UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN TEMA

SGSI PARA EL LABORATORIO DE COMPUTACIÓN A LA UNIDAD EDUCATIVA ALIDA ZAMBRANO GARCIA

APELLIDOS Y NOMBRES

ZAMBRANO GARCÍA GINA YADIRA

TUTOR

INGENIERA CLARA GUADALUPE POZO HERNÁNDEZ

EL CARMEN, AGOSTO 2024

CERTIFICACIÓN DEL TUTOR

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

CERTIFICACIÓN

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

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante **Zambrano García Gina Yadira**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2023(2)-2024(1), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es **"SGSI (SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION) PARA EL LABORATORIO DE COMPUTACIÓN A LA UNIDAD EDUCATIVA ALIDA ZAMBRANO GARCIA"**

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

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

El Carmen, 22 de julio del 2024

Lo certifico,

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

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EL CARMEN

APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con modalidad Proyecto Integrador, titulado: AUDITORÍA INFORMÁTICA EN SGSI PARA EL LABORATORIO DE COMPUTACIÓN A LA UNIDAD EDUCATIVA ALIDA ZAMBRANO GARCIA" cuya auditoría es de la señorita: ZAMBRANO GARCÍA GINA YADIRA estudiante de la Carrera de Ingeniería en Tecnologías de la Información, y como tutor de Trabajo de Titulación Ing. Pozo Hernández Clara Guadalupe.

Para constancia firman:

Ing. Wladimir Minaya, Mg
Presidente de tribunal

Ing. Clara Guadalupe Pozo
Docente tutor

Ing. Rocío Mendoza, Mg
Tribunal 2

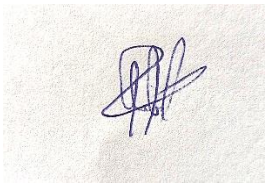
Ing. Saed Reascos, Mg
Tribunal 3

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: SGSI Sistema de Gestión seguridad de la información para el laboratorio de computación a la unidad educativa Alida Zambrano García corresponde exclusivamente a: Gina Yadira Zambrano García con CI.235005508-9 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.



Gina Yadira Zambrano García

C.I. 235005508-

DEDICATORIA

Esto se lo dedico a Dios, San Antonio y a mi mamá la Sra. María García, ella ha sido mi pilar fundamental para llegar hoy en día a esta meta tan anhelada, mami gracias por enseñarme a soñar en grande y nunca rendirme, usted ha sido mi luz que me ha guiado en cada paso de este camino que a veces decía ya no puedo mami y usted siempre me decía si puede mijita este logro es el reflejo de su amor y fe en mí. Sus consejos sabios y guía amorosa han sido fundamental en mi vida, gracias por estar a mi lado apoyándome en cada desafío de mi vida siempre acompañaren en las desveladas preocupada por mí nunca has dejado de confiar en mí siempre has disfrutados de cada uno de mis triunfos. Esta meta esta tesis es tanto suya como mía gracias a ti estoy aquí logrando este sueño.

No hay palabras suficientes para expresar todo mi agradecimiento por usted.

Gracias por creer en mi cuando más lo necesitaba.

Con amor su niña Zambrano Gina

AGRADECIMIENTO

A mi maravillosa familia Zambrano García, por ser ese pilar en mi vida y brindarme su apoyo inquebrantable que ha sido fundamental a lo largo de este camino universitario, en los momentos difíciles como también de celebración.

A mi Papa el Sr. José Zambrano de una u otra manera por haber apoyado en mi etapa universitaria, aunque no tengamos la mejor relación entre padre e hija te agradezco por todo.

A mi hermana la Sra. María Elena Zambrano García por su amor, apoyo fuente de motivación por cada día impulsarme a alcanzar mis metas, gracias por celebrar y compartir mis alegrías y triunfos como si fueses suyos eres la mejor hermana que Dios me pudo dar.

A mis dos hermanos

Sr. Ricardo y Julio Zambrano García, por siempre estar pendiente de mí, de mis estudios y por sus consejos cuando más los necesitaba por confiar y dejarme rendir por siempre estar pendiente de mí y cuidarme como su niña…

A mi tutora Ingeniera Clarita Pozo, por siempre darme ese apoyo y bríndame sus consejos y por tenerme paciencia a lo largo de mi carrara y en el transcurso de la tesis muchas gracias Ing.

Con amor su niña Zambrano Gina …….

ÍNDICE GENERAL

INDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1 ÍNDICE DE ANEXOS

RESUMEN

El propósito de este proyecto fue realizar la Auditoría informática al laboratorio de computación a la Unidad Educativa Alida Zambrano García, durante el transcurso del año 2024. Esta propuesta nace por la necesidad de conocer la situación actual del laboratorio de computación con relación los controles de seguridad para garantizar el buen funcionamiento de los mismos como parte del trabajo de investigación en diferentes fuentes bibliográficas de la seguridad de la información relacionada tanto como la auditoría informática como a los equipos de computación para diagnosticar la problemática usando encuestas a los docentes y entrevistas al rector de la unidad educativa sobre los controles que se aplican actuantemente en el laboratorio de computación de la institución

La propuesta consistió en la aplicación de una auditoría de seguridad informática para lo cual se utilizó la metodología MAGERIT que permite analizar riesgos de seguridad informática, en lo cual se elaboró varios instrumentos basado en la ISO 270001 para evaluar el nivel de seguridad de cinco riesgos obteniendo como resultado que el nivel de seguridad fue de 38% considerado como un nivel bajo siendo el nivel de riesgo el de mayor gravedad identificado el robo y el de menor gravedad daño de equipos finalmente se adjunta un manual de políticas de seguridad destinado a entregar en la institución que le sirva de ayuda y guía y así lograr una mejor gestión de seguridad en el laboratorio de computación.

ABSTRACT

The purpose of this project was to conduct a computer audit of the computer laboratory at the Alida Zambrano Garcia Educational Unit, during the year 2024. This proposal was born out of the need to know the current situation of the computer laboratory in relation to security controls to ensure the proper functioning of the same as part of the research work in different bibliographic sources of information security related both as computer audit and computer equipment to diagnose the problem using surveys to teachers and interviews with the rector of the educational unit on the controls that are currently applied in the computer laboratory of the institution.

The proposal consisted in the application of a computer security audit for which the MAGERIT methodology was used to analyze computer security risks, The result was that the security level was 38%, considered as a low level, being the most serious risk identified as theft and the least serious one as damage to equipment. Finally, a security policy manual is attached to be delivered to the institution to serve as a guide and help it achieve better security management in the computer laboratory.

CAPÍTULO I

1.1 Introducción

La información es muy valiosa en la actualidad y es importante protegerla para evitar su manipulación por personas no autorizadas. A nivel mundial, la gestión de seguridad de la información es una práctica que busca proteger la información que necesita la organización, garantizando su confidencialidad, integridad y disponibilidad. Esto permite a las organizaciones operar de manera segura y confiable en un entorno cada vez más digitalizado y vulnerable.

Dentro de este marco, los sistemas de gestión seguridad de la información, están innovando constantemente para disminuir el aumento de incidentes en las organizaciones. Se utilizan para los procesos, prácticas diseñadas para proteger las redes, dispositivos, programas, datos de posibles ciberataques, hackeos y acceso no autorizado a la seguridad de la información. Estos ataques pueden afectar no solo los procesos, sino también la continuidad operativa del negocio o institución lo que puede ocasionar problemas económicos e incluso legales. No obstante, es fundamental encontrar una solución efectiva para combatir o minimizar el impacto de estas amenazas y garantizar la seguridad de los procesos de la integridad y seguridad. Por lo tanto, las instituciones educativas deben implementar y establecer las medidas de seguridad para su mejora en las vulnerabilidades que pueden tener y la protección de sus datos.

La presente auditoría de sistemas de gestión de seguridad de la información (SGSI) al laboratorio de computación de la Unidad Educativa Alida Zambrano García tubo como propósito identificar y evaluar los riesgos de la seguridad física en donde la protección del laboratorio es crucial ,esta auditoría busca el cumplimiento de las normativas y mejoramiento de la confianza en las capacidades de la institución para salvaguardar sus activos informáticos lo cual tuvo como objetivo determinar las vulnerabilidades en el entorno físico del laboratorio

de computación y de los activos informáticos para así evaluar el nivel de seguridad y medir el grado de protección actual frente a posibles amenazas digitales como físicas.

Se empleó la metodología MAGERIT reconocida por su eficacia en el análisis de gestión de riesgos de seguridad informática lo cual facilita la identificación de amenazas y riesgosa que proporciona un enfoque exhaustivo y sistemático basado en los estándares de la ISO 27001 lo cual como resultado de esta auditoría se elaboró un manual de políticas de seguridad que se proporcionará e la institución que servirá como guía para mejorar la gestión de seguridad del laboratorio y estables procedimiento claro y escritos para mitigar los riesgos identificados.

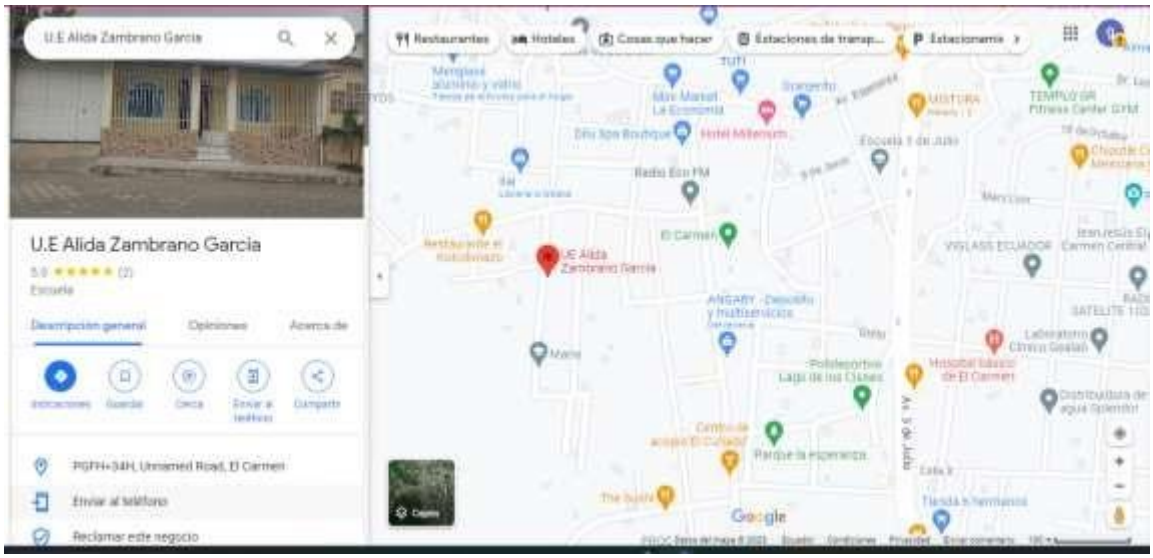
1.2 Presentación del tema

SGSI (Sistema de Gestión seguridad de la información) para el laboratorio de computación a la unidad educativa Alida Zambrano García

1.3 Ubicación y contextualización de la problemática

La Unidad Alida Zambrano García fue fundada el 5 de mayo en el año 1981. Está ubicada en Nuevo Naranjal, Lotización Los Rosales, Vía Venado, en la provincia de Manabí, cantón El Carmen y parroquia El Carmen. Ofrece educación regular en los niveles de Inicial, Educación Básica y Bachillerato. Es una unidad educativa fiscal de zona urbana según el INEC, con régimen escolar costa y educación en español en modalidad presencial y jornada matutina.

Ilustración 1: ***Gráfico ubicación de la unidad educativa***



El acceso se realiza por vía terrestre y cuenta con un total de 49 docentes y 1580 estudiantes, cuenta con un laboratorio de computación que son veintes computadores con la marca LG, ubicado en la ciudad de Manabí en el Cantón EL Carmen. Calle Av. La Esperanza y vía Venado.

1.4 Planteamiento del problema

1.4.1 Problematización

La utilización de las tecnologías informáticas y de comunicación en las empresas ha tenido un gran impacto en el mundo actual, generando un incremento en el procesamiento de datos. Sin embargo, esto también ha hecho que muchas organizaciones sean vulnerables a riesgos debido a ataques de usuarios expertos a los activos de información en las empresas el crecimiento de la información requiere la implementación de controles que eviten amenazas a los activos de la información.

La innovación de la nueva era de la información, producto del desarrollo tecnológico, ha generado cambios en las actividades cotidianas y ha hecho que el suministro de información

a las organizaciones sea más oportuno y eficiente, las organizaciones se han convertido en verdaderos centros de generación de datos, que son manejados internamente en beneficio del procesamiento de la información es fundamental para comprender de manera gráfica y estadística los comportamientos del mercado o de una actividad económica.

1.4.2 Génesis del problema

El origen del problema en la Unidad Educativa Alida Zambrano García surgió a partir de la instalación del laboratorio de computación y la posterior conexión a Internet. Estos cambios introdujeron nuevas herramientas tecnológicas en la institución, pero también revelaron una serie de vulnerabilidades que antes no existían. La infraestructura digital no estaba completamente preparada para gestionar las complejidades asociadas con la seguridad de la información, lo que dejó al laboratorio expuesto a potenciales riesgos.

Estas vulnerabilidades han generado varios problemas, como riesgos laborales debido al mal manejo de los sistemas, fugas de información sensible y afectaciones directas a la integridad de los datos. Además, la falta de control sobre el acceso a la información ha comprometido la confidencialidad de las personas involucradas, incluidos los docentes, que manejan datos privados y académicos en el laboratorio. Esta deficiencia en la gestión de la información ha revelado un vacío en las medidas preventivas de seguridad.

Esta situación ha derivado en consecuencias negativas para la protección de la información dentro del laboratorio, afectando tanto a la operatividad diaria como a la confidencialidad de los usuarios. La falta de mecanismos adecuados ha evidenciado debilidades que han expuesto tanto los sistemas informáticos como los datos almacenados, generando preocupación dentro de la institución.

1.4.3 Estado actual del problema

El problema se efectuó cuando el encargado del laboratorio de cómputo dejó su puesto, lo que provocó una falta de mantenimiento en los equipos. Esta situación permitió la

acumulación de polvo, dañando las computadoras y reduciendo su vida útil. Además, la ausencia de controles en el uso de los equipos de cómputo permitió que cualquier estudiante los utilizara sin restricciones, lo que agravó el desgaste de los dispositivos.

El desconocimiento o la ausencia de políticas de seguridad también representó un riesgo importante, ya que no solo los cables estaban desordenados y tirados en el suelo, sino que esto aumentaba el peligro de cortocircuitos o daños por descargas eléctricas. La falta de mantenimiento y control ha sumido al laboratorio en un estado de desorganización, lo que ha derivado en la pérdida de componentes como cables, adaptadores, mouse, teclados, entre otros.

Esto refleja una inadecuada gestión uso de los equipos de cómputo afectando la operatividad del laboratorio y comprometiendo tanto la seguridad de los equipos como de los usuarios.

En la actualidad, el laboratorio de computación de la Unidad Educativa Alida Zambrano García continúa enfrentando serias deficiencias en su gestión de la seguridad de la información. A pesar de contar con una infraestructura tecnológica operativa, las medidas de control y protección no han sido actualizadas ni optimizadas desde su instalación. Esto ha dejado al laboratorio vulnerable frente a diversos riesgos, tales como el acceso no autorizado a información sensible, la falta de auditorías regulares, y la exposición a posibles ataques cibernéticos que comprometen la integridad de los datos almacenados.

1.5 Diagrama causa – efecto del problema

Ilustración 2: Gráfico Diagrama causa – efecto del problema

1.6 Objetivos

1.6.1 Objetivo general

Elaborar una Auditoría informática para los Sistema de Gestión de Seguridad para laboratorio de computación a la Unidad Educativa Alida Zambrano García.

1.6.2 Objetivos específicos

- Identificar problemas de seguridad de la información en la Unidad Educativa Alida Zambrano García para el laboratorio de computación
- Aplicar métodos y técnicas de investigación para justificar el problema y diagnosticar la existencia de vulnerabilidades en el área de seguridad de la información en la institución
- Evaluar riesgos de seguridad de la información al laboratorio de computación para realizando una evaluación de riesgos en el laboratorio de computación.

- Elaborar un informe de auditoría con los resultados obtenidos de la investigación para que delinee los riesgos y vulnerabilidades existentes en el laboratorio de computación.

1.7 Justificación

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Unidad Educativa Alida Zambrano García es esencial para abordar las deficiencias actuales en la protección de datos. Este sistema proporciona una estructura integral que permite identificar, evaluar y gestionar riesgos asociados con la seguridad de la información. Al adoptar un SGSI, la institución puede asegurar la protección de información sensible, mejorar la confidencialidad y la integridad de los datos, y garantizar el cumplimiento de normativas legales.

Una de las principales ventajas de implementar un SGSI es la mejora en la protección de datos confidenciales. El sistema establece controles rigurosos para evitar accesos no autorizados, pérdida o daño de información crítica, asegurando que los datos de estudiantes y personal docente se mantengan seguros. Esto no solo protege la privacidad de los individuos, sino que también mantiene la integridad de los procesos educativos y administrativos.

Además, el SGSI ayuda a reducir los riesgos al permitir una evaluación continua de las vulnerabilidades y amenazas. Esto facilita la toma de decisiones informadas y la implementación de medidas preventivas y correctivas, disminuyendo la probabilidad de incidentes de seguridad que puedan afectar la operación de la institución. La identificación temprana de riesgos permite una respuesta más efectiva y oportuna.

La implementación del SGSI contribuye al cumplimiento de regulaciones y estándares de seguridad, evitando sanciones legales y fortaleciendo la confianza en la gestión de la seguridad de la información. Asimismo, mejora la eficiencia operativa al estandarizar procedimientos de seguridad y capacitar al personal, promoviendo una cultura de seguridad y minimizando errores humanos. Esta solución integral no solo aborda los problemas actuales,

sino que también prepara a la institución para enfrentar futuros desafíos en la gestión de la seguridad de la información.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Los laboratorios de computación, especialmente en las instituciones educativas, el SGSI introduce una capa adicional de protección a la infraestructura tecnológica existente. Al integrar herramientas y controles de seguridad avanzados, como firewalls, sistemas de detección de intrusiones y cifrado de datos, se fortalece la defensa contra amenazas cibernéticas. Esto asegura que los equipos y sistemas informáticos estén mejor protegidos contra ataques y accesos no autorizados, prolongando la vida útil de la infraestructura tecnológica y reduciendo la necesidad de costosas reparaciones o actualizaciones emergentes procesamiento de datos.

1.8.2 Impacto social

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Unidad Educativa Alida Zambrano García tiene un impacto social positivo significativo. Al fortalecer la protección de datos personales y académicos, se incrementa la confianza de estudiantes, padres y personal en la capacidad de la institución para manejar información sensible de manera segura. Esto no solo protege la privacidad de los individuos y mantiene la integridad de los registros académicos y administrativos, sino que también fomenta una cultura de responsabilidad y ética en la gestión de la información. En última instancia, el SGSI contribuye a un ambiente educativo más seguro y confiable, promoviendo el bienestar general de la comunidad educativa.

1.8.3 Impacto ecológico

El impacto ecológico de la auditoría informática en una unidad educativa se verá reflejado en varios aspectos. En el futuro, la implementación de medidas derivadas de la

auditoría permitirá una mejor gestión de los recursos tecnológicos, promoviendo el uso eficiente de la energía y la reducción de residuos electrónicos. Además, se fomentará la adopción de prácticas sostenibles, como el reciclaje de equipos obsoletos y la utilización de tecnologías más ecológicas.

La auditoría también identificará áreas donde se pueden implementar mejoras para minimizar el consumo energético de los equipos informáticos y optimizar su vida útil. Esto contribuirá a disminuir las emisiones de carbono asociadas a la unidad educativa. Asimismo, se desarrollarán políticas y procedimientos que promuevan el uso responsable de los recursos informáticos, incentivando a la comunidad educativa a ser más consciente de su impacto ambiental. En conjunto, estas acciones transformarán a la unidad educativa en un modelo de sostenibilidad tecnológica.

CAPÍTULO II

2 Marco teórico

2.1 Antecedentes históricos

2.1.1 Historia de la Gestión de Seguridad

Según los autores Whitman y Mattord (2019) menciona lo siguiente: La historia de la seguridad de la información se origina en la protección de datos y la preservación de su integridad. Este concepto emergió durante la Segunda Guerra Mundial, cuando se introdujeron los primeros mainframes para facilitar el descifrado de comunicaciones estratégicas. Con el fin de resguardar la confidencialidad de la información, se implementaron diversas medidas de seguridad. Por ejemplo, el acceso a lugares críticos estaba restringido mediante credenciales autorizadas y sistemas de reconocimiento facial. La creciente preocupación por mantener la seguridad nacional impulsó el desarrollo de estrategias de ciberseguridad cada vez más sofisticadas y tecnológicamente avanzadas. En esos primeros años, la seguridad de la información era un proceso simple que consistía principalmente en seguridad física y sistemas de clasificación de documentos simples. Las principales amenazas de seguridad eran el robo físico de dispositivos, el espionaje de los productos del sistema y el sabotaje.

Según los autores Silva et al. (2023), el Sistema de Gestión de la Seguridad de la Información (SGSI) se define como la parte del sistema general de gestión que abarca la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para el desarrollo la gestión de la seguridad de la información en una organización. Gestionar la seguridad de la información implica llevar a cabo una serie de tareas y procedimientos que aseguren los niveles de seguridad requeridos en una organización. Es importante tener en cuenta que los riesgos no pueden ser eliminados por completo, pero sí pueden ser gestionados.

2.1.2 Orígenes y evolución laboratorio de computación

De acuerdo con Ortiz (2010) describe que el laboratorio de computación ha experimentado una transformación significativa desde sus inicios en las décadas de 1960 y 1970. En ese entonces, las computadoras eran grandes y costosas, principalmente utilizadas en entornos académicos y empresariales. Sin embargo, con la miniaturización de la tecnología, estas se volvieron más accesibles, lo que propició el surgimiento de laboratorios de computación en universidades y centros de investigación. El origen de las máquinas de calcular se remonta al ábaco chino, utilizado para operaciones de adición y sustracción. Luego, en el siglo XVII, Blas Pascal inventó una máquina que realizaba sumas y restas, seguido por Leibnitz en el siglo XVIII, quien desarrolló una más avanzada para operaciones de producto y cociente. En el siglo XIX, se comercializaron las primeras máquinas de calcular, y Charles Babbage diseñó la Máquina Analítica. El avance de la electrónica en el primer tercio del siglo XX permitió superar problemas técnicos, y durante la Segunda Guerra Mundial, se construyeron los primeros ordenadores, como el Mark I basado en interruptores mecánicos. Posteriormente, en 1944, se creó el Eniac, considerado el primer ordenador práctico. Con el desarrollo del Univac I y el Univac II en 1951, se marcó el inicio de los ordenadores de acceso común. La informática influye en diversos aspectos de la sociedad y la formación de las personas. Desde la educación informática en todos los niveles del sistema educativo hasta su impacto en la cultura actual, la informática se ha vuelto omnipresente en la sociedad moderna.

2.2 Antecedentes de investigaciones relacionadas al tema presentado

a) **Desarrollo del modelo de Sistema de Gestión de Seguridad de la Información basado en la Norma NB/ISO/IEC 27001 aplicado al área de ti en Empresas Corredoras de Seguros y Reaseguros**.

El objetivo de este fue desarrollar un modelo de gestión de la seguridad de la información fundamentado en la norma ISO 27001:2013 aplicando al área de tecnología de la

información de las empresas catadoras de seguros y reaseguros que operan em la cuidad de la paz se según la conclusión fue que en muchas empresas corredoras de seguros y reaseguros ,se llevó a cabo que consideran los sistemas de seguridad Tecnologías de Información, coincidieron que es necesario el uso de algunos formularios, como ser los procedimientos de control de cambios en sistemas. Que es parte del décimo control: adquisición, desarrollo y mantenimiento del sistema (Poma, 2020).

b) **Procedimiento para implementar un sistema de gestión de seguridad de la información como contribución a la calidad de la información de los servicios de consultoría**.

