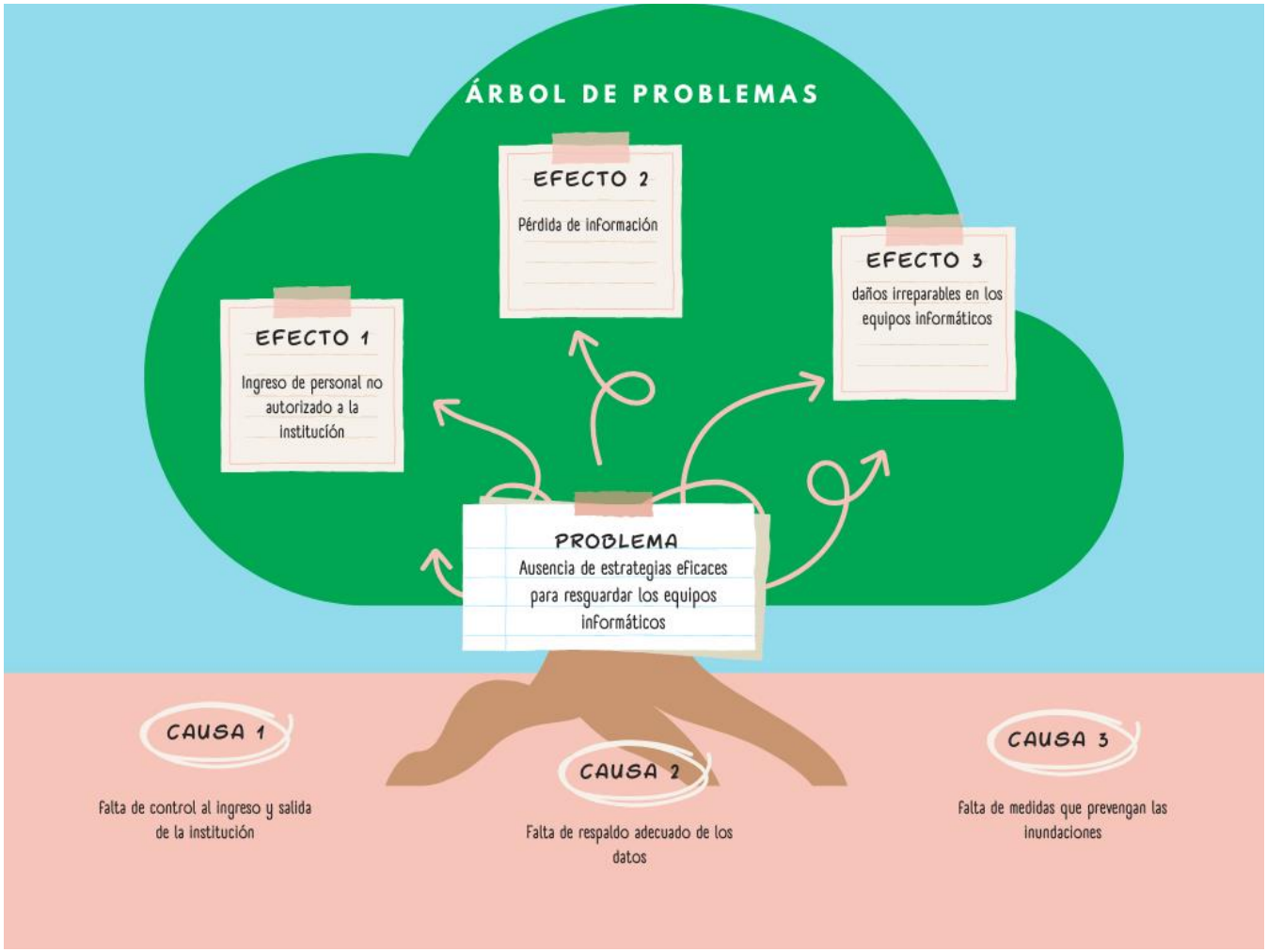


Ilustración 1
Diagrama de causa - efecto del problema

1.6 Objetivos

1.6.1 Objetivo general

Aplicar una Auditoría informática de seguridad física del laboratorio de computación de la Unidad Educativa Americano.

1.6.2 Objetivos específicos

1. Recopilar fundamentos teóricos en artículos especializados que permitan mejorar la protección los equipos informáticos.

2. Realizar un diagnóstico mediante la inspección física para identificar posibles fallos de los equipos informáticos de la Unidad Educativa Americano.
3. Diseñar una auditoría para identificar los riesgos de seguridad informática en la institución.
4. Elaborar una guía de auditoría con recomendaciones para mejorar los procedimientos utilizados en la institución.

1.7 Justificación

En la actualidad, existen diversos componentes fundamentales para realizar una auditoría a una institución educativa. Uno de los motivos principales para llevar a cabo esta investigación es el impacto que tuvo la pandemia, ya que durante este periodo no se realizó un mantenimiento adecuado de los equipos informáticos. Como resultado, muchos dispositivos presentan fallas que afectan la eficiencia operativa del laboratorio de computación de la Unidad Educativa Americano.

Esta institución no cuenta con un sistema de auditoría informática completo implementado, lo que ha llevado a problemas en el proceso de mantenimiento y la gestión de sus equipos tecnológicos. La realización de una auditoría es fundamental para identificar vulnerabilidades y establecer un plan de acción que asegure la integridad y confidencialidad de la información, además de proteger los activos tecnológicos de la institución.

Investigaciones previas, como las realizadas en la Universidad Laica Eloy Alfaro de Manabí (ULEAM), han abordado auditorías relacionadas con seguridad física. Sin embargo, estas no han sido aplicadas a la realidad de la Unidad Educativa Americano. Justificar esta investigación resulta esencial para identificar las necesidades específicas de la institución, proponer soluciones adaptadas a su contexto y fortalecer la seguridad de sus recursos informáticos, asegurando un entorno tecnológico más confiable y eficiente.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

La auditoría informática de seguridad física que se llevará a cabo en el laboratorio de computación de la Unidad Educativa Americano tiene como objetivo principal evaluar la efectividad y eficiencia de las medidas de seguridad implementadas. Este proceso nos permitirá

identificar fortalezas y debilidades en los sistemas actuales, así como oportunidades de mejora que podrían optimizar la protección de los activos tecnológicos de la institución. La auditoría también proporcionará datos relevantes que podrán ser utilizados para justificar inversiones en tecnología de punta, como sistemas de videovigilancia avanzados, cerraduras electrónicas controladas remotamente o software especializado para la gestión de la seguridad física.

Además, la identificación de vulnerabilidades en la infraestructura tecnológica permitirá proponer soluciones personalizadas que garanticen la continuidad operativa del laboratorio. Esto incluye la introducción de dispositivos más modernos, como servidores con mejores mecanismos de respaldo y equipos con protecciones adicionales contra pérdida de datos. De esta manera, la auditoría no solo protegerá los activos actuales, sino que también fomentará un entorno tecnológico más robusto y preparado para el futuro.

1.8.2 Impacto social

La implementación de medidas de seguridad física en el laboratorio de computación también tendrá un impacto significativo en la comunidad educativa. Por un lado, el fortalecimiento de la seguridad contribuirá a reducir incidentes como robos o vandalismo, lo que se traduce en un menor gasto en reparaciones o reemplazos de equipos. Por otro lado, al reducir la posibilidad de interrupciones en el servicio del laboratorio, se garantizará que los estudiantes puedan continuar desarrollando sus competencias tecnológicas sin interrupciones.

Otra repercusión importante es el potencial ahorro energético que podría derivarse de medidas como la automatización del encendido y apagado de equipos o la optimización de sistemas de climatización en el laboratorio. Estas mejoras no solo benefician al presupuesto de la institución, sino que también fomentan una conciencia ambiental en la comunidad educativa. Finalmente, el compromiso con la protección de los activos tecnológicos fortalece el sentido de pertenencia y responsabilidad entre estudiantes y docentes, creando un entorno más seguro y colaborativo.

1.8.3 Impacto ecológico

La realización de esta auditoría de seguridad física informática puede contribuir a brindar tranquilidad a la comunidad educativa de la Unidad Educativa Americano, al garantizar

la integridad y confidencialidad de la información que se maneja en el laboratorio de computación. Asimismo, implementar medidas de seguridad puede incrementar una cultura de protección de la información y la conciencia de la importancia de la seguridad informática en los entornos educativos.

Desde una perspectiva ecológica, la auditoría de seguridad física también tiene implicaciones relevantes. Proteger los activos tecnológicos del laboratorio reduce significativamente la necesidad de reemplazar equipos de manera frecuente debido a daños, robos o negligencias. Esto se traduce en una menor generación de residuos electrónicos, que son una de las principales preocupaciones medioambientales en la actualidad debido a su difícil disposición y alto impacto contaminante.

Agregando que, al implementar medidas de seguridad sostenibles, como sistemas de energía eficiente y controles automatizados, se promueve un uso más responsable de los recursos energéticos. Estas acciones no solo contribuyen a la disminución de la huella de carbono de la institución, sino que también establecen un ejemplo positivo para los estudiantes sobre la importancia de la sostenibilidad en la tecnología. Este impacto ecológico indirecto ayuda a generar una mayor conciencia ambiental dentro y fuera de la institución.

1.8.4 Impacto educativo y cultural

Tomando en cuenta que uno de los impactos más significativos de esta auditoría es la promoción de una cultura de seguridad y protección de la información dentro de la comunidad educativa. Al garantizar la integridad y confidencialidad de los datos manejados en el laboratorio de computación, se genera un entorno de confianza que permite a los estudiantes y docentes enfocarse en sus actividades académicas y profesionales.

La auditoría también fomenta la educación en seguridad informática, sensibilizando a los usuarios sobre la importancia de seguir buenas prácticas en la protección de datos y activos tecnológicos. Esto no solo prepara a los estudiantes para entornos laborales más exigentes, sino que también contribuye al desarrollo de ciudadanos responsables y conscientes de los desafíos de la era digital. En conjunto, estos impactos fortalecen el papel de la institución como un referente en educación tecnológica segura y sostenible.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

Las instituciones educativas en el país están en un proceso constante de innovación, siendo una de las más relevantes la incorporación de tecnologías y acceso a internet. Esto ha dado lugar a nuevas metodologías para integrar el uso de las TICS. Sin embargo, estas innovaciones también han traído consigo amenazas, tanto físicas como virtuales, ya que existen personas que intentan robar información como números de cuentas bancarias, dinero, direcciones, entre otros. Además, se han identificado problemas relacionados con la gestión de los activos electrónicos, lo que genera pérdidas o daños debido a errores en los procesos necesarios para mantener los equipos en óptimas condiciones, afectando la calidad de los laboratorios educativos. Por lo tanto, la implementación de medidas de seguridad resulta crucial, ya que estas ayudan a prevenir el robo de información, mantener los equipos en buen estado y asegurar un uso adecuado de los mismos.

La revisión preliminar de este estudio esta referida, por una parte, a la auditoría informática, donde se destaca su importancia en la integridad de los activos informáticos de las instituciones educativas; por otro lado, se considera que este tipo de auditoría influye en la seguridad física de los laboratorios. Por ello se presenta el siguiente estudio local de investigación:

Paladines (2023) realizó una investigación con el objetivo de elaborar un informe de auditoría para evaluar y verificar el cumplimiento de las normas de seguridad en la infraestructura tecnológica de la institución. Se realizó un diagnóstico interno para identificar los problemas, utilizando como técnicas de investigación la encuesta y la entrevista, las cuales fueron clave para la recopilación de información. Para este proceso, participaron 18 docentes, así como la máxima autoridad de la institución y la inspectora general. La propuesta consistió en realizar una auditoría de seguridad física al laboratorio de cómputo, aplicando la metodología MAGERIT. Esta metodología facilitó diversas etapas como la identificación de activos y amenazas, el diseño de instrumentos, la tabulación, el análisis de riesgos y la elaboración de la matriz de riesgos. Entre los resultados más relevantes, se determinó que el

nivel de seguridad es del 43%. Las principales vulnerabilidades encontradas fueron la exposición a los siguientes riesgos: 1) robo de información con un 95% de nivel de riesgo, 2) virus con un 83% de riesgo alto. Otros riesgos, como el robo, incendio, daños a equipos e inundación presentaron resultados mucho más bajos. Finalmente, se elaboró un informe de auditoría junto con una guía de recomendaciones que incluye los pasos necesarios para prevenir estos riesgos de seguridad informática.

Este estudio contribuye a la presente investigación con la elección de instrumentos, la propuesta y los resultados. Además, al ser un estudio local hace deducir que los resultados podrían ser similares y confiables

2.1.1 Diseño de una guía para la función de auditoría interna en las organizaciones de carácter empresarial de la ciudad de Sucre

El presente trabajo tiene como objetivo abordar un aspecto fundamental dentro de las organizaciones empresariales del departamento de Sucre: la función de la Auditoría Interna. En el contexto actual, caracterizado por constantes cambios y transformaciones en el entorno empresarial, se hace cada vez más necesaria la implementación de mecanismos eficaces de supervisión y control. Esta realidad plantea la necesidad de un mayor monitoreo dentro de las organizaciones, siendo la Auditoría Interna una herramienta clave para responder a dicha exigencia.

En este sentido, se llevó a cabo una investigación enfocada en analizar la aplicación de prácticas internacionales en el ejercicio de la función de Auditoría Interna. La investigación incluyó un diagnóstico sobre cómo esta función evalúa actualmente la gestión de riesgos, el sistema de control interno, y el seguimiento de las acciones correctivas o preventivas que se acuerdan con la organización. Todo ello con el fin de identificar fortalezas, debilidades y oportunidades de mejora en el desempeño de la Auditoría Interna como soporte estratégico para la toma de decisiones y la sostenibilidad empresarial. (Gutierrez, 2019)

2.1.2 Auditoría informática dentro de la empresa “Promaelec” de la ciudad de Quevedo, en tiempo de COVID-19

Durante la pandemia, las Pymes se vieron obligadas a adaptarse, evidenciando la necesidad de innovar. Esta investigación se desarrolló en la empresa PROMAELEC de Quevedo, mediante una auditoría informática realizada en el contexto del COVID-19. El estudio permitió conocer la situación actual de sus sistemas informáticos y aplicar metodologías que facilitaron la identificación de problemas. A partir de ello, se propuso una mejora en los procesos, fortaleciendo la gestión administrativa de forma automatizada. (Albarracín Zambrano, Marín Vilela, Lozada Calle, & Martínez Matute, 2021)

2.1.3 El rol de la auditoría informática en la era de la protección de datos personales en Ecuador

La auditoría informática es un proceso clave de control que evalúa la integridad, seguridad y eficiencia de los sistemas informáticos en instituciones públicas y privadas. Va más allá del enfoque financiero tradicional, incorporando análisis de riesgos, controles internos y cumplimiento normativo. Su importancia se relaciona con la protección de los recursos digitales y la gestión eficiente de la información. Esta investigación también analizó los cambios en la auditoría informática tras la implementación de la Ley de Protección de Datos en Ecuador. (Lucero, 2023)

2.1.4 Estrategias de IA aplicada a la auditoria informática

La auditoría de TI ha superado conceptos erróneos y se ha convertido en una herramienta clave para la gestión de riesgos y la protección de información en entornos digitales. Actualmente, se promueve el uso de inteligencia artificial para optimizar el proceso de auditoría, mediante el análisis de grandes volúmenes de datos y la automatización de tareas. Esto mejora la eficiencia, fortalece los controles internos y aumenta la seguridad de los activos digitales. La investigación explora cómo la IA puede transformar las recomendaciones de TI, generando más precisas. (Reyes, 2023)

2.1.5 Escalabilidad y Sostenibilidad en Implementaciones de Blockchain para Auditoría Informática: Retos y Soluciones Futuras

El artículo analiza la escalabilidad y sostenibilidad en la implementación de blockchain aplicada a la auditoría informática. Se consideran aspectos como el rendimiento, la capacidad de procesamiento y las diferencias entre tipos de blockchain. También se abordan las dimensiones económica, ambiental y social de la sostenibilidad, con énfasis en el consumo energético y la inclusión tecnológica. La propuesta incluye una revisión de retos y soluciones para una implementación eficiente. Esto contribuye a fortalecer el uso responsable y efectivo de blockchain en auditoría. (Pinto, 2023)

2.2 Definiciones conceptuales

2.2.1 Auditoría informática

La auditoría informática surge con la incorporación de computadoras y sistemas de información en sectores institucionales, médicos, financieros, entre otros, donde el uso de tecnologías automatizadas se volvió esencial. Estos sistemas permiten el registro continuo y ágil de las actividades diarias, así como el almacenamiento seguro de información relevante. Su propósito principal es garantizar la integridad de los datos y facilitar futuras revisiones legales. La auditoría informática asegura que estos procesos tecnológicos cumplan con los estándares requeridos. Así, se convierte en un soporte clave para la transparencia y el control organizacional. (Robalino, Yanza Chávez, & Montoya Lunavictoria, 2022)

Este trabajo realizó una revisión teórica sobre normas y estándares internacionales aplicados a auditorías informáticas, destacando su relevancia en la seguridad informática. Con un enfoque cualitativo y exploratorio, se analizaron fuentes académicas de alto impacto y estudios recientes. La investigación evidenció que la auditoría informática es clave para generar transparencia y confianza en el entorno digital. Asimismo, se concluyó que la implementación de normas y estándares es esencial para proteger los activos informáticos y mejorar la gestión de riesgos. Estos marcos proporcionan estructuras sólidas para enfrentar desafíos de seguridad actuales. (Minaya Macias, Minaya Macias, Intriago Navarrete, & Intriago Navarrete, 2023)

La auditoría informática es un proceso sistemático que tiene como objetivo evaluar y verificar los controles, políticas y procedimientos implementados en los sistemas de

información de una organización. Su propósito fundamental es asegurar la integridad, confidencialidad y disponibilidad de los activos informáticos.

De acuerdo con Hurtado (2021), la auditoría informática se divide en dos grandes dimensiones:

- **Seguridad Lógica:** abarca la protección del software, datos y redes mediante controles digitales.
- **Seguridad Física:** se enfoca en la protección de los activos tangibles y la infraestructura física.

La seguridad física es un pilar esencial dentro del marco general de la seguridad informática, ya que garantiza que los sistemas estén protegidos contra accesos no autorizados, daños intencionados o accidentales y desastres ambientales. Esta forma de seguridad incluye medidas como el control de acceso a las instalaciones, la vigilancia mediante cámaras, alarmas y sistemas de detección de intrusos.

El artículo propone estrategias de auditoría informática adaptadas al contexto de la transformación digital. A través de una revisión bibliográfica, se identificaron marcos normativos clave como ISO/IEC 27000, ITIL, COBIT y PCI DSS, fundamentales para proteger la información. Las estrategias incluyen la evaluación continua de riesgos, auditorías periódicas y cumplimiento normativo. También se promueve la mejora continua para enfrentar los desafíos tecnológicos emergentes. Estas prácticas fortalecen la seguridad y preparan a las organizaciones para un entorno digital dinámico. (Angamarca, Estrategias de auditoría informática en la era de la transformación digital, 2022)

Según Gutiérrez y Márquez (2020), la omisión de controles físicos puede vulnerar los sistemas informáticos, incluso si la seguridad lógica está implementada de manera rigurosa. Por tanto, resulta imperativo aplicar auditorías periódicas que verifiquen la eficacia de las medidas físicas implementadas. Estas auditorías permiten identificar debilidades en la infraestructura y tomar acciones correctivas antes de que ocurran incidentes.

2.2.1.1 Historia y evolución de la auditoría informática

La auditoría informática tiene sus orígenes en la década de 1960, cuando las organizaciones comenzaron a adoptar sistemas computarizados para manejar grandes volúmenes de datos. Inicialmente, estas auditorías estaban centradas en verificar la precisión de los procesos de cálculo y el funcionamiento adecuado de las computadoras. Sin embargo, con la proliferación de redes, sistemas distribuidos y amenazas cibernéticas, la auditoría informática evolucionó para abordar un espectro más amplio de riesgos y controles. Según (Singleton, 2018), esta transformación ha sido clave para adaptar la auditoría a los nuevos desafíos tecnológicos y de seguridad.

Hitos importantes en su evolución incluyen:

- El desarrollo de normas internacionales como COBIT (Control Objectives for Information and Related Technology) en los años 90.
- La introducción de marcos de cumplimiento como la Ley Sarbanes-Oxley en 2002, que subrayó la importancia de las auditorías en TI para la transparencia financiera (Gallego & Luna, 2020).
- La integración de principios de ciberseguridad en las auditorías informáticas modernas (ISACA, 2023).

2.2.1.2 Objetivos de la Auditoría Informática

Los principales objetivos de la auditoría informática incluyen:

- Garantizar la Seguridad de la Información: Verificar que los sistemas implementen controles adecuados para proteger los datos contra accesos no autorizados, alteraciones o destrucción (Whitman & Mattord, 2021).
- Evaluar el Cumplimiento Normativo: Asegurar que los sistemas cumplen con leyes, regulaciones y estándares internacionales aplicables, como ISO/IEC 27001.
- Optimizar los Recursos Tecnológicos: Identificar ineficiencias y oportunidades de mejora en el uso de la infraestructura tecnológica (Gallego & Luna, 2020).
- Mitigar Riesgos: Analizar los riesgos asociados a las TI y proponer medidas para minimizarlos.

- Aumentar la Confiabilidad del Sistema: Garantizar que los sistemas operen según los niveles esperados de confiabilidad y disponibilidad (Reynolds, 2021).

2.2.1.3 Áreas de aplicación

La auditoría informática tiene un alcance amplio dentro de las organizaciones, ya que no solo se limita a la revisión técnica de los sistemas, sino que también evalúa aspectos estratégicos y operativos. Su enfoque incluye la verificación de la integridad de los datos, la eficiencia de los procesos informáticos, el cumplimiento de las políticas de seguridad, la gestión de riesgos tecnológicos y la protección de los activos digitales. Además, permite identificar vulnerabilidades, optimizar recursos y fortalecer el control interno, contribuyendo así a una mejor toma de decisiones y al logro de los objetivos institucionales.

- **Infraestructura Tecnológica**

La auditoría de la infraestructura tecnológica implica la revisión de todos los componentes físicos y virtuales que soportan los sistemas de información de una organización. Esto incluye servidores, redes, dispositivos de almacenamiento, centros de datos y equipos terminales. El objetivo principal es garantizar la disponibilidad, integridad y seguridad de los recursos tecnológicos mediante:

- Evaluaciones de capacidad y rendimiento de hardware y redes.
- Inspecciones de vulnerabilidades en configuraciones de sistemas y dispositivos.
- Verificación de redundancia, respaldo y planes de recuperación ante desastres.

- **Sistemas de Gestión**

Los sistemas de gestión, como ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) y otros softwares empresariales, son auditados para garantizar su correcta operación y la exactitud de los datos que procesan. La auditoría en esta área incluye la evaluación de la integridad de los datos, la revisión de controles de acceso y la verificación del cumplimiento de procesos definidos. También se analiza la trazabilidad de la información, la automatización de tareas clave y la protección frente a posibles brechas de seguridad. Estas acciones permiten asegurar que el sistema funcione de manera eficiente y contribuya a la toma de decisiones estratégicas dentro de la organización.

- **Ciberseguridad**

La auditoría en ciberseguridad se centra en la identificación y mitigación de amenazas digitales que puedan comprometer los sistemas y la información crítica de la organización. Incluye la evaluación de políticas de seguridad, análisis de vulnerabilidades, pruebas de penetración y revisión de configuraciones de red y sistemas. Además, verifique la eficacia de los controles de acceso, la gestión de incidentes y la protección frente a malware y ataques externos. Estas auditorías ayudan a fortalecer la postura de seguridad, garantizar la continuidad del negocio y cumplir con las normativas vigentes.

- **Procesos de TI**

La auditoría de procesos de TI abarca análisis exhaustivo de las prácticas, políticas y procedimientos relacionados con la gestión tecnológica dentro de una organización, con el objetivo de asegurar que estos se alineen con los estándares de calidad, eficiencia y seguridad operativa establecidos. Esta auditoría incluye

- Ciclo de vida del desarrollo de software (SDLC).
- Gestión de cambios y configuraciones en sistemas.
- Eficiencia de los planes de contingencia y recuperación ante desastres.
- Evaluación de procesos de mantenimiento y soporte técnico.

