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 INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

AUDITORÍA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DEL LABORATORIO DE CÓMPUTO EN LA UNIDAD EDUCATIVA SIMÓN BOLÍVAR

AUTOR

DOMINGUEZ ZAMBRANO MERLY MISHELLE

TUTOR

ING. CLARA GUADALUPE POZO HERNÁNDEZ, MG.

EL CARMEN, ENERO 2025

CERTIFICACIÓN DEL TUTOR

Uleam UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 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 **DOMINGUEZ ZAMBRANO MERLY MISHELLE**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(1)-2024(2), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es **"Auditoría Informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar".** 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, 19 de diciembre del 2024

Lo certifico,

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

TRIBUNAL DE SUSTENTACIÓN

TRIBUNAL DE SUSTENTACIÓN

Uleam

Universidad Laica Eloy Alfaro de Manabí

Extensión El Carmen

Carrera de Ingeniería en Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Título del Trabajo de Titulación:
Auditoría Informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar.

Modalidad:
Proyector Integrador

Autor:
Domínguez Zambrano Merly Mishelle

Tutor:
Ing. Clara Guadalupe Pozo Hernández, Mg.

Tribunal de Sustentación:

- **Presidente:** Ing. Mora Marcillo Alex Bladimir, Mg _____
- **Miembro:** Ing. Arévalo Hermida Rómulo Danilo, Mg _____
- **Miembro:** Ing. Mendoza Villamar Rocío Alexandra, Mg _____

Fecha de Sustentación:
23/01/2025

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido del proyecto integrador siendo el tema: Auditoría Informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar, propio de Dominguez Zambrano Merly Mishelle con C.I 1315108421, los derechos de la misma corresponden a la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen.

Mishelle D.

DOMINGUEZ ZAMBRANO MERLY MISHELLE

C.I. 131510842-1

DEDICATORIA

El presente trabajo de Titulación es para mis padres, Medardo Domínguez y Magali Zambrano desde pequeña me educaron y me guiaron por un buen camino ahora estoy aquí mostrándole un logro más, siempre con la sencillez que me caracteriza para realizar las cosas, planteándome en mis conocimientos para fundamentarlo y aprender día a día.

A mis queridos hermanos, ellos siempre han velado por mis sueños, brindándome ese apoyo incondicional que sólo como hermanos nos entendemos mutuamente, soy la mayor es por eso que siempre cuando no están mis padres tengo que cuidarlos de la mejor manera, siempre les digo lo mismo que desde que nacieron se convirtieron en mis pilares fundamentales en mi vida.

A mi novio, por prestarme de su tiempo en trasladarme a la Universidad, sé que sin tus preocupaciones de cuando me rendía y no podía más, estabas ahí brindándome una mano y diciéndome en que te puedo ayudar para no abandonar mis sueños, muy gratificante de su parte.

Finalmente, dedico mi logro a todos mis familiares y amistades que de alguna manera me ayudaron para que esto fuera posible alcanzando el propósito requerido.

Dominguez Zambrano Merly Mishelle

AGRADECIMIENTO

Agradeciendo en primer lugar a mi Padre Celestial Dios, por ser mi guía escucharme todas las noches lo que le pedía para mi vida, finalmente me está cumpliendo unos de mis sueños anhelados, en él encomiendo todos mis esfuerzos y triunfos.

A mis padres, no me cansaré de darles las gracias por saber que era bueno para mí y aun así brindando sabiduría para que no decayeran mis sueños, sino haciéndose realidad para que lo pueda disfrutar de una manera sana sin vicios ni nada, despojando en mí toda su confianza de hermana mayor para enseñarles con ejemplos que los sueños si se cumplen sólo tienes que ser paciente.

A mi tutora del proyecto integrador: Ing. Clara Pozo Hernández, Mg por darme todas sus enseñanzas, brindándola de la mejor manera posible para que le entendiera, su experiencia y conocimientos han sido de gran ayuda en este proyecto puesto que mi sumo interés de entender lo comprendido.

A la Coordinadora la Lic. Karina Intriago y Docente de la Institución la Lic. Gabriela Alvarado por ayudarme a ingresar a la Institución, para poder realizar mi Auditoría en el laboratorio de cómputo de la Escuela Simón Bolívar, por permitir evaluar la información para el proceso de Investigación.

Por último y no menos importante, quiero agradecerle mis infinitas gracias a la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen por haber aceptado mi cupo de estudio, brindado la oportunidad de estudiar en sus Instalaciones durante los últimos 5 años, sin ello no hubiera podido ser posible este logro más en mi vida.

A todos ustedes, mi más sincero agradecimiento del fondo de mi corazón.

Dominguez Zambrano Merly Mishelle

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto integrador corresponde a una Auditoría Informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar. El objetivo fue evaluar la seguridad informática que presenta la Escuela determinando los riesgos que está expuesto la seguridad física teniendo en consideración su zona rural, situada en San Luis de Cajones. Para determinar la veracidad de la información requerida, se investigó en diferentes fuentes bibliográficas, la evaluación se llevó a cabo de manera global para asegurar una compresión completa y precisa. Es así como se realizó la encuesta a las docentes y entrevista a la coordinadora, efectuando su verdadera problemática que presenta la sala de informática, de no tener un registro del ingreso al laboratorio de cómputo. Como propuesta se aplicó la auditoría con la metodología Magerit encontrando los riesgos de robo, incendio, inundación, daño de equipo y malware; teniendo presente el nivel de seguridad general que cuenta la escuela Simón Bolívar es de 80% siendo éste un nivel alto de seguridad, los recursos contra amenaza interna y externa obteniendo como resultado que la escuela está propensa a robo, por tener una mayor exposición por el medio de ingreso a particulares. Finalmente se sugiere un manual de buenas prácticas en éste incluye lo que son los cinco niveles de riesgos a considerar, apreciando las medidas de seguridad que cuenta con situaciones que se presenta en el establecimiento, como parte responsable de la escuela las docentes y alumnos quienes son que conforman la institución básica Simón Bolívar.

ABSTRACT

This integrative project corresponds to a Computer Audit of the technological infrastructure of the computer lab at the Simón Bolívar Educational Unit. The objective was to evaluate the computer security presented by the School, determining the risks to which physical security is exposed, taking into consideration its rural area, located in San Luis de Cajones. To determine the veracity of the required information, research was carried out in different bibliographic sources. The evaluation was carried out globally to ensure a complete and precise understanding. This is how the survey was carried out on the teachers and the coordinator was interviewed, carrying out the real problem that the computer room presents, of not having a record of the entry to the computer lab. As a proposal, the audit was applied with the Magerit methodology, finding the risks of theft, fire, flooding, equipment damage and malware; Taking into account that the general security level of the Simon Bolivar school is 80%, which is a high level of security, the resources against internal and external threats, resulting in the school being prone to theft, due to having a greater exposure through the means of entry to individuals. Finally, a manual of good practices is suggested. This includes the five levels of risk to consider, appreciating the security measures that it has in situations that occur in the establishment, as the responsible part of the school, the teachers and students who make up the Simon Bolivar basic institution..

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

La auditoría de seguridad física resulta esencial para identificar las vulnerabilidades y debilidades de seguridad a las que están expuestos los activos tecnológicos de un laboratorio de cómputo, proponiendo medidas que protejan dichos recursos. La protección física de estos activos es fundamental para garantizar la integridad de los recursos y la continuidad del aprendizaje en instituciones educativas. Estas instituciones generan una gran cantidad de datos e información que requieren almacenamiento eficiente y seguro.