Aplicación en el CIGET de Holguín, en el cual se plantío el objetivo de: Desarrollar un procedimiento para la implementación de un SGSI normalizado en el 4 Ciget de Holguín que contribuya a elevar la calidad de la información de los servicios de consultoría, llegando a la conclusión de dar a conocer los resultados obtenidos en el proceso de auditoría, especificando cómo el auditado cumple con los criterios de auditoría previamente definidos grado de cumplimiento y cuántas no conformidades se detectaron por áreas o procesos (Argota y Yudelkis, 2019).

c) **Modelo de gestión de incidentes de seguridad de la información en la red informática, basado en la ISO/IEC 27002**.

La importancia de esta investigación es dar cumplimiento a los siguientes objetivos, primero analizar los riesgos de vulnerabilidad de la información del departamento de administración de redes, luego identificar los aspectos a tener en cuenta en la definición de un modelo de gestión de incidentes de seguridad de la información, una vez identificado los posibles riesgos se procede a diseñar el modelo del sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002la conclusión de este tema de investigación fue desarrollar un modelo de gestión de incidentes de seguridad de la información en la red

informática. Para mitigar las vulnerabilidades que afectan a la red de la FISEI, así como minimizar los riesgos a los que su infraestructura se encuentra expuesta, es importante que la institución se acoja a lo dispuesto en la Norma ISO/IEC 27002 con el objetivo de asegurar en todo momento la integridad, disponibilidad y confidencialidad de la información (Guevara y Salto, 2023)

2.3 Definiciones conceptuales

2.3.1 Sistema de Gestión de Seguridad de la Información

2.3.1.1 Auditoría

En el sector de TI, la auditoría surge cuando las organizaciones se dan cuenta de que la información que adquieren archiva digitalmente, procesan y publican es un activo muy importante. En este momento, las instituciones y empresas están comenzando a darse cuenta de que su credibilidad en la sociedad está estrechamente relacionada con la protección que ofrecen a los datos de sus usuarios y, por ende, a los grupos que la poseen. (Manrique, 2019)

2.3.1.2 Gestión de incidentes de seguridad informática

Para preservar la integridad, confidencialidad y disponibilidad de los datos en entornos digitales, las inversiones en Tecnologías de la Información (TSI) deben generar un valor óptimo para la organización, equilibrando costo, riesgo y beneficio. Es fundamental que estas inversiones sean eficientes y se alineen con los objetivos de gestión, facilitando el cambio y proporcionando soporte y servicios adecuados. Asimismo, es indispensable contar con recursos técnicos y de negocio competentes y disponibles para ejecutar programas y llevar a cabo los cambios organizacionales necesarios, asegurando así una implementación exitosa. (Moreno, 2022)

2.3.1.3 SGSI (Sistema de Gestión Seguridad de la Información) Para el laboratorio de computación

La investigación referente a la implementación de un buen Sistema de Gestión de Seguridad de la Información (SGSI) se centra en identificar los procesos específicos sobre los cuales el SGSI va a actuar, sin necesidad de aplicarlo a toda la actividad de la organización. Al definir el alcance, es importante considerar los recursos disponibles. Generalmente, es más práctico limitar inicialmente el SGSI a los procesos o servicios más importantes para la organización y, en ciclos posteriores de mejora continua, ir incorporando los restantes (Pérez, 2020).

2.3.1.4 Seguridad en equipos informáticos

La seguridad en equipos informáticos es esencial para proteger la integridad, confidencialidad y disponibilidad de la información en la era digital. Los equipos informáticos, como computadoras de escritorio, laptops y servidores son objetivos principales para los ataques cibernéticos, que pueden variar desde malware y virus hasta ataques de phishing y ransomware. Por lo tanto, es fundamental implementar medidas robustas para garantizar la seguridad de estos dispositivos. Esto incluye la instalación y actualización regular de software antivirus y antispyware, así como el uso de firewalls para filtrar el tráfico no autorizado. Los datos confidenciales deben ser cifrados para evitar accesos no autorizados en caso de pérdida o robo del equipo. Además, se deben establecer políticas de respaldo regulares para garantizar que los datos importantes estén protegidos contra la pérdida accidental o el daño pueden reducir significativamente el riesgo de violaciones de seguridad y proteger la integridad de su información y sistemas informáticos (Vasquez, 2023).

2.3.1.5 Seguridad y gestión de ciber riesgos

La seguridad y gestión de ciber riesgos son fundamentales en la era digital debido a las constantes y cada vez más sofisticadas amenazas cibernéticas. La seguridad cibernética implica

medidas preventivas como firewalls y software antivirus, mientras que la gestión de ciber riesgos se centra en identificar, evaluar y mitigar amenazas. Esto incluye evaluaciones regulares, planes de respuesta, políticas de seguridad y educación para empleados sobre prácticas seguras. Además, implica transferir riesgos a través de seguros y colaborar con expertos para mantenerse al día con las últimas amenazas y técnicas de mitigación. Estos enfoques integrales son esenciales para proteger sistemas y datos en un entorno digital cada vez más complejo (Pérez, 2020).

2.3.2 Análisis de riesgos

El análisis de riesgos desempeña un papel fundamental en la seguridad de los equipos informáticos al evaluar las posibles amenazas y vulnerabilidades que podrían afectar la integridad y disponibilidad de la información. Durante este proceso, se identifican y evalúan diversos riesgos, como ataques de malware, intrusiones, pérdida de datos y fallas en el sistema, para determinar su probabilidad de ocurrencia y el impacto potencial en los equipos es esencial para la seguridad informática al identificar amenazas como malware y pérdida de datos. Permite a las organizaciones comprender estas amenazas y tomar medidas informadas, como encriptación y concientización del personal. Además, ayuda a asignar recursos de manera eficiente, focalizándolos en áreas críticas, como programas anti-phishing. Este análisis proactivo es fundamental para proteger la integridad y disponibilidad de la información en un entorno cibernético complejo informáticos (Imbaquingo et al. 2018).

En cuanto, a los riesgos operativos son una preocupación central para las organizaciones, ya que pueden afectar la eficiencia, la continuidad del negocio y la reputación. Estos incluyen amenazas como errores humanos, fallos tecnológicos, desastres naturales y fraudes. La gestión efectiva implica identificar y evaluar amenazas, implementar controles y procedimientos, promover la responsabilidad y transparencia, capacitar a empleados para reducir errores y desarrollar planes de contingencia. La tecnología juega un papel crucial a

través de sistemas de monitoreo y automatización para mejorar la eficiencia. Una cultura organizacional proactiva y colaborativa es fundamental para mitigar riesgos y asegurar la estabilidad a largo plazo (Villacrés, 2023).

2.3.2.1 Fallos del programa

Los problemas y errores recurrentes que han sido identificados en el software utilizado para gestionar las actividades académicas en el laboratorio de computación. Estos fallos han afectado diversas áreas de funcionamiento del programa, desde la pérdida inesperada de datos hasta errores en la interfaz de usuario y falta de sincronización adecuada con la base de datos. Estos problemas han tenido un impacto negativo en la eficiencia y la productividad del laboratorio, generando inconvenientes en el seguimiento de las tareas asignadas a los estudiantes y dificultades en el acceso a la información actualizada. La presencia de estos fallos ha destacado la urgente necesidad de una revisión exhaustiva del programa para corregir estos errores y asegurar un funcionamiento sin problemas en el futuro (Briano, 2023).

2.3.2.2 Vulnerabilidades y malware

Las amenazas más importantes en el mundo digital actual. Las vulnerabilidades son debilidades en los sistemas operativos, aplicaciones o redes que los atacantes pueden explotar para acceder, modificar o destruir datos sin permiso. Estas vulnerabilidades pueden ser causadas por errores de software, configuraciones incorrectas o la falta de actualizaciones de seguridad. Por otro lado, el malware, abreviatura de software malicioso, incluye varios programas diseñados para dañar, robar datos o interrumpir el funcionamiento normal de dispositivos y sistemas informáticos (Gargallo, 2023).

Estos programas maliciosos incluyen virus, troyanos, ransomware y spyware, entre otros. La combinación de vulnerabilidades no parcheadas y la presencia de malware pueden tener consecuencias devastadoras, incluyendo la pérdida de datos sensibles, la interrupción de servicios y la violación de la privacidad del usuario. Por tanto, es crucial implementar medidas

de seguridad robustas, como actualizaciones regulares de software, firewalls y programas antivirus, para protegerse contra estas amenazas y garantizar la seguridad digital (Aroca, 2022).

2.3.3 Laboratorio de Computación

2.3.3.1 Políticas de Seguridad al Laboratorio de Computación

Son fundamentales para garantizar un entorno digital seguro y protegido estas políticas son meticulosamente diseñadas para salvaguardar la integridad de los datos, la confidencialidad de la información y la disponibilidad de los recursos tecnológicos las políticas del laboratorio incluyen medidas de autenticación de usuarios, con controles de acceso para limitar la entrada a personas autorizadas solamente. Además, se implementan protocolos de encriptación robustos para proteger los datos mientras se transmiten a través de la red (Pazmiño, 2023).

La gestión de contraseñas seguras y la actualización regular de estas son prácticas estándar para prevenir accesos no autorizados. También se establecen pautas claras para el uso adecuado de los dispositivos y recursos informáticos, así como para la instalación y actualización de software. La monitorización continua de actividades sospechosas y la respuesta rápida ante posibles amenazas son parte integral de estas políticas, asegurando así que el laboratorio de computación opere en un entorno seguro y protegido contra las crecientes amenazas cibernéticas (Farfán, 2023)

2.3.3.2 Seguridad de Hardware

En un laboratorio de computación, el equipo desempeña un papel clave en el funcionamiento efectivo y eficiente de las actividades tecnológicas. El hardware ha provocado cambios significativos en todos los segmentos involucrados en el procesamiento de datos. El hardware consiste en elementos físicos del sistema de información (SI). Los elementos de hardware son el elemento final, los canales y los soportes de información, dispositivos electrónicos y electromecánicos que proporcionan capacidades de recolección de datos,

cálculos y métodos de representación, y transmisión de datos. Esto incluye dispositivos como sensores, dispositivos de procesamiento y almacenamiento, y monitores. (Avenía, 2017)

2.3.3.3 Seguridad Software

La seguridad del software abarca las estrategias y acciones destinadas a resguardar las aplicaciones y sistemas de software de accesos no autorizados, filtraciones de datos y ataques cibernéticos. Esto incluye la identificación y mitigación de vulnerabilidades en el software para asegurar su confidencialidad, integridad y disponibilidad. La seguridad del software es crucial, ya que un ataque de malware puede infligir daños severos en cualquier programa, comprometiendo su integridad, autenticación y disponibilidad. Si los desarrolladores consideran la seguridad durante la fase de programación en lugar de después, pueden prevenir los daños antes de que ocurran (Campos, 2011).

2.3.3.4 Seguridad de Red

En la seguridad de una red pública como Internet, está expuesta a que cualquier persona o intruso pueda acceder a ella, por lo que se debe garantizar la seguridad de la información durante el envío. Las redes privadas virtuales permiten que la información viaje segura por entornos de conexiones públicas, ante esta situación se desarrolla la presente investigación la cual tiene como objetivo elaborar una metodología adaptativa basada en un modelo de seguridad informática en redes privadas virtuales de la institución (Patil, 2023).

2.3.3.5 Dispositivos externos de entrada y salida

Estos dispositivos incluyen teclados, ratones, escáneres, cámaras, micrófonos, impresoras y pantallas, y son fundamentales para introducir y visualizar información, así como para comunicarse de manera efectiva. Estos dispositivos no solo facilitan la entrada y salida de datos, sino que también mejoran la productividad y la eficiencia en el laboratorio. La elección adecuada y la configuración óptima de estos dispositivos son esenciales para garantizar un flujo

de trabajo sin problemas y aprovechar al máximo las capacidades del laboratorio, permitiendo a los usuarios realizar sus tareas de manera efectiva y precisa (Facchini, 2022).

2.3.4 Estructura de redes de computadores

Este tema abarca muchos puntos de consideración en el estudio de las redes informáticas modernas. Estas forman una combinación de dispositivos, tecnologías y sistemas de comunicación que han surgido desde finales del siglo XIX. Desde entonces, han existido redes de área local, conexiones de datos de larga distancia a través de enlaces marítimos o satélites, Internet, servicios de telefonía móvil, etc. Estas son un gran número de tecnologías que definen las redes informáticas que utilizamos. Para obtener una buena visión general de estas tecnologías y entender las razones de su creación, se recomienda considerar el desarrollo histórico de las telecomunicaciones, que desde mediados del siglo XX está estrechamente relacionado con la historia de la computación, el concepto de redes de paquetes, en contraste con las redes de conmutación, que son el punto de partida tanto de las redes locales como de Internet (Barceló, 2022)

2.3.4.1 Mantenimiento de equipos informáticos

En el mantenimiento del equipo informático, el enfoque principal es mantener las computadoras en funcionamiento y reducir los daños que pueden ocurrir durante la vida útil del equipo. Este tipo de protección de equipos es muy reconocida por empresas e instituciones, por lo que la mayoría de ellas contratan personal especializado para gestionar la tecnología informática y lograr el mejor rendimiento de las computadoras, ya que siempre hay algunas perturbaciones en su estructura informática (Vargas, 2021).

2.3.4.2 Memoria RAM

La memoria RAM (memoria de acceso aleatorio) desempeña un papel crucial en el rendimiento y la eficiencia de los sistemas informáticos. La RAM actúa como una memoria de trabajo temporal para el procesador, permitiendo el acceso rápido a datos y programas en

ejecución. Una cantidad suficiente de RAM es fundamental para garantizar que las aplicaciones se ejecuten de manera fluida y sin retrasos, especialmente al manejar tareas intensivas en datos o ejecutar programas complejos. En el contexto del laboratorio de computación, donde se llevan a cabo actividades académicas y de investigación que a menudo involucran software especializado y grandes conjuntos de datos, contar con una cantidad adecuada de memoria RAM es esencial para la realización eficiente de experimentos, simulaciones y análisis computacionales. (Goñas, 2022)

Las RAM son consideradas como uno de los dispositivos emergentes con mayor proyección de futuro en aplicaciones tanto analógicas como digitales, sobre todo en chips de memoria, circuitos lógicos, redes neuronales y seguridad hardware. Entre sus características más importantes se encuentran, la velocidad de escritura/lectura, el bajo consumo de energía, la novolatilidad, la escalabilidad y su compatibilidad con procesos de fabricación de tecnología CMOS. Además, la velocidad y la capacidad de la memoria RAM son consideraciones importantes, ya que influyen directamente en la velocidad de procesamiento y la capacidad de respuesta del sistema. Por tanto, la elección de una memoria RAM adecuada y su gestión eficiente son aspectos clave para optimizar el rendimiento y la productividad en el laboratorio de computación (Campos, 2011).

2.3.4.3 Puertos y Conectores

En un entorno de laboratorio, la variedad y disponibilidad de puertos son fundamentales para la versatilidad y la interoperabilidad de los equipos. Por ejemplo, los puertos USB son universales y se utilizan para una amplia gama de dispositivos, desde unidades flash hasta cámaras. Los puertos Ethernet son esenciales para mantener una conexión de red estable y rápida, fundamental para compartir recursos y acceder a Internet. Además, los puertos HDMI son esenciales para proyectar presentaciones y contenido multimedia en pantallas externas. La correcta identificación y utilización, de los puertos y conectores desempeñan un papel crucial

al facilitar la interconexión de dispositivos electrónicos. Estos puertos permiten la conexión de periféricos como teclados, ratones, impresoras, unidades de almacenamiento y dispositivos móviles a las computadoras. Además, los puertos USB, HDMI, Ethernet y otros tipos de conectores son esenciales para establecer conexiones de red, transmitir datos, audio y video, y cargar dispositivos (Samaniego, 2018).

2.3.4.4 Cableado de la red

El cableado de la red juega un papel fundamental en garantizar una conectividad confiable y eficiente entre los dispositivos. La infraestructura de cableado, que incluye cables Ethernet, conectores y dispositivos de red, establece la base para la transmisión rápida y segura de datos y la comunicación en red. Un diseño cuidadoso del cableado es esencial para evitar interferencias y pérdida de señal, especialmente en entornos donde múltiples dispositivos están conectados simultáneamente, como en un laboratorio de computación. Además, el cableado estructurado permite una fácil expansión y reconfiguración de la red para adaptarse a las necesidades cambiantes del laboratorio. Los estándares de cableado, como el estándar Ethernet, garantizan la compatibilidad y la interoperabilidad entre los dispositivos de red. La instalación adecuada y la gestión eficaz del cableado no solo garantizan una conexión estable y de alta velocidad, sino que también reducen los tiempos de inactividad y mejoran la eficiencia operativa del laboratorio. En última instancia, un cableado de red bien planificado y ejecutado es esencial para mantener un entorno de laboratorio de computación que sea moderno, adaptable y totalmente funcional (Samaniego, 2018).

2.3.5 Metodología de desarrollo

2.3.5.1 MAGERIT

La metodología por desarrollar es MAGERIT es un enfoque oficial en España para el análisis y gestión de riesgos en sistemas de información. Desarrollada por el antiguo consejo superior de administración electrónica y mantenida por el Ministerio de Asuntos Económicos

y Transformación Digital, junto con el Centro Criptológico Nacional, MAGERIT se utiliza para evaluar los riesgos de seguridad en sistemas informáticos y redes. Se basa en estándares internacionales y se aplica principalmente en entidades sujetas al Esquema Nacional de Seguridad (ENS). La metodología consta de tres fases: inventario de activos, análisis y evaluación de riesgos, y gestión de riesgos. Proporciona un enfoque estructurado para entender y mitigar los riesgos de seguridad de la información, permitiendo a las organizaciones tomar decisiones informadas sobre la gestión de riesgos en sus sistemas de información, evaluación de las amenazas, vulnerabilidades e impactos asociados con los activos de información para determinar los riesgos (López, 2019).

Gestión de Riesgos desarrollo e implementación de medidas de seguridad para mitigar los riesgos identificados, seguido por un proceso de seguimiento y revisión constante para asegurar la efectividad de estas medidas. MAGERIT proporciona un marco estructurado para ayudar a las organizaciones a proteger sus sistemas de información y a tomar decisiones informadas sobre la gestión de riesgos en el ámbito de la seguridad de la información (Alvarado y Martillo 2019) (Guerrero, 2022).

El método MAGERIT es la abreviatura de Metodología de Gestión y Análisis de Riesgos de los Sistemas de Información Gubernamentales. Cabe señalar que este método incluye una fase AGR (Análisis y Gestión de Riesgos). En la gestión integral de la seguridad de un sistema de información basado en la norma ISO 27001, MAGERIT constituye el centro de todas las actividades organizadas en este ámbito., incide en todas las etapas estratégicas y determina la profundidad de las etapas logísticas. En sucesivas versiones de MAGERIT, el objetivo es evaluar, aceptar y certificar la seguridad de los sistemas de información (SSI) según la norma ISO 27001 (López, 2019).

2.3.5.2 Fases de la metodología MAGERIT

Según Ávila et al, (2021), la metodología de MAGERIT se puede desglosar en cinco pasos fundamentales.

- La determinación de activos.
- La determinación de amenazas
- La determinación de riesgos
- La determinación de salvaguardas
- La determinación de residual

2.4 Conclusiones del marco teórico

El SGSI se presenta como una herramienta indispensable para la protección de la información en las organizaciones. A lo largo del marco teórico, se ha demostrado que la implementación de un SGSI permite a las instituciones gestionar de manera eficiente los riesgos asociados a la seguridad de la información. Al establecer políticas claras, procedimientos y controles rigurosos, se asegura la integridad, disponibilidad y confidencialidad de los datos, mejorando la resiliencia de la organización ante posibles amenazas. En conclusión, el SGSI es un componente esencial en la gestión de la seguridad en entornos digitales, promoviendo un ambiente de confianza y protección.

El análisis del laboratorio de computación revela la importancia de contar con medidas de seguridad robustas que garanticen un entorno protegido para el manejo de información crítica. A través del marco teórico, se concluye que la vulnerabilidad de los laboratorios de computación ante amenazas cibernéticas requiere la implementación de controles que aseguren no solo la operatividad de los equipos, sino también la seguridad de los datos. Las brechas en la seguridad en estos entornos pueden comprometer tanto los recursos tecnológicos como la información sensible, haciendo imprescindible la aplicación de buenas prácticas de seguridad.

Por lo tanto, un laboratorio de computación eficiente depende de una infraestructura segura y una gestión adecuada de los riesgos.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

El presente capítulo contiene información de los tipos de investigación que se realizarán para diagnosticar e identificar problemas de seguridad de la información en la institución" Unidad Educativa Alida Zambrano García" los cuales son Aplicar métodos y técnicas de investigación que justifiquen el problema, y diagnosticar , las vulnerabilidades en la seguridad de la información mediante la aplicación de los métodos y técnicas a través de encuestas y entrevistas para evaluar riesgos de seguridad de la información en el laboratorio de computación, y así reducir el problema en general y enfocarse realmente al área de estudio al que se desea aplicar una la auditoría, eso ayudara a realizar el estudio desde lo general de problema e irlo desglosando hasta llegar a los especifico, así tomando las mejores decisiones al momento de desarrollar un manual de usuario para las buenas prácticas de seguridad informática. dentro de los instrumentos aplicados para la recolección de datos se tomó en cuenta la aplicación de entrevistas y encuestas, la entrevista fue aplicada al rector de la institución porque él cuenta con conocimiento de los acontecimientos dentro de la unidad educativa "Alida Zambrano García " y su información es de gran ayuda para obtener un resultado favorable por otra parte las encuesta fueron aplicadas a los docentes de la institución quien son el objetivo de la auditoría, son ellos los que aportan más información, , posteriormente los resultados fueron tabulados para obtener indicadores que permitan establecer nuevos parámetros que ayuden a mejorar la seguridad informática dentro de la institución, y así Elaborar un informe de auditoría que detallen los riesgos y vulnerabilidades que existen en el laboratorio de computación.

3.2 Tipos de investigación

3.2.1 Investigación cualitativa

La investigación cualitativa implica la recopilación y el análisis de datos cuantitativos para comprender conceptos, opiniones o experiencias, así como datos sobre experiencias vividas, sentimientos o comportamientos y los significados que las personas les atribuyen. Por lo tanto, los resultados se expresan en palabras. También puede ser útil explorar cómo o por qué ocurrió un incidente, explicar el incidente y ayudar a describir qué hacer (Sandoval, 2020).

La investigación cualitativa se empleó para explicar y recopilar actividades directamente vinculadas con el problema identificado. Este enfoque permitió una comprensión profunda de los factores involucrados, capturando las percepciones y experiencias de los participantes. A través del análisis cualitativo, se logró obtener información coherente y relevante que aportó a la elaboración de soluciones efectivas y fundamentadas. Este método facilitó resultados óptimos al destacar las dinámicas subyacentes que influyen en el contexto del estudio.

3.2.2 Investigación cuantitativa

El diseño de este estudio cuantitativo es método empírico común a la mayoría de las ramas de la ciencia, propósito de la investigación cuantitativa es obtener conocimientos básicos y elección, el modelo más adecuado que permite conocer la realidad más justa, ya que se recopilan y analizan datos a través de conceptos y variables medibles. La investigación cuantitativa sirve para recopilar y evaluar datos procedentes de diversas fuentes, la investigación cuantitativa utiliza técnicas informáticas, estadísticas y matemáticas para obtener resultados. Se trata de cuantificar el problema y comprender su importancia buscando resultados que se puedan predecir para una población más grande. (Dueñas, 2019)

La investigación cuantitativa fue de mucha ayuda ya que se utilizó para evaluar y así identificar la inexistencia de seguridad de la información dentro del laboratorio de computación

esto desempeñó un papel fundamental en el estudio, ya que se utilizó para la investigación a través de entrevistas y encuestas. Estos métodos permitieron obtener datos estructurados y cuantificables sobre las percepciones, conocimientos y prácticas relacionadas con la seguridad informática en el laboratorio de computación de la Unidad Educativa "Alida Zambrano García".