2.2.1.4 Fases de la auditoría informática

El proceso de auditoría informática generalmente sigue las siguientes etapasplanificación, en la cual se define el alcance, los objetivos y los recursos necesarios para la auditoría; evaluación preliminar, donde se recopila información general sobre el entorno tecnológico de la organización; ejecución, que implica la recolección y análisis de evidencias mediante pruebas, entrevistas y revisión de documentación; y finalmente, la etapa de informe, en la que se presentan los hallazgos, conclusiones y recomendaciones para mejorar los controles y la seguridad de los sistemas auditados. Este proceso garantiza una revisión estructurada y efectiva del entorno informático. (Whitman & Mattord, 2021):

a) **Planificación:**

En esta etapa se definen claramente los objetivos, el alcance y la metodología que guiará la auditoría informática, estableciendo el marco de trabajo para todo el proceso. Se identifican los riesgos clave asociados al entorno tecnológico y se determinan los recursos humanos, técnicos y documentales que serán necesarios. Además, se elaboran cronogramas y se asignan responsabilidades específicas para cada fase. Esta fase es fundamental para asegurar una auditoría eficaz y bien estructurada.

b) Recopilación de Datos:

Se lleva a cabo la recolección de información mediante entrevistas al personal clave, inspección de documentación relevante y ejecución de pruebas técnicas sobre los sistemas. También se emplean herramientas automatizadas que facilitan el análisis masivo de datos, permitiendo detectar irregularidades o desviaciones respecto a los controles establecidos. Esta etapa busca obtener evidencias objetivas y suficientes que respalden las evaluaciones posteriores. La calidad de esta información es esencial para la precisión de los hallazgos.

c) Evaluación de Controles:

Durante esta fase se prueban tanto los controles generales como los específicos que han sido implementados en los sistemas y procesos de la organización. La auditoría abarca controles lógicos, físicos y administrativos, verificando su efectividad frente a riesgos tecnológicos y operativos. Se analiza si estos controles están adecuadamente diseñados, documentados y operativos en la práctica. Este análisis permite identificar debilidades y proponer mejoras en la gestión de la seguridad informática.

d) Informe Final:

En la etapa final, se presentan los resultados de la auditoría en un informe estructurado que incluye hallazgos, conclusiones y recomendaciones prácticas. Este documento detalla los riesgos identificados, el impacto potencial y las áreas críticas que requieren atención. Asimismo, se diseña un plan de acción correctiva que la organización pueda implementar para fortalecer sus controles y sistemas. El informe es una herramienta clave para la toma de decisiones estratégicas y para el cumplimiento de normativas vigentes.

2.2.1.5 Herramientas de auditoría informática

La auditoría informática generalmente cuenta con las siguientes herramientas como software de escaneo de vulnerabilidades, analizadores de logs, sistemas de detección de intrusos (IDS) y aplicaciones para pruebas de penetración. Estas herramientas permiten identificar fallas de seguridad, monitorear actividades sospechosas y evaluar la configuración de los sistemas. También se utilizan plataformas de gestión de auditorías que ayudan a documentar hallazgos y automatizar procesos. Todas estas tecnologías fortalecen la precisión y eficiencia del proceso de auditoría (Whitman & Mattord, 2021):

- **Herramientas de Escaneo de Vulnerabilidades**

Nessus: Herramienta que permite identificar y clasificar vulnerabilidades en sistemas y redes, proporcionando informes detallados sobre los riesgos detectados.

Qualys: Plataforma de seguridad en la nube que automatiza el escaneo y la evaluación de vulnerabilidades en tiempo real.

- **Sistemas de Análisis de Registros**

Splunk: Software que recopila, analiza y monitoriza registros (logs) en tiempo real para detectar anomalías y generar alertas de seguridad.

ELK Stack (Elasticsearch, Logstash, Kibana): Conjunto de herramientas de código abierto que permiten la recopilación, procesamiento y visualización de datos log en grandes volúmenes.

- **Simuladores de Ataques**

Metasploit: Framework utilizado para realizar pruebas de penetración simulando ciberataques con el fin de evaluar la resistencia de los sistemas.

Burp Suite: Herramienta que permite identificar vulnerabilidades en aplicaciones web mediante pruebas de seguridad, como ataques de inyección y análisis de tráfico HTTP.

- **Herramientas de Gestión de Cumplimiento**

SolarWinds: Proporciona soluciones de monitoreo y control para asegurar el cumplimiento de políticas y estándares.

Open-Audit: Herramienta que realiza inventarios de hardware y software, facilitando la auditoría del cumplimiento normativo.

2.2.2 Seguridad física

La seguridad física abarca todas las medidas de protección y control que se aplican sobre los recursos tangibles de una organización, como edificios, equipamientos y sistemas críticos. ISO/IEC 27001 (Organización Internacional de Normalización, 2022) define la seguridad física como la implementación de controles que eviten accesos no autorizados, daños físicos o interrupciones accidentales en los activos informáticos.

Las principales características de la seguridad física incluyen:

a) **Protección del acceso:** mecanismos de control que restringen la entrada física a áreas sensibles.
b) **Protección ambiental:** medidas para mitigar riesgos asociados a desastres naturales, incendios, inundaciones, entre otros.
c) **Control de infraestructura:** aseguramiento de la integridad de cableado, sistemas eléctricos y dispositivos físicos.
d) **Vigilancia y monitoreo:** uso de tecnologías como cámaras de seguridad, alarmas y sistemas de detección.

De acuerdo con Pérez (2019), estas características deben ser evaluadas de manera constante mediante auditorías para garantizar su efectividad frente a las amenazas emergentes. Este enfoque permite detectar debilidades antes de que sean explotadas y aplicar medidas correctivas oportunamente. Además, fomenta una cultura de mejora continua en la gestión de la seguridad informática dentro de la organización.

2.2.2.1 Importancia de la Seguridad Física en Laboratorios de Computación

Los laboratorios de computación representan espacios críticos en instituciones educativas, corporaciones y centros de investigación. En estos entornos, se concentran recursos tecnológicos esenciales para las operaciones diarias, tales como servidores, estaciones de trabajo, dispositivos de red y equipos periféricos.

La importancia de la seguridad física en estos entornos radica en los siguientes puntos clave:

- Protección del patrimonio: prevención de robos o daños a los equipos.
- Garantía de continuidad operativa: mitigación de interrupciones que puedan afectar las actividades académicas o laborales.
- Seguridad de la información: protección de datos sensibles almacenados en los sistemas informáticos.
- Cumplimiento de normativas: alineación con estándares y regulaciones de seguridad.

Según Martínez (2020), un laboratorio de computación sin controles físicos adecuados está expuesto a riesgos como:

- Accesos no autorizados: entrada de individuos sin permiso.
- Robo de equipos: extracción de dispositivos que contienen información valiosa.
- Daños accidentales: caídas de equipos, derrames de líquidos o fallos eléctricos.
- Daños ambientales: afectaciones por incendios, inundaciones o variaciones de temperatura.

2.2.2.2 La auditoría de seguridad física

La auditoría de seguridad física es un proceso metodológico que tiene como objetivo evaluar la eficacia de los controles implementados para proteger los activos tangibles de una organización. Según López y Ramírez (2021), el proceso de auditoría debe ser sistemático, estructurado y basado en marcos de referencia reconocidos, como ISO/IEC 27001 o COBIT 2019.

2.2.2.3 Fases de la auditoría de seguridad física

El proceso de auditoría consta de las siguientes fases:

- **Planificación:**
  - Definición de objetivos y alcance.
  - Identificación de recursos y herramientas a utilizar.
- **Ejecución:**
  - Evaluación de controles físicos existentes.
  - Inspecciones visuales y pruebas de acceso.
- **Análisis de hallazgos:**
  - Identificación de brechas y vulnerabilidades.
  - Clasificación de riesgos según su nivel de impacto.
- **Informe de resultados:**
  - Documentación de hallazgos y recomendaciones.
  - Propuesta de mejoras basadas en estándares internacionales.

2.2.2.4 Herramientas y métodos utilizados

Las herramientas utilizadas en una auditoría de seguridad física incluyen:

- **Listas de verificación:** guías para evaluar los controles existentes.
- **Sistemas de monitoreo:** revisión de grabaciones de cámaras de seguridad.
- **Pruebas de penetración física:** simulación de accesos no autorizados.
- **Encuestas y entrevistas:** recopilación de información sobre el conocimiento del personal.

De acuerdo con Gómez (2018), la combinación de estas herramientas proporciona una visión integral sobre la seguridad física. Esto permite identificar posibles vulnerabilidades en el entorno físico que podrían afectar la infraestructura tecnológica. Asimismo, facilita la toma

de decisiones informadas para fortalecer los controles y proteger los activos críticos de la organización.

2.2.2.5 Beneficios de la auditoría de seguridad física en laboratorios de computo

Realizar una auditoría periódica proporciona los siguientes beneficios:

- Identificación y mitigación de vulnerabilidades.
- Aseguramiento de la continuidad operativa.
- Cumplimiento de regulaciones y estándares.
- Reducción de riesgos de robo o daños accidentales.
- Mejora continua de las políticas de seguridad.

De acuerdo con Castro (2022), la auditoría contribuye a una gestión proactiva de los riesgos físicos y a la protección de los activos informáticos críticos. Esta práctica permite anticiparse a posibles incidentes mediante la identificación temprana de amenazas y vulnerabilidades. Además, refuerza la implementación de controles preventivos que aseguran la continuidad operativa y la integridad de los recursos tecnológicos.

2.2.2.6 Metodología MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología desarrollada por el Gobierno de España, específicamente por el *Centro Criptológico Nacional (CCN)*, con el propósito de ayudar a las organizaciones a identificar, evaluar y gestionar los riesgos que podrían afectar la seguridad de los sistemas de información. Esta herramienta está orientada a la protección tanto de los activos informáticos como de la información contenida en ellos, permitiendo gestionar los riesgos asociados a los sistemas de manera estructurada y efectiva.

Según la Guía MAGERIT del CCN (2020), esta metodología se aplica tanto a riesgos derivados de amenazas informáticas como de otros tipos de amenazas físicas, sociales y ambientales. En el contexto de una auditoría de seguridad física, MAGERIT es una herramienta clave para evaluar los riesgos relacionados con la infraestructura física de los sistemas de información, como los equipos, las redes, y el entorno en el que se encuentran.

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una herramienta desarrollada para identificar, analizar y gestionar los riesgos que afectan a los sistemas de información. Su enfoque permite evaluar tanto los activos como las amenazas y vulnerabilidades, estableciendo medidas de protección adecuadas. MAGERIT facilita la toma de decisiones en materia de seguridad mediante un análisis estructurado y sistemático. Es ampliamente utilizada en auditorías informáticas por su capacidad de alinear la gestión de riesgos con los objetivos organizacionales. Su aplicación contribuye a mejorar la seguridad y continuidad de los servicios tecnológicos. (Balverdi Cruz, Linares Fernández, & Cuellar, 2023)

Se aplicó la metodología MAGERIT para identificar y clasificar amenazas, vulnerabilidades y riesgos asociados a los activos críticos en sectores como gobierno, salud y energía. Las amenazas fueron organizadas según su origen: errores humanos, fallos técnicos, ataques deliberados y desastres naturales. La evaluación consideró el impacto en la confidencialidad, integridad y disponibilidad de la información. También se estimó la probabilidad de ocurrencia para calcular el nivel de riesgo. Los datos personales, financieros y clínicos, así como la información gubernamental, fueron identificados como los activos más vulnerables. (Guamán, Carrillo Zenteno, Flores Urgilés, Flores Urgilés, & Egas, ProSciences, 2023)

2.2.2.7 Objetivos de MAGERIT

La investigación propuso un modelo de gestión de riesgos de la información, basado en la metodología MAGERIT, enfocado en su aplicación en notarías de la Región Lima. Se utilizó un enfoque cualitativo con diseño de investigación-acción y técnicas como entrevistas, observación y análisis documental. El objetivo fue fortalecer la seguridad de los sistemas de información notariales a través de una gestión estructurada de riesgos. MAGERIT demostró ser una herramienta efectiva para identificar, analizar y tratar amenazas, reflejándose en un plan de seguridad integral. Esto permite garantizar la continuidad de los procesos y proteger la información sensible manejada por las notarías. (Ampuero Herrera, 2021)

El objetivo principal de MAGERIT es proporcionar un marco metodológico para evaluar los riesgos, basándose en un análisis detallado que permita identificar las amenazas y vulnerabilidades asociadas a los activos tecnológicos. A través de este análisis, se busca

implementar medidas correctivas y preventivas que permitan mitigar los riesgos y mejorar la seguridad de los sistemas informáticos. En términos específicos, MAGERIT tiene los siguientes objetivos:

- **Identificar activos y recursos:** Establecer y clasificar los elementos que componen los sistemas de información, como servidores, redes, bases de datos y dispositivos.
- **Evaluar amenazas y vulnerabilidades:** Determinar los factores de riesgo que podrían comprometer la seguridad de los sistemas, tanto desde el ámbito tecnológico como desde el físico.
- **Evaluar impactos:** Analizar los posibles efectos que una amenaza podría tener sobre los activos, incluyendo consecuencias operativas, económicas, legales y reputacionales.
- **Determinar la probabilidad de riesgos:** Establecer la probabilidad de que una amenaza se materialice en función de las vulnerabilidades existentes.
- **Proponer medidas de mitigación:** Diseñar estrategias y controles para reducir los riesgos identificados a niveles aceptables.

2.2.2.8 Fase 1: Definición del Alcance

En esta fase, se determina el ámbito de la auditoría, identificando los sistemas, activos y procesos que serán evaluados. Esto incluye la clasificación de los activos informáticos y físicos dentro del laboratorio de computación, como los servidores, estaciones de trabajo, redes, equipos de respaldo, sistemas de control de acceso, etc. Es fundamental que esta fase esté claramente definida, ya que el alcance determinará el tipo de riesgos que se evaluarán.

2.2.2.9 Fase 2: Identificación de Activos y Recursos

Aquí se realiza un inventario detallado de los activos implicados en el laboratorio de computación, diferenciando entre activos de información (bases de datos, documentos electrónicos, etc.) y activos físicos (equipos, instalaciones, infraestructura). Esta fase también incluye la identificación de las personas o grupos responsables de cada activo, lo que facilita la evaluación de las amenazas que podrían afectar a cada uno.

2.2.2.10 Fase 3: Identificación de Amenazas y Vulnerabilidades

En esta fase se identifican las amenazas externas e internas que podrían afectar a los activos del laboratorio de computación. Las amenazas pueden ser de origen físico (robo, incendio, inundación) o virtual (ataques cibernéticos, malware, acceso no autorizado). A su vez, se deben evaluar las vulnerabilidades, como la falta de controles físicos (por ejemplo, acceso sin restricciones al laboratorio), defectos en las instalaciones o equipos obsoletos.

2.2.2.11 Fase 4: Evaluación de Impactos

Se realiza una valoración del impacto que tendría la materialización de una amenaza sobre cada activo. Este impacto se evalúa en términos de confidencialidad, integridad y disponibilidad de la información. También se toman en cuenta aspectos como la reputación de la institución y el cumplimiento normativo. En el caso de los laboratorios de computación, el impacto de una posible pérdida de datos o de un robo de equipos sería crítico, por lo que esta fase es fundamental para priorizar los riesgos.

2.2.2.12 Fase 5: Evaluación de Probabilidades

Se evalúa la probabilidad de que las amenazas identificadas se materialicen, basándose en la experiencia, el historial de incidentes anteriores y las características del entorno. Para cada riesgo, se calcula una probabilidad que servirá para calcular la gravedad del riesgo. En un laboratorio de computación, la probabilidad de amenazas físicas como el robo podría ser más alta si no se cuentan con las medidas de seguridad adecuadas.

2.2.2.13 Fase 6: Establecimiento de Medidas de Control

Una vez evaluados los riesgos, se proponen medidas de control para reducir tanto la probabilidad de que los riesgos se materialicen como su impacto. Esto puede incluir la implementación de medidas de seguridad física como cámaras de vigilancia, controles de acceso, alarmas, protección ante incendios y otros sistemas de protección.

2.2.2.14 Fase 7: Monitorización y Revisión

La última fase consiste en la monitorización continua de los riesgos identificados y la revisión periódica de las medidas de control implementadas. Este proceso permite ajustar y mejorar las medidas de seguridad en función de los cambios en el entorno tecnológico y físico del laboratorio.

2.2.2.15 Beneficios de Utilizar MAGERIT en Auditorías de Seguridad Física

El uso de la metodología MAGERIT en auditorías físicas permite identificar y evaluar de forma estructurada los activos críticos de una organización, determinando su nivel de riesgo frente a diversas amenazas. Este enfoque facilita la implementación de salvaguardas específicas que fortalecen la protección de equipos e infraestructura tecnológica. Además, permite priorizar acciones según el impacto y la probabilidad de ocurrencia, optimizando los recursos disponibles. MAGERIT contribuye a diseñar planes de contingencia eficaces, asegurando la continuidad operativa ante eventualidades. En consecuencia, mejora la capacidad de respuesta y recuperación en entornos físicos vulnerables. (Morillo Cadena, 2024)

La metodología MAGERIT ofrece varios beneficios cuando se aplica en auditorías de seguridad física, especialmente en entornos educativos como los laboratorios de computación:

- **Identificación de riesgos sistemática:** Permite realizar un análisis exhaustivo de los riesgos físicos y cibernéticos, asegurando que no se pase por alto ninguna amenaza importante.
- **Mejora de la protección de activos:** A través de la evaluación detallada de vulnerabilidades, MAGERIT ayuda a establecer las medidas adecuadas para proteger los equipos y la información.
- **Priorización de recursos:** Al evaluar el impacto y la probabilidad de los riesgos, se pueden asignar recursos de manera más efectiva para mitigar los riesgos más críticos.
- **Cumplimiento normativo:** MAGERIT ayuda a garantizar que los sistemas de información cumplan con las normativas de seguridad, lo que es crucial en el entorno educativo y empresarial.

El uso de MAGERIT en auditorías de seguridad física ofrece un enfoque estructurado y metodológico para identificar, analizar y gestionar riesgos relacionados con los activos tecnológicos. Su aplicación permite evaluar el impacto y la probabilidad de amenazas específicas, facilitando la toma de decisiones informadas para implementar medidas de seguridad efectivas. Además, al ser una metodología basada en estándares internacionales, MAGERIT asegura que los procesos y resultados sean consistentes, auditables y alineados con las mejores prácticas en gestión de riesgos.

Otro beneficio importante es que MAGERIT promueve la optimización de recursos, permitiendo priorizar las acciones correctivas según su criticidad y costo-beneficio. Esto no solo mejora la eficiencia en la protección de los activos tecnológicos, sino que también refuerza la sostenibilidad de las medidas implementadas. Asimismo, al incluir una documentación detallada de los riesgos y controles, la metodología facilita la comunicación y sensibilización entre los miembros de la institución educativa, fomentando una cultura de seguridad integral.

2.3 Conclusiones del marco teórico

- La auditoría informática es una herramienta esencial para garantizar la seguridad, confiabilidad y eficiencia de los sistemas de información en un entorno tecnológico cada vez más complejo.
- A través del uso de metodologías rigurosas, herramientas especializadas y un enfoque basado en riesgos, las organizaciones pueden enfrentar los desafíos de la era digital con confianza.
- En este sentido se hace énfasis en que la auditoría de seguridad física en laboratorios de computación es un proceso esencial para garantizar la protección de los activos tangibles y asegurar la continuidad operativa.
- La implementación de controles basados en estándares internacionales y la realización de auditorías periódicas permiten identificar vulnerabilidades y establecer acciones correctivas de manera oportuna.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

En el capítulo que se presenta a continuación se observa los aspectos fundamentales en el diseño de la metodológico en la investigación realizada en la institución. Se abordan contenidos sobre los tipos de investigación que se utilizaron como lo son investigación bibliográfica, investigación descriptiva e investigación de campo.

Siguiendo la misma secuencia de contenidos de investigación, en el desarrollo de lo misma utilizando fuentes de información primarias y segundarias. Continuando con la implementación de estrategias operacionales basándonos en la recolección de datos en la población que se realizó la auditoria, técnica de muestreo, segmentación y tamaño de la muestra.

Se identificó el análisis de herramientas para la recolección de datos. Dentro de los instrumentos aplicados para la recolección de datos se tomó en cuenta la aplicación de entrevistas y encuestas, la entrevista se aplicó al director de la unidad educativa “Americano”, así como podemos identificar la presentación y descripción de los resultados obtenidos. Finalizando, reflejando las conclusiones para el marco investigativo.

3.2 Tipos de investigación

3.2.1 Investigación de enfoque mixto

La investigación es de enfoque mixto (cuali-cuantitativo), con un diseño no experimental, longitudinal, y de tipo descriptivo. Combina la revisión bibliográfica con el trabajo de campo, observando y analizando fenómenos en su contexto natural a lo largo del tiempo, sin manipular variables, con el objetivo de describir sus características y evolución (Sánchez & Mejias, 2022).

3.2.2 Investigación bibliográfica o documental

Para Pérez (2021), la investigación documental proporciona una introducción a los otros tipos de investigaciones, dado que se obtiene datos e información definiéndose, así como una primera etapa para la recolección en la búsqueda de (teorías, resultados, instrumentos y técnicas usadas) acerca del tema propuesto por el investigador y el problema que se propuso resolver mediante la investigación inicial.

Con el propósito de recolectar información confiable para la auditoria, se implementó este tipo de investigación para obtener material bibliográfico tanto de libros y revistas que contengan información que beneficie a los contenidos sobre la auditoria física, como para la fundamentación teórica de las variables propuestas en las hipótesis de la investigación.

3.2.3 Investigación de campo

Tipo de investigación en la que se efectúa la comprensión y resolución de situaciones o problemas en un ambiente determinado, trabajando en el entorno natural en el que se desarrollan como individuo o grupos donde forman parte las personas o fuentes consultadas. Siendo estas orientadas a descubrir interacciones y conflictos en estructuras sociales o laborales en aspectos como: sociológicas, psicológicas y educativas (Beltrán & Bernal, 2021).

Para la ejecución de este tipo de investigación es fundamental realizar la recolección y registro de manera ordenada para el análisis de los datos obtenidos, utilizando técnicas como encuestas, entrevistas o cuestionarios. En esta investigación de campo se aplicaron encuestas a 8 profesores de la institución, con el objetivo de conocer los riesgos que afectan a la institución. Además, se realizó una entrevista al rector y se documentaron las actividades de recolección en visitas realizadas durante dos fines de semana consecutivos. Esta información permitió obtener una visión clara de la problemática local.

3.2.4 Investigación descriptiva

Se utiliza para analizar en detalle cómo se observa el fenómeno, los componentes y como estos se desarrollan. Permitiendo así el estudio minucioso de cómo se manifiestan en un entorno y las interacciones o relaciones que manifiestan estos fenómenos. Identificando las características del fenómeno o universo que está siendo estudiado, como los patrones de

comportamientos y actitudes, dando especificaciones sobre comportamientos específicos, descubierto y verificado asociaciones entre variables de a la investigación. De acuerdo con los objetivos planteados, el investigador indica el tipo de descripción propuesto (Valle, 2022).

La investigación descriptiva se utilizó para describir la situación actual de la unidad educativa Americano por medio del uso de instrumentos de recolección como son: encuestas, entrevistas aparte de la observación que sirvió también como otro instrumento. Esto contribuirá significativamente a la investigación, ya que permite obtener información sobre las debilidades en cuanto a la seguridad física dentro de la institución.

3.3 Métodos de investigación

3.3.1 Analítico – Sintético

El método analítico sintético estudia los hechos, descomponiendo por partes para el estudio minucioso del objeto de manera individual; siendo esta parte el análisis, ya que cada uno de los componentes son estudiados de manera particular para comprender el comportamiento y establecer teorías a partir de lo analizado. En cuanto al método sintético se comprende que este implica la síntesis, ya que va de lo abstracto a lo sintético siendo así la complementación de elementos abstractos a lo real y concreto (Herszenbaun, 2022).

En este caso la unión de estos dos métodos brinda ayuda en la identificación de distintos elementos que componen el fenómeno u objeto estudiado, las causas, efectos, la finalidad del establecimiento de parámetros posibilitando examinar el comportamiento de los estudiantes de la institución y de los docentes encargados de los laboratorios. Desglosando todo el proceso en sus partes, características, relaciones, propiedades y componentes para lograr un análisis más preciso y estructurado.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias y secundarias

En la elaboración del presente trabajo, se emplearon varias fuentes de información como: encuestas, entrevistas, cuestionarios, dado la naturaleza de estas herramientas implementadas de forma presencial, oral o escrita. Brindándole al entrevistador recopilar información directamente del entrevistado, evitando así obtener respuestas ambiguas. Tal como

otras fuentes empleadas como: libros, revistas, fuentes bibliografías o publicaciones académicas en la investigación, las cuales son de origen secundario.

3.4.2 Fuente primaria: Entrevista

Para Martínez (2022), la entrevista consiste en la interacción entre dos personas, es decir, el entrevistador y el entrevistado. El primero realiza la indagación de las preguntas al segundo de forma que se complementan ambas dinámicas para avanzar con la investigación, permitiendo a la entrevista actuar como un filtro e instrumento con el que se logra obtener información sobre el mundo interior del entrevistado o su percepción del fenómeno que se investiga a través de varias preguntas.