A través de evaluaciones y análisis detallados, se identifican las necesidades específicas para gestionar la seguridad en un establecimiento educativo, tanto en aspectos internos como externos. Esto permite desarrollar una visión más acertada para la toma de decisiones organizacionales y la formulación de políticas. En este contexto, la infraestructura del laboratorio de cómputo se convierte en un área prioritaria, destacando la importancia de medidas como el control del acceso de personas no autorizadas y el mantenimiento adecuado de los sistemas, lo que asegura el correcto funcionamiento de los procesos tecnológicos.

La implementación de mecanismos de defensa dentro del laboratorio de cómputo contribuye a garantizar un entorno seguro para los usuarios, preservando la infraestructura tecnológica en condiciones óptimas y minimizando los riesgos de daños a los equipos informáticos. En el caso de la Escuela Simón Bolívar, se evaluaron cinco niveles de riesgo, identificándose que uno de ellos está asociado a la falta de protección física. Las medidas de seguridad necesarias no requieren tecnología avanzada, pero sí un enfoque eficaz que permita el control informático adecuado. Actualmente, la institución utiliza paquetes de software como Office para el registro de información; sin embargo, la falta de espacio en disco puede ocasionar la pérdida de archivos importantes.

Los activos del laboratorio de cómputo fueron evaluados con el propósito de definir medidas de seguridad que se plasman como propuestas de mejora en un manual de buenas prácticas. Este manual incluye políticas de seguridad diseñadas para mitigar riesgos en diversos

niveles, incluyendo aquellos derivados de desastres naturales, facilitando la toma de decisiones oportunas en situaciones críticas.

La infraestructura tecnológica en un laboratorio de cómputo requiere de medidas preventivas constantes que garanticen su correcto funcionamiento y la protección de los equipos informáticos. Estas medidas incluyen la implementación de prácticas que aseguren la seguridad y eficiencia en el entorno educativo, así como la realización de actualizaciones periódicas de hardware que permitan mantener los equipos en condiciones óptimas.

1.2 Presentación del tema

Auditoría Informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar.

1.3 Ubicación y contextualización de la problemática

La Escuela General Básica Simón Bolívar se encuentra en el Cantón El Carmen, en el Sitio Río Cajones, San Luis de Cajones. Esta institución, de carácter fiscal, está situada en un entorno rural y su estructura principal está construida de cemento. Además de su ubicación, la escuela se destaca por contar con un entorno natural que incluye áreas boscosas.

En relación con sus instalaciones, la Escuela General Básica Simón Bolívar dispone de dos canchas de cemento, siete aulas (seis en el interior del edificio y una al aire libre), un laboratorio de cómputo, un área administrativa, un espacio para la venta de alimentos, así como tres baños y un urinario para niños, complementados con lavamanos.

En lo que concierne al personal docente, la Escuela cuenta con tres profesionales: la Licenciada Karina Intriago Moreira, quien no solo es Coordinadora de la institución, sino también docente de sexto y séptimo grado; la Licenciada Gabriela Alvarado, quien imparte clases a alumnos de primero y segundo grado; y la Licenciada Marisol Molina, encargada de los cursos de cuarto, quinto y sexto grado.

Actualmente, la Escuela General Básica Simón Bolívar tiene una matrícula de 63 estudiantes, quienes se benefician de estas instalaciones del laboratorio de cómputo, en tanto

las docentes comprometidas con su educación transmitiendo desde los conocimientos, habilidades y valores haciéndolos ciudadanos críticos.

La Escuela general Básica Simón Bolívar cuenta con un único laboratorio de cómputo. 19 computadores están dedicados para los estudiantes y un computador para el docente que imparte clase en dicho laboratorio, 20 reguladores de energía, 1 switch y 1 router que proporciona el acceso a internet en todo el establecimiento. Actualmente el laboratorio no cuenta con personal dedicado al mantenimiento de los equipos informáticos, tanto a nivel de hardware como software.

1.4 Planteamiento del problema

1.4.1 Problematización

A nivel mundial, las instituciones educativas están adoptando un enfoque proactivo para proporcionar a los estudiantes acceso directo y personalizado a tecnologías avanzadas. Este esfuerzo tiene como objetivo organizar herramientas que faciliten el desarrollo del conocimiento de los estudiantes. Para alcanzar estos objetivos, se están instalando grandes laboratorios y se están implementando tecnologías dedicadas exclusivamente a salvaguardar la integridad de las infraestructuras educativas.

En Ecuador por su parte, las unidades educativas deben tener toda la información detallada sobre el uso de los equipos informáticos, en caso de algún inconveniente contar con una documentación y controles adecuados. Si las unidades educativas no cuentan con información referente a un proceso de control, que permita mantener a buen recaudo la integridad de los equipos, éstos pueden sufrir daños o incluso pérdidas de los inventarios con lo que sería deficiente el servicio que deben brindar a los estudiantes.

En el Cantón El Carmen, perteneciente a la provincia de Manabí, en Ecuador, se encuentra la Escuela Básica General Simón Bolívar, esta cuenta con un único laboratorio de cómputo para los estudiantes de todo el plantel. El laboratorio cuenta con una infraestructura tecnológica básica sin las seguridades del caso ya que el ingreso al laboratorio no ofrece mayor resistencia o dispositivos que puedan prevenir su sustracción o evento climático que genere el caso de la intensa lluvia que se presenta en el sector, dando como resultado obstrucciones de todo tipo por el viento y las precipitaciones, es importante desarrollar políticas claras sobre el

uso del laboratorio, para que conste la responsabilidad de quienes utilizan los equipos informáticos.

1.4.2 Génesis del problema

El problema se viene dando desde la misma instalación del laboratorio pues no se ha tomado las precauciones del caso, con el tiempo se va evidenciando la falta de seguridad que existe tanto en la infraestructura, así como en el software de los equipos, por tal motivo es importante tomar decisiones que solucionen este inconveniente.

La gestión de accesos es otro aspecto clave a considerar. Implementar sistemas de control de acceso, como identificación biométrica o tarjetas de acceso, puede limitar la entrada a personas autorizadas. Esto no solo protege los equipos contra el uso indebido, sino que también asegura que los datos sensibles estén resguardados.

1.4.3 Estado actual del problema

La Escuela Simón Bolívar mantiene el laboratorio limpio y ordenado, sin embargo, no existe un proceso de controles adecuado para la infraestructura del laboratorio, tanto de forma física como lógica, al contar con equipos no actualizados que ponen en peligro la información de los estudiantes que utilizan los equipos informáticos.

El problema que existe en la Escuela Simón Bolívar es la inseguridad de los equipos de cómputo en el laboratorio de informática, siendo una de las causas que los conectores de red alojados en el suelo cuyo efecto es el daño en la infraestructura de la red ya que los estudiantes pueden tropezar constantemente con los cables dañándolos en su defecto al jalarlos producir caídas de los equipos informáticos, por otra parte, la falta de mantenimiento de los equipos tiende a situaciones de alto riesgo pues pueden sobrecalentarse y dañar los dispositivos, la ubicación del aire condicionado está en la parte superior, puede que al momento de que se filtre agua esté derrame encima de los equipos informáticos, finalmente sistemas informáticos no actualizados tienen como efecto daños físicos y pérdida de datos en la seguridad de información ya que al volverse obsoletos son más posible a sufrir Hacker cibernéticos o simplemente los discos duros ya no pueden procesar a la velocidad requerida. El mantenimiento si recibe por parte de los técnicos del Distrito de Educación contaba la escuela

con esta ayuda al momento de surgir situaciones que se salían de la mano como conectores de red dañados, computadoras que no prendían o servicio de arreglar algún botón de un pc.