3.2.3 Investigación descriptiva

Se utilizan para analizar cómo se ve un fenómeno, y sus componentes y como se manifiestan. Permiten el detalle del fenómeno se estudia básicamente midiendo una o más de sus propiedades. Identificar las características del universo estudiado, mostrar patrones de comportamiento y actitudes del universo estudiado, establecido 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 fundar (Vásquez Hidalgo, 2005).

La investigación descriptiva se utilizó para la recopilación de datos tanto, la investigación descriptiva en el laboratorio de computación de la Unidad Educativa "Alida Zambrano García" ha permitido identificar y describir las vulnerabilidades, deficiencias y áreas de mejora en términos de seguridad informática, proporcionando una base sólida para la formulación de recomendaciones y la implementación de medidas correctiva la situación actual en cuanto a la seguridad informática, este tipo de investigación ha implicado la recopilación de datos a través de encuestas y entrevistas con los docentes del laboratorio, así como el análisis estadístico de los mismos para obtener una visión clara de las percepciones, conocimientos y prácticas relacionadas con la seguridad informática.

3.3 Métodos de investigación

3.3.1 Método inductivo

Es el método científico de sacar conclusiones generales basadas en suposiciones o antecedentes específicos. A menudo se basa en observar y experimentar eventos y acciones específicas para llegar a una solución o conclusión general sobre ellos; es decir, en este proceso se parte de datos y se termina con una teoría, por lo que se puede decir que va de lo particular a lo general. La inferencia va de lo particular a lo general (Carbajal, 2019).

Se empleó el método inductivo para analizar situaciones específicas relacionadas con la seguridad de la información en el laboratorio de computación de la Unidad Educativa Alida Zambrano García. Este enfoque permitió observar y recopilar datos sobre los problemas de seguridad que enfrentaba el laboratorio, tales como la vulnerabilidad de los equipos y la falta de protocolos adecuados. A partir de estos eventos y antecedentes particulares, se logró inferir conclusiones generales sobre la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

3.3.2 Método deductivo

El tipo de razonamiento lógico caracterizado por el hecho de que la conclusión se sigue necesariamente de varias premisas se denomina método o razonamiento deductivo. La deducción puede definirse como el proceso de derivar una conclusión válida, verificable y aplicable a partir de una o varias premisas generales. (Uriarte, 2022).

El método deductivo se utilizó para aplicar principios generales a situaciones específicas relacionadas con la seguridad de la información en el laboratorio de computación. Este enfoque parte de teorías o principios generales aceptados, como las normas y estándares internacionales de seguridad, y los aplica a casos concretos dentro del contexto del laboratorio.

3.3.3 Método Analítico

Consiste en clasificar el todo, descomponiéndolo en partes o factores para observar sus causas, naturaleza y efectos. El análisis es la observación y el examen de un hecho particular para comprender su naturaleza, es necesario conocer la naturaleza del fenómeno y el objeto de estudio. Este método nos posibilita conocer más sobre el objeto de estudio, que a su vez puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías (Ruiz, 2006).

El método analítico se empleó para descomponer el problema de seguridad en el laboratorio de computación en partes más manejables y entender cómo cada componente contribuye al problema general. Este enfoque permitió una evaluación detallada y sistemática de los distintos aspectos relacionados con la seguridad de la información.

3.3.4 Método sintético

El enfoque sintético es un proceso de análisis inferencial que busca una forma de reconstruir eventos de manera generalizada utilizando los diversos bloques de construcción presentes en el desarrollo de eventos. Este enfoque permite a las personas resumir lo que ya saben. La síntesis es un proceso mental que comprime la información en la memoria. Este proceso muestra la capacidad humana para reconocer todas las cosas conocidas y extraer de ellas las propiedades más importantes (Reyqui, 2019).

El método sintético se utilizó para integrar y combinar los hallazgos obtenidos de diferentes componentes del análisis de seguridad en el laboratorio de computación, creando una visión coherente y comprensiva del problema general. Este enfoque permitió construir un entendimiento global a partir de la evaluación de partes individuales.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias

Las fuentes primarias son documentos o registros originales que proporcionan datos directos sobre un tema. Estos incluyen investigaciones originales, documentos oficiales, entrevistas y textos históricos, que presentan información sin intermediarios. Por ejemplo, un informe de auditoría reciente en un laboratorio de computación es una fuente primaria que ofrece detalles directos sobre la situación de seguridad. Por otro lado, las fuentes secundarias interpretan, analizan o resumen la información proveniente de fuentes primarias. Incluyen artículos de revisión, libros que compilan investigaciones previas y ensayos que discuten datos obtenidos de otras fuentes. Estas fuentes ofrecen contexto y evaluación de los datos originales, facilitando una comprensión más amplia del tema (Tipton, 2018).

Entre las fuentes primarias tenemos:

- Rector de la institución
- Los equipos dentro del laboratorio

3.4.2 Fuentes secundarias

El investigador recurre también a las fuentes secundarias, es decir información que proporcionan las personas que no observaron directamente la situación. Las fuentes 25 primarias y secundarias pueden hacer que el investigador modifique el esquema del problema cuando la información indique que ello es necesario (Moguel, 2005).

Entre las fuentes secundarias tenemos:

- Los docentes de la institución

3.5 Encuestas

La encuesta se suele considerar como una entrevista estructurada mediante un cuestionario en el cual el encuestado responde a una serie de preguntas predeterminadas. Esta

metodología permite la recolección de datos de manera sistemática y uniforme, facilitando el análisis de información específica sobre el tema de interés y asegurando que se obtenga una amplia gama de respuestas relevantes (Ahamah, 2019).

La encuesta fue mediante instrumento que es el cuestionario de 10 preguntas, sobre los procedimientos de seguridad de la información en las políticas las esta misma se la realizo a 6 docentes de la institución de manera física para obtener información y así evaluar periódicamente los resultados, la encuesta tienes como finalidad obtener resultados óptimos sobre las vulnerabilidades que existe en el laboratorio de computación esto nos brinda una mejor ventaja y así poder realizar la de datos debido a la precisión que posee.

3.6 Entrevista

Una entrevista es una técnica de recolección de información que consiste en un diálogo entre dos o más personas, donde una de ellas, el entrevistador, formula preguntas y la otra, el entrevistado, proporciona respuestas. Las entrevistas pueden ser estructuradas, semiestructuradas o no estructuradas, dependiendo del grado de libertad que tenga el entrevistador para desviar de un guion preestablecido. Se utilizan en diversos campos como la investigación social, el periodismo, la selección de personal y la psicología, entre otros, para obtener datos cualitativos y cuantitativos, profundizar en la comprensión de un tema y explorar las experiencias y opiniones de los entrevistados (Seid, 2016).

Se le realizó una entrevista al Rector de la Unidad Educativa Alida Zambrano para recabar información importante sobre temas de Gestión de seguridad de la información para el laboratorio de computación de la institución, esto facilita la obtención de información detallada y precisa sobre la seguridad que existe en la institución.

3.7 Estrategia operacional para la recolección de datos

3.7.1 Población y muestra

3.7.1.1 Población -Segmentación

La población se trata de un conjunto de elementos los cuales contienen características en la cual se lleva a cabo una investigación sobre lo que se pretende estudiar. En ocasiones la población puede ser accesible, es decir donde el número de elementos sea menor y esté delimitado, en otros casos la población es demasiado grande y el investigador no tiene acceso a ella (Ventura, 2017).

La población es de 59 docentes de la Unidad Educativa "Alida Zambrano García sin embargo solo 6 docentes de les realizo la encuesta porque no todos los docentes imparten clases en el laboratorio de computación de la institución

3.7.1.2 Muestra

Es un subconjunto o parte del universo o población en la que se llevara a cabo la investigación. Hay procesos para el número de componentes de muestreo, como fórmulas, lógicas y otros componentes que se verán a continuación. Las muestras son parte del representante de la población (López, 2004).

En el caso de la investigación sobre el SGSI para el laboratorio de computación de la Unidad Educativa Alida Zambrano García, no se consideró el cálculo de la muestra debido a que la población es pequeña y accesible la población en este caso consiste en 59 docentes, lo que la convierte en una población pequeña. Esto significa que es posible encuestar a toda la población sin que ello represente un esfuerzo significativo, además, la población es accesible, ya que todos los docentes están registrados en la institución educativa. Esto facilita el proceso de encuesta, ya que no es necesario realizar un muestreo aleatorio para seleccionar a los participantes la decisión de no considerar el cálculo de la muestra en este caso es adecuada, ya que permite encuestar a toda la población de forma precisa y eficiente.

3.7.2 Análisis de las herramientas de recolección de datos a utilizar

3.7.2.1 Encuesta

La investigación de SGSI para el laboratorio de computación de la Unidad Educativa Alida Zambrano García utilizó las siguientes herramientas de recolección de datos por medio de los cuales se utilizó para recopilar información sobre la concienciación de la seguridad de la información en los laboratorios de informática. La encuesta se la realizo a los docentes del laboratorio de computación.

3.7.2.2 Entrevista

En la Entrevista que se pudo utilizar para recopilar información detallada sobre las políticas actuales del SGSI del laboratorio de computación. Se realizaron entrevistas al responsable del laboratorio de computación e informática en este caso al Rector se utiliza para identificar amenazas y vulnerabilidades a la seguridad de la información en laboratorios de computación. Las observaciones fueron realizadas por el investigador durante la visita al laboratorio.

Se realizo análisis de estas herramientas de recolección de datos nos permite identificar maneras sobre la seguridad de la información la conciencia aún es baja la seguridad. Sobre la información almacenada en el laboratorio como también las actividades actuales existen vulnerabilidades en la seguridad del hardware, la seguridad del software y la seguridad de la red. Amenazas y en el laboratorio de computación Estas amenazas incluyen acceso no autorizado, robo de información y alteración de información en general, las herramientas de recopilación de datos utilizadas en este estudio fueron suficientes para recopilar la información necesaria para evaluar el laboratorio de computación del SGSI y hacer recomendaciones para su mejor

3.7.3 Estructura de los instrumentos de recolección de datos aplicados

3.7.3.1 Plan de recolección de datos

La encuesta y la entrevista se realizó con la finalidad de recolectar datos y resultados en la encuesta hubo un total de 10 preguntas y en la entrevista hubo 10 preguntas, para obtener análisis óptimos recolectados descritos en el material y métodos y presenta las pruebas que apoyan estos resultados. Por medio de gráficos.

La recolección de datos referente a la encuesta y entrevista mediante el método presencial. para recopilar datos información y verificar que existen en el laboratorio de computación las encuesta y las entrevista son dirigidas los docentes de la institución Para ello, se les entregaran la hoja con las 10 preguntas para que ellos puedan resolver las encuestas y las preguntas. Este cronograma detallado nos va a permitir obtener información de diferentes fuentes y perspectivas, para saber cuáles son las falencias que tiene el laboratorio de computación y las vulnerabilidades lo que el análisis y las conclusiones para lograr obtener datos recolectados. el uso de dos métodos diferentes de recolección de datos nos asegura una mayor validez y fiabilidad de los resultados obtenidos en la encuesta y las entrevistas

4 Tabla 1: Cronograma Plan recolección de datos

Actividad de recolección de datos	**Fecha de inicio**	**Fecha de finalización**	**Método**	**Dirigido a**
Recolectar datos mediante encuesta	22/1/2024	22/1/2024	Presencial	Se realizo la encuesta a 6 docentes de la institución
Entrevista	23/1/2024	23/1/2024	Presencial	Personal encargado de la institución que es el Rector Andrés Cagua

4.1 Encuesta

Universidad Laica "Eloy Alfaro" de Manabí

Extensión El Carmen

Objetivo: Identificar problemas de seguridad de la información en el Laboratorio de Computación

Encuesta Dirigida a: DOCENTES de la U.E Alida Zambrano García

1. ¿Conoce usted de las Políticas de seguridad en el laboratorio de computación?

___ Si ___ No

2. ¿Ha recibido capacitación regular sobre las mejores prácticas de seguridad?

___ Si ___ No

3. ¿Considera que es importante la Gestión de seguridad de la información en el laboratorio de computación?

___ Si ___ No

4. ¿Ha tenido algún incidente de seguridad de la información en el laboratorio de computación?

___ Si ___ No

5. ¿Conoce usted de los ataques informáticos?

___ Si ___ No

6. ¿Ha sido víctima de un ataque Informático?

___ Si ___ No

7. ¿Considera que se da mantenimientos a los equipos en el laboratorio de computación?

___ Si__ _No A veces___

8. ¿Usted conoce si los equipos tienen instalado antivirus?

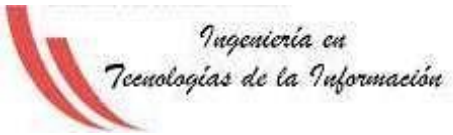
___ Si ___ No

9. ¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el laboratorio de computación?

___ Si ___ No

10. ¿Existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica?

___ Si ___ No



4.2 Entrevista

Universidad Laica "Eloy Alfaro" de Manabí

Extensión El Carmen

Objetivo: Identificar problemas de seguridad de la información en el Laboratorio de Computación

Entrevista Dirigida al: RECTOR de la U.E Alida Zambrano García

1. ¿La institución cuenta con políticas de seguridad para el uso del laboratorio?
2. ¿Se ha capacitado a los docentes sobre políticas de seguridad informática?
3. ¿Qué considera que son los principales riesgos de seguridad de la información en el laboratorio de computación?
4. ¿Cuáles son las principales vulnerabilidades que usted cree que existe en el laboratorio de computación en términos de seguridad?
5. ¿Ha existido algún tipo de incidente informático dentro de la institución, qué procedimientos se realizaron para solucionar el problema?
6. ¿Brindas cursos de capacitación a los docentes sobre seguridad informática?
7. ¿Considera que los docentes de la institución están listos para enfrentar un ataque informático?
8. ¿Existen procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de que uno que este en uso, se le esté dando mantenimiento?
9. ¿Existe una persona responsable de la seguridad informática dentro de la institución?
10. ¿Existen evaluaciones periódicas para medir el nivel de conciencia de seguridad entre los usuarios?

4.3 Análisis y presentación de resultados

4.3.1 Análisis de datos obtenidos a través de la entrevista

4.3.1.1 Entrevista realizada al Rector de la institución Alida Zambrano García

Tabla 1: Resultado de la entrevista al rector

Pregunta	Respuesta	Interpretación
1 ¿La institución cuenta con políticas de seguridad para el uso del laboratorio?	La respuesta del Sr. Rector indica que sí, cuenta con políticas de seguridad, incluyen horarios para el acceso al laboratorio y están alineados con los horarios de clases para el ingreso fuera de los horarios asignados, los estudiantes o usuarios	La institucione Alida Zambrano García parece tener medidas claras para garantizar un ambiente adecuado dentro del laboratorio de computación
2. ¿Se ha capacitado a los docentes sobre políticas de seguridad informática?	El rector indica que, aunque inicialmente se tomaron medidas para capacitar a los docentes al principio del año en temas de seguridad informática, este proceso se interrumpió debido a un cambio de materias en la institución lo cual en este año no se dio la materia de informática a los estudiantes	Esto podría indicar una falta de continuidad en la capacitación en seguridad informática para el personal docente, lo que podría plantear preocupaciones sobre la preparación del personal en este aspecto crucial de la seguridad institucional.
3. ¿Qué considera que son los principales riesgos de seguridad de la información en el laboratorio de computación?	La falta de conocimiento sobre de seguridad informática por parte de los estudiantes y docentes que puedan descargar software malicioso o compartir información confidencial sin precaución. O en la interrupción de las operaciones del laboratorio.	Esto indica que no todos los docentes tienen conocimiento de la seguridad informática

4. ¿Cuáles son las principales vulnerabilidades que usted cree que existe en el laboratorio de computación en termino de seguridad	Lo que indica que la principal vulnerabilidad es la falta de seguridad es el uso de wifi en la institución porque no hay un laboratorista lo cual por muchos años a permanecido con la misma contraseña y los estudiantes lo han podido hackear	la falta de actualización en las medidas de seguridad, como cambiar regularmente las contraseñas de wifi, representa una seria vulnerabilidad en el laboratorio de computación. El hecho de que los estudiantes hayan podido hackear
5. ¿Ha existido algún tipo de incidente informático dentro de la institución, qué procedimientos se realizaron para solucionar el problema?	El rector indica, aunque no ha habido un incidente informático específico recientemente, en años anteriores hubo un problema relacionado con un programa llamado Ubuntu. Este programa causó problemas en las computadoras, haciendo que funcionaran lentamente y, en algunos casos, dejando de funcionar debido a la falta de capacidad, aunque persiste el problema con cinco computadoras que no encienden, Sin embargo, el Sr. Rector menciona que se han resuelto en la actualidad con respecto al programa en cuestión	La institución menciona que aún persiste un problema con cinco computadoras que no encienden. Esta situación sugiere un problema de hardware más que un incidente informático, lo que implica que podría haber un problema con la fuente de alimentación, la placa base u otros componentes de estas computadoras ha enfrentado desafíos tanto relacionados con el software como con el hardware en el pasado.

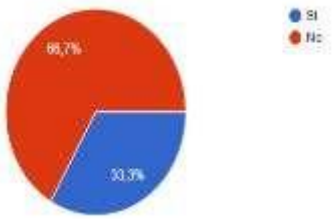
6. ¿Brindas cursos de capacitación a los docentes sobre seguridad informática?	La respuesta del rector fue que, aunque en la actualidad no se están ofreciendo cursos de capacitación a los docentes sobre seguridad informática, existe interés en recibir dicha capacitación en el futuro. Sin embargo, se espera que esta capacitación sea proporcionada por el gobierno de forma gratuita, para que los docentes tengan más conocimiento sobre la seguridad informática	La institución reconoce la importancia de la seguridad informática y está interesada en preparar a su personal docente para enfrentar posibles ataques informáticos. Al expresar que preferirían que la capacitación sea proporcionada de manera gratuita por el gobierno, recursos externos para cumplir con este objetivo de capacitación en seguridad informática. los desafíos de seguridad en el entorno digital.
7. ¿Considera que los docentes de la institución están listos para enfrentar un ataque informático?	La respuesta del entrevistado sugiere que los docentes de la institución no están preparados para enfrentar un ataque informático. Esto se debe a dos razones principales primero, porque nunca han estado expuestos a un ataque informático directo, y segundo, porque no han recibido capacitación específica en seguridad informática en la actualidad.	La falta de experiencia previa en enfrentar ataques informáticos y la ausencia de capacitación actualizada en este campo pueden dejar a los docentes vulnerables ante posibles amenazas cibernéticas. Esto resalta la necesidad de implementar programas de capacitación en seguridad informática para el personal docente, a fin de fortalecer

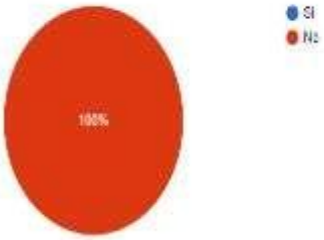
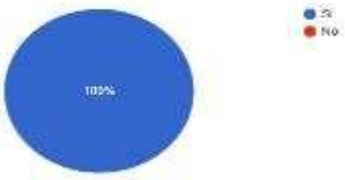
8.¿Existen procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de que uno que este en uso, se le esté dando mantenimiento?	Bueno como ya lo dije anteriormente si hay reglamentos de seguridad establecidos para el uso de los computadores en el laboratorio de computación. en cuanto al mantenimiento de los equipos, se menciona que actualmente se lleva a cabo por parte de los estudiantes que vienen a realizar sus prácticas universitarias.	el uso de los equipos de cómputo, el enfoque en el mantenimiento parece depender en gran medida de la participación de los estudiantes en prácticas universitarias. Esto es de preocupaciones sobre la consistencia y la calidad del mantenimiento realizado, ya que puede variar según la disponibilidad y habilidades de los estudiantes. mantenimiento, lo que podría afectar la productividad y el funcionamiento del laboratorio de computación.
9.¿Existe una persona responsable de la seguridad informática dentro de la institución?	Bueno por el momento no hay una persona designada específicamente como responsable de la seguridad informática en el laboratorio de computación dentro de la institución. En su lugar, como rector asumo la responsabilidad de supervisar el laboratorio de computación debido a la falta de un laboratorista designado. Pero en este nuevo año electivo ya se van a dar nuevamente la materia de computación	La ausencia de un laboratorista designado para gestionar la seguridad informática puede indicar una debilidad en la capacidad de la institución para abordar adecuadamente los desafíos de seguridad cibernética. Además, la carga de responsabilidad recae en el rector, lo que

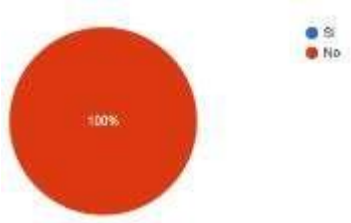
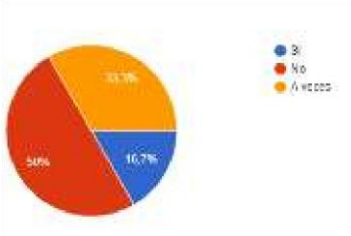
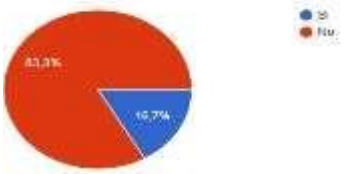
		puede resultar en una distribución inadecuada de tareas y prioridades, así como en una falta de enfoque especializado en seguridad informática. Esto resalta la necesidad de establecer roles claros y responsabilidades definidas en materia de seguridad informática dentro de la institución.
10. ¿Existen Evaluaciones periódicas para medir el nivel de conciencia de seguridad entre los usuarios?	indica que actualmente si se llevan a cabo evaluaciones para medir el nivel de conciencia de seguridad entre los usuarios, tanto estudiantes como docentes.	Estas evaluaciones son fundamentales para identificar áreas de mejora y fortalecer la seguridad de la institución. Al incluir a estudiantes y docentes entro de la institución.