Partiendo de este contexto, se empleó la técnica de la entrevista para obtener información por parte del rector de la institución educativa. En primera instancia, se formularon 11 preguntas enfocadas en la seguridad física de los equipos informáticos, orientadas a detectar posibles riesgos. Dichas preguntas fueron dirigidas al rector con el propósito de recolectar datos sobre el estado actual y las amenazas que podrían comprometer la seguridad en la institución.

3.4.3 Fuente secundaria: Encuesta

Para López (2021), la encuesta es una de las herramientas más utilizadas en la recolección de datos en la investigación cualitativa, permitiendo obtener datos por medio de un cuestionario que se aplica a un grupo objetivo de la población, con el objetivo de indagar a los sujetos de estudio.

En base a este pensamiento, se aplicó la técnica de la encuesta al personal docente que realiza actividades en el laboratorio de la Unidad Educativa Americano. Se diseñaron 10 preguntas, con el fin de identificar posibles riesgos. Estas encuestas fueron dirigidas a los docentes de la institución, incluyendo al responsable del área de laboratorios, con el objetivo de recopilar información sobre el estado de las instalaciones y las amenazas que podrían afectar la seguridad institucional.

3.5 Estrategia operacional para la recolección de datos

Responsable	Actividad	Dirigido	Fecha

Cevallos Bravo Karen Mishelle	Entrevista	Rector de la institución Cristóbal Tobar	09/10/2024
	Encuesta	Docentes de la institución	15/08/2024

Tabla 1 Estrategia operacional para la recolección de datos

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

3.5.1.1 Población

Según Veiga y Torres (2020), la población se define como un conjunto de personas, animales o cosas de la misma especie en donde se desea conocer algún acontecimiento o hecho que se encuentre en un momento y lugar determinado durante una investigación que se esté realizando a las personas que habitan en cierta área geográfica.

La Unidad Educativa Americano cuenta con un laboratorio informático disponible para el uso del personal docente y demás miembros de la institución. Esta investigación considera a todos los usuarios que participan en actividades dentro del laboratorio. Para la recolección de información, se empleó un muestreo aleatorio, lo que permitió seleccionar una muestra representativa dentro de un grupo reducido. La población estuvo conformada por un total de nueve personas: ocho docentes, incluyendo al encargado del laboratorio, y el rector de la institución. El propósito fue obtener opiniones y criterios del personal involucrado en relación con los parámetros de seguridad informática.

3.5.1.2 Muestra

La muestra o muestreo permite obtener datos estadísticos de una determinada población de estudio. En esta se selecciona una pequeña parte de la población a estudiar, cuya finalidad es tomar cada parte de los elementos de estudio para aplicarlos a un subconjunto de la población (García & Toribio, 2022).

En la presente investigación, se tomó una muestra basada en la población, empleando el método de muestreo aleatorio simple. Este tipo de muestreo se caracteriza en que cada elemento de la población tiene la misma probabilidad de ser seleccionado para formar parte de la muestra. Para ello, se censó la población y se asignó un número a cada grupo o individuo

estudiado; posteriormente, se eligió la muestra de manera aleatoria. La fórmula utilizada para calcular el tamaño de la muestra en poblaciones pequeñas es la siguiente:

$$n = \frac{N}{1 + (N-1) \cdot e^2}$$

Donde:

n = tamaño de la muestra

N = tamaño de la población (en este caso, 9 personas)

e = margen de error (se utilizó un 5%, es decir, e=0.05e=0.05)

Aplicando la fórmula:

$$n = \frac{9}{1 + (9-1) \cdot 0.05^2}$$

$$n = \frac{9}{1 + 8 \cdot 0.0025}$$

$$n = \frac{9}{1 + 0.02}$$

$$n = \frac{9}{1.02}$$

$$n \approx 8.82$$

Por lo tanto, el valor obtenido para el tamaño de la muestra es 9 personas (redondeado al número entero más cercano).

Distribución en los segmentos de la población:

Dado que la población está compuesta por 9 personas (8 docentes y el rector), la muestra incluye a todos los miembros de la población. Los segmentos de la población son los siguientes:

8 docentes, incluyendo al encargado del laboratorio.

1 rector.

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.5.2.1 Encuesta - Entrevista

3.5.2.1.1 Encuesta

En la presente investigación se les aplicó la encuesta a los docentes relacionados con el uso de los laboratorios de la institución, a través de preguntas cerradas y semiestructurada. fueron analizados en la herramienta de Office con el Excel para la elaboración de las gráficos y tablas, siendo empleada de manera anónima.

3.5.2.1.2 Entrevista

La entrevista se realizó al rector de la unidad educativa Americano, estructurada con preguntas abiertas con la finalidad de diagnosticar el estado de los equipos informáticos en base a parámetros de seguridad informática de los laboratorios de la institución. Se realizo de manera personalizada para asegurar la veracidad de la información obtenida, permitiendo argumentar sus respuestas e identificando áreas de mejora.

3.5.2.2 Estructura de los instrumentos de recolección de datos aplicados

La entrevista estuvo dirigida al Rector como parte de la muestra de la Unidad Educativa para la aplicación y obtención de datos recolectados. Estructurada por 13 preguntas con el objetivo de realizar un diagnóstico acerca de la situación actual de los laboratorios de la Unidad Educativa Americano. Se buscó identificar posibles riesgos y amenazas que pudieran afectar el correcto funcionamiento de los laboratorios.

La encuesta al igual que la entrevista fue realizada con el propósito de recolectar datos del manejo de los equipos del laboratorio de la institución para analizar la seguridad física, fue realizado a 8 docentes

3.5.3 Plan de recolección de datos

El presente estudio tuvo como plan de recolección de datos para la aplicación de auditoria informática de seguridad física del laboratorio de computación de la unidad educativa "Americano" analizando la infraestructura y los posibles riesgos que se dan en el laboratorio de la institución para emplear medidas para evitar riesgos en los equipos informáticos.

Fue aplicado por la investigadora en la semana 3 del mes de agosto 2024. Empleando instrumentos para la recolección de información como la encuesta y la entrevista, entrevista la cual fue realizada de forma directa, por otro lado, la encuesta fue de forma anónima a los usuarios que utilizan los equipos informáticos del laboratorio de la unidad educativa.

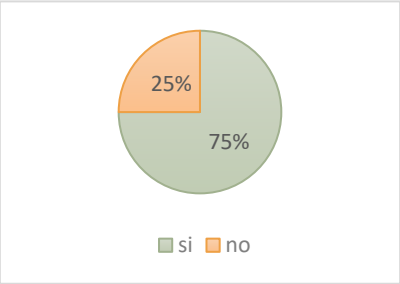
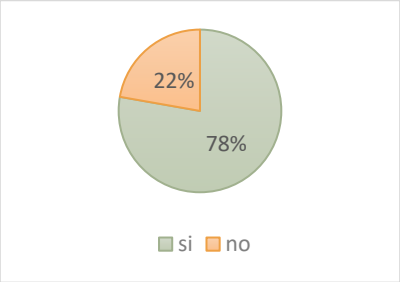
3.6 Análisis y presentación de resultados

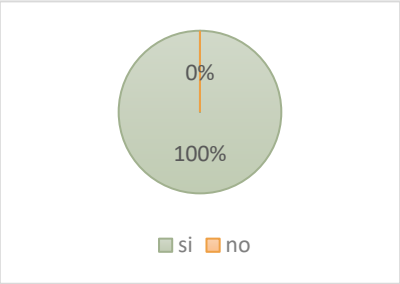
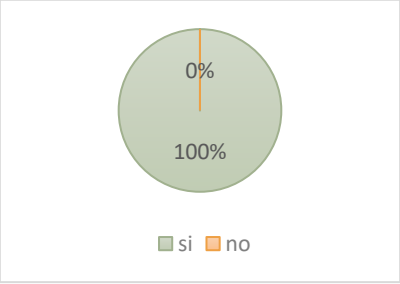
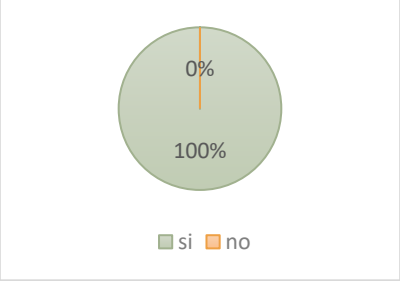
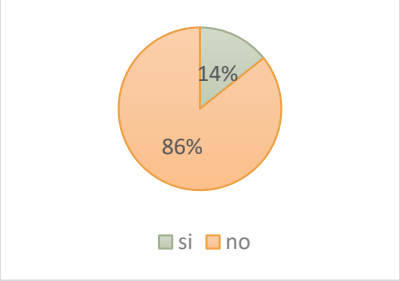
3.6.1 Tabulación y análisis de los datos de las encuestas realizadas

A continuación, se muestra el proceso de tabulación y análisis de los datos recolectados a través de las encuestas representa una etapa crucial en el desarrollo de la auditoría informática de seguridad física en la Unidad Educativa "Americano".

Esta fase tiene como propósito principal transformar los datos brutos en información útil y comprensible que permita identificar patrones, tendencias y áreas críticas relacionadas con la seguridad física del laboratorio de computación. La correcta organización y evaluación de estos datos facilita la generación de diagnósticos precisos y fundamentados que respaldan las conclusiones y recomendaciones del estudio.

Pregunta	Gráficos	Interpretación

1. ¿La institución cuenta con un departamento encargado a las tecnologías de la información?		La gráfica muestra que una parte considerable de los encuestados reconoce la existencia de un departamento encargado de las tecnologías de la información dentro de la institución. Esto sugiere que, en general, la comunidad educativa tiene conocimiento de una estructura organizada que gestiona y supervisa los recursos tecnológicos.
2. ¿Existen avisos que ayuden a prevenir desastres dentro de los centros informático la institución?		La gráfica muestra que una gran mayoría de los encuestados confirma la presencia de avisos destinados a prevenir desastres que puedan afectar a los componentes informáticos. Esto indica que la institución ha implementado medidas de prevención, lo que refleja una preocupación por la protección de los recursos tecnológicos.

3. ¿Se ha definido e informado a usted cuales son las sanciones de los usuarios por infringir las normas?		Todos los encuestados afirman ser conscientes de las sanciones impuestas en caso de incumplir las normas establecidas para el uso de los espacios informáticos.
4. ¿Se lleva un inventario de los dispositivos informáticos que posee la institución?		Los encuestados en su totalidad concuerdan que si se lleva un inventario de los dispositivos que posee la institución.
5. ¿Se realizan con frecuencia mantenimientos a los equipos informáticos del laboratorio de computación?		En su totalidad los encuestados aseguran que si se realizan mantenimiento a los equipos con frecuencia.
6. ¿El encargado del laboratorio de computación es alguien con preparación como técnico informático?		La mayoría de los encuestados consideran que la persona encargada del laboratorio no tiene una formación adecuada en tecnología informática.

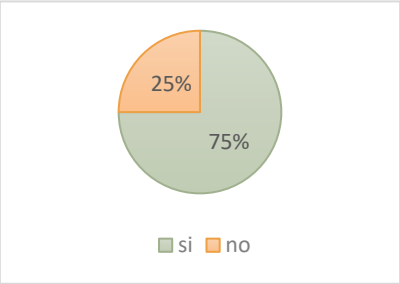
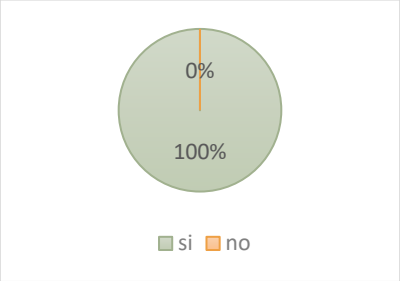
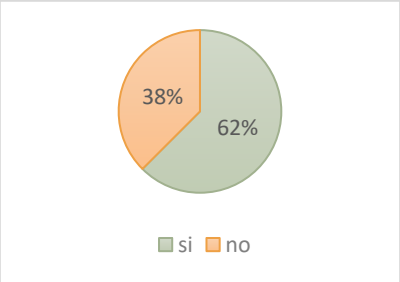
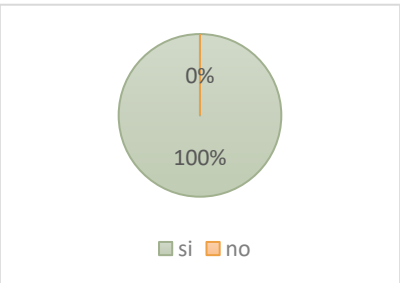
7. ¿Con frecuencia el responsable del laboratorio comprueba que los equipos procesen la información de forma adecuada?		La mayoría de los encuestados afirman que la persona encargada realiza una revisión adecuada del estado de los equipos.
8. ¿Cuándo usted accede al laboratorio el responsable le hace firmar en una lista de control de acceso?		En su totalidad aseguran firmar una lista para el control de acceso al laboratorio.
9. ¿Se ha socializado a los estudiantes las normas de uso para el laboratorio?		Un poco más de la mitad asegura que los estudiantes han recibido la socialización de normas para el uso del laboratorio.
10. ¿Para acceder a las instalaciones informáticas existe algún tipo de política para el acceso a las mismas?		En su totalidad se asegura que existen políticas para el acceso a la instalación informática.

Tabla 2
Tabulación y análisis de los datos de las encuestas realizadas

3.6.2 Presentación y análisis de datos de las entrevistas realizadas

Pregunta	**Respuesta**	**Interpretación**

1. ¿Existen registros del inventario que posee la unidad educativa en cuanto a equipos tecnológicos?	Si, la institución lleva un inventario de los equipos informáticos.	Si se cuenta con inventario de los dispositivos informáticos que posee el laboratorio de la institución.
2. ¿Se ha aplicado en los últimos 7 años una auditoria informática dentro de la institución?	No, no se ha realizado una auditoria informática en los últimos 7 años en la institución.	No se ha realizado un trabajo sobre auditoria durante el tiempo estimado en la institución.
3. ¿Qué orientaciones y / o capacitaciones ha recibido usted como directivo para proyectar con sus trabajadores acciones de seguridad informática en los laboratorios de computación?	En realidad, no se han recibido orientaciones a profundidad sobre el tema.	Solo se han recibido charlas sobre temas básicos con respecto a seguridad informática.
4. ¿Existe en la Unidad Educativa alguna estrategia para garantizar la seguridad en el laboratorio de computación?	No existen documentadas, pero se emplean medidas de seguridad para mantener seguro el laboratorio.	Solo se emplean estrategias de conocimiento general para garantizar el funcionamiento y cuidado de los equipos informáticos.
5. ¿Existen políticas relacionadas al ingreso y	No, no existen políticas para la seguridad	Solo se cuentan con medidas para prevenir,

salida de Hardware dentro de la institución, que aseguren la seguridad informática de los docentes?	informática de los docentes.	pero socializadas entre el personal, no existe una documentación al respecto para la seguridad informática de los docentes.
6. ¿Brindas cursos de capacitación a los docentes sobre seguridad informática?	No, solo se socializan medidas para evitar riesgos en la institución.	Solo socializaciones, pero no se habla a profundidad sobre la seguridad informática en sí.
7. ¿Sabe si existe personal que se encargue del departamento de tics en la unidad educativa?	Si, existe un encargado. Pero lo ejerce un docente de la institución.	Se cuenta con alguien al cuidado del laboratorio, pero no es alguien preparado en su totalidad para ejercer esa labor.
8. ¿Conoce la cantidad de equipos informáticos que posee la institución?	Si, tengo conocimiento sobre la cantidad de equipos.	La institución cuenta con 26 computadoras.
9. ¿Existen alguna política que se deba respetar al momento de acceder a los laboratorios de informática?	Si, como el no ingresar alimentos o bebidas al laboratorio.	Si cuentan con políticas, pero son basadas en conocimientos básicos sobre el cuidado de equipos informáticos.

10. ¿En la Unidad Educativa se realiza el mantenimiento de los equipos informáticos solo cuando hay roturas o están debidamente planificados en diferentes períodos del año lectivo?	Si, se realiza el mantenimiento después de ver si hay algún problema en algún equipo.	Se realizan mantenimientos después de analizar si algún equipo tiene algún problema en su funcionamiento.
11. ¿Cree usted importante que se realice en la Unidad Educativa una auditoría informática al laboratorio de cómputo para brindarle a usted un informe de evaluación de riesgos que le permita tomar decisiones para el área informática?	Si, es muy beneficiario para la institución realizar una auditoría.	Es relevante realizar una auditoria informática en los equipos de la institución para evitar riesgos, porque no se ha realizado una.

Tabla 3
Presentación y análisis de datos de las entrevistas realizadas

3.6.3 Presentación y descripción de los resultados obtenidos

En cuanto a la estructura organizativa de las Tecnologías de la Información (TI), la Pregunta 1 de la encuesta sugiere que la institución cuenta con un departamento específico encargado de la gestión de estas tecnologías, lo cual denota una percepción positiva sobre la existencia de una unidad especializada. No obstante, la Pregunta 7 de la entrevista revela una discrepancia importante, ya que, aunque se menciona que existe una persona responsable de las TI, esta figura recae en un docente que carece de formación técnica especializada en el área. Esta incongruencia subraya una posible deficiencia en la profesionalización del rol asignado, lo que podría generar limitaciones en la efectividad de la gestión y el aprovechamiento adecuado de las TI en el contexto institucional.

Respecto al mantenimiento de los equipos informáticos, la Pregunta 5 de la entrevista señala que dicho mantenimiento se realiza con frecuencia, lo que podría inferirse como una

buena práctica. Sin embargo, la Pregunta 10 de la misma entrevista proporciona una clarificación crítica, ya que específica que el mantenimiento no es sistemático ni programado, sino que solo se lleva a cabo de manera reactiva, es decir, cuando surgen problemas con los equipos. Esta falta de un plan de mantenimiento preventivo y programado podría indicar una deficiencia en la gestión de recursos tecnológicos, lo cual es fundamental para optimizar la vida útil de los equipos y evitar interrupciones en el servicio debido a fallos imprevistos.

Por otro lado, en cuanto a las políticas de seguridad informática y acceso a las instalaciones de TI, la Pregunta 10 de la encuesta establece que los encuestados consideran que existen políticas para el acceso a las instalaciones tecnológicas, sugiriendo una estructura normativa básica para el control de los recursos informáticos. Sin embargo, la Pregunta 9 de la entrevista ofrece una perspectiva más detallada y matizada, indicando que las políticas existentes son de naturaleza general y carecen de documentación formal. Además, se aclara que estas políticas no tienen un enfoque integral ni especializado en seguridad informática, lo cual es una vulnerabilidad crítica dado el entorno tecnológico actual. La ausencia de políticas detalladas y específicas en ciberseguridad pone en riesgo la protección de la infraestructura tecnológica de la institución frente a amenazas externas e internas, lo que podría comprometer tanto la confidencialidad como la integridad de los datos gestionados.

3.6.4 Informe final del análisis de los datos

Los resultados obtenidos mediante la aplicación de instrumentos en la gestión de riesgos de la unidad educativa se observa una disonancia entre las respuestas proporcionadas en la encuesta y la entrevista, lo que refleja una falta de alineación entre las percepciones institucionales sobre la gestión de las TI y la realidad práctica. Además, se identifican áreas clave de mejora, como la necesidad de profesionalizar el cargo encargado de las TI, establecer un sistema de mantenimiento preventivo de los equipos y desarrollar políticas de seguridad informática más robustas y detalladas.

La mayoría de los usuarios no están al tanto de las políticas y prácticas relacionadas con la gestión de los recursos tecnológicos, lo que pone de manifiesto una falta de información o comunicación interna sobre las normativas y procedimientos establecidos. Este desconocimiento puede contribuir a una gestión inadecuada de los riesgos, ya que los usuarios no cuentan con las directrices necesarias para identificar y abordar posibles amenazas o

vulnerabilidades en los sistemas. Los resultados indican que existen deficiencias en la seguridad informática, lo que refleja una falta de un análisis exhaustivo y un manejo adecuado de los riesgos dentro de los laboratorios informáticos, lo cual compromete la protección de los recursos tecnológicos de la institución.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

En este apartado se tiene en cuenta los factores necesarios para llevar a cabo la planificación del proyecto, por tanto, se van a incluir todos los recursos necesarios y utilizados para la realización de este, como los recursos humanos, tecnológicos y económicos de manera minuciosa para cumplir con el objetivo de la propuesta.

La metodología utilizada para llevar a cabo el proyecto es la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Para Guamán et. al (2023), esta metodología permite identificar, analizar y valorar los riesgos asociados a los sistemas de información, proporcionando una base sólida para la toma de decisiones en cuanto a la gestión de riesgos. Su objetivo primordial es realizar un análisis exhaustivo de las amenazas y vulnerabilidades que pueden afectar a los sistemas informáticos, y proponer medidas correctivas y preventivas para mitigar dichos riesgos, optimizando así la protección de los activos tecnológicos.

También se incluyeron los lineamientos establecidos en la ISO/IEC 27001 (Martín, 2021). Que establece los lineamientos internacionales para la gestión de la seguridad de la información. Esta norma ofrece un marco estructurado y detallado que abarca los aspectos relacionados con la confidencialidad, integridad y disponibilidad de la información dentro de una organización. La incorporación de la ISO/IEC 27001 en la investigación aporta un enfoque normativo y técnico que refuerza la validez y precisión de los resultados obtenidos a través de la auditoría, y facilita la identificación de vulnerabilidades y riesgos en un contexto más amplio y alineado con estándares internacionales.

Una vez realizados los procesos de recopilación y análisis de datos, se llevó a cabo la tabulación de estos, obteniendo resultados clave para identificar las vulnerabilidades presentes en la infraestructura tecnológica de la Unidad Educativa Americano. Este análisis detallado permitió evaluar los activos informáticos de la institución, destacando aquellos elementos críticos que requieren atención inmediata en términos de seguridad.

En cuanto a los recursos y metodologías, se emplearon herramientas especializadas para la recolección de datos y la evaluación de riesgos, incluyendo software de auditoría y análisis de seguridad informática. Además, las fases del proyecto se estructuraron de acuerdo con un enfoque sistemático que abarcó desde la planificación inicial y la recolección de datos, hasta la elaboración de propuestas de mejora y la implementación de medidas correctivas.

El análisis y evaluación de los activos se realizó con base en los criterios establecidos por la metodología Magerit y la norma ISO/IEC 27001, permitiendo una visión integral de las áreas vulnerables y las medidas correctivas necesarias para fortalecer la seguridad informática en la institución. Este enfoque metodológico y normativo asegura que los resultados obtenidos sean completos, precisos y alineados con las mejores prácticas internacionales en la gestión de riesgos informáticos.

4.2 Objetivos

- Realizar una auditoría informática en seguridad física de los equipos informáticos del laboratorio de la unidad educativa Americano.
- Fortalecer la seguridad física mediante la implementación de controles y estrategias orientadas a minimizar las vulnerabilidades detectadas.
- Diseñar e implementar estrategias de mejora continua en los sistemas de seguridad física, garantizando la protección de las instalaciones, el personal y los activos críticos, mediante la integración de tecnologías avanzadas y procedimientos efectivos, alineados con las mejores prácticas

4.3 Descripción de la propuesta

En respuesta a la problemática identificada en la investigación, la propuesta consiste en implementar una solución integral que permita mitigar y prevenir posibles vulnerabilidades en los equipos informáticos del laboratorio de la institución. Esta solución está diseñada para

cumplir con los objetivos establecidos, enfocados principalmente en la protección y fortalecimiento de la infraestructura tecnológica, con el fin de garantizar la seguridad de los sistemas y la integridad de la información manejada.

Esta revisión se enfoca en la identificación de mejores prácticas, marcos normativos y metodologías actualizadas relacionadas con la seguridad informática y la gestión de riesgos, tales como la norma ISO/IEC 27001 y la metodología Magerit, que proporcionan los principios y controles necesarios para la protección de sistemas informáticos.

Para obtener datos relevantes y específicos sobre la situación actual de la institución, se llevarán a cabo herramientas de recolección de datos, como encuestas, entrevistas y cuestionarios, los cuales serán diseñados para identificar las vulnerabilidades existentes en los equipos informáticos del laboratorio. Estas herramientas permitirán obtener información precisa sobre las percepciones y el conocimiento del personal docente y administrativo respecto a las políticas de seguridad, así como sobre las fallas en los procedimientos de mantenimiento y gestión de riesgos. Los resultados obtenidos servirán como base para la resolución de la problemática planteada y para la identificación de los puntos críticos que requieren atención inmediata.