1.5 Diagrama causa – efecto del problema

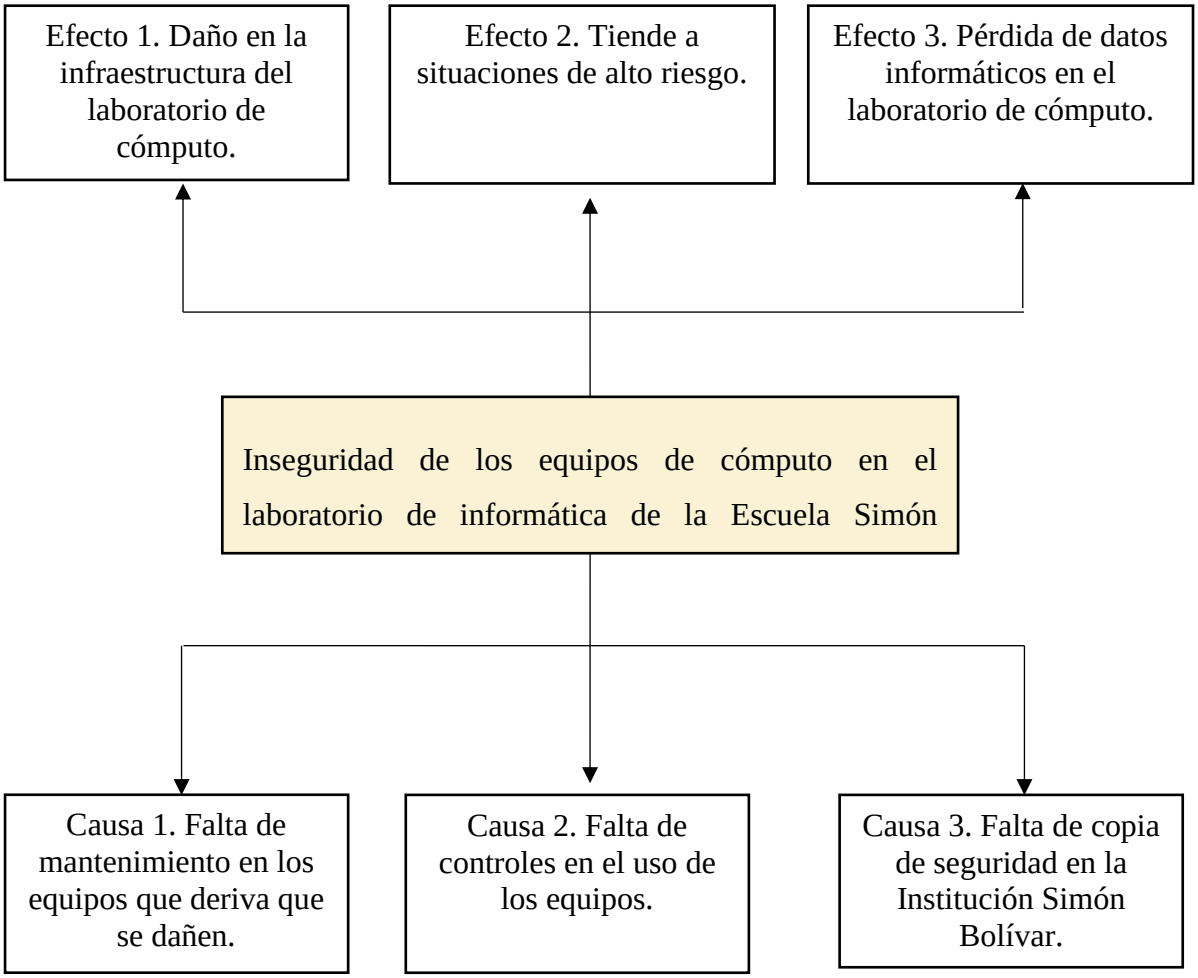


Ilustración 1Diagrama causa – efecto del problema

1.6 Objetivos

1.6.1 Objetivo general

Realizar una Auditoría Informática en la infraestructura tecnológica del laboratorio de cómputo ubicado en la Escuela General Básica Simón Bolívar, en el Sector Río Cajones del cantón El Carmen, provincia de Manabí.

1.6.2 Objetivos específicos

Para llevar a cabo una Auditoría Informática en la infraestructura tecnológica del laboratorio de cómputo en la Escuela Simón Bolívar, por el Sector Río Cajones, establecida en San Luis de Cajones del Cantón El Carmen, provincia de Manabí, se deben seguir lo siguiente:

1. Identificar el problema que se encuentra establecido en la Escuela Simón Bolívar, retomando los impactos que se presenta.
2. Investigar en diferentes fuentes bibliográficas que fundamentalmente las variables dependiente e independiente.
3. Evaluar encuesta y entrevista a docentes del establecimiento para diagnosticar la problemática.
4. Aplicar una auditoría tomando en consideración la metodología Magerit para evaluación de riesgos.
5. Elaborar informe de auditoría que evidencie los principales riesgos de seguridad, incluyendo un manual de buenas prácticas.

1.7 Justificación

La presente investigación es de interés por cuanto el laboratorio de cómputo es de gran importancia para el desarrollo del aprendizaje de los estudiantes de la Escuela Simón Bolívar que requieren formación de calidad en el área de informática. Este estudio permitirá evaluar el estado actual de la seguridad que se mantiene sobre las computadoras y su información, además el informe de auditoría permitió identificar las vulnerabilidades y proponer las medidas de seguridad que se requiere para el mejoramiento requerido.

El desarrollo del proyecto generará beneficios a la institución en el informe final de Auditoría develará las conclusiones y recomendación para utilizar un manual de buenas prácticas en la Escuela que cuenta con protecciones de sobre aviso. Realizar distintas medidas de prevención para e laboratorio de cómputo como el acceso controlado y la protección de los equipos informáticos que pueden reflejarse mejorías porque reduciría el acceso a personas no autorizadas que con el tiempo se reflejaría al momento de posibles daños internos o externos del establecimiento.

Desde el punto de vista de la vialidad, se dispone el apoyo de las autoridades de la Escuela Simón Bolívar, padres de familia y maestros, sin embargo, requiere un seguimiento a nivel de gestiones en el Distrito de Educación para poder ejercer completamente las recomendaciones, formado una parte fundamental dentro del desarrollo educativo que la escuela provee dentro de los planteles y del laboratorio de cómputo que se necesita de la Auditoría para la infraestructura tecnológica.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

La tecnología ha tenido un profundo impacto en la sociedad, generando mejoras significativas en la atención médica, transporte, comunicación y otras áreas. Llevando un aislamiento social, manteniéndose conectada entre sí, los teléfonos inteligentes ofrecen una variedad de capacidades que antes solo estaban disponibles en las computadoras de escritorio (Parra, 2023).

La presente investigación pretende salvaguardar la infraestructura del laboratorio de cómputo en la Escuela General Básica Simón Bolívar, a través de la aplicación de métodos y herramientas tecnológicas que le permitan al estudiante y profesores el uso del laboratorio de informática con la garantía del caso tanto en lo referente al cuidado del hardware. En la actualidad es importante proteger de la delincuencia el acceso de los equipos informáticos además que es necesario proteger la información que existe.