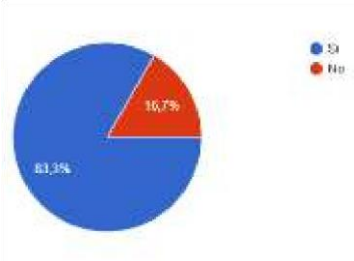
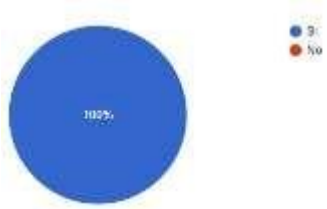
4.3.1.2 Entrevista realizada a los docentes

Tabla 2: Análisis de resultados de la encuesta dirigida al docente

Pregunta	Grafico	Interpretación
1 ¿Conoce usted de las Políticas de seguridad en el laboratorio de computación?		El encuestado demostró un conocimiento adecuado sobre las políticas de seguridad en el laboratorio de computación. Esto implica que está consciente de las normas y reglamentos establecidos para garantizar un ambiente seguro.
2 ¿Ha recibido capacitación regular sobre las mejores prácticas de seguridad?		La mayoría de los encuestados no han recibido capacitación regular sobre las mejores prácticas de seguridad. Pero una tercera parte manifestó, si haber recibido capación en años anteriores. Esto puede indicar una falta de programas de capacitación en seguridad informática dentro de la institución

3. ¿Considera que es importante la Gestión de seguridad de la información en el laboratorio de computación		La totalidad de los encuestados consideran que si es importantes ya que la seguridad de la información dentro del laboratorio es esencial para asegurar la calidad y validez de los resultados. Esto prevendría la pérdida de datos en el futuro, ya sea debido a hackers, virus, desastres naturales u otros problemas.
4 ¿Ha tenido algún incidente de seguridad de la información en el laboratorio de computación?		Según la gráfica la totalidad n000000o ha tenido incidentes de seguridad de información los encuestaos corroboraron no haber habido problemas relacionados con la seguridad de la información en el laboratorio.
5. ¿Conoce usted de los ataques informáticos?		Todos están conscientes de la existencia y posibilidad de ataques informáticos en el laboratorio de computación. Esta respuesta indica un nivel de conciencia sobre los riesgos de seguridad cibernética

6¿Ha sido víctima de un taque Informático?		Según su respuesta ninguno de los encuestados ha sido víctima de un ataque informático en el laboratorio de computación. como un resultado positivo, ya que sugiere que hasta el momento no ha habido incidentes graves de seguridad informática que hayan afectado a los usuarios.
7.Considera que se da mantenimientos a los equipos del laboratorio de computación?		En esta pregunta la mitad indicaron que sí se realiza mantenimiento existe diversas opiniones entre los encuestados con respecto al mantenimiento de los equipos en el laboratorio de computación.
8¿Usted conoce si los equipos tienen instalado antivirus ?		La mayoría de los docentes no tiene conocimiento si los equipos de hardware tienen instalado antivirus, en su gran mayoría se preguntaban entre hechos para poder responder, pero hubo una mínima audiencia que dieron que si sabían que los equipos si tiene instalado antivirus lo cual me da a entender que no tienen conocimientos básicos

9¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el laboratorio de computación?		La mayoría de los encuestados afirmó haber recibido comunicación sobre sus responsabilidades en cuanto a la seguridad en el laboratorio de computación, lo cual sugiere que la institución ha tomado medidas para educar a los usuarios sobre este tema.
10. ¿Existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica?		Si existe un existe un sistema de bloqueo implementado. Este sistema parece ser un programa proporcionado por el gobierno, diseñado para bloquear todas las páginas web que no estén relacionadas con temas educativos.

4.3.2 Presentación y descripción de los resultados obtenidos

Basando en las respuestas proporcionadas por los encuestados, los cuales fueron los docentes de la Unidad Educativa Alida Zambrano García se pueden resumir los resultados de cada una de las preguntas de la siguiente manera, la pregunta número 1. Que va en referencia a los Conocimiento de las Políticas de Seguridad: Todos los encuestados afirmaron conocer las políticas de seguridad en el laboratorio de computación, lo cual es un indicador positivo de la conciencia sobre las reglas y normativas de seguridad. Pero esto no garantiza necesariamente que tengan una comprensión completa de todas las normas y procedimientos establecidos para proteger la seguridad de la información en el laboratorio, puede conducir a prácticas inseguras

por parte de los usuarios, lo que aumenta el riesgo de incidentes de seguridad y perdidas de datos en el laboratorio

Con la pregunta número 2 que es sobre las Capacitación en Seguridad Informática: con respecto a la respuesta de la entrevista parece tener medidas para garantizar un ambiente adecuado dentro del laboratorio de computación. La mayoría de los encuestados indicaron que no haber recibido capacitación regular sobre las mejores prácticas de seguridad, lo que sugiere una oportunidad de mejora en cuanto a la formación del personal en temas de seguridad informática.

La pregunta número 3 La interpretación de esta pregunta los encuestados reconocen la importancia de la gestión de seguridad de la información en el laboratorio de computación. refleja la comprensión de que la seguridad de la información sobre los riesgos asociados con la falta de seguridad de la información y la importancia de implementar medidas adecuadas de seguridad para proteger los datos y sistemas en el laboratorio de computación, Aunque esto no garantiza necesariamente que se estén tomando todas las medidas necesarias para proteger efectivamente los datos y sistemas en el laboratorio. Ya que interpretando la respuesta del entrevistado manifiesta que no todos los docentes tienen conocimiento de los riesgos que puede haber dentro del laboratorio Este es un problema una falta de implementación de medidas de seguridad, como la adquisición de software de seguridad, la realización de actualizaciones periódicas de software y hardware, o la contratación de personal capacitado en seguridad informática

En la pregunta 4 les preguntamos sobre si ha tenido algún incidente de seguridad de la información en el laboratorio de computación todos respondieron que No.

Si bien todos los encuestados afirmaron que no han experimentado ningún incidente de seguridad de la información, es posible que algunos incidentes no hayan sido detectados, reconocidos o informados adecuadamente, esto es un problema que podría deberse a una falta

de comprensión de lo que constituye un incidente de seguridad de la información, por parte de del entrevistado la falta de actualización en las medidas de seguridad, como cambiar regularmente las contraseñas de wifi, la falta de un proceso formalizado para reportar incidentes podría dificultar la identificación y gestión adecuada de situaciones de seguridad. Por ello, es importante implementar mecanismos claros y accesibles para reportar incidentes de seguridad dentro del laboratorio de computación y fomentar que promuevan la transparencia y la responsabilidad en la gestión de la seguridad de la información.

con la pregunta número 5 que les preguntamos si conoce de los Ataques Informáticos: Todos los encuestados afirmaron conocer los posibles ataques informáticos en el laboratorio de computación, con respecto a la respuesta del entrevistado indica que tiene un nivel básico de conciencia sobre las amenazas cibernéticas. Eso no nos da la seguridad de que ellos podrían detectar, prevenir y mitigar diferentes tipos de ataques informáticos, como malware, phishing, ataques de denegación de servicio (DDoS) y otros.

Además. La falta de conocimientos completa sobre los ataques informáticos y sus implicaciones puede dejar al laboratorio de computación vulnerable a diversas amenazas cibernéticas, lo que podría resultar en la pérdida de datos sensibles, interrupciones en el funcionamiento del laboratorio y daños a la reputación de la institución. Por eso es importante abordar este problema mediante la educación y concienciación continua sobre las amenazas y la implementación de medidas de seguridad efectivas para proteger el laboratorio de computación contra estos ataques.

Con respecto a la pregunta número 6 si ha sido víctima de un de Ataques Informáticos: Ningún encuestado reportó haber sido víctima de un ataque informático en el laboratorio de computación, lo que es un problema potencial derivado a la falta de reportes de ataques informáticos por parte del entrevistado indica es la posibilidad de que los ataques no hayan

sido detectados o reconocidos correctamente, porque no se ha recibido conocimientos adecuados

por eso recomendamos instalar software de seguridad especializado que pueda monitorear continuamente el tráfico de red, detectar actividades sospechosas y alertar sobre posibles amenazas. Esto podría incluir firewalls, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y soluciones antivirus avanzadas.

Por lo cual llegamos a la pregunta número 7 que es referente si considera que le dan Mantenimiento de Equipos: La mirad de los encuestados respondieron que No por lo cual la respuesta de los encuestados es la falta de un mantenimiento adecuado y profesional de los equipos en el laboratorio de computación. El entrevistado confirma que al depender únicamente de los estudiantes universitarios que realizan prácticas para llevar a cabo el mantenimiento de los equipos, sin la supervisión de un experto en la materia, se presentan varios desafíos por lo cual una solución a este problema, sería implementar un plan de mantenimiento estructurado y profesionalizado, con la asignación de recursos adecuados para contratar a personal capacitado o para proporcionar la supervisión necesaria a los estudiantes durante las prácticas universitarias. Esto garantizaría que los equipos reciban el mantenimiento necesario para su óptimo funcionamiento y prolongar su vida útil, así como para reducir los riesgos asociados con una gestión deficiente de los recursos tecnológicos.

La pregunta número 8 que hace referencia; ¿Usted conoce si los equipos tienen instalado antivirus? La falta de conocimiento por parte de una gran parte de los docentes sobre si los equipos de hardware tienen instalado antivirus sugiere una falta de conciencia o comprensión básica sobre temas de seguridad informática. Esta situación puede indicar varios problemas verificando la respuesta del entrevistado nos indicó que algunos docentes no tienen el conocimiento es porque no imparten clases en el laboratorio de computación

En la pregunta 9 se menciona de los Comunicación de Responsabilidades de Seguridad: los encuestados declararon haber sido informados acerca de sus responsabilidades para asegurar la seguridad en el laboratorio de computación, pero al no tener un encargo experto en la materia que tenga conocimientos de seguridad y les comparta contante comunicación a los usurares sobre la conciencia sobre la importancia de la seguridad, verificando la respuesta del entrevistado en manifestó que por el momento no tiene un laboratoristas y que por ahora él está encargado del laboratorio Así mismo se elabora la pregunta número 10 si existes sistema de Bloqueo de Páginas Web: Se confirmó por late de los encuestado y por el entrevistado que si existe un sistema de bloqueo de páginas web que no tengan fines académicas en el laboratorio de computación, proporcionado por el gobierno para la seguridad de docentes y estudiantes.

4.3.3 Informe final del análisis de los datos

El análisis de los datos revela que la capacitación en seguridad informática dentro del laboratorio de computación es insuficiente. La mayoría de los encuestados, aproximadamente el 67%, no ha recibido capacitación regular sobre las mejores prácticas de seguridad. Solo una tercera parte ha participado en sesiones de formación en años anteriores. Esta deficiencia en la capacitación sugiere una brecha significativa en el conocimiento de los usuarios, lo que podría comprometer la efectividad de las medidas de seguridad existentes. La falta de formación continua indica una necesidad urgente de desarrollar y mantener programas de capacitación para mejorar la preparación del personal ante amenazas cibernéticas.

Un hallazgo clave del estudio es el alto nivel de desconocimiento entre los docentes sobre la instalación de antivirus en los equipos del laboratorio. Aproximadamente el 75% de los encuestados no está seguro si los equipos están protegidos con software antivirus. Este desconocimiento refleja una falta de información básica sobre las medidas de protección esenciales, lo que puede aumentar el riesgo de infecciones y ataques informáticos. La falta de

claridad en este aspecto subraya la necesidad de proporcionar formación específica y asegurar que todos los equipos estén adecuadamente protegidos contra amenazas cibernéticas.

El análisis de la percepción sobre el mantenimiento de los equipos en el laboratorio muestra una división de opiniones. El 50% de los encuestados cree que se realiza mantenimiento a los equipos, mientras que el otro 50% tiene dudas al respecto. Esta falta de consenso indica que la gestión del mantenimiento no es claramente comunicada o efectiva. La falta de información clara sobre el mantenimiento puede afectar el rendimiento y la seguridad de los equipos, resaltando la necesidad de establecer procedimientos de mantenimiento regular y de comunicar de manera efectiva estas prácticas a todos los usuarios.

El estudio muestra que, aunque ningún encuestado ha sido víctima de un ataque informático en el laboratorio, todos están conscientes de los riesgos asociados a los ataques cibernéticos. Esta conciencia es un aspecto positivo, ya que indica que los usuarios reconocen la importancia de la seguridad informática. Sin embargo, la ausencia de incidentes reportados podría reflejar una falta de mecanismos de reporte o de detección de problemas. Es crucial que la institución implemente medidas proactivas para monitorear y gestionar incidentes de seguridad, garantizando así una protección continua y efectiva contra posibles amenazas.

CAPÍTULO IV

5 MARCO PROPOSITIVO

5.1 Introducción

El presente capítulo tiene como finalidad Realizar una auditoría de seguridad informática al laboratorio de cómputo de la Unidad Educativa “Alida Zambrano García “para evaluar las vulnerabilidades de este e identificar los posibles riesgos a los que está expuesto.

SGSI (Sistema de Gestión Seguridad de la Información) para el laboratorio de computación Descripción de la propuesta

5.2 Descripción de la propuesta

La propuesta consiste el en desarrollo de la auditoria informática física ", utilizando la metodología Magerit, en el pedido 2024 por ellos la metodología, desarrollada por el Centro Criptológico Nacional de España, es ampliamente reconocida y utilizada para la gestión de riesgos de seguridad de la información. así se puede revela la realidad la identificación de los riesgos de seguridad física en el laboratorio de computación esto es un paso crucial hacia las garantías de un entorno seguro y protegido.

Al analizar exhaustivamente los sistemas, protocolos y prácticas de seguridad, hemos identificado áreas de fortaleza y posibles vulnerabilidades. Este análisis es esencial para comprender y abordar las amenazas potenciales que podrían comprometer la integridad, confidencialidad y disponibilidad de la información crítica alojada en el entorno del laboratorio.

Es por ello por lo que se realizó la estimación del riesgo mediante la modelación de impacto, probabilidad y riesgo utilizando escalas cualitativas, siguiendo la metodología MAGERIT. La planificación que se realizó la auditoría tuvo como meta principal realizar un análisis de riesgos de los equipos informáticos ubicados en los laboratorios de computación de

la Unidad Educativa " Alida Zambrano García", ", utilizando la metodología MAGERIT. El objetivo específico consistió en calcular la estimación del riesgo modelando el impacto, la probabilidad y el riesgo a través de escalas cualitativas en la unidad de análisis 12 ítems o preguntas.

5.3 Determinación de recursos

5.3.1 Humanos

Los recursos humanos que se utilizarán para llevar a cabo la auditoría son los propios docentes y el rector de la institución. Esto implica que se espera que los docentes participen activamente en el proceso de elaboración del manual y en la implementación de las políticas de seguridad, lo que puede ayudar a garantizar su aceptación y cumplimiento por parte de todo el personal involucrado en el laboratorio de computación.

Tabla 3: Recursos humanos del proyecto

Cantidad	Recursos	Función	Actividad
1	Ing. Clara Guadalupe Pozo Hernández	Tutora del proyecto de Titulación	Colaboradora que brindará orientación al estudiante encargado de la auditoria
1	Ing. Andrés Cagua	Rector de la Institución “Alida Zambrano García donde se realizará la auditoria	Colaborador que brinda Su conocimiento de la institución para determinar un diagnóstico
1	Ing. Gina Zambrano	Auditora	Persona que lleva a cabo la revisión sistemática y documentada de las actividades, sistemas y procesos para evaluar los estándares establecidos, identificar áreas de mejora y mitigar riesgos.

5.3.2 Tecnológicos

Tabla 4: Recursos tecnológicos del proyecto

Cantidad	Recurso	Actividad
1	Portátil lenovo Core i7 12 GB de RAM	Equipo informático es fundamental en una auditoría, ya que proporciona la capacidad de llevar a cabo la investigación de manera eficiente y portátil.
1	Teléfono	Desempeñar un papel importante en una auditoría, especialmente para la comunicación rápida y el acceso a la información mientras se está en movimiento
1	Impresora EpsonL380	Muy importante para imprimir documentos importantes, informes preliminares, evidencia recopilada u otros materiales relevantes que necesiten ser revisados en formato físico
1	Cámara	Para capturar evidencia visual durante el proceso de auditoría.
1	Office	Aplicaciones como Word, Excel, entre otras. Estas aplicaciones son esenciales en una auditoría para la creación de documentos, hojas de cálculo, presentaciones, informes y otros materiales necesarios para registrar y comunicar los hallazgos de la auditoría.
	Conexión de internet	Es Indispensable en una auditoría, ya que permite acceder a recursos en línea, comunicarse con otros miembros del equipo, enviar y recibir correos electrónicos, acceder a bases de datos y herramientas en la nube, así como realizar investigaciones adicionales según sea necesario durante el proceso de auditoría.

5.3.3 Económicos

El principal recurso disponible para el desarrollo de la auditoría son los elementos electrónicos.

Tabla 5: Recursos económicos del proyecto

Cantidad	Descripción	Precio Unitario	Subtotal
1	Portátil lenovo Core i7 12 GB de RAM	$700	$700
1	Teléfono	$600	$600
1	Impresora EpsonL380	$460	$460
1	Cámara	$500	$500
1	Conexión de internet	$30	$30
		Total :2290	Total :2290

5.4 Desarrollo Según Metodología MAGERIT

Para desarrollar este capítulo se realizó una investigación exhaustiva en donde se terminó que la metodología MAGERIT es la mejor opción en el proceso de identificación, análisis y gestión de los riesgos de seguridad de la información en el laboratorio de computación, y se guiaron con los cuales la aplicación de la metodología MAGERIT y la ejecución de estos pasos, para garantizar un adecuado nivel de seguridad de la información en el laboratorio de computación, protegiendo los datos y los sistemas de posibles amenazas y vulnerabilidades.

a) **Determinación de Activos:** Se identificarán y clasificarán todos los activos de información y recursos tecnológicos relevantes en el laboratorio de computación, como equipos, datos, software y redes, así también el análisis de Amenazas y Vulnerabilidades que se evaluarán las posibles amenazas y vulnerabilidades que podrían afectar a los activos de información identificados, utilizando técnicas como análisis de riesgos, evaluación de impacto y de amenazas.

b) **Determinación de Amenazas:** Se identificaron las amenazas que podrían haber comprometido la seguridad de los activos del laboratorio de computación, considerando factores como ataques cibernéticos, fallos técnicos, errores humanos y desastres naturales, y se evaluó su posible impacto en el entorno de la institución.

c) **Determinación de Riesgos:** Se evaluaron los riesgos de seguridad asociados con las amenazas identificadas, determinando la probabilidad de que ocurriesen y el impacto potencial que habrían tenido en los activos del laboratorio de computación, con el objetivo de priorizarlos para su gestión.

d) **Salvaguardas y Medidas de Seguridad:** Se seleccionaron y priorizaron salvaguardas y medidas de seguridad específicas para mitigar los riesgos identificados en el laboratorio de computación, tomando en cuenta su eficacia, viabilidad técnica y los costos asociados a su implementación.

e) **Determinación del Riesgo Residual:** Se realizó un análisis del riesgo residual después de la implementación de las medidas de seguridad, evaluando qué riesgos aún permanecieron y cómo se podrían haber gestionado o aceptado de acuerdo con la tolerancia al riesgo de la institución.

5.4.1 Fase I Planificación

5.4.1.1 Programa de Auditoría

Uleam	Programa de auditoría de seguridad física al laboratorio de cómputo de la Unida Educativa Alida Zambrano García

Objetivo

Identificar los riesgos de seguridad física en el laboratorio de computación de la Unidad Educativa "Alida Zambrano García".

Evaluar nivel de seguridad informática del laboratorio de computación Unidad Educativa Alida Zambrano García

Procedimientos	Definición papel	Fecha
Revisar metodología Magerit	4.4.1.1 4.4.1.4	10/12/2023
Identificación y valoración de Activos	4.4.1.5	10/05/2024
Identificación y valoración de amenazas	4.4.1.6	10/05/2024
Diseño de instrumentos	5	20/05/2024
Evaluación de Riesgos	4.3.1.1.8	20/05/2024
Analizar riesgos y calcular impactos Selección de	6.1	5/06/2024
Medidas de Seguridad:		7/06/2024
Documentación de Políticas de Seguridad		15/06/2024
Elaborar informe de auditoria		15/06/2024
Elaboración de políticas		5/07/2024

Realizado por: Gina Zambrano Fecha:15/01/2024	Revisado por: Ing. Clarita Pozo Fecha: 17/01/2024

5.5 Revisar Metodología Magerit

MAGERIT consiste en un método sistemático para el análisis y gestión de los riesgos derivados del uso de la información. Su propósito es comunicar los riesgos y la necesidad de gestionarlos a los responsables de la actividad, además de facilitar la identificación y planificación de un plan adecuado para tratarlos. La metodología se basa en una serie de principios y etapas que incluyen la identificación de activos, amenazas y vulnerabilidades, así como la evaluación del impacto potencial y la probabilidad de ocurrencia de los riesgos. Una vez identificados y evaluados los riesgos, MAGERIT guía en la selección y aplicación de controles y medidas de seguridad para mitigar los riesgos a niveles aceptables (Santiago 2019).

En consideración a los elementos descritos, se determinó que para la Unidad Educativa "Alida Zambrano García" es adecuado emplear la metodología Magerit. El objetivo es realizar un análisis de riesgos de los equipos informáticos mediante una auditoría informática física y lógica. Esto permitirá establecer un protocolo que garantice un uso más eficiente y seguro de los medios informáticos en los laboratorios de computación de la institución. Además, se implementará un proceso de gestión de riesgos dentro de un marco de trabajo que permita a los directivos tomar decisiones informadas sobre los riesgos asociados al uso de tecnologías de la información en la unidad educativa.

5.5.1 Valoración de activos

ID	NOMBRE DEL ACTIVO	CARACTERISTICAS	OBSERVACION			
A1	PC	Marca: lg modelo: w1343cv estado solido sistema operativo: de 64 bits, procesador Ram: 4,00 g	20 equipos de igual marca y procesador	1	1	1

A2	SISTEMA OPERATIVO	Tiene, instalado Windows Minios10	20 todas tienen los sistemas operativos, pero no están actualizados	2	2	2
	PAQUETE DE OFFICE	Microsoft Office 2013	20 todas tienen como, word, powers poin, Excel, Outlook	1	1	1
A1	ROUTER	Marca: Ubiquiti Network	están ubicados en rack	2	2	2
ID	NOMBRE DEL ACTIVO	CARACTERISTICAS	OBSERVACION			
A2	CPU	Marca: Intel, incide computer código: dn2820fyk línea: computadores peso1.55 k	20 todas tienen	1	1	1
A3	MOUSE	Marca: Genios Codigo:GM04003A	20 todas tienen	2	2	2
A4	RED	22 punto de red cableado	20 todas tienen	1	2	2
A5	PROYECTOR ANTIGUO	Marca: BENQ Modelo: MW853UST+3.200 Lúmenes	1 unidad, se utilizando un solo cable y en cualquier entorno de aprendizaje y reuniones.			
A6	PROYECTOR ACTUAL	Marca: Epson powerlite x17 xga 3lcd modelo: v11h569020	1unidad, se utilizando un solo cable y en cualquier entorno de aprendizaje			

5.5.2 Definición de la escala

Escala	Integridad	Confidencialidad	Disponibilidad
1	La pérdida o modificación de la información tiene un impacto negativo en los equipos informáticos	La difusión de la información no autorizada tiene un impacto bajo los equipos informáticos	La falta del activo de información tiene un impacto negativo para los equipos informáticos.
Escala	Integridad	Confidencialidad	Disponibilidad
2	La pérdida o modificación de la información tiene un impacto tolerable en los equipos informático	La difusión no autorizada de la información tiene un impacto considerable para los equipos informáticos.	La falta del activo de información tiene un impacto tolerable para los equipos informáticos
3	Equipos informáticos la pérdida o modificación de la información tiene un impacto alto en los equipos informático de riesgo	La difusión de la información tiene un impacto muy alto de riesgos	La falta del activo de información tiene un impacto de alto riesgo para los equipos informáticos

5.5.3 Escala de valor de activo

Valor	Valor activo
1-3	Bajo
3.1 – 6	Medio
6.1-9	Alto

5.5.4 Identificación y valoración de activos

Valoración de activos de información		Ref. B			
No. activo	Nombre del activo	Valoración de activos de información C: Confiabilidad I: Integridad D: Disponibilidad			
		C	I	D	VA
A1	PC ANTIGUAS 2013	3	3	3	9/alto
A2	Sistema operativo 2013	1	2	3	6/medio
A3	Reuter	1	3	3	7/alto
A4	Paquete office	1	2	2	5/medio
A5	Antivirus	1	2	3	6/medio
A6	Navegador web	3	3	3	9/alto
A8	CPU	2	2	2	6/medio
A9	Servicio de red cableada	3	3	3	9/alto
A10	Servicio de internet	3	3	3	9/alto
A11	Cámara de Vigilancia	3	3	3	9/alto
A12	Extintor	1	1	2	4/bajo
A13	Cajetines	2	2	2	6/medio
A14	Regulador de voltaje	2	2	2	6/medio

A15	Proyector	2	2	2	6/medio
	Proyector	2	2	2	6/medio

5.5.5 Identificación y valoración de amenazas y vulnerabilidades

Identificación de Riesgos		Ref. C
No. activo	Nombre del activo	Amenaza
A1	PC	Pérdida o robo de equipos. Fallas del equipo. A Ataque de virus.
A2	Sistema operativo.	Caída del sistema. Infección de virus. • Robo de información clasificado. Capacidad del equipo no es compatible con el sistema. Realizar actividades ilegales. Errores de configuración
A3	Reuter •	Fallas del equipo. Fácil de hackear. Puede ser interferido por hackers. • Estar al alcance de cualquier persona.
A4	Proyector	Pueden enfrentar desafíos en términos de durabilidad y mantenimiento.
A5	Paquetes de office	Paquete office no oficial. No tener licencia de activación. Daño del paquete office.
A6	Antivirus.	Eliminación del antivirus. Ataque mediante el uso de ingeniería social. Eliminación de ficheros importantes para el S.O. Falta de actualización del antivirus.