En paralelo, se llevará a cabo un análisis detallado de las vulnerabilidades existentes en los equipos informáticos, siguiendo los lineamientos y controles establecidos en la norma seleccionada, particularmente en lo relacionado con la evaluación de riesgos. Este análisis incluirá la identificación de amenazas, posibles vulnerabilidades en el software y hardware, y la evaluación de los posibles impactos que cada vulnerabilidad podría tener en la operación del laboratorio.

Con base en los resultados obtenidos, se procederá a la elaboración de un manual de usuario, el cual describirá de manera clara y detallada las vulnerabilidades encontradas durante el análisis, incluyendo la clasificación y priorización de los riesgos en función de su nivel de impacto y probabilidad de ocurrencia. Además, el manual proporcionará una serie de recomendaciones prácticas y medidas preventivas para mitigar los riesgos identificados. Estas recomendaciones estarán alineadas con las mejores prácticas de seguridad informática y las políticas de protección de la información, y estarán orientadas a promover una cultura de seguridad dentro de la institución.

El manual incluirá, además, un conjunto de procedimientos y pasos a seguir para la prevención de riesgos en los equipos informáticos, proporcionando pautas claras sobre cómo los usuarios deben actuar para evitar posibles vulnerabilidades, realizar actualizaciones de software de manera regular, asegurar el acceso físico y remoto a los sistemas, y fomentar las buenas prácticas de ciberseguridad. El objetivo final de la propuesta es garantizar que los equipos informáticos del laboratorio funcionen de manera óptima y segura, minimizando la exposición a amenazas y vulnerabilidades, y promoviendo un entorno educativo más seguro y protegido.

4.4 Determinación de recursos

4.4.1 Humanos

A continuación, se detallan los integrantes que conforman el equipo de recursos humanos involucrados en la investigación. En primer lugar, se cuenta con la figura del rector, quien ejerce el liderazgo y supervisión general del proyecto, asegurando el cumplimiento de los objetivos institucionales y facilitando la toma de decisiones a nivel estratégico. El rector tiene un rol clave en la validación de la propuesta y en la asignación de recursos necesarios para la ejecución del proyecto.

Cantidad	Recurso	Función	Actividad
1	Cevallos Bravo Karen Mishelle	Investigadora	Realización de la auditoria.
1	Lic. Cristian Tobar	Vicerrector de la institución	Participación en realizar la entrevista, siendo la máxima autoridad de la institución.
7	Docentes	Profesores de tercer nivel de bachillerato	Fueron población participe de la encuesta para la obtención de datos.
1	Docente	Encargado de laboratorio	Participación en realizar la encuesta, siendo quien lleva el control del laboratorio de la institución.

Tabla 4
Recursos humanos

Además, el equipo de investigación está compuesto por ocho profesores de diversas disciplinas que forman parte de la unidad educativa. Estos docentes no solo participan activamente en la recolección de datos, sino que también colaboran en el análisis y desarrollo de las soluciones propuestas. Entre ellos, se encuentra el profesor encargado de los laboratorios, quien tiene un rol fundamental en la gestión diaria de los equipos informáticos y la supervisión de las actividades académicas relacionadas con las tecnologías de la información dentro de los laboratorios. Esta figura específica es esencial para la implementación de las estrategias de seguridad y la ejecución de los planes de acción establecidos en el proyecto.

4.4.2 Tecnológicos

Los recursos tecnológicos necesarios para la ejecución de este proyecto incluyen una variedad de equipos y herramientas especializadas en el ámbito de la seguridad informática y la gestión de riesgos. Esto abarca hardware como servidores, estaciones de trabajo, dispositivos de red y equipos de respaldo, así como software especializado en auditoría de seguridad, análisis de vulnerabilidades y gestión de proyectos.

Cantidad	Recurso	Actividad
1	Teléfono móvil	Desarrollar el proyecto de auditoria
1	Computadoras portátiles	Toma de fotografías como evidencia
1	Microsoft office	Herramienta para el desarrollo de la documentación y tabulación de datos obtenidos.
1	Conexión a internet	Búsqueda de fuentes bases para el desarrollo teórico del proyecto.
1	Impresora	Utilizado para la impresión de los instrumentos de evaluación y documento final.
1	Microsoft Forms	Herramienta para el desarrollo de recolección de datos de las encuestas realizada a los docentes.

Tabla 5
Recursos tecnológicos

Es fundamental contar con tecnología actualizada que permita llevar a cabo el análisis detallado de los sistemas informáticos de la institución y aplicar las medidas correctivas necesarias. Asimismo, se evaluará la infraestructura existente en la Unidad Educativa,

identificando posibles necesidades de actualización o ampliación de los recursos tecnológicos para garantizar la efectividad del proyecto en todas sus fases.

4.4.3 Económicos

Los recursos económicos del proyecto se gestionarán mediante la asignación de un presupuesto detallado, que cubra todos los aspectos necesarios para su correcta ejecución. Este presupuesto incluirá los costos asociados a la contratación de personal especializado, la adquisición de equipos y software, así como los gastos operativos relacionados con la implementación de medidas de seguridad informática y la formación del personal.

Cantidad	Descripción	Precio Unitario	Subtotal
1	Teléfono móvil para la toma de evidencia en audio y foto de la información obtenida.	$180,00	$180,00
11	Viáticos en servicio de pasaje para movilización a la institución.	$2.50	$27,50
1	Computadora portátil Hp para documentación y desarrollo del proyecto.	$850.00	$850.00
1	Internet	$5,00	$5,00
100	Hojas de instrumentos de evaluación.	$0,05	$5
		Total	$1.067,50

Tabla 6
Recursos económicos

La correcta asignación de recursos económicos es crucial para el éxito del proyecto y para garantizar que las soluciones propuestas sean sostenibles a largo plazo.

4.5 Etapas del desarrollo de la propuesta

El desarrollo de la propuesta se llevará a cabo a través de una serie de etapas estructuradas y organizadas, con el objetivo de implementar mejoras en los equipos informáticos de la institución, enfocándose en la seguridad informática.

Cada etapa estará orientada a alcanzar los objetivos establecidos en el proyecto, utilizando los recursos humanos y tecnológicos disponibles de manera eficiente, y maximizando la colaboración entre las distintas partes involucradas. Las actividades se llevarán a cabo con la participación del director de la institución, el encargado del laboratorio, y los docentes responsables de las áreas académicas vinculadas con las tecnologías de la información.

4.5.1 Antecedentes

El Colegio Particular Mixto Americano, ubicado en El Carmen, Ecuador, fue fundado en 1981, inicialmente ofreciendo un jardín de infantes y los primeros dos grados del nivel primario. En 1982, la institución obtuvo su permiso definitivo mediante el acuerdo No 035-DT, permitiéndole expandir su cobertura. Durante el ciclo lectivo 1983-84, se completó la oferta del nivel primario en jornada vespertina. Los maestros fundadores del nivel primario fueron la Dra. Mariana Gálvez, el Dr. Fabián Arízaga y el Dr. Vicente Verdezoto.

En 1984, la institución inició con el Primer Curso de Ciclo Básico, y en 1986 y 1987 se expandió a los cursos Segundo y Tercero, respectivamente. En 1996, se creó la sección nocturna con el Primer Curso de Ciclo Diversificado en la especialidad de Computación. En ese período, se contó con la dirección del Lcdo. Carlos Yugcha Armas, y la colaboración de los docentes Lcda. Mery Giler, Lcda. Emperatriz Alcívar, Lcdo. Walberto Vélez, Lcdo. Gutemberth Garcés, Ing. Carlos Pinargote y Sr. Adrián Olaya. Posteriormente, con el acuerdo No 00134 en 1998, se autorizaron nuevos cursos de Bachillerato Técnico en Comercio y Administración con especialización en Computación, tanto en jornada diurna como nocturna. Por otro lado, el acuerdo ministerial No 976-bis, en el año 2000 modificó y autorizó el funcionamiento del Bachillerato Técnico en Comercio y Administración, Especialidad en Informática, en jornada matutina y nocturna.

Actualmente, el Colegio sigue ofreciendo una educación integral, adaptándose a las demandas del sistema educativo ecuatoriano y continúa siendo un referente en la región. La institución ofrece programas académicos de calidad que cubren desde el nivel inicial hasta el ciclo diversificado, enfocándose en áreas técnicas y científicas, con una formación sólida que prepara a sus estudiantes para los desafíos del futuro.

La institución se caracteriza por su compromiso con la formación académica y el desarrollo integral de sus estudiantes, adaptándose a las necesidades educativas contemporáneas y manteniendo altos estándares de calidad en la enseñanza, promoviendo un ambiente propicio para el aprendizaje y el crecimiento personal de los estudiantes. Además, la institución mantiene una comunicación activa con la comunidad educativa y participa en diversas actividades y eventos que enriquecen la experiencia educativa de sus alumnos.

4.5.1.1 Datos informativos

NOMBRE DE LA INSTITUCIÓN:	Unidad Educativa “Americano”
Código AMIE	13H04538
Ubicación Geográfica	Urbana
Zona	4
Distrito	13D05
Fundada	En el año 1981
Ciudad	El Carmen
Niveles educativos	Inicial, Educación Básica y Bachillerato
Carácter	Particular
Jornada	Matutina
Genero	Mixto

Número de estudiantes	148
Número de docentes	18
E-mail	u.e.amer@hotmail.com

Tabla 7
Datos informativos de la institución

4.5.1.2 Misión

El Instituto Particular Mixto Americano, fiel a su filosofía entrega todos sus esfuerzos para servir a los sectores de la población de El Carmen con Educación inicial, Educación Básica de calidad y Bachillerato con nuevas Especialidades técnicas. Nuestros egresados se desempeñan con solvencia profesional y prestigio social en las unidades productivas, lo que refiere en la calidad de vida de ellos y sus familias que se sienten satisfechos de participar activamente en el desarrollo sustentable del Cantón EL Carmen.

4.5.1.3 Visión

En el 2028 el Instituto Particular Mixto Americano será el referente y el líder en la Educación Técnica del Cantón El Carmen por su acertado liderazgo Administrativo Pedagógico y Tecnológico. Además, por contar con la infraestructura totalmente adecuada para el eficaz desarrollo del proceso enseñanza-aprendizaje. Su sistema financiero contable, eficiente y confiable, su clima institucional armonioso, donde participan activamente y comprometidos con la institución. Directivos, Docentes y empleados altamente capacitados para ejercer sus funciones.

Entregará Bachilleres Técnicos formados con los más altos estándares de calidad educativa y adiestramiento profesional para su realización personal en el trabajo honesto, entregándoles una profesión rentable que les permita involucrarse con éxito en el mercado del trabajo como colaboradores de servicios técnicos o empresarios de prestancia social, moral y técnica.

4.5.2 Organigrama de la institución

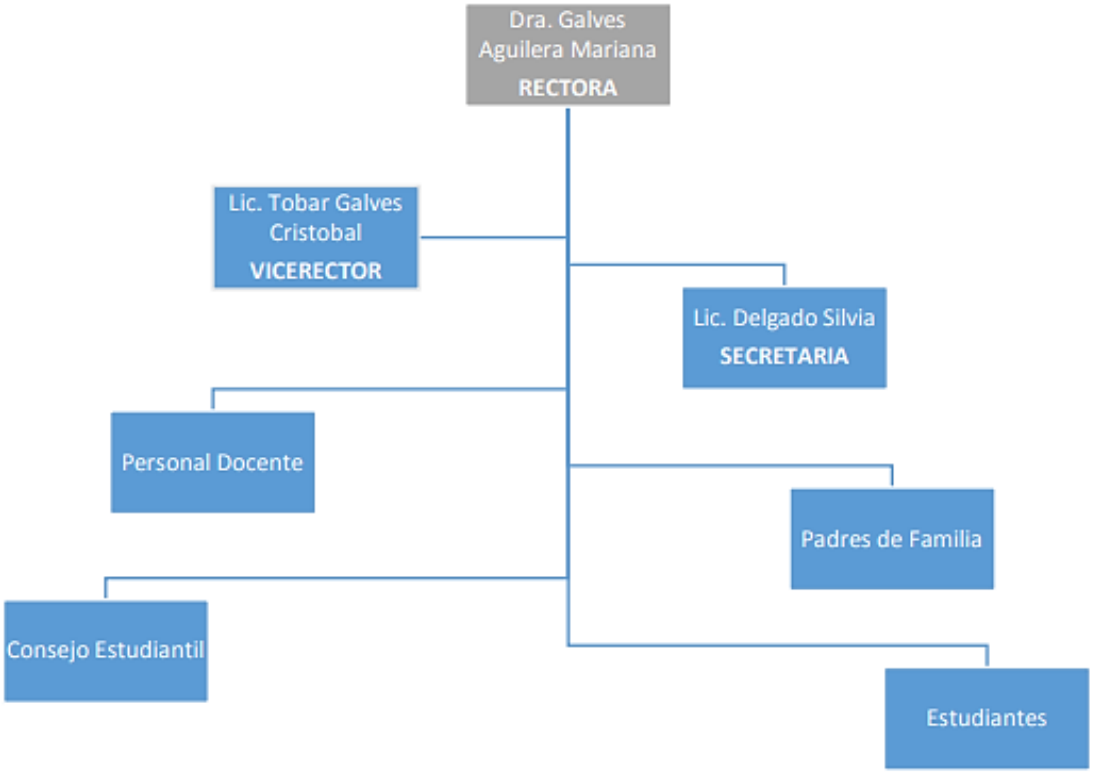


Ilustración 2
Organigrama de la institución

. A través de este esquema, se podrá observar cómo se distribuyen las tareas y cómo se coordinan los esfuerzos para garantizar el cumplimiento de los objetivos educativos, la gestión eficiente de los recursos y la mejora continua de los procesos académicos y administrativos.

4.5.2.1 Programa de auditoria informática

Este programa tiene como objetivo principal identificar vulnerabilidades, analizar riesgos y garantizar la integridad, confidencialidad y disponibilidad de los recursos tecnológicos de la institución. La auditoría informática se lleva a cabo a través de un proceso meticuloso que incluye la revisión de infraestructuras tecnológicas, políticas de seguridad, sistemas de gestión de información, y el comportamiento de los usuarios.

En el contexto de la institución, el programa de auditoría informática se implementa con la finalidad de fortalecer la seguridad informática, detectar posibles fallas en los sistemas, evaluar el cumplimiento de las normativas internas y externas, y proporcionar recomendaciones específicas para mitigar los riesgos.

4.5.2.2 Planificación

Programa de auditoría informática de seguridad física del laboratorio de computación de la Unidad Educativa Americano.

Objetivo General:

- Programa de auditoría informática de seguridad física al laboratorio de computación de la Unidad Educativa Americano.

Objetivos Específicos:

- Identificar principales riesgos de seguridad que existen en la Unidad Educativa Americano.
- Analizar y verificar el nivel se seguridad de los componentes informáticos de la institución.

Técnicas y procedimientos	Referencias papel de trabajo	Fecha
1.1. Fundamentación teórica sobre la seguridad de la información y normas, leyes, políticas, relacionada a la misma.	F1	26-09-2024
1.2. Revisar metodología MAGERIT junto a los pasos de su ejecución.	F2	02-10-2024
1.3. Definir activos	A1	13-10-2024
1.4. Definir Amenazas	A2	24-10-2024
1.5. Elaborar instrumentos de auditoría con base a normas, leyes, políticas. (Diseño de instrumento)	K1	25-10-2024
1.6. Aplicación de instrumentos de investigación	K1	05-10-2024
1.7. Tabulación y análisis de datos.	T1	27-10-2024
2. identificación de salvaguardas (Medidas de prevención)	T2	30-10-2024
2.1. Evaluación de riesgos (Matriz de riesgos)	T3	06-11-2024
2.2. Tratar los riesgos y elaboración del manual de contingencia.	M	20-11-2024
3. Elaboración de informe final	Z	29-11-2024

Elaborado por: Cevallos Bravo Karen Mishelle **Revisado por:**

Fecha: 29-09-2024 **Fecha:**

Observaciones:

Tabla 8
Programa de auditoria informática (planificación)

4.5.2.3 Normas de seguridad

- **ISO 27001**

La norma ISO 27001 es un estándar internacional que establece los parámetros necesarios para implementar, mantener y realizar mejoras continuas en un Sistema de Gestión de Seguridad de la Información (SGSI). La ISO 27001 puede ser implementada en cualquier tipo de organización, permitiéndoles responder a sus necesidades en el ámbito de la seguridad del recurso más valioso que poseen actualmente las empresas: la información.

Al proporcionar a las empresas un marco integral de seguridad de la información, esta norma les permite identificar y corregir oportunamente posibles riesgos relacionados con dicha seguridad. Además, mediante una implementación exitosa, las organizaciones pueden ser certificadas por una entidad independiente, lo que demuestra que gestionan la seguridad de la información de manera responsable, cumpliendo con los estándares de la ISO 27001 (Guiller, Cahuaya, & René, 2023).

4.5.2.4 Metodología Magerit

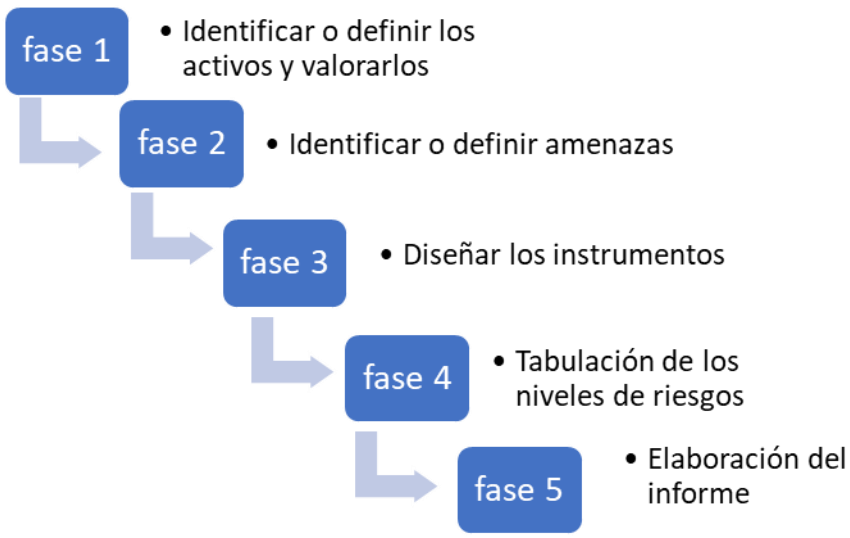
La metodología Magerit Consiste en un método sistemático para el análisis y gestión de los riesgos que derivan del uso de la información. Su fin es informar de los riesgos y de la necesidad de gestionarlos a los responsables de la actividad, así como ayudar a encontrar y planificar un plan adecuado para tratarlos (Torres & Tapia, 2021).

La aplicación de la metodología Magerit en el contexto de la Unidad Educativa Particular Mixto Americano se justifica debido a su capacidad para abordar de manera sistemática y profunda los riesgos asociados a los equipos informáticos y la infraestructura tecnológica del centro educativo. En particular, el uso de esta metodología se centra en la auditoría informática física de los laboratorios de computación, lo que permite identificar posibles vulnerabilidades físicas (como la seguridad de los dispositivos y el acceso no autorizado) y tecnológicas (como la configuración de software y sistemas). A través de este análisis, se busca obtener una visión clara de las debilidades que podrían comprometer la integridad, confidencialidad y disponibilidad de los datos y recursos informáticos de la institución.

Además de la identificación de riesgos, la metodología se enfoca en la planificación de un protocolo de seguridad que guíe en el uso eficiente y seguro de los medios informáticos en los laboratorios. Esto incluye la implementación de medidas de protección que ayuden a reducir los riesgos tecnológicos y fomenten el cumplimiento de buenas prácticas en cuanto al manejo de la información y los dispositivos tecnológicos. El objetivo final es establecer un marco de trabajo para la **gestión de riesgos** que permita a la unidad educativa tomar decisiones informadas y precisas, asegurando la continuidad operativa de los sistemas informáticos y minimizando las consecuencias de posibles incidentes.

No solo proporciona un diagnóstico de la situación actual, sino que también permite trazar estrategias a largo plazo para mejorar la seguridad informática de la institución, adaptándose a los cambios tecnológicos y a las nuevas amenazas cibernéticas. Su aplicación efectiva dentro de la unidad educativa contribuirá a la creación de un entorno más seguro y eficiente para el aprendizaje, protegiendo tanto a los estudiantes como a los docentes de los riesgos derivados del uso de las tecnologías de la información en el ámbito académico. Además, establecer un plan de acción claro y documentado con las medidas correctivas y preventivas necesarias permitirá a la institución mantener un alto estándar de seguridad informática y cumplir con las normativas y mejores prácticas del sector educativo.

4.5.2.5 Gráfico de las fases de la metodología Magerit



4.5.2.6 Aplicación de metodología Magerit

La aplicación de Magerit implica realizar una evaluación detallada de todos los componentes de la infraestructura tecnológica, desde los sistemas informáticos hasta las políticas de seguridad que rigen el acceso y el uso de los recursos digitales. A través de esta metodología, se busca identificar los riesgos que podrían comprometer la integridad de los datos, la continuidad de las operaciones educativas y la seguridad general de la institución.

4.5.2.6.1 Valor Activos

VA	Descripción	Valor de riesgo
5	Todos los equipos están seguros y operando según su función.	Bastante seguro
4	Si ocurre un problema en algún componente, seguirá operando.	Seguro
3	Si llega a paralizarse algún componente, seguirá operando para realizar actividades básicas escolares.	Seguro confiable
2	Se debe empezar a tomar medidas para reducir fallas.	Riesgo manejable
1	Si el componente deja de funcionar no se podrán realizar las actividades estudiantiles.	Riesgo grave

Tabla 9
Valoración de activos

4.5.2.7 Definición y valoración de activos

Los activos definidos dentro de la metodología Magerit está constituidos en dos tipos que son:

- Software
- Hardware

Nombre	Código	Descripción	Valor	D	I	C	VA

Computadora de escritorio	CE0001	Monitor 14", Procesador Intel i5, Periféricos	5 - Bastante seguro	5	5	5	5
Impresora	IL0001	Impresora láser con red integrada	4 – Seguro	4	4	4	4
Proyector	PL0001	Proyector con resolución Full HD	4 – Seguro	4	4	3	3.67
Router	RL0001	Router inalámbrico de alta velocidad	3 - Seguro confiable	3	3	3	3
Aire acondicionado	A005	Equipo de enfriamiento de ambiente	2 - Riesgo manejable	2	2	2	2
Servidor	L006	Servidor central con redundancia	5 - Bastante seguro	5	5	5	5
Switch de red	SW008	Switch con 24 puertos de alta velocidad	4 - Seguro	4	4	3	3.67
Sistema de cámaras	C009	Cámaras de vigilancia IP Full HD	4 - Seguro	4	4	4	4
UPS	CPV02	Sistema de respaldo eléctrico	5 - Bastante seguro	5	5	5	5

Tabla 10
Definición y valoración de activos

Dentro de la aplicación de la metodología Magerit es un paso clave en el proceso de auditoría de riesgos, ya que permite identificar y priorizar los activos más críticos de la infraestructura tecnológica de la Unidad Educativa Particular Mixto Americano. Estos activos pueden incluir tanto los recursos físicos, como los equipos informáticos y servidores, como los recursos lógicos, tales como bases de datos, aplicaciones o sistemas de gestión de información. El valor de estos activos es fundamental para comprender su impacto en las operaciones de la institución y determinar el nivel de protección necesario para garantizar su seguridad y funcionamiento adecuado.

4.5.2.8 Identificación de amenazas

En el marco de la gestión de riesgos, la identificación de amenazas constituye un paso esencial para proteger los activos tecnológicos de una organización, siguiendo los lineamientos de la metodología Magerit.

Activo	Amenazas
PCs	• Incendio • Robo • Inundación • Daño de equipos
Impresora	• Daños • Fallos
Sistema operativo	• Falta de antivirus • Desactualizados • sin antivirus

Tabla 11
Identificación de amenazas

En este contexto, se realizó un análisis detallado de las amenazas que podrían afectar tres activos fundamentales: las computadoras personales, las impresoras y los sistemas operativos. Los resultados preliminares indican que las PCs están expuestas a riesgos significativos como incendios, robos, inundaciones y daños físicos, los cuales comprometen la disponibilidad, integridad y confidencialidad de los datos.

Las impresoras, como dispositivos periféricos críticos, presentan vulnerabilidades frente a daños mecánicos y fallos operativos, que afectan directamente la continuidad de los procesos dependientes de ellas.

Finalmente, los sistemas operativos representan un área de riesgo clave debido a la falta de antivirus, actualizaciones pendientes y la ausencia de medidas de seguridad adecuadas, lo que incrementa la probabilidad de ataques cibernéticos y fallos de software.

4.5.2.8.1 Análisis de Riesgos

El examinar riesgos y estimar impactos se explica en qué medida es confiable el robo en la unidad educativa Americano, así como la integridad frente al incendio y la disponibilidad respecto a los perjuicios en los equipos del laboratorio de informática para los estudiantes que forman parte de la institución.