1.8.2 Impacto social

Según Kvam (2018), es importante reconocer que los riesgos e impactos sociales pueden ser diferentes en las distintas etapas del proyecto, se dan circunstancias imprevistas el análisis social, la participación de las partes interesadas y la actualización de los planes y los sistemas de gestión deben incorporarse como elementos básicos a lo largo del proyecto

Con la aplicación de la auditoría, la institución cuenta con un manual de buenas prácticas que su aplicación creará una cultura tanto en estudiantes como docentes de cuidar los espacios y equipos, para proteger su información privada.

1.8.3 Impacto ecológico

Es un proceso de evaluación y control de las prácticas ambientales de una organización su objetivo principal es garantizar que las prácticas sean sostenibles con el medio ambiente, incluyendo la revisión de políticas, procedimientos que gestione su impacto ambiental, la revisión de informes, registros y la inspección de instalaciones (ITSQMET, 2024).

La investigación permite que a través de la adecuada prevención se precautele los equipos de cómputo aumentando sus años de vida útil y por lo tanto evitando el desecho de los equipos que causan un grave daño ambiental por los elementos que lo componen, en tal virtud un mejor cuidado evita desperdicios nocivos al medio ambiente.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

La auditoría informática comenzó a consolidarse como una disciplina formal durante los años 60 y 70, cuando las empresas empezaron a integrar sistemas computacionales en sus operaciones. En sus primeras etapas, el foco principal era asegurar la precisión, fiabilidad de los datos manejados por estos sistemas. La adopción de tecnologías de procesamiento de datos en el ámbito empresarial hizo imperativo establecer mecanismos de control y procedimientos de auditoría para verificar que los sistemas operativos de las aplicaciones funcionaran adecuadamente y cumplieran con los estándares requeridos. Para Smith y Johnson (2022), la necesidad de auditar los sistemas de información se volvió crucial cuando se evidenció que los datos computarizados empezaban a tener un impacto considerable en la toma de decisiones en la eficacia operativa de las empresas.

En los años 80, la auditoría informática avanzó significativamente con la incorporación de nuevas metodologías con normas más rigurosas. La fundación de ISACA (Asociación de Auditoría y Control de Sistemas de Información) en 1969, que posteriormente se convirtió en una autoridad clave en la estandarización de la auditoría de TI, marcó un hito crucial en el desarrollo de la profesión. Según Brown y Miller (2023), la creación de ISACA y el establecimiento de sus marcos normativos han sido esenciales para la formalización de las prácticas de auditoría informática, proporcionando a los auditores herramientas teniendo directrices necesarias para evaluar la efectividad de los controles tecnológicos.

La infraestructura tecnológica se refiere al conjunto de hardware, software, redes, servicios que permiten el funcionamiento a la gestión de sistemas informáticos en una organización. Este entorno incluye servidores, dispositivos de almacenamiento, equipos de red estaciones de trabajo, que trabajan en conjunto para asegurar la disponibilidad, integridad y seguridad de la información. Según Rodríguez y Gómez (2023), la infraestructura tecnológica es fundamental para el desempeño eficiente de las operaciones empresariales, ya que proporciona la base necesaria para el almacenamiento, procesamiento y transmisión de datos

en un entorno seguro y confiable. La adecuada configuración del mantenimiento de estos componentes es crucial para la estabilidad, el rendimiento de los sistemas de TI.

Además de los equipos físicos, la infraestructura tecnológica también abarca la gestión de redes, servicios en la nube que se han convertido en componentes esenciales para la flexibilidad, escalabilidad de las operaciones modernas. Los avances recientes en virtualización de servicios en la nube han permitido a las organizaciones optimizar sus recursos en tanto reducir costos operativos, mientras mejoran su capacidad para adaptarse a cambios en la demanda. La integración de soluciones de nube y virtualización en la infraestructura tecnológica permite a las empresas no solo gestionar de manera más eficiente sus recursos, sino también responder de manera ágil a las necesidades del mercado los desafíos tecnológicos (Chen & Wang, 2022).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

Auditoría Informática al Departamento de Sistemas de la Unidad Educativa "San Felipe Neri" de la ciudad de Riobamba, Provincia de Chimborazo, período 2018.

Este proyecto establece como objetivo evaluar el uso y aprovechamiento adecuado de los recursos informáticos en su desarrollo, este estudio concluye que: la Institución incumple con la normativa de control interno 410, por lo que recomienda realizar Auditorías informáticas anuales que hacer un seguimiento a las recomendaciones realizadas (Yumbillo, 2020).

Auditoría informática aplicando metodología COBIT en los laboratorios de cómputo de la facultad de ciencias técnicas de la Universidad estatal del sur de Manabí.

Este estudio cuyo objetivo fue conocer el estado actual de los laboratorios de cómputo en seguridad y manipulación de información en la institución, la investigación recomienda el desarrollo de amplias investigaciones e implementaciones acerca de la Auditoría COBIT no solo para ciertas áreas sino para toda la Universidad (Barreto, 2021).

Auditoría informática interna de los módulos de matriculación y notas del sistema de gestión académica de la ESPAM MFL.

Esta investigación cuyo objetivo fue determinar el nivel de cumplimiento de su reglamento Institucional correspondiente, concluyó que se pudo elaborar un informe de Auditoría y un plan de mejora (Cobeña & Mendoza, 2021).

Control y monitoreo en tiempo real de los equipos informáticos para los laboratorios 1-2-3 de informática de la Universidad Estatal Península de Santa Elena.

Este proyecto cuyo objetivo fue administrar los equipos de cómputo en tiempo real en el laboratorio de informática, el estudio recomienda que se necesita capacitación a los técnicos de mantenimiento de las diferentes funcionalidades de la herramienta que se implementó de los laboratorios (Gòmez, 2020).

Auditoría de Seguridad Informática para Infraestructura Tecnológica en la Unidad Educativa Antonio José de Sucre en el periodo 2022.

Este trabajo investigativo cuyo objetivo fue elaborar un informe de Auditoría donde se evaluó y verifico el cumplimiento de normas de seguridad de la infraestructura tecnológica que posee la Institución, el estudio recomienda necesario ejecutar una guía de recomendaciones que servirán para prevenir desastres en la infraestructura tecnológica dentro de la Unidad Educativa Antonio José de Sucre puede ejecutar a una guía de recomendaciones que servirán para prevenir desastres en la infraestructura tecnológica dentro de la Unidad Educativa Antonio José de Sucre (Paladines, 2023).

2.3 Definiciones conceptuales

2.3.1 Auditoría informática

La Auditoría Informática, puede ser definida como el procedimiento que implica la recopilación, organización y evaluación de pruebas con el fin de verificar si un sistema informático garantiza la protección de los activos digitales al mismo tiempo asegura la integridad de la fiabilidad de los datos. Este proceso requiere establecer metas claras relacionadas con la protección de los activos de la integridad de la información (Solano & Riasco, 2021).

El constante avance de la creciente complejidad de los sistemas de información ha generado la necesidad de contar con expertos en informática que se dediquen a verificar su funcionamiento, detectar posibles vulnerabilidades que requieran acciones correctivas o preventivas. Esto es crucial para evitar la pérdida de información valiosa, que podría tener costos significativos para las organizaciones. Es por lo que la figura del Auditor informático se ha vuelto cada vez más importante en las empresas. Este profesional, independiente y capacitado, evalúa la eficacia de los sistemas informáticos haciendo recomendaciones para mejorar, asegurando la integridad o precisión de los datos garantizando un servicio de calidad conforme a estándares establecidos (Chicano, 2024).