A7	Navegador web	Infección de virus. Actualizaciones falsas. Suplantación Perdida de información. Enlaces maliciosos. Navegación lenta
A8	Red cableada	Daño intencionado en el cable Mal estado del cable. Descarga eléctrica.

5.6 5.4.1.6 Diseño de instrumentos

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 1-5

- **Robo**

PREGUNTAS	RESPUESTA		OBSERVACION
	SI	NO	
1. ¿Ha sido victima de un taque Informático?			
2. ¿Se realizan regularmente inspecciones de seguridad en el laboratorio de computación?			
3. ¿Las cámaras de seguridad están funcionando correctamente?			
4. ¿Se lleva registro de los equipos y su mantenimiento regular?			
5. ¿El laboratorio tiene medidas para prevenir el acceso no autorizado?			
6. ¿Las puertas del laboratorio cuentan con cerraduras de alta seguridad?			
7. ¿El laboratorio cuenta con tarjetas de acceso?			
8. ¿La institución cuenta con cerramiento?			
9. ¿La institución cuenta con un laboratorista?			
10. ¿La institución ha sufrido de robo en el laboratorio?			
11. ¿La infraestructura del laboratorio de computación esta adecuada Para los estuantes			
12. ¿Se cuenta con un procedimiento para proteger de robo de equipo en la institución?			
13. ¿Existen protocolos establecidos para el cierre y aseguramiento del laboratorio al finalizar las actividades,			
14. ¿Se lleva a cabo regularmente la revisión y mantenimiento de las cámaras de vigilancia para garantizar su funcionamiento óptimo			
15. ¿La institución cuenta con cámaras de videovigilancia?			
16. ¿Hay un registro de acceso al laboratorio donde los usuarios deben firmar al entrar y salir?			
17. La institución cuenta con un cerramiento adecuado para mayor seguridad			
18. ¿Existe un protocolo claro para manejar situaciones de robo?			
19. ¿La zona donde está ubicada la institución tiene alumbrado público?			
20. ¿El aire acondicionado funciona en el laboratorio de computación?			
21. ¿El laboratorio tiene un sistema de inventario detallado?			
22. ¿El inventario se actualiza periódicamente?			
23. ¿El laboratorio cuenta con un seguro contra robos?			
24. ¿Hay procedimientos para reportar el documento a cualquier equipo faltante o sospechoso?			
25. ¿El techo del laboratorio es seguro?			

REALIZADO POR: Zambrano Gina	REVISADO POR:
FECHA:07/05/2024	FECHA:

CONCLUSIONES
OBSERVACIONES

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 3-5

- **Daño de Equipos**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿Los cables y enchufes están organizados y protegidos para evitar tropiezos y daño?			
2. ¿Se lleva registro de los mantenimientos realizados?			
3. ¿Las computadoras tienen software antivirus actualizados para protegerse contra amenazas?			
4. ¿Los computadores están conectados a reguladores de energía?			
5. ¿Se realiza una verificación de los equipos después de cada uso para asegurar que estén en buen estado?			
6. ¿Están los equipos protegidos contra el polvo?			
7. ¿Se dispone de herramientas y materiales adecuados para el mantenimiento y reparación de los equipos?			
8. ¿El laboratorio de computación tiene protocolos para la instalación y actualización de software que aseguren la compatibilidad y el buen funcionamiento de los equipos?			
9. ¿Se prohíbe el consumo de alimentos en el laboratorio?			
10. ¿Están los equipos de computación elevados del suelo para prevenir daños por posibles inundaciones?			
11. ¿Los equipos están asegurados físicamente para evitar caídas o golpes?			
12. ¿El laboratorio está equipado con sistemas de ventilación adecuados para evitar el sobrecaliento de los equipos?			
13. ¿Se han establecido procedimientos claros para la limpieza regular de los equipos para evitar la acumulación de polvo y suciedad?			
14. ¿Se utilizan sistemas de alimentación ininterrumpida (UPS) para proteger los equipos en caso de cortes de energía?			
15. ¿Están los cables de conexión y las interfaces de los equipos en buen estado, sin cortes o desgastes que puedan causar problemas eléctricos y posibles daños?			
16. ¿Existen protocolos para reportar y documentar cualquier daño o problema en los equipos?			
17. ¿Se llevan a cabo inspecciones regulares para detectar daños en el cableado y conexiones de los equipos?			
18. ¿Existe un procedimiento para la actualización regular del software de los equipos para asegurar su óptimo funcionamiento?			
19. ¿Se realizan inspecciones regulares en los equipos?			
20. ¿Los equipos están protegidos contra insectos y roedores?			
21. ¿Los equipos están protegidos contra interferencias electromagnéticas?			
22. ¿Se han implementado sistemas de monitoreo ambiental?			
23. ¿El laboratorio cuenta con un área designada para la reparación y mantenimiento de equipos dañados?			
24. ¿Se han implementado políticas de uso fuera del horario laboral?			
25. ¿Se han establecido procedimientos para la rápida recuperación y restauración de datos en caso de fallo de equipos?			

REALIZADO POR: Zambrano Gina	REVISADO POR:
FECHA:**07/05/2024**	FECHA:
CONCLUSIONES OBSERVACIONES	

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 4-5

- **Malware**

PREGUNTAS	RESPUESTA		OBSERVACIÓN
	SI	NO	
1. ¿Se actualizan regularmente las computadoras de virus en el software antivirus?			
2. ¿Se realizan análisis de vulnerabilidades en los sistemas?			
3. ¿Se recibe formación básica sobre cómo identificar posibles amenazas de malware?			
4. ¿Existen políticas para el uso de dispositivos de almacenamiento externo?			
5. ¿Existe capacitaciones de comunicación efectivo a los estudiantes para reportar incidentes de seguridad?			
6. ¿Se mantiene un registro detallado de eventos y actividades en las computadoras del laboratorio?			
7. ¿Se monitorean los registros en busca de patrones sospechosos de actividad?			
8. ¿Se implementa algún tipo de filtro o bloqueo para correos electrónicos sospechosos?			
9. ¿Se llevan a cabo auditorías periódicas de seguridad para evaluar la eficacia de las medidas implementadas contra el malware?			
10. ¿Se realizan escaneos periódicos de la red en busca de posibles intrusiones?			
11. ¿Se tienen políticas claras sobre el uso de dispositivos USB y otros medios extraíbles en las computadoras del laboratorio?			
12. ¿Los usuarios son instruidos para no abrir archivos adjuntos ni hacer clic en enlaces de correos electrónicos sospechosos?			
13. ¿Se utilizan herramientas para analizar y filtrar posibles amenazas al conectar dispositivos extraíbles?			
14. ¿Se implementan políticas de seguridad para el uso de redes Wi-Fi en el laboratorio?			
15. ¿Se utiliza alguna forma de filtrado web para bloquear sitios maliciosos conocidos?			
16. ¿Los sistemas del laboratorio tienen configuradas políticas de seguridad estrictas para el manejo de correos electrónicos?			
17. ¿Se implementa algún tipo de filtro o bloqueo para correos electrónicos sospechosos?			
18. ¿Se implementan políticas estrictas de uso para reducir el riesgo de infecciones en las computadoras?			
19. ¿El laboratorio tiene un proceso de revisión y autorización para el uso de software en las computadoras?			
20. ¿Hay restricciones para la descarga e instalación de software no autorizado?			
21. ¿Se utiliza software antivirus en todos los dispositivos?			
22. Los estudiantes utilizan los recursos informáticos únicamente con fines educativos y académicos.			
23. Los estudiantes dejan cerrando sesión y desconectando sus cuentas al finalizar cada sesión en las computadoras del laboratorio.			
24. ¿Se han implementado políticas de uso fuera del horario laboral?			
25. ¿Se proporciona a los usuarios formación continua sobre las nuevas amenazas de malware y cómo evitarlas?			

REALIZADO POR: Zambrano Gina	REVISADO POR:
FECHA:07/05/2024	FECHA:

CONCLUSIONES
OBSERVACIONES

CUESTIONARIO PARA ANALIZAR RIESGOS	C1
	Pág. 4-5

• Inundación PREGUNTAS	RESPUESTA SI	 NO	OBSERVACIÓN
1. ¿Los cables y conexiones eléctricas están protegidos y aislados para prevenir daños por contacto con el agua?			
2. Las paredes del laboratorio resumen agua cuando llueve			
3. ¿Los equipos informáticos y sistemas críticos están ubicados a una altura segura para prevenir daños en caso de inundación?			
4. ¿Se han implementado estantes elevados u otras medidas para elevar los equipos del suelo?			
5. ¿Se colabora estrechamente con el personal de mantenimiento para abordar cualquier problema relacionado con la infraestructura y prevenir daños por agua?			
6. ¿Se realizan inspecciones para detectar posibles debilidades en el material del techo?			
7. ¿El material del techo es resistente al agua y ha sido evaluado para garantizar su durabilidad?			
8. ¿Existe un procedimiento para de inmediato cambiar elementos dañados?			
9. ¿Se realizan inspecciones regulares de todas las puertas y ventanas para asegurarse de que estén cerradas herméticamente?			
10. ¿Las ventanas cuentan con sistemas de drenaje efectivos para evacuar el agua de lluvia de manera rápida y eficiente?			
11. ¿Se ha instalado un sistema de alarma para detectar infiltraciones de agua y alertar al personal de inmediato?			
12. ¿El personal y los estudiantes están capacitados y familiarizados con el plan de respuesta a inundaciones del laboratorio de computación?			
13. ¿Los sistemas eléctricos críticos, como los paneles eléctricos, están protegidos contra posibles daños por agua durante inundaciones?			
14. ¿Se han sellado adecuadamente las ventanas y puertas para prevenir filtraciones de agua durante lluvias intensas o inundaciones?			
15. ¿El laboratorio de computación está ubicado en una zona propensa a inundaciones?			
16. ¿Se realizan inspecciones regulares de los techos para identificar y reparar posibles filtraciones de agua?			
17. ¿Los cables y enchufes eléctricos están protegidos contra el contacto con el agua en caso de inundación?			
18. ¿El laboratorio cuenta con sensores de agua o sistemas de detección temprana de inundaciones			
19. ¿Los equipos de computación están elevados del suelo para protegerlos en caso de inundación?			
20. ¿Existen planes de emergencia específicos para la evacuación de equipos en caso de inundación?			
21. ¿Los cables y conexiones eléctricas están protegidos y aislados para prevenir daños por contacto con el agua?			
22. ¿Se han tomado medidas para proteger los sistemas de ventilación y conductos contra la entrada de agua durante una inundación?			
23.			
24. ¿Se implementan prácticas de mantenimiento preventivo para reducir el riesgo de daños a los equipos debido a inundaciones?			
25. ¿El personal está capacitado para desconectar y mover equipos electrónicos rápidamente en caso de una inundación?			

REALIZADO POR: Zambrano Gina FECHA:07/05/2024	REVISADO POR: FECHA:
CONCLUSIONES OBSERVACIONES	

5.7 Ejecución de auditoría

La Auditoria se aplicó mediante entrevista al rector el licenciado Andrés Cagua de la Unidad Educativa Alida Zambrano García los cuales dio información de cómo es el manejo de las instalaciones del laboratorio de computación de las vulnerabilidades que existe

Los cuales los datos fueron recolectados mediante la entrevista para identificar problemas de seguridad de la información en el laboratorio de computación

Fotografía de la entrevista

Ilustración 3: Ilustración entrevista con el Rector

Ilustración 4: Foto del laboratorio de computación y cableado del Rack

Ilustración 5 Ilustración caja de Rack

Ilustración 6: Extinto y aire acondicionado

5.8 Tabulación de datos

Estando en la hoja de Excel en la tabulación que se realizó elaboramos otros la cual es la que se representa con 1,2,0 esta hoja de cálculos nos ayuda para poder identificar de mejor manera los riesgos en el laboratorio de computación donde la respuesta **1= Representa seguridad .2 = No aplica y 0 = Representa riegos**

HOJA DE CODIGOS	
1	Representa seguridad
2	No aplica
0	Representa riesgo

5.8.1 Ilustración Porcentaje de riesgos

Para poder realizar la tabulación se realizó la herramienta de Excel con lo cual nos ayudó con las fórmulas para poder llegar a un resultado optimo en el registro de los formularios en Excel primero procedimos a elaborar la tabla de cálculo con las correspondientes preguntas de una manera clara y ordenada para poder obtener datos favorables y de mejor compilación de los cálculos adecuados una que tenemos la formulación creada procedemos a tabular las respuestas mediante las fórmulas de suma, Promedio, contar, para obtener los con estos pasos obtuvimos la tabulación de manera precisa, eficiente.

	riesgo ROBO	
	PREGUNTA	RESPUESTA
1	Ha sido víctima de un taque Informático?	0
2	¿Se realizan regularmente inspecciones de seguridad en el laboratorio de computación?	0
3	¿Las cámaras de seguridad están funcionando correctamente?	2
4	¿Se lleva registro de los equipos y su mantenimiento regular?	0
5	¿El laboratorio tiene medidas para prevenir el acceso no autorizado?	0
6	¿Las puertas del laboratorio cuentan con cerraduras de alta seguridad?	0
7	¿El laboratorio cuenta con tarjetas de acceso?	0
8	¿La institución cuenta con cerramiento?	1
9	¿La institución cuenta con un laboratorista?	0
10	¿La institución ha sufrido de robo en el laboratorio?	1
11	¿La infraestructura del laboratorio de computación es adecuada para los estudiantes y es segura	1
12	¿Se cuenta con un procedimiento para proteger de robo de equipo en la institución?	0
13	¿Existen protocolos establecidos para el cierre y aseguramiento del laboratorio al finalizar las actividades,	0
14	¿Se lleva a cabo regularmente la revisión y mantenimiento de las cámaras de vigilancia para garantizar su funciona	0
15	¿La institución cuenta con cámaras de videovigilancia?	1
16	¿Hay un registro de acceso al laboratorio donde los usuarios deben firmar al entrar y salir?	0
17	La institución cuenta con un cerramiento adecuado para mayor seguridad	2
18	¿Existe un protocolo claro para manejar situaciones de robo?	0
19	¿La zona donde está ubicada la institución tiene alumbrado público?	1
20	¿El aire acondicionado funciona en el laboratorio de computación ?	0
21	¿El laboratorio tiene un sistema de inventario detallado?	0
22	¿El inventario se actualiza periódicamente?	0
23	¿El laboratorio cuenta con un seguro contra robos?	0
24	¿Hay procedimientos para reportar el documento a cualquier equipo faltante o sospechoso?	0
25	¿El techo del laboratorio es seguro?	1
	TOTAL CONTROLES NO APLICADOS:	2
	TOTAL DE CONTROLES EVALUADOS	23
	TOTAL CONTROLES SEGURIDAD:	6
	TOTAL CONTROLES RIESGO:	17
	PORCENTAJE SEGURIDAD	26%
	PORCENTAJE RIESGO	74%
		100%

5.8.2 Análisis de riesgos

En el análisis de riesgos, en el laboratorio de computación, el nivel robo se identifica como el riesgo más crítico debido a su potencial impacto en la confidencialidad y la integridad de los datos críticos utilizados para fines educativos e investigativos. Para mitigar este riesgo, es esencial implementar controles estrictos de acceso físico y lógico, cifrar datos sensibles,

promover la concienciación en seguridad entre el personal y los estudiantes, realizar auditorías periódicas y mantener actualizados los sistemas y software. Estas medidas son fundamentales para proteger los activos digitales y minimizar la exposición a amenazas en el laboratorio.

5.8.3 Tabla de escala nivel de aparición probabilidad

Es la tabla de escala de valor de los resultados nos ayude y fue de guía para poder calificar los el nivel de aparición de las probabilidades de riesgos los cuales obtuvimos de la tabulación de las preguntas

ESCALA PARA ASIGNAR VALOR DE APARICIÓN		
NIVEL DE APARICIÓN (PROBABILIDAD)		
1	MAS BAJO	1%-10%
2	BAJO	10%-30%
3	MEDIO	30%-50%
4	ALTO	50%-75%
5	MÁS ALTO	75%-100%

5.8.3.1 Ilustración 6Escala de valor de aparición

La tabla de leyenda es muy fundamenta para los resultados que ya hemos venido observando en las diferentes tablas de riesgo, pero en esta tabla tenemos la guía de colores de impacto de riesgo de los cuales son MUY ALTO, ALTO, MEDIO, BAJO, Y MUY BAJO con esta tabla pedimos obtener resultados y cálculos de veracidad

LEYENDA							
			GRAVEDAD (IMPACTO)				
			MUY BAJO	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

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

5.9 Matriz de riesgo

GRAVEDAD (IMPACTO)		CONSIDERACIONES
1	MAS BAJO	Las instalaciones quedan temporalmente cerrada o no puede operar, pero puede continuar su
2	BAJO	La difusión de la información no autorizada tiene un impacto bajo los equipos informáticos
3	MEDIO	La falta del activo de información tiene un impacto de riesgo considerable para los equipos informáticos.
4	ALTO	Equipos informáticos la pérdida o modificación de la información tiene un impacto alto en los equipos informático de riesgo
5	MÁS ALTO	Daños irreparables en instalaciones / afectada más allá del uso habitable. La mayoría de los

La tabla de cálculo de impacto es donde podemos calcular de manera óptima la confidencialidad, sobre las vulnerabilidades que existe en el laboratorio de computación y la también la disponibilidad de los equipos y computo, así como la integridad sobre los datos o información

	CONFIDENCIALIDAD	DISPONIBILDAD	INTEGRIDAD	PROMEDIO
INCENDIO	2	5	3	4
DAÑO DE EQUIPOS	3	5	3	4
INUNDACIÓN	2	5	3	3
MALWARE	4	3	4	4
ROBO	5	5	5	5

Ilustración 8tabla de cálculo de impacto

En la imagen se muestra un resultado del 60% de riesgo esta calificación es la más alta que obtuvimos sobre el nivel de impacto de riesgo y amenazas sobre el los malware

	RIESGO MALWARE	
	PREGUNTA	RESPUEST.
1	¿Se actualizan regularmente las computadoras de virus en el software antivirus?	1
2	¿Se realizan análisis de vulnerabilidades en los sistemas?	0
3	¿Se recibe formación básica sobre cómo identificar posibles amenazas de malware?	0
4	¿Existen políticas para el uso de dispositivos de almacenamiento externo?	1
5	¿Existe capacitaciones de comunicación efectivo a los estudiantes para reportar incidentes de seguridad?	0
6	¿Se mantiene un registro detallado de eventos y actividades en las computadoras del laboratorio?	0
7	¿Se monitorean los registros en busca de patrones sospechosos de actividad?	0
8	¿Se implementa algún tipo de filtro o bloqueo para correos electrónicos sospechosos?	0
9	¿Se llevan a cabo auditorías periódicas de seguridad para evaluar la eficacia de las medidas implementadas contra el malware	0
10	¿Se realizan escaneos periódicos de la red en busca de posibles intrusiones?	0
11	¿Se tienen políticas claras sobre el uso de dispositivos USB y otros medios extraíbles en las computadoras del laboratorio?	0
12	12. ¿Los usuarios son instruidos para no abrir archivos adjuntos ni hacer clic en enlaces de correos electrónicos sospechosos?	0
13	13. ¿Se utilizan herramientas para analizar y filtrar posibles amenazas al conectar dispositivos extraíbles?	0
14	14. ¿Se implementan políticas de seguridad para el uso de redes Wi-Fi en el laboratorio?	1
15	15. ¿Se utiliza alguna forma de filtrado web para bloquear sitios maliciosos conocidos?	1
16	16. ¿Los sistemas del laboratorio tienen configuradas políticas de seguridad estrictas para el manejo de correos electrónicos?	0
17	17. ¿Se implementa algún tipo de filtro o bloqueo para correos electrónicos sospechosos?	0
18	18. ¿Se implementan políticas estrictas de uso para reducir el riesgo de infecciones en las computadoras?	0
19	19. ¿El laboratorio tiene un proceso de revisión y autorización para el uso de software en las computadoras?	0
20	20. ¿Hay restricciones para la descarga e instalación de software no autorizado?	1
21	21. ¿Se utiliza software antivirus en todos los dispositivos?	1
22	22. Los estudiantes utilizan los recursos informáticos únicamente con fines educativos y académicos.	0
23	23. Los estudiantes dejan cerrando sesión y desconectando sus cuentas al finalizar cada sesión en las computadoras del labo	1
24	24. ¿Se han implementado políticas de uso fuera del horario laboral?	0
25	25. ¿Se proporciona a los usuarios formación continua sobre las nuevas amenazas de malware y cómo evitarlas?	1
	TOTAL CONTROLES NO APLICADOS:	0
	TOTAL DE CONTROLES EVALUADOS	25
	TOTAL CONTROLES SEGURIDAD:	8
	TOTAL CONTROLES RIESGO:	17
	PORCENTAJE SEGURIDAD	32%
	PORCENTAJE RIESGO	68%

Ilustración 9tabla de malware resultado

5.10 Matriz de riesgos

La matriz de riesgo es el resultado de toda la valoración de riesgo que está enfrentado el laboratorio de computación esta matriz muestra detalladamente el nivel de riesgo y gravedad

MATRIZ DE RIESGOS				
RIESGO	Aparición	Gravedad	Valor del	Nivel de Riesgo
ROBO	4	4	16	Muy grave
INCENDIO	4	3	12	Importante
DAÑO DE EQUIPOS	3	4	12	Muy grave
INUNDACION	4	4	16	Muy grave
MALWARE	4	3	12	Importante

Ilustración Matriz de riesgos

CAPÍTULO V

6 EVALUACIÓN DE RESULTADOS

Informe de Auditoría

Él informa que se presenta a continuación detalla cada una de los hallazgos exhaustivos y conclusiones obtenidas durante la Auditoria informática los cuales fue tonta física como lógica que se llevó a cabo en la Unidad Educativa Alida Zambrano García la cual fue realizada minuciosamente a lo largo del periodo 2023-2024 el objetivo principal de esta auditoria fue evaluar y asegurar la integridad ,seguridad y la eficiencia de los sistema informático utilizados en la institución abarcando desde los procedimientos operativos como también el hardware ,y software estos procedimientos operativo se identificó las vulnerabilidades y funcionamiento de seguridad dentro del laboratorio de computación como también la infraestructura los cuales se procedió a realizar recomendaciones para la mejora optima de funcionamiento de la infraestructura tecnológica de la institución garantizando un entorno seguro y eficiente para todos los usuarios ,estudiantes docentes de esta auditoria son esenciales para la planificación futura y la toma de decisiones estratico en el ámbito educativo y tecnológico de la institución.

4.4.8 Planificación de la evaluación

DIRIGIDO A:

Al Rector de la Unidad Educativa Alida Zambrano García al Licenciado Andrés Cagua

MOTIVO

Cumplir con los requerimientos académicos de la aplicando conocimientos avanzados en la auditoria informática y fortaleciendo de seguridad y gestión teológica a la institución con el objetivo de mitigar vulnerabilidades en los sistemas tecnológicos

OBJETIVO

Identificar los riesgos de seguridad física en el laboratorio de computación de la Unidad Educativa "Alida Zambrano García".