	Integridad	Confiabilidad	Disponibilidad	Valor de impacto
Robo	3	3	4	3
Incendio	4	4	3	2
Daño de equipos	4	4	2	2
Inundación	2	2	3	4
Malware	3	2	5	3

Ilustración 3

Calculo del impacto

El riesgo se calculó mediante la fórmula R= P × I, donde *P* es la probabilidad de ocurrencia y *I* es el impacto asociado. Con base en los valores de impacto y probabilidad estimada, se establecieron niveles de prioridad para las amenazas.

El cálculo del impacto en una auditoría de seguridad es una parte fundamental del análisis de riesgos. En el contexto del análisis presentado en la tabla, el cálculo del impacto se realiza evaluando cómo una amenaza afecta a tres dimensiones clave: integridad, confiabilidad y disponibilidad.

4.5.2.9 Diseño de instrumento para analizar riesgos

Cuestionarios para identificar riesgos (Robo). "Controles para robo".	**K1**	
	Pág. 1-5	
Preguntas	**Si**	**No**
1.- ¿Existe personal responsable de la seguridad?		
2.- ¿Existe vigilancia por medio de cámaras de seguridad?		
3.- ¿Existe control de acceso a las computadoras?		
4.- ¿El laboratorio cuenta con sistemas de control de acceso biométrico?		
5.- ¿Se utilizan tarjetas de autenticación para registrar entrada y salida?		
6.- ¿Se realizan revisiones periódicamente de registro de acceso?		
7.- ¿Los equipos de cómputo están asegurados físicamente con anclajes?		
8.- ¿Se realizan inventario regular de los equipos y dispositivos?		
9.- ¿El personal o usuarios reciben capacitaciones en seguridad física?		
10.- ¿Se realiza monitoreo constante de las cámaras de seguridad?		
11.- ¿Las puertas y ventanas tienen cerraduras seguras?		
12.- ¿Se utilizan sensores de movimiento en las áreas críticas?		
13.- ¿Existe procedimientos para asegurar periféricos?		
14.- ¿El laboratorio tiene iluminación exterior adecuada?		
15.- ¿Se utilizan mecanismos de bloqueo automático para las puertas?		
16.- ¿Se han realizado evaluaciones de riesgo de seguridad recientemente?		
17.- ¿Se verifican regularmente las cerraduras y sistemas de acceso?		
18.- ¿Existen planes de mejora continua para la seguridad física?		
19.- ¿El laboratorio da al exterior?		
20.- ¿Hay un protocolo para notificar intentos de acceso no autorizado?		
21.- ¿El área está protegida por un cerco perimetral?		
22.- ¿Existe simulacros contra robos?		
23.- ¿Se supervisan las áreas donde almacenan los dispositivos de mantenimiento?		
24.- ¿Se han registrado intentos previos de robo en el laboratorio?		
25.- ¿Se cuenta con vigilancia las 24 horas?		
Realizado por: • Cevallos Bravo Karen Mishelle	**Revisado por:**	
Fecha: 26/10/2024	**Observación:**	

Tabla 12 Cuestionarios para identificar riesgos (Robo)

Cuestionarios para identificar riesgos (Incendio). "Controles para Incendio".	**K1**	
	Pág. 1-5	
Preguntas	**Si**	**No**
1.- ¿El laboratorio tiene detectores de humo operativos?		
2.- ¿Los equipos eléctricos están conectados a tomas de corrientes con protección contra sobretensiones?		
3.- ¿Hay alarmas contra incendios instaladas en el área?		
4.- ¿Se realizan simulacros de evacuación?		
5.- ¿Están almacenados de manera segura y etiquetados los materiales inflamables?		
6.- ¿Hay materiales aislantes de incendios, como cortafuegos, instalados donde sea necesario?		
7.- ¿Los extintores están visibles y accesibles para el personal?		
8.- ¿Se realiza una evaluación regular de riesgos de incendio en el laboratorio?		
9.- ¿El laboratorio cumple con las normativas locales contra incendios?		
10.- ¿Se realiza inspección periódica de los sistemas eléctricos?		
11.- ¿Los muebles y equipos están fabricados con materiales retardantes de incendios?		
12.- ¿Se utilizan sensores de movimiento en las áreas críticas?		
13.- ¿Los cables eléctricos están organizados y protegidos?		
14.- ¿El laboratorio tiene rociadores automáticos?		
15.- ¿Las puertas de emergencia están libres de obstrucciones?		
16.- ¿Se verifica la funcionalidad del sistema de detección periódicamente?		
17.- ¿Los equipos están diseñados para evitar sobrecalentamiento?		
18.- ¿Se limita el uso de enchufes múltiples?		
19.- ¿El sistema de aire acondicionado está libre de acumulación de polvo?		
20.- ¿Se han registrado incendios previos en el laboratorio?		
21.- ¿El personal de mantenimiento está capacitado para prevenir incendios?		
22.- ¿El laboratorio tiene un protocolo de revisión post-incendio?		
23.- ¿Se cuenta con un listado de contactos de emergencia?		
24.- ¿Hay un suministro adecuado de equipos de primeros auxilios y se encuentran accesible?		
25.- ¿Los equipos quedan apagados al finalizar su labor?		

Realizado por:

- Cevallos Bravo Karen Mishelle

Revisado por:

Fecha: 26/10/2024

Observación:

Tabla 13Cuestionarios para identificar riesgos (Incendio)

Cuestionarios para identificar riesgos (Inundación). "Inundación".	**K1**	
	Pág. 1-5	
Preguntas	**Si**	**No**
1.- ¿El laboratorio está ubicado en una zona propensa a inundaciones?		
2.- ¿Existen sistemas de drenaje alrededor del laboratorio?		
3.- ¿Los equipos están ubicados en lugares elevadas?		
4.- ¿Se realizan inspecciones regulares de las tuberías del laboratorio?		
5.- ¿El personal tiene conocimientos sobre algún protocolo en caso de inundación?		
6.- ¿Se cuenta con algún sistema de detección temprana de agua?		
7.- ¿Cuenta con un plan de evacuación en caso de inundación?		
8.- ¿Los sistemas eléctricos están protegidos contra el contacto con agua?		
9.- ¿Los servidores están ubicados en salas con control de humedad?		
10.- ¿Se han instalado barreras físicas contra el agua en puntos vulnerables?		
11.- ¿Se inspeccionan periódicamente los techos para prevenir filtraciones?		
12.- ¿Los activos valiosos están protegidos contra posibles filtraciones?		
13.- ¿El laboratorio tiene seguro contra daños por inundación?		
14.- ¿Los sistemas de alarma están diseñados para funcionar en caso de inundación?		
15.- ¿Se tiene un plan de recuperación ante desastres naturales?		
16.- ¿Se limita el uso de agua en áreas cercanas a los equipos?		
17.- ¿El laboratorio cuenta con un protocolo de respuesta rápida ante inundaciones?		
18.- ¿Se utilizan pisos resistentes al agua en áreas sensibles?		
19.- ¿se cuenta con herramientas para sellar fugas de emergencia?		
20.- ¿Se han realizado simulacros relacionados con emergencias de agua?		
21.- ¿Las paredes de las oficinas o laboratorios tienen daño por humedad?		
22.- ¿Se verifica que los sistemas de alarma sean resistentes a la humedad?		
23.- ¿Se realizan análisis de impacto financiero ante posibles inundaciones?		
24.- ¿Alguna vez se filtró agua por las ventanas?		
25.- ¿Anteriormente ha existido daños en los equipos por agua?		
Realizado por: • Cevallos Bravo Karen Mishelle	**Revisado por:**	
Fecha: 26/10/2024	**Observación:**	

Tabla 14 Cuestionarios para identificar riesgos (Inundación)

Cuestionarios para identificar riesgos (Malware). "Controles para Malware".	**K1**	
	Pág. 1-5	
Preguntas	**Si**	**No**
1.- ¿Se han realizado auditorías de seguridad informática?		
2.- ¿Todos los equipos cuentan con un software antivirus actualizado?		
3.- ¿Se realizan análisis a las descargas hechas en los equipos?		
4.- ¿Se realizan análisis periódicos de malware en todos los equipos?		
5.- ¿El personal reciben formación sobre cómo identificar y evitar malware?		
6.- ¿Los equipos de la red están protegidos con contraseñas seguras?		
7.- ¿El acceso a los dispositivos está limitado a personal autorizado?		
8.- ¿Se cuenta con políticas de uso de dispositivos extraíbles para prevenir la propagación de malware?		
9.- ¿Se lleva un registro de las modificaciones realizadas en los sistemas para detectar posibles cambios maliciosos?		
10.- ¿Se cuenta con medidas de protección ante posibles ataques de denegación de servicios?		
11.- ¿Se utilizan firewalls para proteger la red?		
12.- ¿Se realizan respaldos regulares de datos críticos?		
13.- ¿Se limita el acceso a sitios web potencialmente peligrosos?		
14.- ¿El laboratorio tiene un sistema de detección de intrusiones?		
15.- ¿Los dispositivos cuentan con cifrado para proteger datos sensibles?		
16.- ¿El laboratorio tiene un plan de respuesta a incidentes de malware?		
17.- ¿Los usuarios tienen permisos limitados en los sistemas?		
18.- ¿El laboratorio tiene un protocolo de aislamiento para equipos infectados?		
19.- ¿El laboratorio cuenta con un seguro contra incidentes cibernéticos?		
20.- ¿Se cuenta con medidas de seguridad en las conexiones Wi-Fi?		
21.- ¿Se lleva un registro de los accesos a los equipos informáticos?		
22.- ¿Se implementan políticas de uso para dispositivos móviles?		
23.- ¿Se realiza una prueba de penetración regularmente?		
24.- ¿El personal está informado sobre el impacto financiero de un ataque de malware?		
25.- ¿Se implementa la segmentación de red para mitigar el riesgo de malware?		

Realizado por: **Revisado por:**

- Cevallos Bravo Karen Mishelle

Fecha: 26/10/2024

Observación:

Tabla 15 Cuestionarios para identificar riesgos (Malware)

Cuestionarios para identificar riesgos (Equipos). "Controles para daño de Equipo".	**K1**	
	Pág. 1-5	
Preguntas	**Si**	**No**
1.- ¿Hay inventario de los equipos en buen estado?		
2.- ¿Se realiza mantenimiento preventivo regular en los equipos?		
3.- ¿Se realiza inspecciones para comprobar el estado de los equipos?		
4.- ¿Se utilizan sistemas de protección eléctrica, como UPS o supresores de picos?		
5.- ¿El personal está capacitado para operar los equipos correctamente?		
6.- ¿El laboratorio tiene un sistema adecuado de ventilación y enfriamiento?		
7.- ¿Los equipos están instalados sobre superficies estables y niveladas?		
8.- ¿Se prohíbe el consumo de alimentos y bebidas cerca de los equipos?		
9.- ¿En caso de que alguien dañe un equipo, hay una política que se le impone?		
10.- ¿Se revisan los cables de los equipos periódicamente para evitar cortocircuitos?		
11.- ¿Se realiza limpieza interna de los equipos?		
12.- ¿Los equipos cuentan con protección sobre tención eléctrica?		
13.- ¿Los equipos están asegurados contra daños accidentales?		
14.- ¿El laboratorio tiene procedimientos para reportar daños?		
15.- ¿Se dispone de repuestos esenciales para equipos críticos?		
16.- ¿Se han implementado controles para evitar el uso indebido de los equipos?		
17.- ¿El personal cuenta con manuales de operación para el uso de los equipos?		
18.- ¿Los equipos portátiles están protegidos contra caídas accidentales?		
19.- ¿Se protegen los cables contra daños por objetos cortantes o desgaste?		
20.- ¿El laboratorio tiene contratos de soporte técnico con los fabricantes?		
21.- ¿El sistema de cableado está correctamente instalado?		
22.- ¿Hay sensor de humedad y temperatura?		
23.- ¿Se establecen límites de uso para evitar el sobrecalentamiento?		
24.- ¿El laboratorio cuenta con políticas para la correcta desconexión de dispositivos?		
25.- ¿El laboratorio tiene un plan de reemplazo para equipos obsoletos?		
Realizado por: • Cevallos Bravo Karen Mishelle	**Revisado por:**	
Fecha: 26/10/2024	**Observación:**	

Tabla 16 Cuestionarios para identificar riesgos (Daños a equipos)

Para elaborar los instrumentos, se tomó en cuenta 5 parámetros en los que se van a analizar riesgos en los cuales son: inundación, incendio, malware, daño de equipos y robo. Siendo estos evaluados mediante la recolección de datos detallados en cada cuestionario que dan del resultado de las preguntas realizadas.

4.5.2.10 Aplicación de instrumentos

Para llevar a cabo la aplicación de los instrumentos de recolección de datos, se estableció una coordinación previa con el responsable del área de laboratorios de la institución educativa, asegurando la autorización para acceder a las instalaciones y la disposición de los recursos necesarios. Este proceso incluyó una reunión inicial con el encargado, donde se expusieron detalladamente los objetivos de la auditoría los procedimientos a implementar y la relevancia de la información a obtener, garantizando la transparencia y la veracidad de los datos recopilados.

Como herramienta de auditoría, se utilizó un cuestionario estructurado, diseñado específicamente para identificar y evaluar los riesgos potenciales asociados al entorno del laboratorio. El cuestionario constaba de 25 preguntas cerradas con respuestas dicotómicas (sí o no), lo que facilitó la sistematización y análisis de los datos. Este instrumento fue aplicado al rector de la institución, considerado como una fuente clave de información debido a su conocimiento integral de la infraestructura, procedimientos y vulnerabilidades del laboratorio.

El análisis de las respuestas proporcionó información clave sobre diversos riesgos, entre los cuales se identificaron amenazas significativas como robo, incendio, daño de equipos, inundación y la presencia de malware. Cabe destacar que cada pregunta abordaba un aspecto específico de la seguridad y la gestión de riesgos, permitiendo un enfoque exhaustivo y detallado. En total, el cuestionario generó 125 respuestas derivadas de la multiplicación del número de preguntas por el número de aspectos evaluados, lo que permitió obtener un panorama integral de las amenazas existentes.

Adicionalmente, los resultados se organizaron y analizaron utilizando herramientas estadísticas descriptivas, lo que permitió identificar patrones recurrentes en los riesgos y establecer una jerarquización basada en su frecuencia y nivel de impacto potencial. Este enfoque contribuyó a fundamentar la propuesta de estrategias de mitigación, alineadas con estándares de gestión de riesgos como los establecidos en la metodología Magerit, asegurando así una evaluación sistemática y científica de los riesgos presentes en el laboratorio de la institución educativa.

4.5.2.11 Tabulación

Para llevar a cabo el proceso de tabulación de los datos recolectados, se utilizó la herramienta Microsoft Excel, la cual permitió organizar y sistematizar la información de manera eficiente. Esta herramienta fue seleccionada por su versatilidad y capacidad para realizar cálculos automáticos y análisis de datos, lo que facilitó el procesamiento de los resultados obtenidos a través de los instrumentos de evaluación aplicados al rector de la Unidad Educativa Americano.

En el diseño de la hoja de cálculo, se creó un esquema que incluyó una hoja de código para categorizar las respuestas y facilitar la identificación de riesgos en el laboratorio de la institución. Los códigos utilizados fueron definidos como:

- 1 = Representa seguridad, indicando que el aspecto evaluado cumple con los parámetros establecidos para garantizar un entorno seguro.
- 2 = No aplica, señalando que el riesgo identificado no es relevante o aplicable en el contexto evaluado.
- 0 = Representa riesgo, evidenciando la presencia de una amenaza o vulnerabilidad que requiere atención inmediata.

para el poder identificar y analizar cada respuesta.

Esta codificación permitió no solo organizar la información de manera estructurada, sino también realizar un análisis más preciso de las respuestas proporcionadas. Cada respuesta fue categorizada y vinculada a los riesgos previamente identificados, tales como robo, incendio,

daño de equipo, inundación o malware, posibilitando su representación gráfica y su análisis estadístico.

Adicionalmente, se implementaron funciones avanzadas en Excel, como tablas dinámicas, filtros y gráficos, para interpretar los resultados de manera clara y eficiente. Esto permitió no solo visualizar la frecuencia y la distribución de los riesgos, sino también identificar patrones y correlaciones que contribuyen a la toma de decisiones basada en datos.

Cuestionarios para identificar riesgos (Robo). "Controles para robo".	K1 Pág. 1-5
Preguntas	**Respuestas**
1.- ¿Existe personal responsable de la seguridad?	**1**
2.- ¿Existe vigilancia por medio de cámaras de seguridad?	**1**
3.- ¿Existe control de acceso a las computadoras?	**1**
4.- ¿El laboratorio cuenta con sistemas de control de acceso biométrico?	**0**
5.- ¿Se utilizan tarjetas de autenticación para registrar entrada y salida?	**0**
6.- ¿Se realizan revisiones periódicamente de registro de acceso?	**1**
7.- ¿Los equipos de cómputo están asegurados físicamente con anclajes?	**1**
8.- ¿Se realizan inventario regular de los equipos y dispositivos?	**1**
9.- ¿El personal o usuarios reciben capacitaciones en seguridad física?	**1**
10.- ¿Se realiza monitoreo constante de las cámaras de seguridad?	**1**
11.- ¿Las puertas y ventanas tienen cerraduras seguras?	**1**
12.- ¿Se utilizan sensores de movimiento en las áreas críticas?	**0**
13.- ¿Existe procedimientos para asegurar periféricos?	**1**
14.- ¿El laboratorio tiene iluminación exterior adecuada?	**1**
15.- ¿Se utilizan mecanismos de bloqueo automático para las puertas?	**1**
16.- ¿Se han realizado evaluaciones de riesgo de seguridad recientemente?	**0**
17.- ¿Se verifican regularmente las cerraduras y sistemas de acceso?	**1**
18.- ¿Existen planes de mejora continua para la seguridad física?	**0**
19.- ¿El laboratorio da al exterior?	**1**
20.- ¿Hay un protocolo para notificar intentos de acceso no autorizado?	**1**
21.- ¿El área está protegida por un cerco perimetral?	**1**
22.- ¿Existe simulacros contra robos?	**0**
23.- ¿Se supervisan las áreas donde almacenan los dispositivos de mantenimiento?	**1**
24.- ¿Se han registrado intentos previos de robo en el laboratorio?	**0**
25.- ¿Se cuenta con vigilancia las 24 horas?	**1**
Total de riesgos no aplica(2)	0
Total de controles evaluados	25
Seguridad (1)	18
Riesgo (0)	7
Porcentaje de seguridad	**72%**
Porcentaje de riesgo	**28%**
	100%

Tabla 17 Cuestionarios para identificar riesgos (Robo)

Cuestionarios para identificar riesgos (Incendio). “Controles para Incendio”.	K1 Pág. 2-5
Preguntas	**Respuestas**
1.- ¿El laboratorio tiene detectores de humo operativos?	**1**
2.- ¿Los equipos eléctricos están conectados a tomas de corrientes con protección contra sobretensiones?	**1**
3.- ¿Hay alarmas contra incendios instaladas en el área?	**1**
4.- ¿Se realizan simulacros de evacuación?	**2**
5.- ¿Están almacenados de manera segura y etiquetados los materiales inflamables?	**1**
6.- ¿Hay materiales aislantes de incendios, como cortafuegos, instalados donde sea necesario?	**1**
7.- ¿Los extintores están visibles y accesibles para el personal?	**1**
8.- ¿Se realiza una evaluación regular de riesgos de incendio en el laboratorio?	**1**
9.- ¿El laboratorio cumple con las normativas locales contra incendios?	**1**
10.- ¿Se realiza inspección periódica de los sistemas eléctricos?	**1**
11.- ¿Los muebles y equipos están fabricados con materiales retardantes de incendios?	0
12.- ¿Se utilizan sensores de temperatura en las áreas críticas?	**0**
13.- ¿Los cables eléctricos están organizados y protegidos?	**1**
14.- ¿El laboratorio tiene rociadores automáticos?	**1**
15.- ¿Las puertas de emergencia están libres de obstrucciones?	**1**
16.- ¿Se verifica la funcionalidad del sistema de detección periódicamente?	**1**
17.- ¿Los equipos están diseñados para evitar sobrecalentamiento?	**1**
18.- ¿Se limita el uso de enchufes múltiples?	**1**
19.- ¿El sistema de aire acondicionado está libre de acumulación de polvo?	**1**
20.- ¿Se han registrado incendios previos en el laboratorio?	**1**
21.- ¿El personal de mantenimiento está capacitado para prevenir incendios?	**1**
22.- ¿El laboratorio tiene un protocolo de revisión post-incendio?	**1**
23.- ¿Se cuenta con un listado de contactos de emergencia?	**1**
24.- ¿Hay un suministro adecuado de equipos de primeros auxilios y se encuentran accesible?	**1**
25.- ¿Los equipos quedan apagados al finalizar su labor?	**1**
Total de riesgos no aplica(2)	1
Total de controles evaluados	24
Seguridad (1)	22
Riesgo (0)	2
Porcentaje de seguridad	**92%**
Porcentaje de riesgo	**8%**
	100%

Tabla 18 Cuestionarios para identificar riesgos (Incendio)

Cuestionarios para identificar riesgos (Inundación). "Inundación".	K1 Pág. 3-5
Preguntas	**Respuestas**
1.- ¿El laboratorio está ubicado en una zona propensa a inundaciones?	**1**
2.- ¿Existen sistemas de drenaje alrededor del laboratorio?	**0**
3.- ¿Los equipos están ubicados en lugares elevadas?	**1**
4.- ¿Se realizan inspecciones regulares de las tuberías del laboratorio?	**1**
5.- ¿El personal tiene conocimientos sobre algún protocolo en caso de inundación?	**1**
6.- ¿Se cuenta con algún sistema de detección temprana de agua?	**0**
7.- ¿Cuenta con un plan de evacuación en caso de inundación?	**0**
8.- ¿Los componentes eléctricos están protegidos contra el contacto con agua?	**0**
9.- ¿Los servidores están ubicados en salas con control de humedad?	**1**
10.- ¿Se han instalado barreras físicas contra el agua en puntos vulnerables?	**0**
11.- ¿Se inspeccionan periódicamente los techos para prevenir filtraciones?	**1**
12.- ¿Los activos valiosos están protegidos contra posibles filtraciones?	**1**
13.- ¿El laboratorio tiene seguro contra daños por inundación?	**1**
14.- ¿Los sistemas de alarma están diseñados para funcionar en caso de inundación?	**0**
15.- ¿Se tiene un plan de recuperación ante desastres naturales?	**1**
16.- ¿Se limita el uso de agua en áreas cercanas a los equipos?	**1**
17.- ¿El laboratorio cuenta con un protocolo de respuesta rápida ante inundaciones?	**0**
18.- ¿Se utilizan pisos resistentes al agua en áreas sensibles?	**2**
19.- ¿se cuenta con herramientas para sellar fugas de emergencia?	**0**
20.- ¿Se han realizado simulacros relacionados con emergencias de agua?	**2**
21.- ¿Las paredes de las oficinas o laboratorios tienen daño por humedad?	**1**
22.- ¿Se verifica que los sistemas de alarma sean resistentes a la humedad?	**1**
23.- ¿Se realizan análisis de impacto financiero ante posibles inundaciones?	**0**
24.- ¿Alguna vez se filtró agua por las ventanas?	**2**
25.- ¿Anteriormente ha existido daños en los equipos por agua?	**1**
Total de riesgos no aplica(2)	3
Total de controles evaluados	22
Seguridad (1)	13
Riesgo (0)	9
Porcentaje de seguridad	**59%**
Porcentaje de riesgo	**41%**
	100%

Tabla 19 Cuestionarios para identificar riesgos (Inundación).