2.3.1.1 Objetivo de la Auditoría Informática

La Auditoría informática no se limita únicamente a la evaluación de equipos de cómputo, sistemas o procedimientos específicos, sino que también abarca la evaluación integral de los sistemas de información. Esto incluye análisis de las entradas de datos, procedimientos, controles, archivos, seguridad y procesos de obtención de información. La Auditoría informática desempeña un papel fundamental en el correcto funcionamiento de los sistemas de información al proporcionar controles necesarios para garantizar su confiabilidad y seguridad (Laedu, 2021).

Es necesaria la existencia de un código deontológico, basado en cuestiones como la moral de la ética profesional que se compone de varios principios: El enfoque principal del Auditor debe ser maximizar los beneficios para su cliente, los intereses personales no deben primar sobre las responsabilidades del Auditor, debe evitar cualquier conflicto de interés o influencia relacionada con marcas, productos o fabricantes. El Auditor debe evitar recomendar acciones que sean innecesarias o que impliquen riesgos injustificados (Menéndez, 2024).

La auditoría de sistemas informáticos implica examinar minuciosamente estos sistemas para detectar, identificar o describir posibles vulnerabilidades. Durante el ejercicio de esta función, los auditores deben adherirse a normas éticas a un código de conducta profesional para cumplir con sus objetivos de manera rigurosa teniendo ética. Este código establece una serie de principios que regulan el comportamiento ético o moral de los profesionales durante su desempeño laboral (Chicano, 2024).

2.3.1.2 Ventajas de realizar una Auditoría Informática

Las auditorías de seguridad informática son valiosas para las pymes y startups, ya que ofrecen varias ventajas para mejorar la ciberseguridad de la organización. Una de estas ventajas principales es la capacidad de identificar o solucionar vulnerabilidades de fallos en los sistemas informáticos, que pueden surgir por diversos motivos como errores humanos, técnicos o de diseño, así como fallos en equipos o programas. Al detectar estas vulnerabilidades, se puede prevenir su explotación por parte de ciberdelincuentes, proteger la información de los recursos de la organización (Gómes, 2023)

No es solo responsabilidad de grandes empresas o corporaciones. Hoy en día cualquier tipo de empresa depende de elementos, dispositivos tecnológicos para poder realizar sus procesos de negocio, por lo que es necesario que evalúe de forma periódica su seguridad. Según Ambit (2021), las principales ventajas que aporta el realizar una Auditoría de Seguridad en una empresa son:

- Reforzar los controles internos de seguridad empresarial.
- Descubre deficiencias en los sistemas de seguridad, como errores, omisiones o fallos.
- Identifica posibles conductas fraudulentas, como accesos no autorizados a datos o robos internos.
- Contribuye a eliminar los puntos débiles en materia de seguridad de la empresa, como sitios web, correo electrónico o accesos remotos.
- Facilita la supervisión de los accesos, tanto físicos como virtuales, mediante la revisión de los privilegios de acceso.
- Facilita la actualización de sistemas y herramientas.

Es esencial que toda la información recopilada durante la Auditoría esté debidamente registrada, las pruebas de la Auditoría son hechos concretos que deben ser verificables, imparciales y estar detalladamente registrados, los estándares de Auditoría están determinados únicamente por la normativa en la que nos basamos, como por ejemplo la ISO 27001, deben ser seguidos sin cuestionamiento. Se deben registrar todas las discrepancias o desviaciones identificadas durante la Auditoría, sin excepción, los hallazgos que sean conformes a los estándares estarán registrados, aunque pueden no incluirse en el informe final por razones de eficiencia (Riveros, 2021).

2.3.1.3 Tipos de Auditorías Informáticas

En una revisión de seguridad informática, se analizan diversos aspectos clave para medir la efectividad de los sistemas de una compañía. Esto implica detectar posibles vulnerabilidades, riesgos en sus redes de sistemas, asegurarse de que se cumplan las políticas y medidas de seguridad existentes, determinar las acciones requeridas para abordar cualquier problema identificado mejorar la seguridad en general. En resumen, el propósito principal es evaluar el nivel de seguridad de la organización tomando medidas para salvaguardar sus activos de información frente a posibles amenazas. La auditoría externa es llevada a cabo por personal que no forma parte de la organización, mientras que la auditoría interna es realizada por individuos que trabajan directamente para la empresa (Unir, 2022).

Es esencial determinar los objetivos que se pretenden lograr con la auditoría de seguridad, no es igual diseñar una auditoría para verificar el cumplimiento de una normativa de seguridad que realizar una auditoría técnica para evaluar el cumplimiento de políticas específicas de seguridad. Una vez definidos los objetivos, se debe planificar los pasos a seguir, seleccionar las herramientas adecuadas, establecer un calendario de actividades e identificar las áreas que serán analizadas para alcanzar dichos objetivos este proceso de planificación es fundamental para asegurar la efectividad del éxito de la auditoría (Ambit, 2021).

Para Ambit (2021), las Auditorías pueden ser de dos tipos:

1. **Internas:** Cuando son realizadas por el personal de la propia empresa.
2. **Externas:** La auditoría la hace un agente externo de la empresa.

Tomando en consideración estas reflexiones sobre el Sistema Informático, podemos afirmar que su funcionamiento óptimo requiere considerar tres aspectos esenciales: el aspecto físico, que incluye todos los dispositivos periféricos que forman parte o están conectados al ordenador; el aspecto lógico, que abarca los programas y aplicaciones que permiten la operatividad del ordenador; el aspecto humano, que se compone de las personas que trabajan con el equipo informático que son responsables de desarrollar nuevas aplicaciones para mejorar el procesamiento de datos.

2.3.1.4 Auditoría de Seguridad Física

Según Guerrón et. al (2020), dentro del ámbito de la informática, existe una categoría conocida como la dimensión física, que abarca más que simplemente los dispositivos periféricos asociados a una computadora, como monitores, teclados, impresoras y cables. Este término se refiere al entorno que rodea o incluye a una computadora, así como a la infraestructura física del Centro de Procesamiento de Datos (CPD). Sin embargo, una vez establecido este entorno, es igualmente importante garantizar que funcione de manera eficaz y esté disponible cuando se necesite, lo cual implica combinar aspectos físicos con funciones.

Para Robalino et. al (2022), la seguridad física de los sistemas informáticos se enfrenta a diversas amenazas externas, como desastres naturales o acciones humanas, que pueden perturbar su correcto funcionamiento. Para protegerse adecuadamente contra estas amenazas, es crucial realizar un análisis detallado de datos que permita tomar decisiones informadas sobre aspectos como la infraestructura de hardware, la disposición de los centros de datos, la interconexión del cableado, la supervisión de las operaciones diarias de los sistemas informáticos.

Por tanto, la protección de activos, individuos e información dentro de una organización requiere una atención especial a la seguridad física. Una auditoría de seguridad física se enfoca en identificar y evaluar los riesgos, vulnerabilidades y medidas de protección presentes en el entorno físico, su objetivo es proporcionar recomendaciones para mejorar la seguridad mitigando los riesgos (C2H, 2023).

2.3.1.5 Técnicas y herramientas en la Auditoría de la seguridad informática

Para Guerrón et. al (2020), en una auditoría se pueden utilizar diversas técnicas para obtener información. La observación implica no solo ser un espectador, sino también participar activamente para verificar que todo esté en orden. La revisión de documentos, políticas, normativas, procedimientos o contratos que proporciona una visión más clara de la situación. Asimismo, las entrevistas con el personal y los directivos, así como las consultas a técnicos o expertos, son importantes para recopilar información relevante. Es crucial realizar estas actividades de manera discreta siempre con el consentimiento del personal involucrado.