Evaluar nivel de seguridad informática del laboratorio de computación Unidad Educativa Alida Zambrano García

ALCANCE

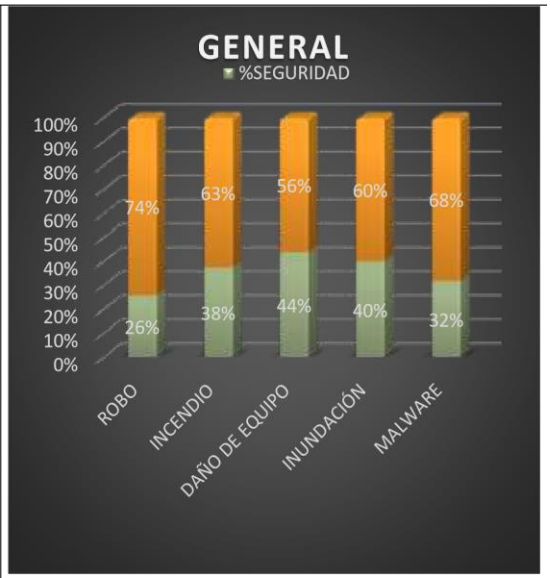
- Revisar metodología MAGERIT
- Identificación y valoración de Activos
- Identificación y valoración de amenazas
- Diseño de instrumentos
- Evaluación de Riesgos
- Analizar riesgos y calcular impactos
- Selección de Medidas de Seguridad:
- Documentación de Políticas de Seguridad
- Elaborar informe de auditoria

Elaboración de políticas PERSONAL RELACIONADO

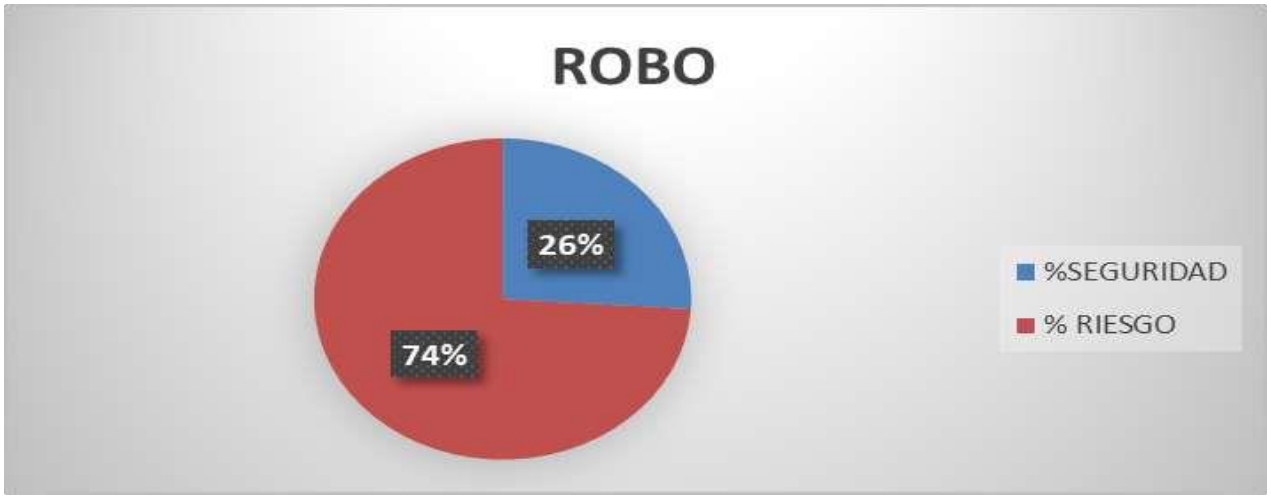
En esta auditoría de seguridad informática están involucrados el rector, vicerrector y personal administrativo de la Unidad Educativa Alida Zambrano García en el que me brindaron información oportuna y necesario para poder realizar y recolectar datos suficientes con veracidad de importancia es la auditoría realizada.

4.4.9 HALLAZGOS

NIVEL DE SEGURIDAD GENERAL



INTERPRETACIÓN: En la primer grafica se muestra los dos niveles de seguridad es del 38% y riesgo 62%que representa un tipo muy alto se pudo identificar que hay mayor vulnerabilidad de riesgo en el robo de los equipos y en otro muestra que hay menor vulnerabilidad en el riesgo de los equipos de computación



INTERPRETACIÓN:

Al analizar los resultados del nivel de riesgo de robo en la cual podemos observar que tiene un nivel de riesgo alto en el promedio de la seguridad que representa un tipo muy grave

CAUSAS

Las cámaras que se encuentran en el laboratorio de computación de están desconectadas y no cuentan con una memoria lo cual pueda guardar la grabación

No lleva un registro de ingreso y salida del laboratorio de computación cuando hacen unos de las maquinas

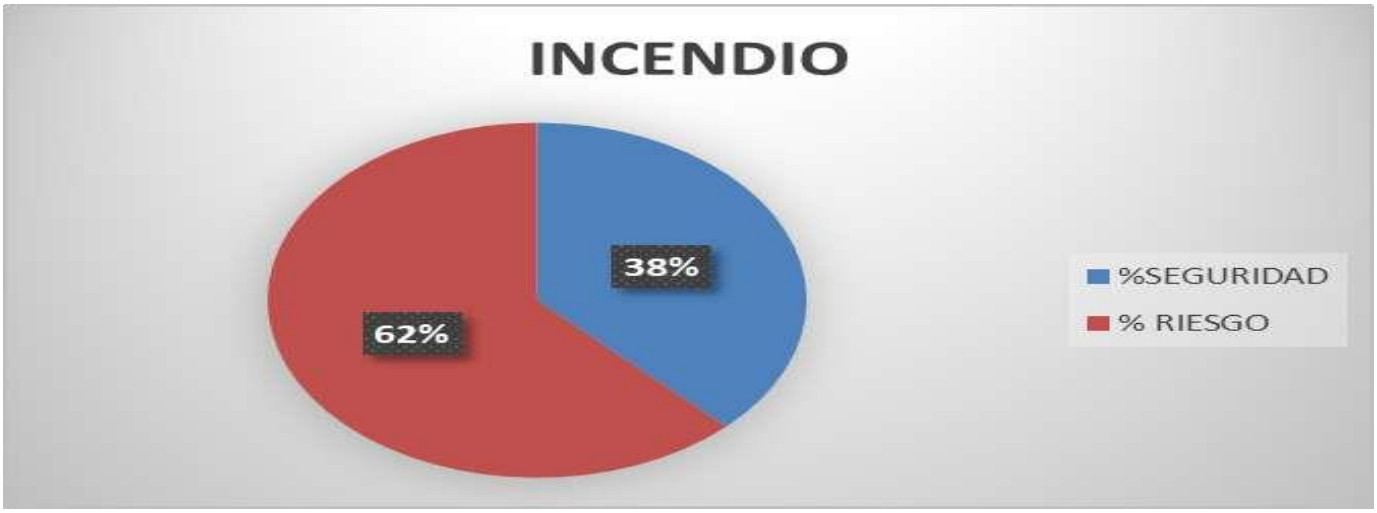
No cuenta con un procedimiento de revisión y mantenimientos en las cámaras de vigilancia para garantizar su funcionamiento optimo

No se lleva un registro de los equipos y mantenimiento regular

No cuenta con laboratorista

No tiene un sistema de inventario detallado

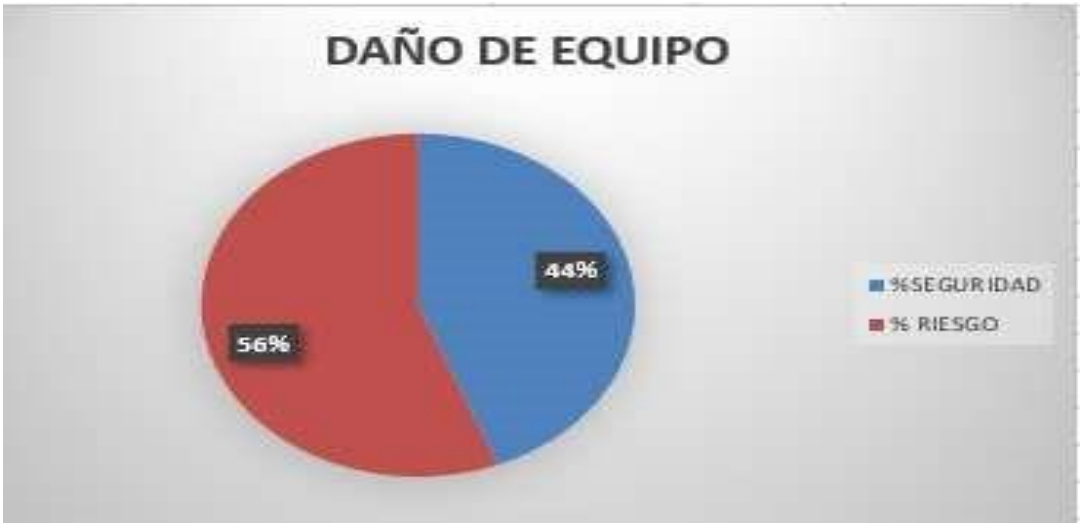
El aire acondicionado de funciona con normalidad y no tiene un óptimo mantenimiento



INTERPRETACIÓN: Al analizar el resultado obtenido del nivel de riesgo de incendio es de 62%se determinó que es un con el tipo importante

CAUSAS

- No cuenta con una inspección regular de los extintores del laboratorio
- no se lleva a cabo mantenimiento regulare en los equipos
- no existe un procedimiento previo para desconectar rápidamente los equipos en caso de emergencia
- no cuenta con detectores de humo
- no se realiza capacitaciones al personal
- no se realizan pruebas de seguridad en el cableado de los equipos
- No cuenta con alarmas de incendio
- El personal no está entrenado para utilizar el extenderos en caso de emergencia



INTERPRETACIÓN: El nivel de riesgo de daño de equipo es de 56% dando un tipo muy grave

CAUSAS

Falta de mantenimiento en los equipos de computo

Falta de capacitación al personal para el uso de los equipos informáticos

No cuenta con políticas de seguridad

Falta de procedimientos para la rápida recuperación uy restauración de datos en caso de fallas en los equipos

No cuenta con un sistema de monitoreo ambiental

No existen protocolos para reportar o documentar cualquier daño de o problema de los equipos de cómputo

INTERPRETACIÓN: En el análisis nivel riesgo es alto de 60% de vulnerabilidad se muestra un tipo de muy grave

En las paredes resume del laboratorio de computación resume agua cuando llueve

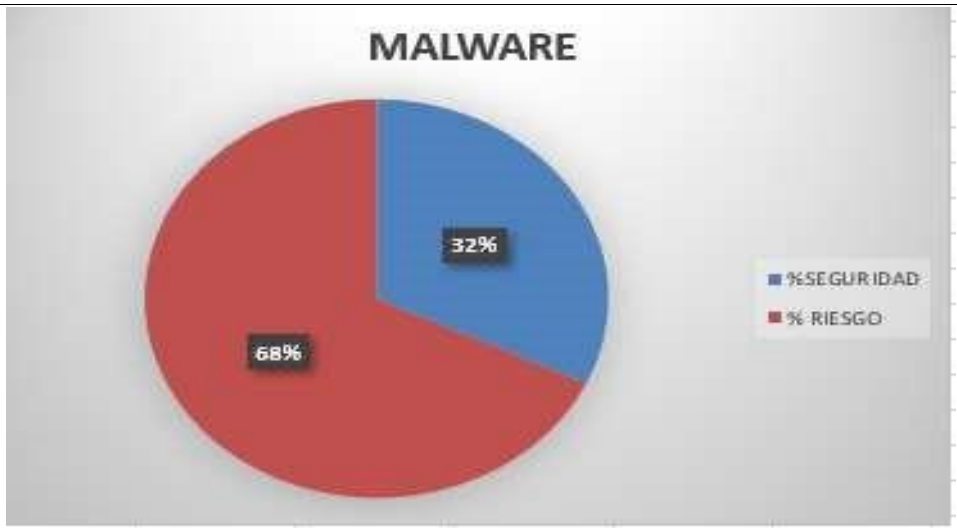
No se realizan inspecciones regulares en las instalaciones

No existe un plan de emergencia para la evacuación de los equipos informáticos en caso de inundación

No están equipos con un sistema de monitoreo de humedad para prevenir daños en los equipos del laboratorio

Falta de prevención y gestión adecuado en la infraestructura

La ausencia de seguros financieros los cuales respalden en caso de una inundación



INTERPRETACIÓN: El análisis revelo el alto riesgo de malware en los equipos de computación con un nivel de 68% de vulnerabilidad, con un valor importante

Falta de control de propagación de virus

Uso inadecuado de la navegación web

Falta de análisis de vulnerabilidades en los sistemas operativos

Falta de capacitación a los estudiantes para que tengan conocimiento de los distintos incidentes de seguridad

Falta de monitoreo de en la búsqueda y patrones sospechosos de las actividades

No se realiza escaneo de periódicos de la red en la búsqueda de posibles intrusos

No existe políticas de seguridad para el uso de redes Wi Fi en el laboratorio

6.1 OPINIÓN

Los riesgos identificados de la gestión de seguridad de la información en el laboratorio de computación de la Unidad Educativa Alida Zambrano García son significativos y requieren de una atención inmediata y detallas en el cual el robo , el daño de equipos , la inundación son calificados como muy grave a lo que se refiera a la vulnerabilidad que podría resultas en perdida de activos , por otro lado el malware considerado como riesgo importante sugiere que se debe fortalecer en la seguridad digital.

ROBO	MUY ALTO
INCENDIO	IMPORTANTE
DAÑO DE EQUIPOS	MUY ALTO
INUNDACION	MUY ALTO
MALWARE	IMPORTANTE

La evaluación del nivel de seguridad del laboratorio de computación es de 38% porcentaje que muestra este resultado indica que en el laboratorio presenta vulnerabilidades significativas en sus controles de seguridad tanto físicos como digitales

CONCLUSIONES

Para asegurar un entorno de enseñanza e investigación seguro y eficiente en el laboratorio de computación de la Unidad Educativa Alida Zambrano García, es esencial implementar una combinación integral de prácticas de seguridad físicas, lógicas y de datos. Para así controlar el acceso, y mantener el hardware y software actualizados, y también educar al personal y estudiantes sobre la seguridad son pilares fundamentales. Adicionalmente, un plan de respuesta a incidentes bien definido y el cumplimiento de normativas garantizarán la protección de los recursos y la información, creando un ambiente confiable y resiliente frente a posibles amenazas.

Se identificaron los riesgos de robo lo cual se registró como muy grave la probabilidad de un incidente a los equipos de computación que indica la necesidad de implementar medidas de seguridad adicionales como las cámaras de violación y las alarmas y reforzar la cerraduras de la institución ,también considerando un riesgo de incendio lo cual es importante y esencial contar con directores de humo y plan de evacuación ,en los daños de equipos de computación considerando lo evaluado como muy grave lo cual establecer políticas de seguridad estrictas para el manejos de las maquinas seria esencial para implementar mantenimiento.

RECOMENDACIONES

Recomiendo adaptar medidas de seguridad correctivas y establecer un sistema de control de acceso robusto, complementado con cámaras de vigilancia y alarmas, para garantizar que solo el personal autorizado pueda ingresar al laboratorio de computación para proteger tanto los equipos como también la información , es crucial realizar actualizaciones regulares de software y hardware, estos riesgos que se presentan considero que tienen que implantar capacitaciones periódicas sobre seguridad para todo el personal y estudiantes, asegurando así la protección de los recursos y la información del laboratorio y que se construya un entorno seguro y confiable.

CAPÍTULO VI

7 CONCLUSIONES Y RECOMENDACIONES

7.1 Conclusiones

- La identificación de los problemas de seguridad de la información en las unidades educativa Alida Zambra García ha revelado que existe vulnerabilidades críticas tanto en los controles físicos como digital del laboratorio de computación esta fase d estudio determino una comprensión detallada de las deficiencias que existen y proporcionando bases solidad para el desarrollo de estrategias de mitigación y mejoras de la seguridad
- La investigación en las diferentes fuentes bibliográficas sobre gestión de seguridad y de computación permitió consolidar un marco teórico robusto, esta revisión de literatura no solo contextualizo la auditoría dentro de los estándares y mejores prácticas proporciono metodologías y herramientas adecuadas para la evaluación de gestión de seguridad de la información en el entorno educativo
- La aplicación de métodos y técnicas de investigación en las cuales fueron las encuestas y entrevistas justifico la existencia de problemas de seguridad y permitió el diagnóstico de las vulnerabilidades especificas los cuales los datos recolectados dieron evidencia de las debilidades en los controles de seguridad y se intervino estratégicamente con la realidad de las condiciones del laboratorio
- La elaboración del informe de auditoría detalló exhaustivamente los riesgos y vulnerabilidades que presenta el laboratorio de computación en la actualidad por lo tanto este documento proporciona un análisis completo de todos los hallazgos y ofrece recomendaciones prácticas y específicas de los riesgos para que sirva de guía fundamental con medidas correctivas y preventivas para el mejoramiento de la seguridad del laboratorio de computación.

7.2 Recomendaciones

- El director debe promover un programa de capacitación regular en seguridad informática dirigido a los docentes y al personal del colegio. Es fundamental que el director colabore con especialistas en seguridad para organizar talleres que aborden la protección de datos, el uso seguro de la tecnología y la prevención de amenazas digitales. Esto garantizará que el personal esté bien informado y preparado para manejar los sistemas del laboratorio de computación de manera segura.

- El responsable de Mantenimiento debe establecer un plan de mantenimiento preventivo de los equipos del laboratorio de computación y asegurar que dicho plan sea seguido de manera estricta. Este mantenimiento debe ser comunicado a los docentes y al personal para que se programen adecuadamente las actividades dentro del laboratorio y se eviten interrupciones por fallos técnicos.

- El responsable del laboratorio debe crear e implementar un sistema de monitoreo y respuesta ante posibles amenazas digitales en el laboratorio de computación. Aunque no se han registrado incidentes graves, es crucial que los docentes y estudiantes reciban orientación sobre cómo identificar y reportar problemas de seguridad. Esto asegurará la protección de la información y la infraestructura tecnológica de la institución.

BIBLIOGRAFÍA

Aroca, E. (2022). *Análisis dinámico de Malware.* Obtenido de https://biblus.us.es/bibing/proyectos/abreproy/94086/fichero/TFG-4086+Aroca+P%C3%A1ez.pdf

Avenía, C. (2017). *Fundamentos de seguridad informática.* Areandino. doi:978-958-5459-618

Barceló, J. (2022). *Redes de computadoras.* Obtenido de https://libros.metabiblioteca.org/server/api/core/bitstreams/2deaa017-ef04-4f73-866c9a81f23ad1c0/content

Briano, C. (2023). *Compilación de apuntes sobre conceptos fundamentales de la Ingeniería de Software* (2 ed.). Obtenido de http://bibliotecadigital.econ.uba.ar/download/libros/Briano_compilacion_apuntes.pdf

Campos, V. (2011). *Ingeniería de Software.* doi:978-607-32-0603-7

Domínguez, J. (2021). *Fundamentos de Auditoría Informática.* Venezuela: IEASS.

Dueñas, M. (2019). *Metodología de la investigación Cuantitativa - Cualitativa y Redacción de la Tesis.* Obtenido de http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf

Facchini, H. (2022). *ARQUITECTURA DE COMPUTADORAS.* 10. doi:978-950-42-0158-8

Farfán , J. (2023). *LABORATORIO DE INFORMÁTICA NORMAS Y PROCEDIMIENTOS.* Universidad Piloto de Colombia. Obtenido de https://www.unipiloto.edu.co/descargas/Normas-y-Procedimientos-Laboratorioinformatica.pdf

Gargallo, E. (2023). *Software Malicioso.* Obtenido de https://openaccess.uoc.edu/bitstream/10609/145186/2/La%20seguridad%20TIC%20en%20la%20infancia_Modulo2_Software%20malicioso.pdf

Goñas, R. (2022). *Memorias Ram.* Obtenido de https://es.scribd.com/document/610405318/1Memorias-ram-2022-20

Guerrero, A. (2022). *sistema de gestión de la seguridad de la información (SGSI) basado en la metodología Magerit V3 y la norma ISO 27001.* Obtenido de https://www.researchgate.net/publication/370819083_Desarrollo_e_implantacion_de_un_sistema_de_gestion_de_la_seguridad_de_la_informacion_SGSI_basado_en_la_metodologia_Magerit_V3_y_la_norma_ISO_270012017_exploiting_y_escalada_de_privilegios_en_GNULinux_

Imbaquingo, D., Pusdá, M., y Jácome, J. (2018). *Fundamentos de Auditoría Informática Basada en Riesgos.* Ibarra: Imprenta Untver3ilaria. Obtenido de https://bibliotecadigital.utn.edu.ec/download/files/original/a00ac87d50e32e2e962e9a3a8cbf90483bbfe5b9.pdf

López, M. (2019). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid. Obtenido de https://www.pilar-tools.com/doc/magerit/v2/methes-v11.pdf

Manrique, J. (2019). *Introducción a la auditoría.* Casco: Ediciones Carolina. doi:978-6124308-14-7

Moreno, M. (2022). *Gestión de incidentes de ciberseguridad.* Bogotá: Ra-ma. doi:978-958792-444-2

Ortiz, F. (2010). *Fundamentos de computación.* Obtenido de https://gc.scalahed.com/recursos/files/r161r/w23942w/unidad_1/Evolucion_de_las_computadoras.pdf

Patil. (2023). *Seguridad de Las Redes.* (1st, Ed.) Nuestro Conocimiento. Obtenido de https://www.perlego.com/es/book/4056135/seguridad-de-las-redes-descubrimientode-la-ruta-ptima-y-segura-mediante-el-anlisis-de-vulnerabilidades-en-redes-dinmicasa-travs-de-grficos-de-ataques-pdf

Pazmiño, I. (2023). *MANUAL PARA EL USO DE LABORATORIOS.* Obtenido de https://web.instipp.edu.ec/Libreria/libro/Manual%20de%20uso%20de%20los%20laboratorios%20de%20computaci%C3%B3n.pdf

Pérez, B. (2020). *Importancia de un SGSI para empresas de tecnología.* Colombia. Obtenido de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6841/Articulo.pdf

Samaniego, E. (2018). *Libro de Fundamentos de REDES.* Universidad Técnica Estatal de Quevedo, Quevedo. doi:978-9942-33-092-5

Sandoval, C. (2020). *Investigacióncualitativa.* Bogotá. Obtenido de https://panel.inkuba.com/sites/2/archivos/manual%20colombia%20cualitativo.pdf

Silva, F., Segadas , L., y Kowask, E. (2023). *Gestión de la seguridad de la información.* Ecuador.