Cuestionarios para identificar riesgos (Malware). “Controles para Malware”.	K1 Pág. 4-5
Preguntas	**Respuestas**
1.- ¿Se han realizado auditorías de seguridad informática?	**0**
2.- ¿Todos los equipos cuentan con un software antivirus actualizado?	**1**
3.- ¿Se realizan análisis periódicos de seguridad informática?	**0**
4.- ¿Se realizan análisis periódicos de malware en todos los equipos?	**1**
5.- ¿El personal reciben formación sobre cómo identificar y evitar malware?	**1**
6.- ¿Los equipos de la red están protegidos con contraseñas seguras?	**1**
7.- ¿El acceso a los dispositivos está limitado a personal autorizado?	**1**
8.- ¿Se cuenta con políticas de uso de dispositivos extraíbles para prevenir la propagación de malware?	**1**
9.- ¿Se lleva un registro de las modificaciones realizadas en los sistemas para detectar posibles cambios maliciosos?	**1**
10.- ¿Se cuenta con medidas de protección ante posibles ataques de denegación de servicios?	**0**
11.- ¿Se utilizan firewalls para proteger la red?	**1**
12.- ¿Se realizan respaldos regulares de datos críticos?	**0**
13.- ¿Se limita el acceso a sitios web potencialmente peligrosos?	**1**
14.- ¿El laboratorio tiene un sistema de detección de intrusiones?	**0**
15.- ¿Los dispositivos cuentan con cifrado para proteger datos sensibles?	**1**
16.- ¿El laboratorio tiene un plan de respuesta a incidentes de malware?	**0**
17.- ¿Los usuarios tienen permisos limitados en los sistemas?	**1**
18.- ¿El laboratorio tiene un protocolo de aislamiento para equipos infectados?	**1**
19.- ¿El laboratorio cuenta con un seguro contra incidentes cibernéticos?	**2**
20.- ¿Se cuenta con medidas de seguridad en las conexiones Wi-Fi?	**1**
21.- ¿Se lleva un registro de los accesos a los equipos informáticos?	**1**
22.- ¿Se implementan políticas de uso para dispositivos móviles?	**1**
23.- ¿Se realiza una prueba de penetración regularmente?	**1**
24.- ¿El personal está informado sobre el impacto financiero de un ataque de malware?	**1**
25.- ¿Se implementa la segmentación de red para mitigar el riesgo de malware?	**0**
Total de riesgos no aplica(2)	1
Total de controles evaluados	24
Seguridad (1)	17
Riesgo (0)	7
Porcentaje de seguridad	**71%**
Porcentaje de riesgo	**29%**
	100%

Tabla 20 Cuestionarios para identificar riesgos (Malware).

Cuestionarios para identificar riesgos (Equipos). “Controles para daño de Equipo”.	K1 Pág. 5-5
Preguntas	**Respuestas**
1.- ¿Hay inventario de los equipos en buen estado?	**1**
2.- ¿Se realiza mantenimiento preventivo regular en los equipos?	**1**
3.- ¿Se realiza inspecciones para comprobar el estado de los equipos?	**1**
4.- ¿Se utilizan sistemas de protección eléctrica, como UPS o supresores de picos?	**1**
5.- ¿El personal está capacitado para operar los equipos correctamente?	**1**
6.- ¿El laboratorio tiene un sistema adecuado de ventilación y enfriamiento?	**1**
7.- ¿Los equipos están instalados sobre superficies estables y niveladas?	**1**
8.- ¿Se prohíbe el consumo de alimentos y bebidas cerca de los equipos?	**1**
9.- ¿Se capacita al personal para el uso adecuado de los equipos?	**1**
10.- ¿Se revisan los cables de los equipos periódicamente para evitar cortocircuitos?	**0**
11.- ¿Se realiza limpieza interna de los equipos?	**1**
12.- ¿Los equipos cuentan con protección sobre tención eléctrica?	**1**
13.- ¿Los equipos están asegurados contra daños accidentales?	**2**
14.- ¿El laboratorio tiene procedimientos para reportar daños?	**1**
15.- ¿Se dispone de repuestos esenciales para equipos críticos?	**0**
16.- ¿Se han implementado controles para evitar el uso indebido de los equipos?	**1**
17.- ¿El personal cuenta con manuales de operación para el uso de los equipos?	**0**
18.- ¿Los equipos portátiles están protegidos contra caídas accidentales?	**1**
19.- ¿Se protegen los cables contra daños por objetos cortantes o desgaste?	**1**
20.- ¿El laboratorio tiene contratos de soporte técnico con los fabricantes?	**0**
21.- ¿El sistema de cableado está correctamente instalado?	**1**
22.- ¿Hay sensor de humedad y temperatura?	**1**
23.- ¿Se establecen límites de uso para evitar el sobrecalentamiento?	**1**
24.- ¿El laboratorio cuenta con políticas para la correcta desconexión de dispositivos?	**1**
25.- ¿El laboratorio tiene un plan de reemplazo para equipos obsoletos?	**0**
Total de riesgos no aplica(2)	1
Total de controles evaluados	24
Seguridad (1)	19
Riesgo (0)	5
Porcentaje de seguridad	**79%**
Porcentaje de riesgo	**21%**
	100%

Tabla 21 Cuestionarios para identificar riesgos (Daños a equipos).

4.5.3 Análisis de resultados

La matriz de riesgo es una herramienta clave en el análisis y gestión de riesgos, ya que permite visualizar de manera clara la relación entre la probabilidad de ocurrencia de un evento y el impacto que este puede generar en los activos o procesos críticos.

En este estudio, se utiliza una matriz de riesgo para evaluar y categorizar las amenazas presentes en los laboratorios informáticos de la Unidad Educativa Americano. A través de un análisis detallado, que incluye amenazas como robo, incendio, daño de equipos, inundaciones y malware, se cruzan los valores de probabilidad e impacto, previamente calculados, para identificar las prioridades de mitigación. Este enfoque busca garantizar la seguridad física de los recursos tecnológicos y contribuir a la continuidad operativa en un entorno educativo cada vez más dependiente de la tecnología.

MATRIZ DE RIESGO

IMPACTO

Riesgo	Impacto	Gravedad	Valor de Riesgo	Nivel de Riesgo
Robo	3	2	6	Riesgo apreciable
Incendio	2	1	2	Riesgo marginal
Daño de equipo	2	2	4	Riesgo apreciable
Inundaciones	4	3	12	Riesgo importante
Malware	3	2	6	Riesgo apreciable

Ilustración 4
Matriz de riesgo

La matriz evidencia que las inundaciones presentan el nivel de riesgo más alto, clasificado como "importante", y deben abordarse con prioridad. Los riesgos como el robo, el daño de equipos y el malware son apreciables y requieren atención moderada, mientras que el

incendio presenta un riesgo marginal.

GRAVEDAD	IMPACTO	CONSIDERACIONES
1	MAS BAJO	Las instalaciones quedan temporalmente cerrada o no puede operar, pero puede continuar su actividad. La interrupcion es menor a 8 horas. Existe un daño limitado de activos. La mayoría de las instalaciones no se verán afectadas
2	BAJO	Interrupción de operaciones por un periodo moderado (8 a 24 horas). Algunos activos pueden resultar dañados pero son recuperables o sustituibles fácilmente. El impacto se localiza en una parte específica de la institución.
3	MEDIO	Afectación significativa de las operaciones normales, con interrupciones entre 1 y 3 días. Se dañan activos importantes, aunque es posible su recuperación. La continuidad de actividades requiere medidas correctivas inmediatas.
4	ALTO	Interrupción grave de actividades por más de 3 días. Se pierden datos o activos importantes y algunos no pueden recuperarse. Varias áreas de la institución quedan inoperativas temporalmente. Se requieren recursos externos o tiempo prolongado para restaurar las operaciones.
5	MÁS ALTO	Daños irreparables en instalaciones / afectada más allá del uso habitable. La mayoría de los datos y activos se pierden, destruyen o dañan sin posibilidad de reparación o restauración.

Tabla 22 Valoración de impacto

	Valor de riesgo	
	Valor	
Mas.Bajo	1	1% - 10%
	2	11% - 30%
	3	31% - 50%
	4	51% - 75%
Mas.Alto	5	76% - 100%

Ilustración 5 Valoración de riesgo del cuestionario

LEYENDA							
			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO
APARICIÓN (probabilidad)	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	10
	MUY BAJA	1	1	2	3	4	5
COLOR	RANGO	NIVEL DE RIESGO	MEDIDAS				
	DE15 A 25	MUY GRAVE	Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el				
	DE 9 A 12	IMPORTANTE	Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.				
	DE 3 A 8	APRECIABLE	Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables				
	DE 1 A 2	MARGINAL	Se vigilará aunque no requiere medidas preventivas de partida				

Ilustración 6 Gravedad de impacto

Se logra apreciar que al analizar y evaluar los parámetros de posibles riegos que tendrían los componentes informáticos de la institución, se obtuvieron resultados de riesgos apreciables y riesgo importante. Para medir el nivel de riesgo se utilizó la siguiente matriz de riesgo leyenda.

La Matriz de Riesgo Leyenda establece una escala de gravedad de impacto que varía en función de los efectos que el riesgo podría generar. Los niveles de gravedad se definen en términos de los efectos inmediatos y secundarios sobre los recursos, la operación, el entorno social y ambiental, así como sobre los objetivos estratégicos del proyecto. Para este propósito, la metodología utiliza una escala cualitativa y cuantitativa que permite una evaluación precisa y diferenciada de los diferentes tipos de riesgos.

La leyenda de gravedad se divide en cinco niveles, los cuales se describen a continuación:

Gravedad Extrema (Nivel 5):

Este nivel representa los riesgos cuyo impacto tiene consecuencias desastrosas e irreparables para el sistema o proyecto. Los efectos de estos riesgos pueden ser fatales para la viabilidad del proyecto, ocasionando daños catastróficos tanto a las personas como a los activos

materiales. Estos eventos pueden afectar gravemente la continuidad operativa, la reputación organizacional y pueden incluso poner en riesgo la sostenibilidad a largo plazo del proyecto. Se consideran eventos de alto impacto, como desastres naturales, incidentes graves de seguridad, o fracasos críticos en la infraestructura.

Gravedad Alta (Nivel 4):

Los riesgos clasificados en este nivel tienen un impacto significativo, alterando sustancialmente las operaciones o resultados esperados. Aunque no sean fatales, sus efectos pueden generar pérdidas considerables en términos de recursos, tiempo y eficiencia, así como un daño considerable a la imagen de la entidad. En términos de la gestión ambiental, este nivel podría implicar una alteración considerable del ecosistema o la comunidad, sin que necesariamente se alcancen niveles extremos de devastación.

Gravedad Moderada (Nivel 3):

En este nivel, los riesgos presentan consecuencias visibles que afectan el rendimiento del proyecto o los resultados operativos, pero sus efectos no son devastadores. Los daños pueden ser reparables a corto plazo y no comprometen gravemente la viabilidad general del proyecto. Este tipo de riesgos podría incluir retrasos operativos o incidentes técnicos que requieran ajustes, pero no representan una amenaza crítica para el éxito del proyecto en su conjunto.

Gravedad Baja (Nivel 2):

Los riesgos de gravedad baja tienen un impacto limitado que no afecta de manera significativa el desarrollo de las operaciones. Estos riesgos pueden ser cosas como problemas menores de logística, fallos en equipos no esenciales o alteraciones en el proceso que no implican interrupciones sustanciales. Las medidas correctivas son relativamente simples y rápidas, y los costos asociados a estos riesgos no superan los presupuestos planeados.

Gravedad Insignificante (Nivel 1):

Los riesgos clasificados en este nivel presentan consecuencias mínimas, sin apenas repercusiones notables sobre la continuidad o el rendimiento del proyecto. Se consideran incidentes de rutina, sin impactos serios sobre los objetivos operativos, financieros o sociales del proyecto. Estos riesgos no requieren medidas correctivas complejas y generalmente se resuelven de forma automática mediante las políticas estándar de operación.

Color	Rango	Tipo riesgo	Descripción
	>=15 y <25	Riesgo muy grande	Requiere medidas urgentes
	>=12 y <15	Riesgo importante	Medidas preventivas obligatorias
	>=3 y <12	Riesgo apreciable	Estudiar si es posible aplicar medidas
	1 y 2	Riesgo marginal	Se vigila, aunque no requiere medidas

Ilustración 7
Matriz de riesgo Leyenda

5 Hallazgos

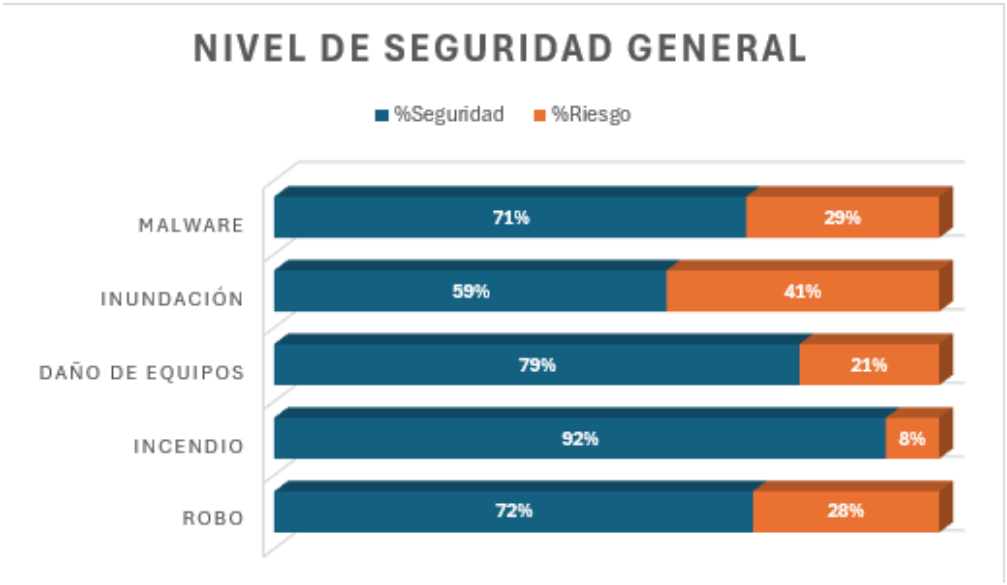


Ilustración 8
Nivel de seguridad general

Interpretación:

El análisis de la Ilustración 11, que representa el nivel general de seguridad en los laboratorios de computación de la Unidad Educativa Americano, destaca el riesgo más crítico en el parámetro de inundación, con un 41% de vulnerabilidad. Este porcentaje indica que existe una alta probabilidad de que este evento ocurra, lo cual podría ocasionar daños irreparables a los dispositivos electrónicos y afectar directamente la continuidad de las actividades académicas. La identificación de este riesgo subraya la necesidad de implementar sistemas eficientes de control de inundaciones, tales como drenajes adecuados, sensores de humedad y planes de acción ante emergencias.

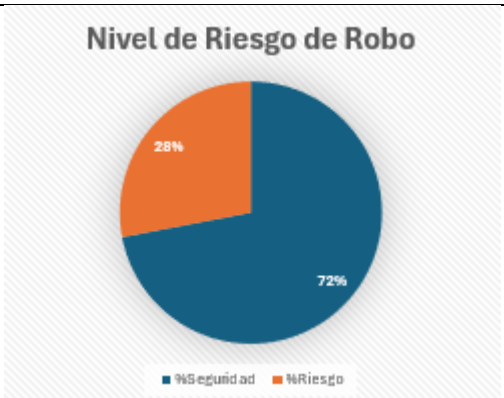
En cuanto al daño de equipos, se presenta una seguridad del 71%, lo cual indica que aún existe un 29% de exposición al riesgo. Este aspecto puede estar relacionado con fallos en el mantenimiento preventivo, condiciones inadecuadas de almacenamiento o fallas en los sistemas eléctricos. Es crucial optimizar las prácticas de mantenimiento, implementar sistemas de monitoreo continuo y garantizar condiciones físicas adecuadas para preservar la integridad de los equipos.

El riesgo relacionado con incendios muestra un control significativo, alcanzando un 92% de seguridad. Este resultado refleja la efectividad de las medidas implementadas, como extintores, detectores de humo y sistemas de evacuación. Sin embargo, debe mantenerse un programa constante de capacitación para el personal, simulacros regulares y mantenimiento de los sistemas de detección y control para garantizar que este nivel de seguridad se mantenga.

Finalmente, el riesgo de robo presenta una seguridad del 72%, indicando un 28% de vulnerabilidad. Este resultado evidencia la necesidad de reforzar los sistemas de acceso restringido, implementar videovigilancia de alta calidad y garantizar la custodia adecuada de los equipos fuera del horario de uso. En este sentido, un enfoque preventivo y proactivo resulta indispensable para disminuir la probabilidad de incidentes en esta área.

6 Nivel de Riesgo de Robo

Gráfico:	**Causas:**

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

Medidas para evitar el ingreso no autorizado al área informática.
Biométricos para restringir el acceso.
Medidas de seguridad física en componentes electrónicos.
Sistemas de detección de movimiento.
Implementación de protocolos de seguridad física en caso de emergencia.
Revisión de registros de acceso con regularidad.

</td>
</tr>
<tr>
<td colspan="2">Interpretación: El análisis del nivel de riesgo de robo indica que el laboratorio de computación de la Unidad Educativa Americano tiene un 72% de seguridad, lo que refleja un control relativamente adecuado en las medidas implementadas. Sin embargo, el 28% restante representa una vulnerabilidad significativa, lo que sugiere la necesidad de reforzar los mecanismos de protección para mitigar los riesgos asociados a posibles intrusiones no autorizadas o hurtos

Entre las causas identificadas que contribuyen a esta vulnerabilidad, se destaca la insuficiencia en medidas específicas como sistemas de control de acceso avanzado, tales como el uso de tecnología biométrica para restringir el ingreso únicamente al personal autorizado. Además, la falta de protocolos regulares de revisión de registros de acceso y la implementación limitada de sistemas de detección de movimiento podrían incrementar las probabilidades de incidentes relacionados con el robo.
Agregando que la seguridad física de los componentes electrónicos requiere ser fortalecida mediante la instalación de gabinetes o cajas de seguridad con cerraduras adecuadas, así como la implementación de protocolos de seguridad en caso de emergencia. Esto garantizaría una protección adicional para los equipos en situaciones críticas que puedan facilitar la sustracción de bienes.

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

Tabla 23
Nivel de Riesgo de Robo

7 Nivel de Riesgo de Inundación

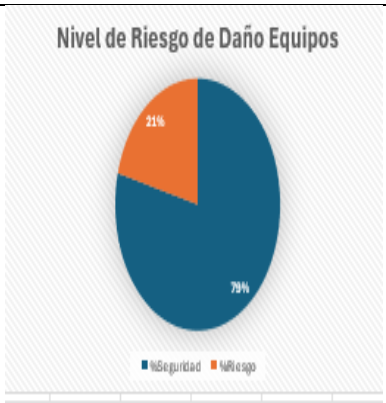
Gráfico:	Causas:
	• Drenaje adecuado alrededor del laboratorio para evitar acumulación de agua. • Sistemas electrónicos adecuados para el contacto al agua. • Protocolos para evacuación en caso de emergencia. • Sistemas de alerta temprana. • Medidas físicas para prevenir el ingreso de agua en áreas críticas. • Ejercicios prácticos de preparación en caso de inundación. • Herramientas para sellar fugas. • Analizar el impacto financiero en caso de perdidas debido a inundaciones.

Interpretación: El análisis del nivel de riesgo de inundación refleja una situación preocupante en los laboratorios de la Unidad Educativa Americano, con un 41% de riesgo asociado a este tipo de eventos. Esto indica que las medidas preventivas y los protocolos existentes no son suficientes para mitigar adecuadamente los efectos de las inundaciones, lo que podría generar daños significativos a los equipos electrónicos y la infraestructura del laboratorio. Por otro lado, el nivel de seguridad alcanza un 59%, lo cual evidencia un área de mejora crucial. • Entre las causas identificadas, se resalta la falta de un drenaje adecuado en las instalaciones para prevenir la acumulación de agua, así como la ausencia de sistemas electrónicos protegidos contra el contacto con líquidos. Además, la carencia de protocolos de evacuación y de un sistema de alerta temprana disminuye la capacidad de respuesta ante situaciones de emergencia, lo que incrementa la probabilidad de daños materiales significativos. • De la misma manera, se observan deficiencias en la implementación de medidas físicas para prevenir la entrada de agua en zonas críticas, como puertas o ventanas vulnerables. La falta de ejercicios prácticos de preparación ante inundaciones también representa un desafío, ya que limita la preparación del personal frente a este tipo de eventualidades. Complementar estas acciones con herramientas especializadas para sellar fugas y un análisis detallado del impacto financiero debido a potenciales pérdidas contribuiría significativamente a reducir el riesgo.

Tabla 24
Nivel de Riesgo de Inundación

8 Nivel de Riesgo de Daño de Equipos

Gráfico:	**Causas:**
	• Verificar con regularidad el estado del funcionamiento de los equipos. • Plan de reemplazo para equipos obsoletos. • Manual de operación o manejo de los equipos para el personal.

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

- Disponibilidad de repuestos para equipos en caso de emergencia.
- Implementar contratos para soporte tecnico.

</td>
</tr>
<tr>
<td colspan="2">

Interpretación: El análisis del nivel de riesgo de daño de equipos en los laboratorios de computación de la Unidad Educativa Americano evidencia un 79% de seguridad, lo que sugiere que la mayoría de los controles actuales son efectivos. Sin embargo, el 21% de riesgo restante representa una vulnerabilidad que podría comprometer la operatividad de los dispositivos electrónicos, afectando el desarrollo de actividades académicas y administrativas.

- Entre las causas principales de este riesgo se encuentra la ausencia de una verificación regular del estado de funcionamiento de los equipos, lo que incrementa la probabilidad de fallos inesperados. Asimismo, la falta de un plan estructurado de reemplazo para equipos obsoletos puede contribuir a que los dispositivos antiguos sufran daños frecuentes, aumentando los costos de mantenimiento y reparación.
- Otro factor relevante es la falta de un manual de operación o manejo de los equipos para el personal, lo cual podría provocar un uso inadecuado de los dispositivos. Adicionalmente, la disponibilidad limitada de repuestos en caso de emergencias técnicas reduce la capacidad de respuesta inmediata para solucionar problemas críticos, incrementando los tiempos de inactividad.

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

Tabla 25
Nivel de Riesgo de Daño de Equipos

9 Nivel de Riesgo de Incendio

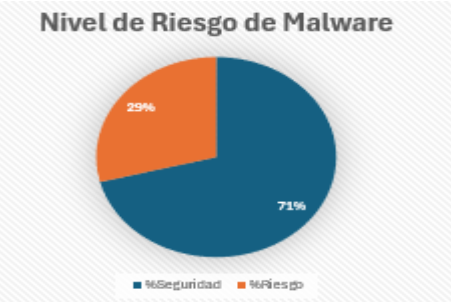
Gráfico:	**Causas:**
	• Equipos muebles y equipos fabricados con materiales retardantes. • Sensores de temperatura en áreas críticas.

Interpretación: El análisis del **nivel de riesgo de incendio** en los laboratorios de computación de la Unidad Educativa Americano refleja un control sobresaliente, alcanzando un **92% de seguridad**, lo que indica que las medidas implementadas son altamente eficaces para prevenir o mitigar incidentes relacionados con incendios. Sin embargo, se mantiene un **8% de riesgo residual**, lo cual sugiere la importancia de seguir fortaleciendo las estrategias de prevención y respuesta ante este tipo de eventos.

- Entre las **causas principales** que sustentan este nivel de seguridad se encuentra el uso de **equipos fabricados con materiales retardantes al fuego**, los cuales disminuyen significativamente la propagación de un incendio en caso de ocurrencia. Asimismo, la instalación de **sensores de temperatura en áreas críticas** permite una detección temprana de posibles anomalías, mejorando la capacidad de respuesta y control frente a situaciones de emergencia.
- Aunque el nivel de riesgo es bajo, es fundamental mantener y optimizar estas medidas preventivas. La revisión periódica de los materiales de los equipos, así como la funcionalidad de los sensores de temperatura, debe ser prioritaria para asegurar su correcto desempeño. También es recomendable realizar simulacros regulares y capacitar al personal en el manejo de extintores y evacuación en caso de emergencia.

Tabla 26
Nivel de Riesgo de Incendio

10 Nivel de Riesgo de Malware

Gráfico:	**Causas:**
	• Implementación de auditorías dirigidas a seguridad informática. • Análisis periódicos en los equipos del laboratorio. • Medidas de protección ante ataques de denegación de servicio. • Respaldo regular de datos críticos. • Sistema de detección de intrusiones (IDS)

	• Plan de respuesta sobre incidentes de malware. • Segmentación de red.
Interpretación: El análisis del nivel de riesgo de malware en los laboratorios de computación de la Unidad Educativa Americano revela un 71% de seguridad, lo que indica que las medidas implementadas han sido efectivas en gran medida para prevenir ataques cibernéticos. Sin embargo, persiste un 29% de riesgo, lo que representa una vulnerabilidad significativa que podría comprometer la integridad de los sistemas y datos almacenados en los equipos de la institución. • Otro factor crucial es la falta de un plan integral de respuesta ante incidentes de malware, el cual permita mitigar rápidamente los efectos de un ataque en caso de que ocurra. La segmentación de red también debe ser considerada para limitar el alcance de un posible brote de malware dentro del laboratorio, protegiendo así las áreas críticas de los sistemas informáticos.	