Según Robalino et. al (2022), la seguridad física implica establecer medidas de protección para salvaguardar los sistemas vulnerables frente a amenazas físicas. Esto implica la creación de barreras de protocolos que controlan como medidas preventivas ante diversas amenazas, ya sean causadas por acciones humanas o eventos naturales, como sabotajes o incendio. Por tanto, las recomendaciones para mantener la seguridad física son:

- Es esencial mantener las computadoras actualizadas y protegidas de forma constante.
- Se requiere personal técnico capacitado para administrar los sistemas informáticos.
- Es importante tener en cuenta las vulnerabilidades de los sistemas informáticos.
- Se debe implementar un control de acceso adecuado.
- Es fundamental restringir el acceso a personal no autorizado.
- Se debe llevar a cabo una gestión de riesgos ante la vulnerabilidad de los equipos informáticos.

Las herramientas de seguridad informática son recursos tecnológicos creados con el propósito de proteger sistemas de computación y redes cibernéticas. Con su ayuda, es posible detectar amenazas tempranamente o desarrollar tácticas para evitar riesgos en la gestión de información, almacenamiento de datos y preservación de la privacidad (Duran, 2023).

Técnicas	• Observación de las instalaciones de sistemas, así como el cumplimiento de normativas y protocolos. • Revisión exhaustiva de documentos, políticas, normas, procedimientos de contratos de manera analítica. • Entrevistas con directivos del personal para obtener información adicional.
Herramientas	• Cuaderno de Campo. • Video Cámaras. • RAC para redes. • Servidores (En caso de que genere guardar información clasificado).
Auditor	• Revisar procedimientos, normas y políticas de la seguridad física. • Evaluar riesgo y emitir informes.

Tabla 1 Herramientas de seguridad

2.3.1.6 Prevención de equipos informáticos catástrofes naturales

Las tecnologías se presentan como un medio para mejorar las condiciones de vida de los ciudadanos impactados por desastres naturales. Pueden ser utilizadas tanto de manera preventiva, para anticipar eventos como grandes tormentas o movimientos sísmicos, como durante la emergencia misma, para guiar a los afectados. Además, los sistemas tecnológicos que usamos en nuestra vida diaria pueden resultar cruciales en situaciones de desastre. Por ejemplo, el envío de mensajes de texto con geolocalización puede contribuir a la búsqueda y rescate de personas desaparecidas. Asimismo, se ha comenzado a emplear drones para obtener imágenes aéreas que permiten identificar áreas afectadas por el desastre así facilitar las labores de intervención de ayuda (Gallo, 2020).

Con la temporada de climas en pleno auge en la posibilidad constante de desastres naturales, es crucial que las empresas, instituciones o laboratorios cuentan con planes de contingencia para proteger sus datos. ¿Por qué es tan importante salvaguardar la información en caso de desastres? Aquellas empresas que descuidan la implementación de medidas de recuperación para sus equipos electrónicos o datos esenciales que enfrentan graves consecuencias financieras cuando ocurre una emergencia. Con el fin de fortalecer la protección de sus activos, las empresas deben elegir un lugar de respaldo situado en una región geográfica distinta para disminuir la probabilidad de que un desastre afecte a ambas ubicaciones simultáneamente (TecnologiaLC, 2021).

Un plan de recuperación ante desastres y un plan de continuidad de negocio tienen el mismo objetivo: garantizar la operatividad de la empresa. Sin embargo, el primero se centra en la infraestructura informática, mientras que el segundo abarca varios aspectos como acciones de emergencia, financiamiento y comunicación. Es esencial que el plan de recuperación forme parte del plan de continuidad, especialmente para empresas donde la tecnología juega un papel fundamental. Esto asegura que, ante un desastre, la empresa pueda seguir operando mientras se restablece la normalidad (Atico34, 2022).

2.3.2 Infraestructura tecnológica

La infraestructura de tecnología de la información (TI) se refiere a los componentes necesarios para gestionar y operar entornos empresariales de TI. Puede estar basada en la nube o localizada en las instalaciones de la empresa. Estos componentes incluyen hardware, software, redes, sistemas operativos y almacenamiento de datos, utilizados para proporcionar servicios y soluciones de TI. Los productos de infraestructura de TI pueden ser implementados como aplicaciones de software que corren sobre los recursos existentes de TI, como el almacenamiento definido por software, o como soluciones en línea ofrecidas por proveedores de servicios, como la infraestructura de servicio (RedHat, 2023).

La infraestructura tecnológica engloba tanto el hardware como el software necesario para el funcionamiento efectivo de una organización, entidad o sociedad. Exploraremos en detalle qué implica, sus componentes de variedades, así como el impacto crucial de su gestión adecuada en el éxito empresarial actual. La infraestructura tecnológica ha pasado a ser el motor principal que impulsa el funcionamiento eficiente, exitoso de las organizaciones en un entorno cada vez más digitalizado. Desde pequeñas empresas hasta grandes corporaciones, desempeña un papel fundamental en la optimización de procesos, la gestión de datos, la seguridad de la información de la mejora comunicación (Castillo, 2023).

La infraestructura tecnológica comprende los recursos físicos, software, hardware, servicios de herramientas necesarios para que una organización o empresa pueda operar o ejecutar sus procesos de manera eficiente y efectiva. Este estudio se centró en desarrollar una infraestructura tecnológica para mejorar la conectividad en el Malecón de Puerto Cayo mediante la tecnología IRS (Superficie Reflectante Inteligente). Esta tecnología tiene el potencial de optimizar considerablemente el rendimiento de las redes de comunicación inalámbrica al reconfigurar de forma inteligente el entorno de propagación inalámbrica mediante el uso de elementos reflectantes pasivos masivos de bajo costo integrados en una superficie plana (Calderon, 2023).

2.3.2.1 Tipos de infraestructura de TI

En el enfoque tradicional, las empresas que poseen y manejan sus propios componentes tecnológicos dentro de sus instalaciones, centrando su atención principalmente en el hardware.

En contraste, en el modelo basado en la nube, los servicios son la piedra angular, donde los proveedores asumen la responsabilidad de administrar o gestionar la infraestructura tecnológica (Vazquez, 2024).

En la infraestructura tradicional, las empresas son responsables de gestionar todos los componentes necesarios, como centros de datos o sistemas de almacenamiento, dentro de sus propias instalaciones. Este tipo de infraestructura se considera costosa debido a la necesidad de grandes cantidades de hardware, como servidores, así como el consumo de energía y el espacio físico requeridos. En contraste, la infraestructura de nube se refiere a los recursos necesarios computación en la nube. Puede establecer una nube privada utilizando recursos dedicados exclusivamente para su uso, o utilizar una nube pública alquilando infraestructura de proveedores como Alibaba, Amazon, Google, IBM o Microsoft. También existe la opción de una nube híbrida, que combina la gestión, organización en portabilidad de cargas del trabajo en múltiples entornos de nube (RedHat, 2023).

La infraestructura hiperconvergente combina características de las infraestructuras tradicional en la nube, buscando integrar la red, el almacenamiento de los datos en una única interfaz. Al consolidar estas funciones en una plataforma definida por software, elimina la necesidad de componentes separados. Generalmente incluye un clúster de servidores básicos con almacenamiento conectado directamente, software de virtualización en una capa de gestión. A diferencia de la infraestructura en la nube híbrida, que mezcla entornos públicos y privados, la hiperconvergente se enfoca específicamente en converger computación, almacenamiento, redes de virtualización dentro de un único sistema de hardware (Wrobel, 2023).