Tipton. (2018). *Information Security Management Handbook.* CRC Press. Obtenido de https://engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf

Vargas, O. (2021). *PLAN DE MANTENIMIENTO PREVENTIVO A LOS EQUIPOS DE CÓMPUTO.* Bogotá. Obtenido de https://comunicarte.idartes.gov.co/sites/default/files/Doc_SIG/PLAN%20DE%20MANTENIMIENTO%20EQUIPOS%20DE%20COMPUTO%202022%20V3.pdf

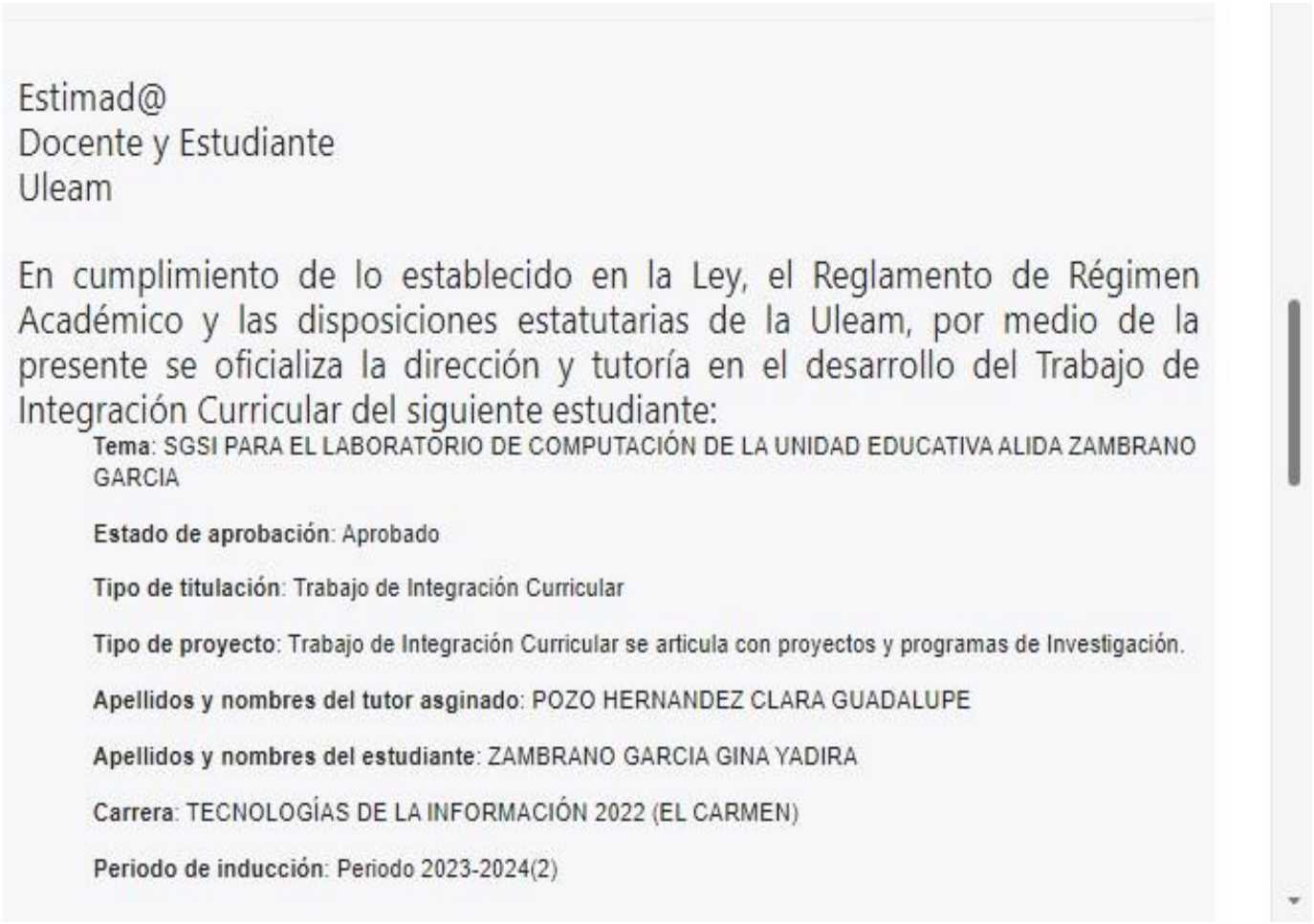
Vasquez, W. (2023). *PLAN DE SEGURIDAD INFORMÁTICA.* Colombia. Obtenido de https://www.corpocesar.gov.co/files/Plan-de-Seguridad-Informatica-2021-2023.pdf

Villacrés, L. (2023). *Análisis de vulnerabilidad en la infraestructura tecnológica de la organización Uniscan en el área funcional de frontera de la empresa.* Universidad Politécnica Salesiana, Cuenca. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/25255/1/UPS-CT010629.pdf

Whitman, M., y Mattord, H. (2019). *Principles of Information Security.* Review.

8 ANEXOS

Anexo A: Asignación de tutor



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: SGSI PARA EL LABORATORIO DE COMPUTACIÓN DE LA UNIDAD EDUCATIVA ALIDA ZAMBRANO GARCIA

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: POZO HERNANDEZ CLARA GUADALUPE

Apellidos y nombres del estudiante: ZAMBRANO GARCIA GINA YADIRA

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2023-2024(2)

Anexo B: Certificado de la empresa

Ministerio de Educación

UNIDAD EDUCATIVA
"ALIDA ZAMBRANO GARCÍA"
Código AMIE: 13H01454
Fundada el 5 de mayo de 1981.
El Carmen – Manabí – Ecuador.

El Carmen, 13 de agosto del 2024

Certificación N° 002-2024-R-UE. D05-C03

CERTIFICACIÓN

Quien suscribe **Lic. Andrés Cagua Ostaiza** con cédula de ciudadanía **092498111-1** Rector de la Unidad Educativa Alida Zambrano García, con sostenimiento fiscal, tengo a bien Certificar:

Que: **ZAMBRANO GARCÍA GINA YADIRA** con cédula de ciudadanía número **2350055089**, ha realizado con éxito el manual de políticas de seguridad para el laboratorio de computación de esta institución Educativa.

Este manual ha sido desarrollado y entregado a la institución educativa bajo la supervisión del rector y cumple con los lineamientos académicos establecidos por la Unidad Educativa "Alida Zambrano García".

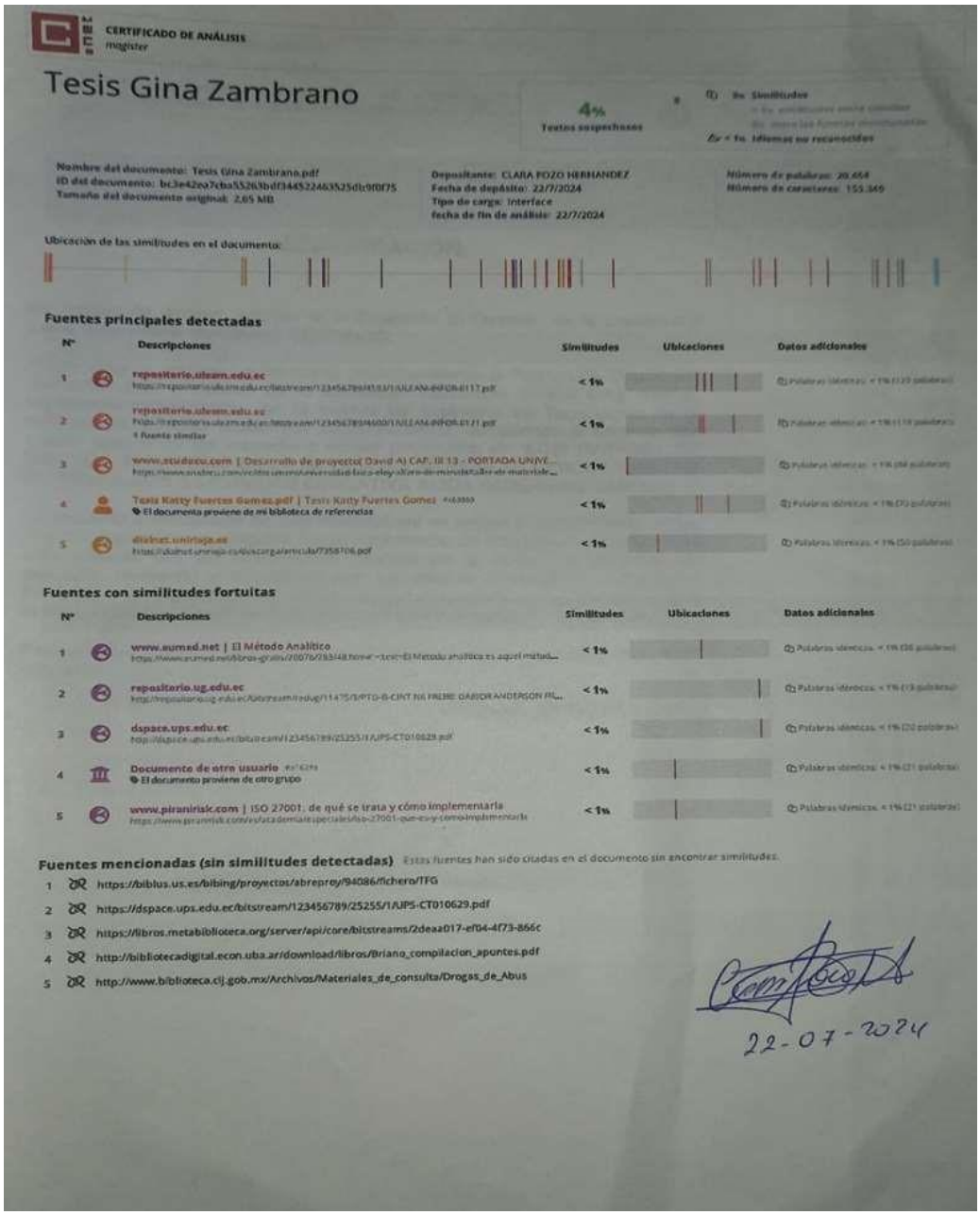
Es todo cuanto certificar en honor a la verdad para que el interesado hago uso de la misma

Atentamente

Lic. Andrés Cagua Ostaiza
RECTOR E.
C.I. 092498111-1
E-mail: andres.cagua@educacion.gob.ec

Barrio Nuevo Naranjales – Vía a Venado - Calle H.
E-mail: d13h01454azg@gmail.com
Telf. 052662001 N°. Celular: 0959930173

Anexo C: Reporte del sistema antiplagio



CERTIFICADO DE ANÁLISIS
magister

Tesis Gina Zambrano

4%
Textos sospechosos

0% Similitudes

< 1% Idiomas no reconocidos

Nombre del documento: Tesis Gina Zambrano.pdf
ID del documento: bc3e42ea7cba5526bbdf3445224635f25db90df75
Tamaño del documento original: 2,65 MB

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 22/7/2024
Tipo de carga: interface
fecha de fin de análisis: 22/7/2024

Número de palabras: 20.464
Número de caracteres: 155.349

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uleam.edu.ec	< 1%		
2	repositorio.uleam.edu.ec 1 fuente similar	< 1%		
3	www.studocu.com | Desarrollo de proyectos(David A) CAP. III 13 - PORTADA UNIVE...	< 1%		
4	Tesis Katty Fuentes Gomez.pdf | Tesis Katty Fuentes Gomez El documento proviene de mi biblioteca de referencias	< 1%		
5	distnet.uniriojа.es	< 1%		

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.eumed.net | El Método Analítico	< 1%		
2	repositorio.ug.edu.ec	< 1%		
3	dspace.ups.edu.ec	< 1%		
4	Documento de otro usuario El documento proviene de otro grupo	< 1%		
5	www.piranirisk.com | ISO 27001, de qué se trata y cómo implementarla	< 1%		

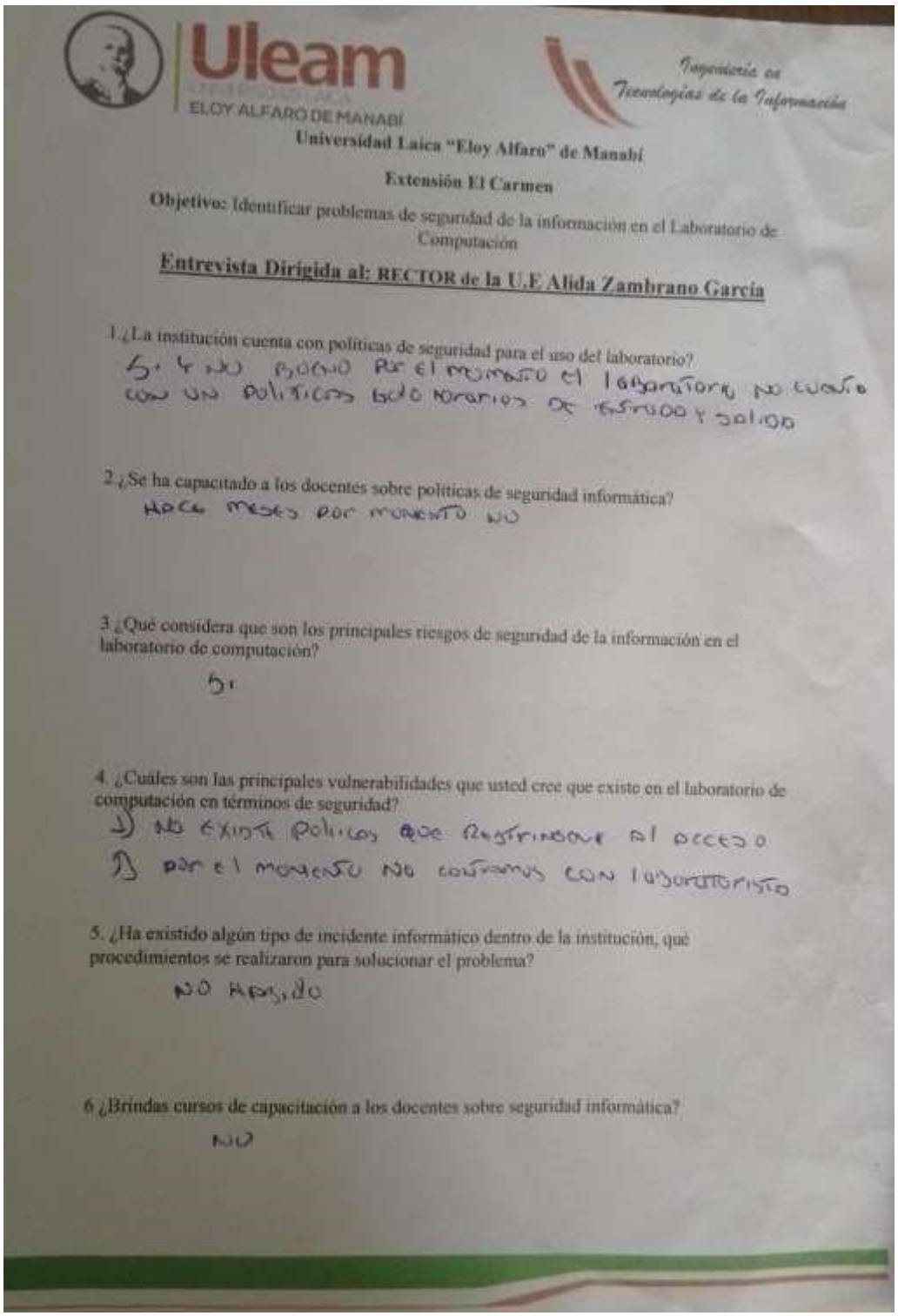
Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://biblus.us.es/bibing/proyectos/abreproy/94086/fichero/TFG
2 https://dspace.ups.edu.ec/bitstream/123456789/25255/1/UPS-CT010629.pdf
3 https://libros.metabiblioteca.org/server/api/core/bitstreams/2deaa017-ef04-4f73-866c
4 http://bibliotecadigital.econ.uba.ar/download/libros/Briano_compilacion_apuntes.pdf
5 http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abus

22-07-2024

Anexo D: Fotografías

Anexo E: Evidencia de aplicación de encuestas y entrevistas



Uleam
ELOY ALFARO DE MANABÍ

Ingeniería en Tecnologías de la Información

Universidad Laica "Eloy Alfaro" de Manabí

Extensión El Carmen

Objetivo: Identificar problemas de seguridad de la información en el Laboratorio de Computación

Entrevista Dirigida al: RECTOR de la U.E Alida Zambrano García

1.¿La institución cuenta con políticas de seguridad para el uso del laboratorio?

5. Y no BUENO Por el momento el laboratorio no cuenta con Políticas solo horarios de estudio y salida

2.¿Se ha capacitado a los docentes sobre políticas de seguridad informática?

Hace meses por momento no

3.¿Qué considera que son los principales riesgos de seguridad de la información en el laboratorio de computación?

5.

4. ¿Cuáles son las principales vulnerabilidades que usted cree que existe en el laboratorio de computación en términos de seguridad?

1) No existe Políticas que Restrinjan al acceso

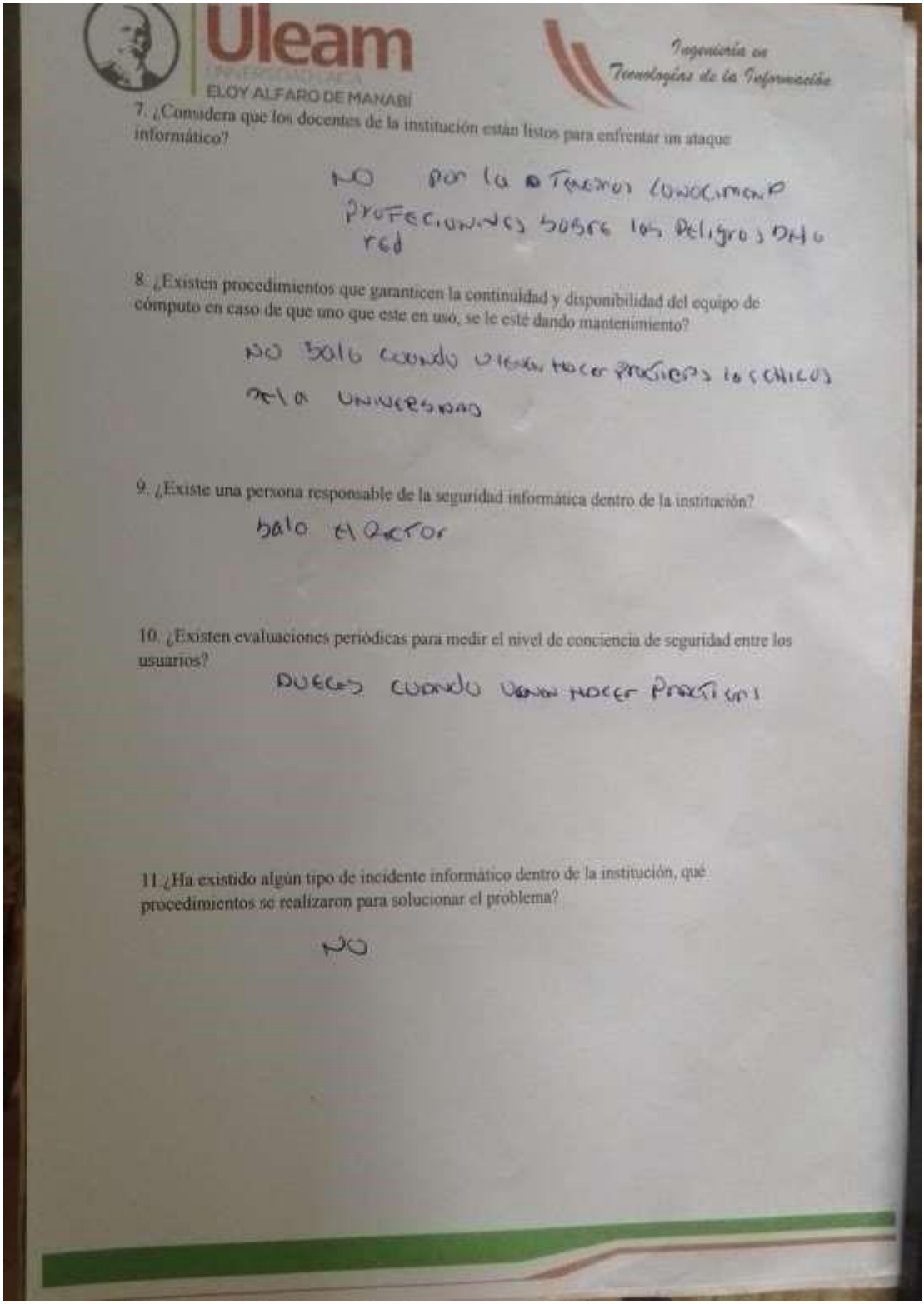
2) por el momento no contamos con laboratorista

5. ¿Ha existido algún tipo de incidente informático dentro de la institución, qué procedimientos se realizaron para solucionar el problema?

No Hay, do

6 ¿Brindas cursos de capacitación a los docentes sobre seguridad informática?

No



Uleam
ELOY ALFARO DE MANABÍ
Ingeniería en Tecnologías de la Información

7. ¿Considera que los docentes de la institución están listos para enfrentar un ataque informático?

NO POR LA MAYORIA DESCONOCEN PROFECIONALES SOBRE LOS PELIGROS DE LA RED

8. ¿Existen procedimientos que garanticen la continuidad y disponibilidad del equipo de cómputo en caso de que uno que este en uso, se le esté dando mantenimiento?

NO SOLO CUANDO VIENEN HACER PRACTICAS LOS CHICOS DE LA UNIVERSIDAD

9. ¿Existe una persona responsable de la seguridad informática dentro de la institución?

SOLO EL DOCTOR

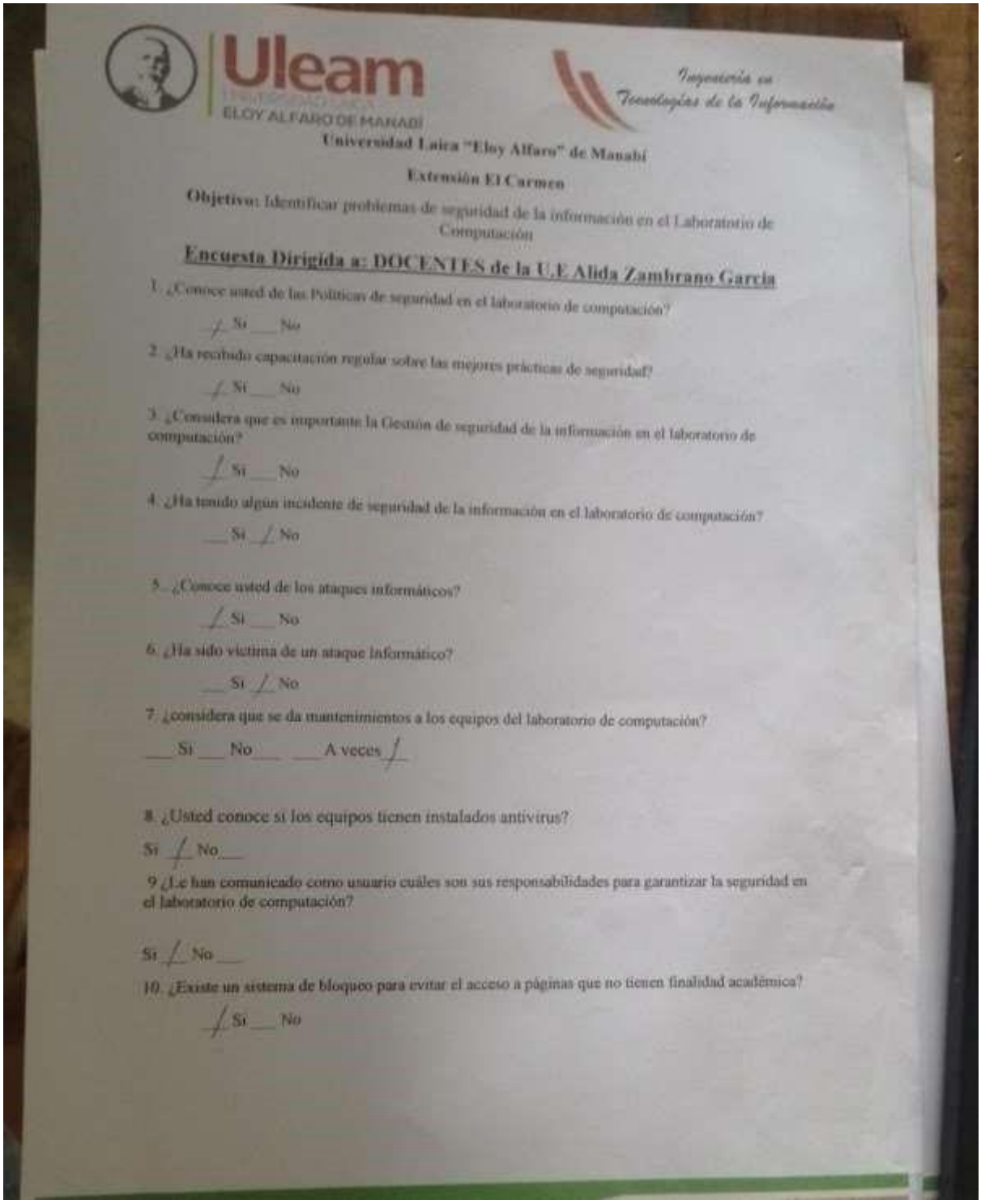
10. ¿Existen evaluaciones periódicas para medir el nivel de conciencia de seguridad entre los usuarios?