Tabla 27
Nivel de Riesgo de Malware

10.1.1 Guía de buenas prácticas informáticas para la seguridad física

A continuación, se presenta una guía enfocada en la seguridad física de entornos informáticos. La protección de equipos y datos es un desafío esencial en nuestra era tecnológica. En primer lugar, quiero destacar la importancia de garantizar una infraestructura adecuada. Los equipos deben estar ubicados en áreas seguras, protegidos de riesgos como inundaciones o incendios. Es fundamental implementar sistemas avanzados de control de acceso, como cerraduras electrónicas y dispositivos biométricos, para evitar el ingreso de personas no autorizadas. Adicionalmente, la instalación de cámaras de videovigilancia en áreas

críticas refuerza la protección física de los espacios, complementada con un diseño ergonómico que facilite el trabajo eficiente y seguro.

La seguridad física en entornos informáticos es esencial para proteger los equipos, la información y garantizar la continuidad operativa. Una adecuada infraestructura debe priorizar la ubicación estratégica de los equipos en áreas seguras, protegidas contra riesgos ambientales como inundaciones o incendios. Además, es fundamental implementar sistemas de control de acceso, como cerraduras electrónicas y dispositivos biométricos, para restringir el ingreso únicamente a personal autorizado. La videovigilancia en puntos críticos y áreas de acceso, junto con un diseño ergonómico del espacio de trabajo, son medidas clave para mitigar riesgos y garantizar un entorno físico seguro.

El mantenimiento preventivo y correctivo es otro aspecto crucial. La revisión periódica del estado de los equipos permite detectar fallas antes de que generen mayores problemas, mientras que la instalación de sistemas de protección eléctrica, como reguladores de voltaje y UPS, protege los dispositivos de cortes y variaciones de energía.

La protección frente a riesgos ambientales debe incluir medidas como sistemas de drenaje para prevenir inundaciones y la instalación de detectores de humo, sensores de temperatura y extintores diseñados para incendios eléctricos. Estas herramientas, combinadas con protocolos de evacuación y simulacros regulares, garantizan una respuesta oportuna ante emergencias. Por último, la capacitación constante del personal sobre manejo de equipos y normativas de seguridad, junto con auditorías regulares y un inventario detallado de equipos, fortalece la seguridad física y asegura la protección integral de los recursos informáticos frente a amenazas internas y externas.

CAPÍTULO V

11 EVALUACIÓN DE RESULTADOS

11.1 Introducción

En este capítulo se procede a la realización detallada del informe de auditoría informática a la seguridad física de los equipos informáticos de la Unidad Educativa Americano, contando con un manual de recomendaciones para evitar riesgos en la seguridad del laboratorio.

Tipo de auditoria

Auditoría informática de seguridad física del laboratorio de computación de la Unidad Educativa Americano.

Dirigido: Lic. Tobar Christobal rector de la institución.

Motivo: Trabajo de titulación

Objetivos:

- Identificar principales riesgos de seguridad que existen en la Unidad Educativa Americano.
- Analizar y verificar el nivel se seguridad de los componentes informáticos de la institución.

Personal relacionado:

- Rector
- Docentes

Alcance:

Para realizar el trabajo de investigación de esta auditoría de seguridad informática física se aplicó la metodología de análisis de Riesgo Magerit. Utilizando parámetros para evaluar:

- Fundamentación teórica sobre la seguridad de la información y normas, leyes, políticas, relacionada a la misma.
- Revisar metodología MAGERIT junto a los pasos de su ejecución.
- Definir activos
- Definir Amenazas

11.2 Resultado de auditoria

En la presente auditoría se realizó un análisis exhaustivo de los riesgos relacionados con la seguridad física en los laboratorios de computación de la Unidad Educativa Americano. Los resultados obtenidos reflejan la importancia de contar con medidas preventivas y correctivas para mitigar amenazas como el acceso no autorizado, inundaciones, daños a equipos, incendios y malware. A través de esta evaluación, se ha logrado identificar tanto fortalezas como áreas de mejora en los sistemas implementados, permitiendo establecer un diagnóstico preciso sobre la situación actual.

Una de las principales fortalezas detectadas es la alta efectividad en las medidas de prevención frente a incendios, donde se evidenció un nivel de seguridad destacado. Esto se debe a la implementación de equipos fabricados con materiales retardantes y sensores de temperatura en áreas críticas, lo cual reduce significativamente la probabilidad de que un incendio afecte la operatividad de los laboratorios. No obstante, se observó que otros riesgos, como las inundaciones, presentan mayores vulnerabilidades debido a la ausencia de sistemas de drenaje adecuados y medidas preventivas suficientes.

En cuanto a la seguridad de los equipos, los resultados muestran que se ha logrado un nivel aceptable de protección en términos de mantenimiento y monitoreo regular. Sin embargo, aún persisten riesgos asociados al envejecimiento de los dispositivos y la falta de un plan integral de reemplazo de equipos obsoletos. Esta situación incrementa la probabilidad de fallas operativas y posibles interrupciones en las actividades académicas, lo que resalta la necesidad de una gestión tecnológica más estratégica y preventiva.

Por último, se evaluó la preparación frente a robos y amenazas informáticas, donde se identificó un nivel de seguridad moderado. Aunque existen sistemas de control de acceso y medidas básicas de protección, es indispensable fortalecer estas iniciativas mediante la incorporación de herramientas más avanzadas, como sistemas biométricos, cámaras de vigilancia con monitoreo en tiempo real y segmentación de redes para minimizar los riesgos de malware. La evaluación general permite concluir que, si bien se cuenta con bases sólidas para la protección de los laboratorios, es necesario implementar mejoras estratégicas que garanticen una seguridad física integral y sostenible a largo plazo.

La imagen presenta un gráfico de pastel titulado "nivel de seguridad general", que muestra dos componentes principales relacionados con la seguridad física según un análisis basado en porcentajes:

1. Porcentaje de Seguridad (75%): Representa la proporción del entorno o sistema evaluado que se considera protegido, confiable y libre de amenazas significativas. Según la metodología Margerit,. Este porcentaje sugiere que la mayoría de los elementos clave están bien gestionados y cumplen con los estándares de seguridad.

2. Porcentaje de Riesgo (25%): Representa la parte del sistema que aún está expuesta a vulnerabilidades, amenazas o falta de medidas adecuadas de protección. En el marco de la metodología Margerit, esto puede reflejar fallos en la evaluación de riesgos, debilidades en las barreras físicas o tecnológicas, o una respuesta inadecuada ante posibles incidentes. Este porcentaje indica áreas que requieren atención prioritaria para minimizar riesgos y mejorar la seguridad general.

11.2.1.1 Guía de buenas prácticas

Ilustración 9
Portada de guía

Introducción

En el presente trabajo es la elaboración de un manual en base a seguridad física para que se emplee en los laboratorios de la Unidad Educativa Americano con el propósito de evitar riesgos en los componentes tecnológicos del área informática, con el cual se tendrán pautas detalladas para el correcto manejo, promoviendo y estableciendo pautas de seguridad para garantizar un entorno de trabajo seguro para los usuarios que realicen actividades en el especio de computación.

Es importante que tanto los usuarios y miembros del laboratorio se familiaricen con tener una responsabilidad compartida en cuanto a la seguridad y las pautas establecidas en el presente documento. Al implementarlas de manera consciente a los recursos tecnológicos se logra mitigar vulnerabilidades y mejorar la integridad, creando un entorno seguro y confiable para todos.

Ilustración 10
Introducción de la guía

Objetivo

- Elaborar un manual de buenas prácticas estableciendo medidas preventivas para garantizar el funcionamiento seguro del laboratorio de cómputo, especificando en cada parámetro que se evaluó para prevenir el impacto y minimizar riesgos, creando un ambiente seguro.

Ámbito de aplicación

El manual se aplica en la Unidad Educativa Americano, especificando el laboratorio de computación de la institución, a, personal docente, administrativo y estudiantes quienes realizan actividades en el laboratorio de informática.

Ilustración 11
Objetivo de la guía

Definiciones

Buenas prácticas: Conjunto de procedimientos, normas y comportamientos recomendados que, al aplicarse, permiten lograr mejores resultados, eficiencia y calidad en tareas específicas. En informática, estas prácticas aseguran la seguridad, el mantenimiento y el rendimiento de los sistemas y equipos.

Informática: Disciplina que estudia y desarrolla métodos, técnicas y herramientas para el procesamiento, almacenamiento y transmisión de información mediante computadoras y sistemas tecnológicos.

Medidas preventivas: Acciones tomadas con anticipación para evitar incidentes, daños o fallos en sistemas y equipos. En informática, estas medidas incluyen respaldos de información, mantenimiento regular y uso de software de seguridad.

Periféricos: Dispositivos externos conectados a una computadora que permiten la entrada, salida o almacenamiento de datos. Ejemplos incluyen teclados, impresoras, ratones, monitores, escáneres y unidades de almacenamiento externas.

Software: Conjunto de programas, aplicaciones y sistemas operativos que permiten el funcionamiento de una computadora y la realización de tareas específicas. Es la parte lógica e intangible de un sistema informático.

Hardware: Componentes físicos y tangibles de un sistema informático, como la computadora, el monitor, el teclado, el disco duro y demás dispositivos electrónicos que permiten el funcionamiento del equipo.

Ilustración 12
Definiciones de la guía

Normativas de seguridad para el uso de los laboratorios de computación

La importancia la implementar un manual es la capacidad y claridad que se da al momento de dar pautas claras estableciendo procedimientos definitivos, utilizándolos para garantizar la seguridad e integridad tanto de las personas, activos e información dentro del laboratorio de la institución: garantizando así la disminución de posibles riesgos.

En lo que respecta a la seguridad de los laboratorios existen varios aspectos los cuales debemos tomar en cuenta para fomentar un espacio tecnológico seguro:

A continuación, se especificarán pautas claras estableciendo medidas en cada componente analizado para mitigar riesgos en el laboratorio de la institución.

Ilustración 13
Normativas de seguridad para el uso de los laboratorios de computación

Riesgo	Recomendación
Robo	• **Implementación de sistemas de cerraduras electrónicas en puertas de acceso** basado en tags con códigos de identificación, permite controlar y registrar de manera precisa quiénes pueden ingresar al laboratorio y en qué momentos. • Crear un registro para el control de acceso y salida de los usuarios en el laboratorio. • Ningún estudiante o visitante puede permanecer en el laboratorio una vez que haya terminado la clase. • Asegurar los componentes físicos con anclajes para evitar la pérdida de algún elemento.

Riesgo	Recomendación
Incendio	• El uso de dispositivos de protección en ubicaciones específicas, como reguladores de voltaje y Sistemas de Alimentación Ininterrumpida (UPS). • Realizar sustitución en cuando a lo posible, los muebles y equipos por unos que estén fabricados con materiales certificados como retardantes de incendios. • Instalar sensores de temperatura en áreas críticas que puedan generar alertas ante cualquier actividad sospechosa o alarmante.

Ilustración 14
Riesgo de robo e incendio

Riesgo	Recomendación
Daño de equipos	• De acuerdo con la protección física de los computadores: Los estudiantes y profesores NO deben consumir ningún tipo de alimento o bebida dentro de los laboratorios, a fin de mantener la limpieza y orden en las instalaciones. • Un aspecto crucial de esta protección es asegurarse de que los cables y conexiones de red estén en buen estado, libres de daños o desgastes que puedan causar cortocircuitos o pérdida de conexión. • El mantenimiento adecuado de los equipos es una práctica esencial para protegerlos de posibles fallas y asegurar un funcionamiento confiable. • Implementar un programa de respaldos periódicos.

Riesgo	Recomendación
Inundación	• Instalar bombas de agua o sistemas de drenaje adicionales para zonas propensas a acumulación de agua. • Usar materiales impermeables para pisos, paredes y mobiliario en áreas críticas. • Instalar sensores de nivel de agua o suscribirse a servicios de alerta meteorológica. • Usar sistemas de desconexión automática para prevenir daños por cortocircuitos. • Instalar generadores y sistemas eléctricos a prueba de inundaciones.

Ilustración 15
Riesgo de daño de equipos e inundación

Riesgo	Recomendación
Malware	• El acceso a los servidores es de **uso exclusivo** de los Laboratorios, se limita a la modificación de solo el personal de laboratorio autorizado y basado en permisos de administrador otorgados previamente, limitando este acceso con credenciales de red. • Los usuarios NO deben usar el computador en actos que vayan en perjuicio de la moral y las buenas costumbres. • Se implementa un proceso regular de instalación de actualizaciones para todo el software utilizado en el laboratorio, incluyendo sistemas operativos(imágenes), aplicaciones, herramientas de seguridad y software de terceros autorizados • Se prohíbe instalar software sin licencia y no autorizado por el Departamento de Ciencias de la Computación. • Realizar auditorías de seguridad informática periódicamente, ya sea mediante personal interno capacitado o con servicios de terceros especializados. • Implementar herramientas de monitoreo continuo que identifiquen vulnerabilidades en tiempo real. • Implementar un programa de respaldos periódicos.

Ilustración 16
Riesgo de malware

11.2.1.2 Propuesta de Política de sanciones por infracciones de seguridad informática en la Unidad Educativa

La implementación de una política de sanciones para infracciones de seguridad informática en la Unidad Educativa es esencial para garantizar el correcto uso de los recursos tecnológicos y prevenir conductas que puedan comprometer la integridad de los datos y sistemas. Esta política tiene como objetivo establecer normas claras sobre las acciones no permitidas y las consecuencias asociadas, fomentando una cultura de responsabilidad en el manejo de los recursos informáticos. La propuesta considera el tipo de infracción, su gravedad y su impacto, para asegurar una aplicación proporcional y justa de las sanciones.

Las infracciones se clasifican en leves, graves y muy graves, según su nivel de impacto. Las infracciones leves incluyen el uso no autorizado de equipos para fines personales o la negligencia en el manejo de contraseñas. Por otro lado, las infracciones graves abarcan acciones como el intento de acceso no autorizado o la introducción de software malicioso. Las muy graves incluyen el robo de información confidencial, el daño intencional a los equipos y el uso de recursos tecnológicos para actividades ilícitas. Esta clasificación permite establecer sanciones adecuadas que van desde advertencias hasta la suspensión prolongada del acceso a los sistemas.

Las sanciones propuestas son progresivas y buscan, además de penalizar, educar a los infractores. Para infracciones leves, se plantean advertencias verbales o escritas y talleres de sensibilización. En casos graves, las sanciones incluyen la suspensión temporal de los recursos tecnológicos, el informe a las autoridades educativas o la obligación de reparar los daños causados. Las infracciones muy graves pueden derivar en la suspensión definitiva del acceso, procesos disciplinarios internos o incluso la denuncia a las autoridades legales en los casos que correspondan.

Propuesta de Política de sanciones por infracciones de seguridad informática en la Unidad Educativa

Clasificación de Infracciones:

Las infracciones se clasifican en tres niveles según su gravedad:

Leves:

- Uso no autorizado de equipos o software.
- Compartir contraseñas o credenciales sin autorización.
- Conexión de dispositivos externos sin aprobación previa.
- Incumplimiento de buenas prácticas básicas para el uso de equipos.

Graves:

- Descarga o uso de software sin licencia.
- Intento de acceder a información o recursos restringidos.
- Introducción de dispositivos contaminados con malware sin precauciones.
- Divulgación de información confidencial o sensible de la institución.

Muy Graves:

- Sabotaje, modificación o destrucción deliberada de datos o sistemas.
- Uso de tecnologías de la institución para actividades ilegales (plagio, hackeo, difusión de contenido inapropiado).
- Suplantación de identidad o acceso no autorizado a cuentas de terceros.
- Reincidencia en infracciones graves.

Ilustración 17
Propuesta de política de sanciones por infracciones de seguridad

11.2.1.3 Sanciones

Sanciones:

Las sanciones serán proporcionales a la gravedad de la infracción, contemplando acciones correctivas, disciplinarias y legales, si corresponde.

Para Infracciones Leves:

- Advertencia verbal y registro en el historial de infracciones.
- Sesión de concienciación o capacitación en seguridad informática.
- Restricción temporal del acceso a los recursos tecnológicos.

Para Infracciones Graves:

- Notificación formal y registro en el expediente del infractor.
- Suspensión temporal del acceso a los recursos tecnológicos.
- Requisito de participación en actividades educativas relacionadas con ética y seguridad informática.

Para Infracciones Muy Graves:

- Suspensión prolongada o definitiva del uso de los recursos tecnológicos.
- Comunicación formal a los representantes legales (en el caso de estudiantes).
- Aplicación de medidas disciplinarias internas (suspensión académica, separación de la institución).
- Notificación a las autoridades competentes si la infracción viola leyes vigentes.

Procedimiento de Aplicación:

1. **Detección:** Identificación de la infracción por parte del personal autorizado.
2. **Investigación:** Análisis detallado de la situación para determinar la gravedad.

Ilustración 18
Sanciones

Procedimiento de Aplicación:

1. **Detección:** Identificación de la infracción por parte del personal autorizado.
2. **Investigación:** Análisis detallado de la situación para determinar la gravedad.
3. **Notificación:** Comunicación del incidente al involucrado y, si aplica, a sus representantes.
4. **Audiencia:** Oportunidad para el involucrado de presentar su versión.
5. **Resolución:** Emisión de la sanción correspondiente por parte del comité disciplinario.
6. **Registro:** Archivo de la resolución en el historial institucional del infractor.

Ilustración 19
Procedimiento de aplicación

11.2.1.4 Propuestas de temas de capacitación para los usuarios del laboratorio sobre buenas prácticas informáticas y seguridad

Tema	Objetivo de la capacitación	Dinámicas de Capacitación
Gestión de Dispositivos Externos.	Manipulación de periféricos (USB, discos duros). Manejo adecuado de los dispositivos para prevenir la propagación de programa maligno y proteger la integridad de los sistemas y datos.	• Enfrentar escenarios reales de phishing o infecciones de malware. • cuestionarios sobre buenas prácticas y seguridad. • Infografías y videos que expliquen de manera sencilla los conceptos claves. • Adaptar los temas según el nivel de conocimiento y necesidades específicas de los usuarios del laboratorio.
Protección contra Malware .	Implementar medidas preventivas y correctivas para proteger los sistemas y datos contra virus, spyware, ransomware y otros tipos de software malicioso.	
Buenas Prácticas para el Uso de Equipos Compartidos.	Garantizar que los equipos utilizados por múltiples usuarios estén configurados y usados de manera segura, minimizando el riesgo de accesos no autorizados o pérdida de información.	
Fundamentos de Seguridad Informática.	Proporcionar los conocimientos básicos sobre los principios de seguridad informática, incluyendo confidencialidad, integridad, disponibilidad, autenticación y autorización.	

Políticas de Seguridad del Laboratorio.	Definir y hacer cumplir normas específicas para el uso seguro de los recursos tecnológicos en el laboratorio, protegiendo tanto los equipos como la información.	
Uso Ético de los Recursos Tecnológicos.	Promover el respeto y cumplimiento de normas éticas al utilizar tecnologías, evitando actividades inapropiadas o ilegales, como el plagio, el acceso no autorizado o el uso indebido de recursos.	
Respuesta ante Incidentes de Seguridad.	Establecer procedimientos claros y efectivos para identificar, contener, mitigar y resolver incidentes de seguridad que puedan comprometer los sistemas o datos.	
Normas de seguridad y políticas de uso.	Detallar reglas y directrices que los usuarios deben seguir para garantizar el uso responsable y seguro de los sistemas, aplicaciones y redes.	
Medidas en caso de incidentes naturales.	Desarrollar protocolos y acciones específicas para proteger los recursos tecnológicos y la información ante desastres naturales como terremotos, inundaciones o tormentas.	

Ilustración 20
Propuestas de temas de capacitación para los usuarios del laboratorio

11.2.2 Informe final del análisis de los datos

El análisis de los datos recopilados en los laboratorios de computación de la Unidad Educativa Americano ha permitido evaluar los niveles de seguridad física y lógica en relación con riesgos como inundaciones, daño de equipos, incendio, malware y robo. Los resultados reflejan áreas de vulnerabilidad significativas, especialmente en la prevención de inundaciones y ciberataques, donde se evidencian deficiencias en las medidas preventivas y los protocolos de respuesta. Estas debilidades podrían comprometer la continuidad operativa de los laboratorios y la integridad de los equipos tecnológicos.

En contraste, los riesgos asociados a incendios y robo presentan una gestión más robusta, lo que demuestra que ciertas medidas implementadas han sido efectivas para mitigar posibles incidentes. La utilización de tecnologías como sensores de temperatura, sistemas de control de acceso y protocolos de emergencia ha fortalecido la seguridad en estas áreas. Sin embargo, aún existen riesgos residuales que requieren ajustes y optimización para alcanzar niveles de protección más elevados.

Finalmente, los resultados obtenidos enfatizan la necesidad de adoptar un enfoque sistemático y científico basado en la **metodología Margerit**. Este enfoque permitirá priorizar los riesgos críticos, optimizar los recursos disponibles y garantizar la mejora continua en los sistemas de seguridad. La planificación estratégica, acompañada de auditorías periódicas y capacitación al personal, asegurará un entorno resiliente y seguro que salvaguarde tanto los equipos como la información en los laboratorios de la institución.

11.2.3 Recomendación de auditoria

Con base en el análisis realizado en los laboratorios de computación de la Unidad Educativa Americano, se recomienda implementar auditorías periódicas orientadas a evaluar y fortalecer la seguridad física. Estas auditorías deben centrarse en identificar vulnerabilidades en los sistemas de control de acceso, monitoreo y protección ambiental, así como en verificar la correcta implementación de protocolos de emergencia. Es esencial que los resultados de estas evaluaciones se traduzcan en un plan de acción estructurado, priorizando la mitigación de los riesgos más críticos y fortaleciendo las medidas existentes para proteger los equipos y la infraestructura.

Una de las áreas prioritarias a evaluar en las auditorías es la preparación frente a riesgos ambientales, como inundaciones e incendios. Es necesario verificar el estado de los sistemas de drenaje, sensores de humo y temperatura, así como la disponibilidad y funcionalidad de los extintores específicos para incendios eléctricos. Adicionalmente, se recomienda incluir ejercicios prácticos, como simulacros, para garantizar que el personal esté capacitado y pueda actuar de manera eficiente ante emergencias. Estas acciones no solo minimizarán los riesgos materiales, sino que también protegerán la seguridad de las personas que interactúan con los laboratorios.

Por otro lado, las auditorías deben abarcar la revisión de los equipos y su mantenimiento preventivo. Es fundamental evaluar el estado físico y funcional de los dispositivos, asegurando que se encuentren en condiciones óptimas. Asimismo, se debe supervisar la correcta implementación de medidas como el uso de reguladores de voltaje, unidades de respaldo eléctrico (UPS) y planes de reemplazo de equipos obsoletos. La falta de mantenimiento adecuado puede resultar en daños irreversibles en los dispositivos, lo que afectaría la operatividad de los laboratorios y supondría un costo elevado para la institución.

CAPÍTULO VI

12 CONCLUSIONES Y RECOMENDACIONES

12.1 Conclusiones

De acuerdo con lo efectuado en esta auditoria la revisión de los artículos especializados ha permitido identificar una amplia gama de fundamentos teóricos esenciales para fortalecer la protección de los equipos. Además, se ha evidenciado la importancia de la concienciación del usuario y formación continua en buenas practicas digitales como complemento indispensable de las medidas técnicas Estos fundamentos teóricos constituyen una base sólida para el diseño e implementación de mecanismos efectivos que contribuyen a reducir las vulnerabilidades y mejorar la resiliencia de los sistemas informáticos frente a amenazas cada vez más sofisticadas.

Durante la investigación y análisis de la infraestructura tecnológica en los laboratorios de la Unidad Educativa Americano, se llevó a cabo una inspección física que permitió evidenciar fallos y deficiencias en varios equipos informáticos. Se observarán problemas como conexiones defectuosas, ventilación inadecuada y desgaste en componentes periféricos. Aunque existen políticas de seguridad establecidas, la aplicación poco rigurosa de estas, sumada al desconocimiento de normas básicas de mantenimiento por parte de algunos usuarios, ha contribuido al deterioro progresivo de los equipos. Este diagnóstico resalta la necesidad de reforzar tanto las acciones correctivas en los dispositivos como la capacitación del personal para garantizar una infraestructura tecnológica eficiente y segura.

Utilizando la metodología MAGERIT como base para el diseño de una auditoría de riesgos, se logró analizar de forma integral los activos informáticos presentes en los laboratorios de la institución. Este enfoque permitió identificar vulnerabilidades. Uno de los hallazgos más relevantes fue la debilidad en la seguridad física, evidenciada por el caso control de acceso a los laboratorios, lo cual representa un riesgo significativo para la integridad de los equipos y la confidencialidad de la información. La auditoría diseñada no solo facilitó la detección de estos riesgos, sino que también constituye una herramienta fundamental para priorizar acciones correctivas y fortalecer la seguridad informática institucional de manera estructurada y sostenible.