2.3.2.2 Hiperconvergente

El concepto de infraestructura hiperconvergente (HCI) se basa en la consolidación de recursos informáticos, de almacenamiento de redes en una plataforma integrada. Este enfoque utiliza un sistema unificado que combina máquinas virtuales gestionadas a través de un hipervisor, almacenamiento definido por software o redes definidas por software. Al integrar estos recursos virtualizados, la hiperconvergencia permite una gestión centralizada desde una única interfaz. Esta tecnología simplifica la estructura de los centros de datos al reducir su complejidad y superficie, facilitando el soporte de cargas de trabajo modernas con arquitecturas de hardware estándar del sector. Gracias a la integración de informática del almacenamiento

definidos por software, la infraestructura hiperconvergente ofrece una mayor flexibilidad de eficiencia operativa (RedHat, 2020).

La hiperconvergencia, o infraestructura hiperconvergente (HCI), se refiere a un enfoque integrado que agrupa todos los componentes de un centro de datos tradicional en un sistema unificado definido por software. Esto incluye almacenamiento (discos duros), recursos informáticos (CPU y RAM), redes (switches) y gestión (software de administración). Este sistema unificado permite gestionar todos estos elementos desde un único punto de control, lo que simplifica la administración, reduce costos, elimina posibles puntos de fallo. La hiperconvergencia es especialmente relevante en entornos de alta disponibilidad, como los clústeres extendidos, donde se busca asegurar una operación continua o eficiente (Salinas, 2021).

Los sistemas de infraestructura hiperconvergente ofrecen varias ventajas significativas, entre ellas la reducción de costos operativos la disminución de la necesidad de recursos administrativos. Además, facilitan la implementación rápida de centros de datos. A diferencia de la infraestructura de TI tradicional, que se basa en múltiples unidades independientes que operan de forma aislada a menudo provienen de diferentes fabricantes, la hiperconvergencia simplifica y optimiza estos procesos. Con el avance de la virtualización, los centros de datos han experimentado una transformación notable. Esta tecnología ha permitido que los centros de datos sean mucho más eficientes y adaptables (CompuSoluciones, 2022).

2.3.2.3 Componentes principales de la infraestructura TI

Los elementos básicos de la infraestructura de tecnologías de la información se dividen en tres grupos principales: hardware, software y redes. La infraestructura tecnológica se configura a partir de una compleja red de componentes interconectados diseñados para asegurar un funcionamiento sin contratiempos eficiente. Estos elementos trabajan en conjunto para soportar y optimizar diversos procesos o servicios dentro de la organización. El software abarca sistemas operativos, aplicaciones, herramientas o programas que facilitan la operación de dispositivos y la realización de tareas. Por otro lado, los sistemas de comunicación se refieren a los medios de protocolos que posibilitan la conexión entre dispositivos y la transferencia de datos (Castillo, 2023).

Aunque estos componentes son fundamentales en la infraestructura convencional, continúan siendo relevantes incluso en entornos basados en la nube, El hardware incluye computadoras, servidores, router, centros de datos, switches, cables, instalaciones y cualquier otro equipo físico tangible (Wrobel, 2023).

Es fundamental utilizar y optimizar adecuadamente los componentes para aprovechar al máximo las ventajas de la era digital asegurándose la competitividad de las organizaciones. No existe un estándar único; cada organización debe seleccionar las soluciones que mejor se adapten a sus requerimientos. En resumen, disponer de la infraestructura adecuada permite a los empleados realizar sus tareas de manera eficiente, centralizada, proteger la información, prevenir vulnerabilidades ante desastres y reducir costos operativos (Vazquez, 2024).

2.3.2.4 La importancia de la seguridad de su infraestructura de TI

La seguridad en tecnología de la información (TI) engloba una serie de estrategias diseñadas para prevenir el acceso no autorizado a computadoras, redes y datos, asegurando así la integridad de confidencialidad de la información al evitar que los atacantes puedan acceder a ella. A medida que los métodos de ataque cibernético se vuelven más sofisticados, se vuelve cada vez más crucial proteger tus recursos digitales o dispositivos de red. Una brecha en la seguridad de tus equipos de TI puede tener serias repercusiones para tu empresa si no se asegura adecuadamente estos activos digitales de dispositivos de red (Darling, 2020).

La infraestructura tecnológica de los servicios informáticos comprende una combinación de componentes como equipos de informática, dispositivos electrónicos, redes y sistemas, entre otros. Estos componentes son gestionados a través de diversos procesos destinados a asegurar la seguridad, eficiencia y prevención. Las empresas pueden obtener grandes beneficios al contar con una infraestructura de TI, ya que esta les permite enfrentar con facilidad una amplia gama de prácticas tecnológicas. Además, podrán aprovechar tecnologías escalables seguras que garantizan la eficiencia de los procesos en la mayoría de los casos. Gracias al uso de redes, computadoras, sistemas, los usuarios pueden comunicarse y realizar diversas tareas que requieren herramientas tecnológicas (Ginzo, 2022).

La conexión entre infraestructura y seguridad informática puede asemejarse a la relación entre una casa y sus sistemas de protección. La infraestructura representa la base

esencial, similar a la estructura de una casa con sus diferentes espacios de funciones. Por otro lado, la seguridad informática se encarga de resguardar esa estructura, al igual que cerraduras, alarmas y cámaras de seguridad protegen una vivienda. La ausencia de uno de estos elementos hace que el otro sea ineficaz; una casa sin medidas de seguridad queda expuesta, mientras que las medidas de seguridad sin una estructura sólida no cumplen su propósito (Tirescue, 2024).

2.3.2.5 Riesgos en la infraestructura tecnológicas

En el entorno empresarial actual, donde la tecnología es fundamental para todas las operaciones, los riesgos asociados con la infraestructura de Tecnologías de la Información (TI) pueden tener efectos devastadores para las organizaciones. Estos riesgos pueden afectar la seguridad, la integridad y la disponibilidad de los sistemas datos empresariales, poniendo en peligro el funcionamiento continuo del negocio. Los riesgos en la infraestructura de TI abarcan amenazas y vulnerabilidades que pueden impactar los sistemas, redes o datos de una organización. Estos riesgos pueden manifestarse de diversas maneras, incluyendo ciberataques, fallos en hardware o software, errores humanos, desastres naturales de cambios en la normativa. La exposición a estos riesgos puede llevar a la pérdida de datos confidenciales, interrupciones en el servicio, daños a la reputación y pérdidas económicas importantes (GRCTools, 2024).

En cualquier organización, contar con herramientas robustas para estructurar una infraestructura tecnológica puede resultar una mayor eficiencia operativa, una mejor capacidad de respuesta, una simplificación en el mantenimiento de soporte, una reducción de costos, lo que a su vez incrementa la productividad. De esta forma, invertir en ciberseguridad no solo mejora la calidad para la empresa, sino también para sus clientes. La ciberseguridad afecta numerosos aspectos del funcionamiento empresarial, y su adecuada implementación puede ser crucial para el desarrollo exitoso de cualquier actividad (Pesantez, 2023).

Los riesgos informáticos comprenden una variedad de amenazas que pueden impactar la seguridad, integridad, disponibilidad de los sistemas de datos. Estos riesgos incluyen ciberataques realizados por hackers para robar información confidencial o interrumpir las operaciones comerciales, así como la pérdida de datos ocasionada por errores humanos, fallos en el hardware o software, desastres naturales. Además, las vulnerabilidades en la seguridad informática pueden dejar a las organizaciones expuestas a intrusiones maliciosas, las amenazas

internas, como el robo de datos por empleados descontentos, también representan un riesgo importante. Una gestión eficaz de estos riesgos es esencial para proteger la infraestructura tecnológica y asegurar la continuidad del negocio (Itsqmet, 2024).