NUNCA CUANDO VIENEN HACER PRACTICAS

11 ¿Ha existido algún tipo de incidente informático dentro de la institución, qué procedimientos se realizaron para solucionar el problema?

NO

Anexo F: Fotos de la cuesta



Uleam
ELOY ALFARO DE MANABÍ

Ingeniería en Tecnologías de la Información

Universidad Laica "Eloy Alfaro" de Manabí

Extensión El Carmen

Objetivo: Identificar problemas de seguridad de la información en el Laboratorio de Computación

Encuesta Dirigida a: DOCENTES de la U.E Alida Zambrano García

1. ¿Conoce usted de las Políticas de seguridad en el laboratorio de computación?

/ Si ___ No

2. ¿Ha recibido capacitación regular sobre las mejores prácticas de seguridad?

/ Si ___ No

3. ¿Considera que es importante la Gestión de seguridad de la información en el laboratorio de computación?

/ Si ___ No

4. ¿Ha tenido algún incidente de seguridad de la información en el laboratorio de computación?

___ Si / No

5. ¿Conoce usted de los ataques informáticos?

/ Si ___ No

6. ¿Ha sido víctima de un ataque informático?

___ Si / No

7. ¿considera que se da mantenimientos a los equipos del laboratorio de computación?

___ Si ___ No ___ ___ A veces /

8. ¿Usted conoce si los equipos tienen instalados antivirus?

Si / No___

9 ¿Le han comunicado como usuario cuáles son sus responsabilidades para garantizar la seguridad en el laboratorio de computación?

Si / No___

10. ¿Existe un sistema de bloqueo para evitar el acceso a páginas que no tienen finalidad académica?

/ Si ___ No

Anexo G: Manual

UNIVERSIDAD LAICA "ELOY ALFARO" DE

MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

ESTUDIANTE:

ZAMBRANO GARCÍA GINA YADIRA

MANUAL DE SEGURIDAD PARA EL LABORATORIO DE COMPUTACION

MANUAL DE POLÍTICAS DE SEGURIDAD PARA EL LABORATORIO DE COMPUTACION

INTRODUCCIÓN

El reglamento de seguridad elaborado para la Unidad Educativa Alida Zambrano García con la finalidad de prevenir incidentes de seguridad para el laboratorio de computación así poder garantizar seguridad y protección dentro del laboratorio mediante estas normativas para minimizar riesgos y llevar un entorno seguro mediante estas políticas de seguridad, está organizado en secciones que abordan diferentes aspectos de la seguridad en el laboratorio de computación de la institución cada sección incluye una descripción de las políticas específicas, los procedimientos a seguir y las responsabilidades asignadas. A través de este enfoque, buscamos proporcionar un marco comprensible y accionable para todos los usuarios, asegurando que el laboratorio de computación funcione de la mejor manera segura, eficiente y conforme a los más altos estándares de seguridad.

La implementación de este manual es esencial para proteger los recursos tecnológicos de la Unidad Educativa Alida Zambrano García y para garantizar la gestión de seguridad de la información y salvaguardar la integridad y confidencialidad que estos recursos continúen contribuyendo de manera efectiva al proceso educativo y al desarrollo profesional de nuestros estudiantes.

OBJETIVO.

El objetivo principal de la elaboración del Manual de Políticas de Seguridad para el Laboratorio de Computación de la Unidad Educativa Alida Zambrano García es establecer un conjunto de directrices y procedimientos claros y efectivos que aseguren la protección, integridad y disponibilidad de los recursos tecnológicos del laboratorio. Esto se logrará

SEGURIDAD FÍSICA

Implica proteger el acceso controlado para limitar que en el laboratorio donde se encuentran las computadoras, solo entre personal autorizado en lo cual sea fundamental el garantizar la seguridad y prioridad la confidencialidad de los recursos presentes y así fomentar una educación con responsalidad en la Unidad Educativa Alida Zambrano García.

Esto garantizan que el acceso esté controlado y que se mantengan altos estándares de seguridad y limpieza, preservando así la integridad de los recursos tecnológicos utilizados para enseñanza

A continuación, medidas para la seguridad del laboratorio de computación

- Utiliza cerraduras electrónicas o tarjetas de identificación, para poder llevar un buen funcionamiento de acceso.
- Cámaras de Seguridad que estén en funcionamiento para monitorear y grabar actividades dentro y fuera del laboratorio.
- Control de Visitantes:
  Es fundamental establecer un sistema de control de visitantes efectivo para garantizar que solo personal autorizado y visitantes identificados puedan acceder al laboratorio. Esto se logra mediante registros de entrada y salida, junto con la verificación de identificación válida.
- Horarios Establecidos:
  Se deben definir horarios precisos de clases dentro de los límites institucionales establecidos. En lo que lleve un registro de entrada y de salida del personal y de los estudiantes. Estos horarios aseguran que los estudiantes y el personal cumplan con las normas del laboratorio, según lo establecido en el Manual de uso del laboratorio.
- Protección Física de Equipos:
  Para proteger los computadores y equipos, es esencial que tanto estudiantes como profesores eviten consumir alimentos o bebidas cerca de los dispositivos. Esto reduce el riesgo de daños y contribuye a mantener un ambiente de trabajo seguro y ordenado, preserva la higiene, y también protege los equipos de posibles daños por derrames accidentales

SEGURIDAD DE SOFTWARE

En el laboratorio de computación es fundamental para proteger los sistemas y datos críticos utilizados en actividades educativas e investigativas. Se refiere a las medidas y políticas diseñadas para prevenir, detectar y responder a amenazas que puedan comprometer la integridad, disponibilidad y confidencialidad de los programas informáticos y los datos almacenados, mantener el software actualizado es crucial para asegurar la protección, eficiencia, y funcionamiento adecuado de los sistemas en el laboratorio de computación, proporcionando una base sólida para todas las actividades

A continuación, medidas para la seguridad del laboratorio de computación.

- Mantén todos los sistemas operativos y software actualizados con las últimas tecnologías de seguridad.
- Instala y actualiza regularmente software antivirus y antimalware.
- Control de aplicaciones para limitar la instalación de software solo a aplicaciones aprobadas y necesarias.
- Establecer procedimientos para la rápida recuperación y restauración de datos en caso de fallas en los equipos
- Establecer protocolos para reportar o documentar cualquier daño de o problema de los equipos de cómputo con un sistema de monitoreo ambiental
- Mantenimiento preventivo y correctivo de manera regular incluirá la actualización de hardware y software para garantizar un rendimiento óptimo y seguro.
- Software actualizado asegura que se pueda recibir ayuda y asistencia en caso de problemas.
- Protección Contra Malware
- Soporte Técnico

PROTECCIÓN CONTRA EL ROBO

La protección contra el robo se refiere a las medidas y estrategias implementadas para prevenir y mitigar el riesgo de sustracción de equipos y dispositivos tecnológicos en un laboratorio de computación. Esto incluye el uso de mecanismos de seguridad física como cerraduras, anclajes y sistemas de alarma, así como controles de acceso que limitan la entrada a personal autorizado. También abarca prácticas de monitoreo y vigilancia mediante cámaras de seguridad, inventarios regulares y etiquetado de activos para facilitar su seguimiento y recuperación en caso de robo.

A continuación, medidas para la seguridad del laboratorio de computación.

- Dispositivos de Rastreo
- Instala alarmas y sensores de movimiento en áreas donde se almacena hardware sensible.
- Usar cámaras de seguridad para monitorear las áreas donde se encuentran los equipos.
- Equipos de Respaldo

102

SEGURIDAD FÍSICA

Implica proteger el acceso controlado para limitar que en el laboratorio donde se encuentran las computadoras, solo entre personal autorizado en lo cual sea fundamental el garantizar la seguridad y prioridad la confidencialidad de los recursos presentes y así fomentar una educación con responsalidad en la Unidad Educativa Alida Zambrano García.

Esto garantizan que el acceso esté controlado y que se mantengan altos estándares de seguridad y limpieza, preservando así la integridad de los recursos tecnológicos utilizados para enseñanza

A continuación, medidas para la seguridad del laboratorio de computación

- Utiliza cerraduras electrónicas o tarjetas de identificación, para poder llevar un buen funcionamiento de acceso.
- Cámaras de Seguridad que estén en funcionamiento para monitorear y grabar actividades dentro y fuera del laboratorio.
- Control de Visitantes:
  Es fundamental establecer un sistema de control de visitantes efectivo para garantizar que solo personal autorizado y visitantes identificados puedan acceder al laboratorio. Esto se logra mediante registros de entrada y salida, junto con la verificación de identificación válida.
- Horarios Establecidos:
  Se deben definir horarios precisos de clases dentro de los límites institucionales establecidos. En lo que lleve un registro de entrada y de salida del personal y de los estudiantes. Estos horarios aseguran que los estudiantes y el personal cumplan con las normas del laboratorio, según lo establecido en el Manual de uso del laboratorio.
- Protección Física de Equipos:
  Para proteger los computadores y equipos, es esencial que tanto estudiantes como profesores eviten consumir alimentos o bebidas cerca de los dispositivos. Esto reduce el riesgo de daños y contribuye a mantener un ambiente de trabajo seguro y ordenado, preserva la higiene, y también protege los equipos de posibles daños por derrames accidentales
- Asegurar de tener detectores de humo y extintores disponibles y en buen estado,
- Llevar un proceso de capacitación al personal para que tengan conocimiento de como actuar en caso de un incidente
- La ubicación de la institución tiene que ser segura

- Integrar medidas de seguridad física y digital para proteger tanto la infraestructura física como los datos y sistemas digitales del laboratorio contra amenazas internas y externas.

SEGURIDAD DE EQUIPOS

Al integrar estas prácticas adicionales, el laboratorio de computación puede fortalecer significativamente su seguridad operativa y proteger de manera efectiva los recursos críticos utilizados para actividades educativas y de investigación de la institución.

A continuación, medidas para la seguridad del laboratorio de computación

- Utiliza anclajes y cerraduras para asegurar computadoras y otros equipos costosos.
- Inventario actualizado de todos los equipos, con números de serie y ubicaciones.
- Realiza mantenimientos preventivos y correctivos regularmente para evitar fallas.
- Implementa políticas claras sobre el uso adecuado de los equipos, incluyendo la prohibición de instalar software no autorizado, descargar archivos no seguros, o realizar modificaciones no autorizadas en la configuración del sistema.
- Establece un plan de respuesta a incidentes que incluya procedimientos específicos para la notificación de pérdida o robo de equipos, así como la recuperación de datos en caso de fallas o violaciones de seguridad.
- verificar el cumplimiento de las políticas de seguridad, revisar el estado de los equipos y asegurar que se mantengan los estándares de seguridad establecidos.
- Realiza mantenimientos preventivos regularmente para detectar y corregir problemas antes de que afecten el rendimiento de los equipos.
- Plan de acción para el mantenimiento correctivo inmediato en caso de fallos inesperados.
-

SEGURIDAD DE REDES

Esta política de seguridad asegurará que el laboratorio de computación opere de manera segura, protegiendo la integridad de los recursos tecnológicos y la confidencialidad de la información crítica utilizada en la institución.

A continuación, medidas para la seguridad del laboratorio de computación.

- Implementa firewalls para proteger la red del laboratorio de accesos no autorizados.
- Divide la red en segmentos para minimizar el impacto de posibles brechas de seguridad, esto ayudara a que la red no se colapse y mitigar robo de información
- control de propagación de virus en la red
- Uso inadecuado de la navegación web
- Falta de análisis de vulnerabilidades en los sistemas operativos
- Capacitación a los estudiantes para que tengan conocimiento de los distintos incidentes de seguridad
- monitoreo de en la búsqueda y patrones sospechosos de las actividades
- realiza escaneo de periódicos de la red en la búsqueda de posibles intrusos

SEGURIDAD DE REDES

Esta política de seguridad asegurará que el laboratorio de computación opere de manera segura, protegiendo la integridad de los recursos tecnológicos y la confidencialidad de la información crítica utilizada en la institución.

A continuación, medidas para la seguridad del laboratorio de computación.

- Implementa firewalls para proteger la red del laboratorio de accesos no autorizados.
- Divide la red en segmentos para minimizar el impacto de posibles brechas de seguridad, esto ayudara a que la red no se colapse y mitigar robo de información
- control de propagación de virus en la red
- Uso inadecuado de la navegación web
- Falta de análisis de vulnerabilidades en los sistemas operativos
- Capacitación a los estudiantes para que tengan conocimiento de los distintos incidentes de seguridad
- monitoreo de en la búsqueda y patrones sospechosos de las actividades
- realiza escaneo de periódicos de la red en la búsqueda de posibles intrusos
- Establecer políticas de seguridad para el uso de redes Wi Fi en el laboratorio
- Instalar protectores contra sobretensiones y sistemas de respaldo de energía (UPS) para asegurar que los equipos estén protegidos contra fluctuaciones eléctricas y para mantener la continuidad operativa durante cortes de energía.
- Mantén actualizados los sistemas operativos, aplicaciones y firmware de los equipos para mitigar vulnerabilidades conocidas y garantizar un rendimiento seguro y eficiente.

SEGURIDAD DE SOFTWARE

En el laboratorio de computación es fundamental para proteger los sistemas y datos críticos utilizados en actividades educativas e investigativas. Se refiere a las medidas y políticas diseñadas para prevenir, detectar y responder a amenazas que puedan comprometer la integridad, disponibilidad y confidencialidad de los programas informáticos y los datos almacenados, mantener el software actualizado es crucial para asegurar la protección, eficiencia, y funcionamiento adecuado de los sistemas en el laboratorio de computación, proporcionando una base sólida para todas las actividades

SEGURIDAD DE SOFTWARE

En el laboratorio de computación es fundamental para proteger los sistemas y datos críticos utilizados en actividades educativas e investigativas. Se refiere a las medidas y políticas diseñadas para prevenir, detectar y responder a amenazas que puedan comprometer la integridad, disponibilidad y confidencialidad de los programas informáticos y los datos almacenados, mantener el software actualizado es crucial para asegurar la protección, eficiencia, y funcionamiento adecuado de los sistemas en el laboratorio de computación, proporcionando una base sólida para todas las actividades

A continuación, medidas para la seguridad del laboratorio de computación.

- Mantén todos los sistemas operativos y software actualizados con las últimas tecnologías de seguridad.
- Instala y actualiza regularmente software antivirus y antimalware.
- Control de aplicaciones para limitar la instalación de software solo a aplicaciones aprobadas y necesarias.
- Establecer procedimientos para la rápida recuperación y restauración de datos en caso de fallas en los equipos
- Establecer protocolos para reportar o documentar cualquier daño de o problema de los equipos de cómputo con un sistema de monitoreo ambiental
- Mantenimiento preventivo y correctivo de manera regular incluirá la actualización de hardware y software para garantizar un rendimiento óptimo y seguro.
- Software actualizado asegura que se pueda recibir ayuda y asistencia en caso de problemas.
- Protección Contra Malware
- Soporte Técnico

GESTIÓN DE USUARIOS

La Gestión de Usuarios es crucial para mantener un entorno seguro, eficiente y en cumplimiento dentro del laboratorio de computación, garantizando que los recursos y datos estén protegidos y se utilicen de manera responsable, implementar mejores prácticas ayudará a proteger los recursos del laboratorio de computación y garantizará un entorno seguro para la enseñanza y la investigación.

A continuación, medidas para la seguridad del laboratorio de computación.

- Contraseñas Seguras requiere contraseñas fuertes y cambia las contraseñas de manera regular.
- Implementa Autenticación Multifactor (MFA) para acceso al sistema
- Asignar roles y permisos de acceso basados en la protección de los datos
- Realiza copias de seguridad de datos importantes y almacénalas en una ubicación segura.
- Capacitación Continua proporciona capacitación regular a los usuarios sobre prácticas de seguridad y concienciación.
- Realiza simulaciones de ataques de phishing para educar a los usuarios sobre cómo identificar y manejar correos electrónicos sospechosos.
- Mantén registros detallados de acceso y eventos para realizar auditorías regulares.
- plan de respuesta a incidentes
- Definir procedimientos claros para responder a incidentes de seguridad.
- Establece un equipo de respuesta a incidentes con roles y responsabilidades definidos.
- Realiza simulacros regulares para asegurarte de que el personal esté preparado para manejar incidentes.
- Asegurase de cumplir con todas las regulaciones y normas aplicables
- Realiza auditorías externas periódicas para evaluar la efectividad de las prácticas de seguridad.

SEGURIDAD FÍSICA DEL HARDWARE

La seguridad física del hardware se refiere a las medidas y prácticas destinadas a proteger los equipos informáticos y dispositivos tecnológicos de daños físicos, robos y accesos no autorizados. Esto incluye el uso de cerraduras, anclajes, cámaras de vigilancia, controles de acceso y sistemas de monitoreo ambiental para asegurar la integridad y disponibilidad del hardware en un entorno determinado.

SEGURIDAD FÍSICA DEL HARDWARE

La seguridad física del hardware se refiere a las medidas y prácticas destinadas a proteger los equipos informáticos y dispositivos tecnológicos de daños físicos, robos y accesos no autorizados. Esto incluye el uso de cerraduras, anclajes, cámaras de vigilancia, controles de

hardware en un entorno determinado
hardware en un entorno determinado.

A continuación, medidas para la seguridad del laboratorio de computación.

- Almacena equipos críticos y sensibles en gabinetes cerrados con llave.
- Etiqueta todo el hardware con identificadores únicos y registra esta información en un inventario centralizado.
- Mantén un inventario detallado de todo el hardware, incluyendo números de serie, modelos, y ubicaciones.
- Realiza auditorías periódicas del inventario para asegurar que todos los equipos estén presentes y en buen estado.
- configuración segura
- Protege la configuración del BIOS o UEFI con contraseñas para prevenir cambios no autorizados.
- Desactivar Puertos No Utilizados: Desactiva puertos USB, FireWire, y otros puertos de entrada y de salida no utilizados en las estaciones de trabajo y servidores.
- Configuración de Red Segura para que las configuraciones de red sean seguras,
- desactivación de servicios y puertos innecesarios.
- mantenimiento y actualización
- mantén el firmware de todos los dispositivos actualizado con las últimas versiones disponibles.
- programa revisiones y mantenimiento regular del hardware para identificar y corregir problemas potenciales antes de que se conviertan en fallas críticas.
- Realiza copias de seguridad regulares de las configuraciones de hardware y software.
- Mantén equipos de respaldo disponibles para reemplazar rápidamente cualquier hardware que falle.
-

POLÍTICAS Y PROCEDIMIENTOS CLAROS

Establecer políticas y procedimientos claros para el uso del hardware,

la gestión de contraseñas, el acceso a datos y la disposición de equipos asegura que todos los usuarios del laboratorio sigan las mismas normas, reduciendo el riesgo de errores humanos y negligencias, protección contra inundaciones para salvaguardar los equipos, datos y recursos tecnológicos del laboratorio de computación en caso de un evento de inundación, implementar estas políticas es crucial para minimizar el daño y asegurar la rápida recuperación operativa.

A continuación, medidas para la seguridad del laboratorio de computación.

- Realizar una evaluación regular de riesgos para identificar las áreas del laboratorio más vulnerables a inundaciones.
- Desarrollar y mantener un plan de contingencia específico para inundaciones, que incluya procedimientos de respuesta y recuperación
- Instalar barreras físicas y sistemas de drenaje alrededor del laboratorio para desviar el agua.
- Utilizar fundas protectoras impermeables para cubrir equipos sensibles y asegurar su protección contra el agua. Implementar sistemas de monitoreo ambiental que incluyan sensores de humedad y detectores de agua para alertar al personal en caso de aumento de niveles de agua.
- Restaurar las paredes y grietas de laboratorio de computación

PROTECCIÓN CONTRA EL ROBO

La protección contra el robo se refiere a las medidas y estrategias implementadas para prevenir y mitigar el riesgo de sustracción de equipos y dispositivos tecnológicos en un laboratorio de computación. Esto incluye el uso de mecanismos de seguridad física como cerraduras, anclajes y sistemas de alarma, así como controles de acceso que limitan la entrada a personal autorizado. También abarca prácticas de monitoreo y vigilancia mediante cámaras de seguridad, inventarios regulares y etiquetado de activos para facilitar su seguimiento y recuperación en caso de robo.

A continuación, medidas para la seguridad del laboratorio de computación.

- Dispositivos de Rastreo
- Instala alarmas y sensores de movimiento en áreas donde se almacena hardware sensible.
- Usar cámaras de seguridad para monitorear las áreas donde se encuentran los equipos.
- Equipos de Respaldo
- Copias de Seguridad de Configuraciones:
- Cables de Seguridad para evitar desconexiones no autorizadas.
- Accesos Controlados limita el acceso físico a los dispositivos a personal autorizado y capacitado.
- Asegúrate de que todos los datos sean eliminados de forma segura antes de deshacerse de cualquier dispositivo
- Establece protocolos claros para que el personal informe cualquier pérdida, robo o daño del hardware inmediatamente.

POLÍTICAS Y PROCEDIMIENTOS CLAROS

Establecer políticas y procedimientos claros para el uso del hardware,

la gestión de contraseñas, el acceso a datos y la disposición de equipos asegura que todos los usuarios del laboratorio sigan las mismas normas, reduciendo el riesgo de errores humanos y negligencias, protección contra inundaciones para salvaguardar los equipos, datos y recursos tecnológicos del laboratorio de computación en caso de un evento de inundación, implementar estas políticas es crucial para minimizar el daño y asegurar la rápida recuperación operativa.

POLÍTICAS Y PROCEDIMIENTOS CLAROS

Establecer políticas y procedimientos claros para el uso del hardware,

la gestión de contraseñas, el acceso a datos y la disposición de equipos asegura que todos los usuarios del laboratorio sigan las mismas normas, reduciendo el riesgo de errores humanos y negligencias, protección contra inundaciones para salvaguardar los equipos, datos y recursos tecnológicos del laboratorio de computación en caso de un evento de inundación, implementar estas políticas es crucial para minimizar el daño y asegurar la rápida recuperación operativa.

A continuación, medidas para la seguridad del laboratorio de computación.

- Realizar una evaluación regular de riesgos para identificar las áreas del laboratorio más vulnerables a inundaciones.
- Desarrollar y mantener un plan de contingencia específico para inundaciones, que incluya procedimientos de respuesta y recuperación
- Instalar barreras físicas y sistemas de drenaje alrededor del laboratorio para desviar el agua.
- Utilizar fundas protectoras impermeables para cubrir equipos sensibles y asegurar su protección contra el agua. Implementar sistemas de monitoreo ambiental que incluyan sensores de humedad y detectores de agua para alertar al personal en caso de aumento de niveles de agua.
- Restaurar las paredes y grietas de laboratorio de computación

9 GLOSARIO

A

sistemas obsoletos

estructura de datos y formatos no compatibles con

el sistema , son equipos que ya no tienen la capacidad de manejar las cargas de trabajo actuales o no son compatible con el software

moderno 22

W

Whitman 108 es el autore del libro Historias de la seguridad de la información