La elaboración de una guía de auditoría permitió establecer recomendaciones claras y aplicables para mejorar los procedimientos de seguridad informática dentro de la institución. Aunque se reconocen los esfuerzos existentes en la implementación de ciertos controles, el análisis evidencia la necesidad de reforzar la capacitación del personal, actualizar las políticas vigentes y establecer mecanismos más rigurosos para asegurar su cumplimiento. Se concluye que la seguridad informática debe abordarse no solo desde el ámbito técnico, sino también desde una perspectiva organizacional. Por ello, es fundamental fomentar una cultura de seguridad que integre a todos los usuarios, promoviendo buenas prácticas y una participación activa en la protección de los recursos tecnológicos institucionales.

12.2 Recomendaciones

En base al análisis realizado en los laboratorios informáticos de la Unidad Educativa Americano, es fundamental incentivar a las autoridades y estudiantes que utilizan estos recursos a recibir capacitación en seguridad informática. Esta formación permitiría mitigar los riesgos asociados al uso de la tecnología, brindándoles una comprensión clara de lo que no se debe hacer y cómo reaccionar adecuadamente en caso de incidentes informáticos. La prevención y preparación son claves para minimizar los impactos negativos de un posible atentado a la seguridad.

Se recomienda al rector mejorar la infraestructura física que se gestionen mejoras en la infraestructura física de los laboratorios informáticos, priorizando la instalación de sistemas de monitoreo y control de acceso más eficientes. Estas acciones permitirán garantizar una protección más adecuada de los activos informáticos, minimizar los riesgos de seguridad y crear un entorno tecnológico más seguro para estudiantes y personal docente.

Al rector de la Unidad Educativa Americano, se le recomienda promover la implementación de auditorías informáticas periódicas en las áreas tecnológicas de la institución. Estas auditorías permiten identificar vulnerabilidades, evaluar el estado actual de los recursos tecnológicos y tomar decisiones estratégicas que fortalezcan la seguridad informática institucional.

Al departamento de tecnologías de la información, se le sugiere garantizar que las políticas de seguridad y las buenas prácticas informáticas estén disponibles, visibles y accesibles dentro de los laboratorios. La colocación de carteles informativos y recordatorios visuales contribuirá a concienciar a los usuarios sobre el uso responsable y seguro de los equipos, ayudando además a prolongar su vida útil.

A los responsables, se les recomienda mejorar las condiciones físicas de los laboratorios, incluyendo la instalación de sistemas de monitoreo y control de acceso más eficientes. Estas medidas permitirán reforzar la protección de los activos informáticos frente a amenazas tanto internas como externas.

BIBLIOGRAFÍA

13 Bibliografía

Albarracín Zambrano, L. O., Marín Vilela, C. M., Lozada Calle, J. C., & Martínez Matute, J. P. (02 de Octubre de 2021). *scielo*. Obtenido de scielo: http://scielo.sld.cu/scielo.php?pid=S2218-36202021000500345&script=sci_arttext

Ampuero Herrera, R. M. (2021). Gestión de riesgos de la información basado en la metodología Magerit para una notaría de la Región Lima, 2021. *alicia*.

Angamarca, L. (2021). *Estrategias de auditoría informática en la era de la transformación digital.* Argentina: digital. Technology Rain Journal, 1(1), e1-e1. doi:https://doi.org/10.55204/trj.v1i1.e1

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

Avila, H. F., González, M. M., & Licea, S. M. (2020). *LA ENTREVISTA Y LA ENCUESTA: ¿MÉTODOS O TÉCNICAS DE INDAGACIÓN EMPÍRICA?* Cuba: Didasc@lia: D&E. Obtenido de https://revistas.ult.edu.cu/index.php/didascalia/article/view/992/997

Balverdi Cruz, L. H., Linares Fernández, E., & Cuellar, I. (2023). Políticas de seguridad de la información y metodología Magerit en la empresa Induamerica Chiclayo S.A.C. *alicia*.

Beltrán, S. M., & Bernal, J. A. (2021). *Los paradigmas de la investigación: un acercamiento teórico para reflexionar desde el campo de la investigación educativa.* Guadalajara: Epub. doi:https://doi.org/10.23913/ride.v11i21.717

García, O., & Toribio, J. (2022). *Estadística y métodos cuantitativos II (Vol. 22).* Servicio de Publicaciones de la Universidad de Huelva. Obtenido de https://books.google.es/books?hl=es&lr=&id=8XeXEAAAQBAJ

Guamán, M., Carrillo Zenteno, J. A., Flores Urgilés, C., & Egas, M. R. (2023). *Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la*

metodología Magerit. Ecuador: Pro Sciences: Revista de Producción, Ciencias e Investigación, 7(49), 139-165. doi: https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp139-165

Guamán, M., Carrillo Zenteno, J. A., Flores Urgilés, C., Flores Urgilés, C., & Egas, M. R. (2023). ProSciences. *Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit*.

Guiller, R., Cahuaya, R., & René, R. (2023). *Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001.* Innovation and Software, 4(1), 96-106. doi:10.48168/innosoft.s11.a57

Gutierrez, M. L. (2019). *Repositorio Digital UASB Sede Bolivia*. Obtenido de Repositorio Digital UASB Sede Bolivia: http://repositorio.uasb.edu.bo/bitstream/20.500.14624/1039/2/2019-049T-EC04.pdf

Herszenbaun, M. (2022). *Método analítico y la carencia de síntesis en "El conocer analítico" de la Ciencia de la lógica de Hegel.* Nuevo Itinerario, 18(2), 92-102. doi:https://doi.org/10.30972/nvt.1826199

López, R. (2021). *La Encuesta.* Bellaterra Universitat Autònoma de Barcelona.

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

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

Martínez, V. (2022). *Técnicas e instrumentos de recolección de datos en investigación.* TEPEXI boletín científico de la escuela superior tepeji del río, 9(17), 38-39. doi:https://doi.org/10.29057/estr.v9i17.7928

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

Morillo Cadena, D. I. (2024). Elaboración de un plan de contingencia para TI en base del análisis de riesgos utilizando la metodología MAGERIT para una empresa textil. *PUCE*.

Nicolás Veiga, L. O. (2020). *Reflexiones sobre el uso de la estadística inferencial en investigación didáctica* (Vol. 7). Uruguay: Universidad de la República, Uruguay. doi:http://doi.org/10.29156/INTER.7.2.10

Paladines, L. (2023). *AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA INFRAESTRUCTURA TECNOLÓGICA EN LA UNIDAD EDUCATIVA ANTONIO JOSÉ DE SUCRE EN EL PERIODO 2022.* Universidad Laica Eloy Alaro de Manabí, El Carmen. Obtenido de https://repositorio.uleam.edu.ec/bitstream/123456789/4583/1/ULEAM-INFOR-0108.pdf

Pérez, S. (2021). *Investigación Documental.* México: Universidad Salazar Virtual.

Pinto, R. (2023). Escalabilidad y Sostenibilidad en Implementaciones de Blockchain para Auditoría Informática: Retos y Soluciones Futuras. *Technology Rain Journal*.

Puente, R. T. (2020). *LOS MÉTODOS DE INVESTIGACIÓN PARA LA ELABORACIÓN DE LAS TESIS DE MAESTRÍA EN EDUCACIÓN.* Perú: PUCP. Obtenido de https://repositorio.pucp.edu.pe/index/handle/123456789/195750

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

Reyes-Ruiz, L. C. (2020). *La investigación documental para la comprensión ontológica del objeto de estudio.* Universidad Simón Bolivar. Obtenido de https://hdl.handle.net/20.500.12442/6630

Robalino, A. P., Yanza Chávez, W. G., & Montoya Lunavictoria, J. K. (2022). Auditoría Informática. En *Auditoría Informática* (pág. 61). Riobamba.

Sampieri, R. H. (2020). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA.* México: McGRAW-HILL. Obtenido de http://www.biblioteca.cij.gob.mx/archivos/materiales_de_consulta/drogas_de_abuso/articulos/sampierilasrutas.pdf

Sánchez, M., & Mejias, M. (2022). *Diseño de Metodologías Mixtas una revisión de las estrategias para combinar.* Revista Electrónica Humanas Enfermería en Red. Obtenido de https://www.portal.uasj.unpa.edu.ar/_files/ugd/f9834d_784cc19611714c87890006bc7cb4715d.pdf#page=10

Torres, R., & Tapia, J. (2021). *Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0.* Ecuador: Ciencias Técnicas y Aplicadas. doi:https://dx.doi.org/10.23857/dc.v7i4.2425

Valle, A. (2022). *La investigación descriptiva con enfoque cualitativo en educación.* Perú: Pontificia Universidad Católica del Perú. Obtenido de https://repositorio.pucp.edu.pe/index/handle/123456789/184559

ANEXOS

Anexo A: Aprobación del tema

Outlook

DPGA | Titulación | Periodo 2024-2025(1) - Notificación de tutor asignado - TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Desde NOTIFICACIONES TITULACION <notificaciones.titulacion@uleam.edu.ec>
Fecha Sáb 27/04/2024 0:28
Para MINAYA MACIAS RENELMO WLADIMIR <renelmo.minaya@uleam.edu.ec>
CC CEVALLOS BRAVO KAREN MISHELLE <e2300698921@live.uleam.edu.ec>

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Universidad Laica Eloy Alfaro de Manabí

Periodo 2024-2025(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 del siguiente estudiante:

Tema: AUDITORÍA INFORMÁTICA DE SEGURIDAD FÍSICA DEL LABORATORIO DE COMPUTACIÓN DE LA UNIDAD EDUCATIVA "AMERICANO".

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

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

Apellidos y nombres del tutor asginado: MINAYA MACIAS RENELMO WLADIMIR

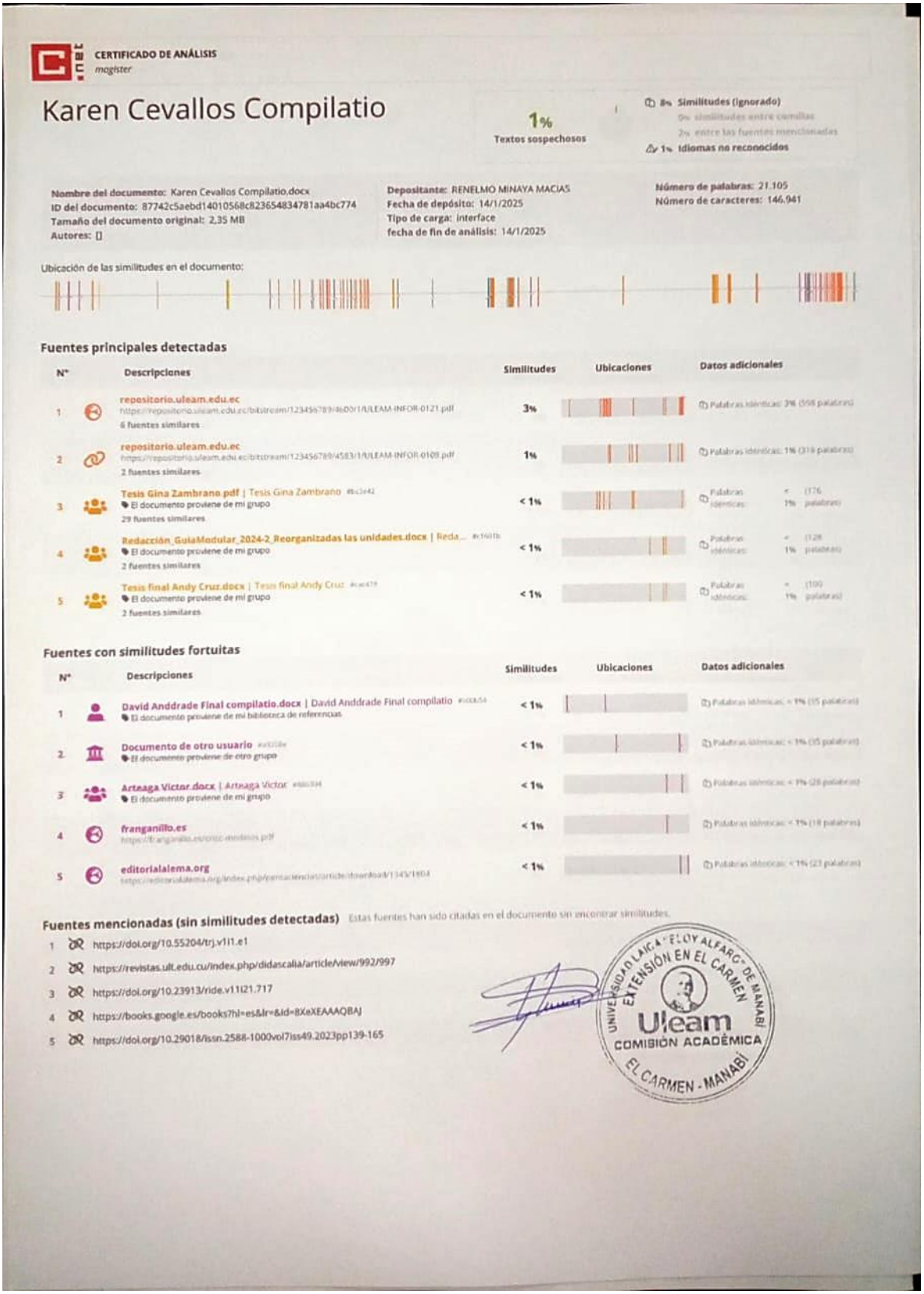
Apellidos y nombres del estudiante: CEVALLOS BRAVO KAREN MISHELLE

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2024-2025(1)

Sírvasen cumplir con lo dispuesto en el Manual de Procedimientos de TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE

Anexo B: Certificado de análisis Compilatio



CERTIFICADO DE ANÁLISIS
magister

Karen Cevallos Compilatio

1%
Textos sospechosos

8% Similitudes (ignorado)
0% similitudes entre comillas
2% entre las fuentes mencionadas
1% Idiomas no reconocidos

Nombre del documento: Karen Cevallos Compilatio.docx
ID del documento: 87742c5aebd14010568c823654834781aa4bc774
Tamaño del documento original: 2,35 MB
Autores: []

Depositante: RENELMO MINAYA MACIAS
Fecha de depósito: 14/1/2025
Tipo de carga: interface
fecha de fin de análisis: 14/1/2025

Número de palabras: 21.105
Número de caracteres: 146.941

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/4bD0r1/1/ULEAM-INFOR-0121.pdf 6 fuentes similares	3%		Palabras idénticas: 3% (598 palabras)
2	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/4583/1/ULEAM-INFOR-0109.pdf 2 fuentes similares	1%		Palabras idénticas: 1% (316 palabras)
3	Tesis Gina Zambrano.pdf | Tesis Gina Zambrano El documento proviene de mi grupo 29 fuentes similares	< 1%		Palabras idénticas: < 1% (176 palabras)
4	Redacción_GuiaModular_2024-2_Reorganizadas las unidades.docx | Reda... El documento proviene de mi grupo 2 fuentes similares	< 1%		Palabras idénticas: < 1% (128 palabras)
5	Tesis final Andy Cruz.docx | Tesis final Andy Cruz El documento proviene de mi grupo 2 fuentes similares	< 1%		Palabras idénticas: < 1% (100 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	David Anddrade Final compilatio.docx | David Anddrade Final compilatio El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (35 palabras)
2	Documento de otro usuario El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (35 palabras)
3	Arteaga Victor.docx | Arteaga Victor El documento proviene de mi grupo	< 1%		Palabras idénticas: < 1% (28 palabras)
4	franganillo.es https://fr.franganillo.es/crisc-modelos.pdf	< 1%		Palabras idénticas: < 1% (18 palabras)
5	editorialalema.org https://editorialalema.org/index.php/pentaciencias/article/download/1343/1804	< 1%		Palabras idénticas: < 1% (23 palabras)

Fuentes mencionadas (sin similitudes detectadas)

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

1 https://doi.org/10.55204/trj.v1i1.e1
2 https://revistas.ult.edu.cu/index.php/didascalia/article/view/992/997
3 https://doi.org/10.23913/ride.v11i21.717
4 https://books.google.es/books?hl=es&lr=&id=8XeXEAAAQBAJ
5 https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp139-165

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

Anexo C:

UNIDAD EDUCATIVA PARTICULAR "AMERICANO"
EDUCACION INICIAL - EDUCACION BASICA - BACHILLERATO
El Carmen - Manabí – Ecuador
AMIE: 13H04538 - TELEF: 2660-809

El Carmen 14 de enero del 2025

CERTIFICACIÓN

El suscrito Vicerrector de la Unidad Educativa "Americano" tiene a bien Certificar que la Srta. **CEVALLOS BRAVO KAREN MISHELLE** con Nro de Cédula: **230069892-1** estudiante de la Universidad Laica Eloy Alfaro de Manabí en la carrera de Tecnologías de la información del segundo periódico académico del 2024 está realizando una **AUDITORIA INFORMÁTICA DE SEGURIDAD FÍSICA DEL LABORATORIO DE COMPUTACIÓN DE LA UNIDAD EDUCATIVA "AMERICANO" .**

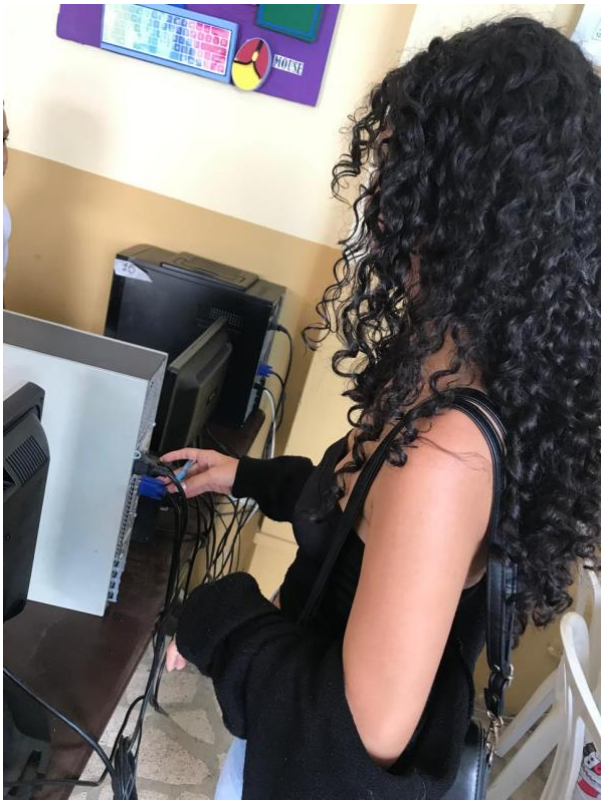
Esto todo cuanto puedo certificar en honor a la verdad.

Atentamente,

Lic. Cristobal Tobar G.
SECRETARIA

UNIDAD EDUCATIVA PARTICULAR "AMERICANO" RECTORADO El Carmen - Manabí

Anexo D: Fotografías



Anexo E: Evidencia de aplicación de encuestas y entrevistas

ENCUESTA

Dirigida a: Docentes

Objetivo: Realizar un diagnóstico acerca de la situación actual de los laboratorios en base a seguridad informática de la Unidad Educativa Americano.

1. ¿La institución cuenta con un departamento encargado a las tecnologías de la información?

   ___ si ___ no
2. ¿Existen avisos que ayuden a prevenir desastres dentro de los centros informático la institución?

   ___ si ___ no
3. ¿Se ha definido e informado a usted cuales son las sanciones de los usuarios por infringir las normas?

   ___ si ___ no
4. ¿Se lleva un inventario de los dispositivos informáticos que posee la institución?

   ___ si ___ no
5. ¿Se realizan con frecuencia mantenimientos a los equipos informáticos del laboratorio de computación?

   ___ si ___ no
6. ¿Los equipos de laboratorio están conectados en red?

   ___ si ___ no
7. ¿Con frecuencia el responsable del laboratorio comprueba que los equipos procesen la información de forma adecuada?

   ___ si ___ no
8. ¿Cuándo usted accede al laboratorio el responsable le hace firmar en una lista de control de acceso?

   ___ si ___ no
9. ¿Seleccione cuál de Un poco más de la mitad las plataformas utilizan la institución?

   ___ si ___ no
10. ¿Para acceder a las instalaciones informáticas existe algún tipo de política para el acceso a las mismas?

    ___ si ___ no

ENTREVISTA

Dirigida a: Rector de la institución

Objetivo: Realizar un diagnóstico acerca de la situación actual de los laboratorios en base a seguridad informática de la Unidad Educativa Americano.

1. ¿Sabe si existe personal que se encargue del departamento de tics en la unidad educativa?
2. ¿Existen registros del inventario que posee la unidad educativa en cuanto a equipos tecnológicos?
3. ¿Se ha aplicado antes una auditoria informática dentro de la institución?
4. ¿Qué orientaciones y / o capacitaciones ha recibido usted como directivo para proyectar con sus trabajadores acciones de seguridad informática en los laboratorios de computación?
5. ¿Existe en la Unidad Educativa alguna estrategia para garantizar la seguridad en el laboratorio de computación? Mencione la estrategia y cuantos actores de la comunidad educativa se ven implicados en su implementación.
6. ¿Existen políticas relacionadas al ingreso y salida de Hardware dentro de la institución, que aseguren la seguridad informática de los docentes?
7. ¿Brindas cursos de capacitación a los docentes sobre seguridad informática?
8. ¿Conoce la cantidad de equipos informáticos que posee la institución?
9. ¿Existen alguna política que se deba respetar al momento de acceder a los laboratorios de informática?
10. ¿El responsable del laboratorio de computación es un técnico informático que tiene solo esa función o son los profesores que imparten esta materia?
11. ¿Qué capacitaciones se han desarrollado en la Unidad Educativa para que los usuarios (estudiantes, docentes y directivos) garanticen la seguridad en el laboratorio de computación?
12. ¿En la Unidad Educativa se realiza el mantenimiento de los equipos informáticos solo cuando hay roturas o están debidamente planificados en diferentes períodos del año lectivo?
13. ¿Cree usted importante que se realice en la Unidad Educativa una auditoría informática al laboratorio de cómputo para brindarle a usted un informe de evaluación de riesgos que le permita tomar decisiones en función de proteger los medios informáticos?

GLOSARIO DE TÉRMINOS

Activo: Todo recurso, equipo o información que tiene valor para la institución y que debe protegerse contra posibles amenazas.

Amenaza: Evento o situación que podría comprometer la seguridad, integridad o disponibilidad de los recursos tecnológicos y físicos de una organización.

Auditoría Informática: Proceso de evaluación sistemática que permite analizar y verificar la seguridad, funcionalidad y cumplimiento de normativas en los sistemas tecnológicos de una organización.

Encuesta: Instrumento de recolección de datos que permite obtener información de un grupo de personas sobre un tema específico.

Entrevista: Técnica de investigación que consiste en la interacción directa con individuos para recopilar información detallada y específica.

Informe de Auditoría: Documento que detalla los hallazgos, análisis y recomendaciones derivados de un proceso de auditoría.

Laboratorio de Computación: Espacio físico dentro de una institución educativa que alberga equipos de cómputo y recursos tecnológicos utilizados para actividades académicas y administrativas.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información): Herramienta utilizada para la identificación, evaluación y gestión de riesgos asociados a activos tecnológicos y procesos de una organización.

Malware: Software malicioso diseñado para infiltrarse, dañar o comprometer la seguridad de sistemas informáticos.

Manual de Recomendaciones: Guía práctica que incluye medidas y estrategias para solucionar problemas, mitigar riesgos y optimizar la seguridad en una organización.

Matriz de Riesgos: Representación estructurada que clasifica y prioriza los riesgos identificados según su probabilidad de ocurrencia y el impacto potencial.

Mitigación: Proceso de implementar medidas para reducir la probabilidad o el impacto de un riesgo identificado.

Normativa de Seguridad: Conjunto de reglas, políticas y procedimientos diseñados para garantizar la protección de recursos y el cumplimiento de estándares en una organización.

Protección de Infraestructura: Estrategias y medidas implementadas para salvaguardar los bienes físicos y tecnológicos de una organización ante posibles daños o pérdidas.

Recursos Tecnológicos: Equipos, software, redes y demás elementos tecnológicos utilizados para el funcionamiento y la operación de una institución.

Riesgos: Potenciales eventos o situaciones que pueden causar daños a los recursos tecnológicos, la infraestructura o la información de una institución.

Seguridad Física: Conjunto de medidas y estrategias destinadas a proteger los recursos tecnológicos, infraestructura y personal contra amenazas físicas como robos, incendios o desastres naturales.

Tecnología de la Información (TI): Conjunto de herramientas, sistemas y procesos utilizados para gestionar, almacenar y proteger información en una organización.

Unidad Educativa: Institución dedicada a la enseñanza y formación de estudiantes, en este caso, la Unidad Educativa Americano.

Vulnerabilidad: Debilidad o punto débil en un sistema o infraestructura que puede ser explotado por amenazas para causar un daño o interrupción.