2.3.2.6 Amenazas comunes de seguridad de la infraestructura

En el entorno empresarial contemporáneo, la tecnología es un componente crucial para el éxito y la expansión de cualquier empresa. Con la creciente sofisticación o conectividad de nuestras infraestructuras de red, también aumentan las amenazas a la seguridad, poniendo en riesgo la integridad de continuidad de las operaciones. Esta realidad subraya la importancia de adoptar medidas proactivas para salvaguardar nuestros negocios contra las ciber amenazas. La protección efectiva frente a estas amenazas no solo es fundamental para mantener la seguridad de la información de los sistemas, sino también para asegurar la estabilidad operativa de la confianza de clientes y socios. Por lo tanto, comprender o gestionar estos riesgos es vital para preservar la integridad y el crecimiento sostenido de la empresa en un entorno cada vez más digitalizado (Pulsar, 2023).

Las amenazas a la seguridad de TI pueden manifestarse de diversas maneras. Un tipo común de amenaza es el malware o software malicioso, que se presenta en varias formas para infectar dispositivos de red, Ransomware este tipo de malware secuestra datos mediante un programa dañino que limita el acceso a ciertos archivos o secciones del sistema operativo infectado exige un rescate para eliminar esta restricción. El spyware es un tipo de malware diseñado para recopilar información de una computadora y transmitirla a una entidad externa sin el conocimiento o consentimiento del usuario (Darling, 2020).

Uno de los riesgos internos más significativos para la ciberseguridad de las empresas está relacionado con los hábitos de los empleados al acceder a los sistemas. Dado que estos empleados tienen autorización para manejar la información de la empresa, incluso un pequeño descuido puede provocar una vulnerabilidad en la seguridad de los datos que terceros podrían explotar. Además, es posible que algunos empleados sean la causa directa de filtraciones de datos, ya sea de manera intencionada o accidental. Por lo tanto, es crucial capacitar a todo el personal en prácticas de seguridad cibernética para reducir las posibilidades de brechas en la seguridad (Santos, 2023).

2.3.2.7 Laboratorio escolar

Los laboratorios escolares son fundamentales porque extienden el aprendizaje más allá del aula de la teoría. Estos espacios ofrecen a los estudiantes la oportunidad de involucrarse de manera activa en el proceso educativo mediante la realización de experimentos o actividades prácticas en distintas áreas, como física, química, biología, matemáticas y tecnología. Además, los laboratorios fomentan el desarrollo de habilidades cruciales como la observación, la resolución de problemas en el pensamiento (VidaEscolar, 2023).

Según Aredes et. al (2022), el laboratorio es un espacio compartido diseñado para realizar pruebas de experimentos, equipado con las herramientas necesarias para llevar a cabo investigaciones o trabajos científicos, tecnológicos o técnicos. Este entorno cuenta con instrumentos de medición y equipos específicos que se utilizan para diversas prácticas, según el área de la ciencia correspondiente. En el contexto educativo, el laboratorio sirve como un área donde se integran la teoría de la práctica, permitiendo que los estudiantes puedan llevar a cabo experiencias que faciliten aprendizajes profundos y significativos. Puede tratarse de un aula o un área especialmente adaptada dentro de la institución para el desarrollo de actividades prácticas y otros trabajos educativos.

El empleo de laboratorios es crucial ya que ofrece a los estudiantes la oportunidad de aprender a través de la experiencia directa aplicando el método científico mediante la experimentación del ensayo. Vivir estas experiencias contribuye a un aprendizaje más significativo, este enfoque hace que el proceso educativo sea más dinámico, interesante y participativo tanto para los estudiantes como para los profesores. La informática se considera una materia esencial en la formación de los estudiantes, ya que les ayuda a entender las conexiones entre la ciencia, la tecnología, el medio ambiente de los problemas sociales actuales, así como las causas o soluciones necesarias para avanzar hacia un futuro sostenible (Quezada, 2019).

2.3.2.8 Laboratorio Informático

No hace mucho tiempo, los laboratorios de informática en los centros educativos eran considerados pilares fundamentales del entorno de aprendizaje. Sin embargo, la situación actual ha cambiado considerablemente, estos laboratorios se han convertido en un tema de gran

controversia. La misma existencia de estos laboratorios es motivo de debate. Hoy en día, muchas escuelas proporcionan un dispositivo informático a cada estudiante, aquellas que aún no lo han hecho están trabajando hacia ese objetivo.

Dado que los presupuestos son limitados y el tiempo es un recurso escaso, los laboratorios de informática se han convertido en un objetivo para la optimización de ambos aspectos. Los defensores de eliminar los laboratorios argumentan que el modelo de un dispositivo por estudiante satisface todas las necesidades informáticas ofrece una solución más eficiente a los desafíos actuales en la educación tecnológica (ViewSonic, 2023).

2.3.2.9 Seguridad en un laboratorio de informática

Delgado (2023) manifiesta que, en cualquier laboratorio, independientemente de su tipo o actividad, se maneja una gran cantidad de información que debe ser protegida o gestionada adecuadamente para asegurar su confidencialidad, disponibilidad e integridad. La seguridad de la información en el laboratorio es crucial para mantener la calidad y validez de los resultados obtenidos. La pérdida de datos o sistemas informáticos ya sea por ataques de hackers, virus, desastres naturales u otros problemas, puede poner en grave peligro la operación del laboratorio. Hoy en día, los ciberataques representan una amenaza significativa para las organizaciones que gestionan información mediante herramientas digitales o tecnología, los laboratorios no son una excepción a esta realidad.

Por tanto, es esencial adherirse a estas normas, ya que ayudan a prevenir accidentes, protegen a las personas evitan daños materiales, asegurando así un entorno de trabajo que incluye:

- Tener a mano un equipo de primeros auxilios.
- Asegurar los cables para evitar tropiezos.
- No consumir alimentos ni bebidas en el área de trabajo.
- Evitar el uso de joyas.
- Ajustar la ropa holgada.
- Prestar atención a las áreas de impresión calientes que manejan voltajes altos.

- Verificar el voltaje de salida de adaptadores de corriente y cargadores antes de conectarlos a los dispositivos.
- Tener precaución con las fuentes de energía de la PC al desensamblarla, ya que pueden ser peligrosas.

Antes de realizar cualquier mantenimiento en la computadora, desconéctala para evitar riesgos de descargas eléctricas. Limpia el interior del equipo, incluyendo los ventiladores y disipadores de calor, utilizando aire comprimido o un paño suave para eliminar el polvo y la suciedad. Revisa todos los componentes de la computadora en busca de desgaste o daños, reemplázalos si es necesario. Cualquier pieza dañada debe ser sustituida (Bolaños & Muñoz , 2024).

Una de las principales estrategias de seguridad es restringir el acceso a la información. Cuantas menos personas tengan acceso a ciertos datos, menor será el riesgo de que estos se vean comprometidos. Por ello, es esencial implementar en los centros educativos un sistema que limite el acceso a información innecesaria para ciertos usuarios, clientes, etc. Para que las medidas de seguridad informática sean efectivas, es crucial involucrar a todos los niveles de la organización, incluidos los agentes externos como clientes o proveedores. A menudo, aunque una empresa tenga sistemas de seguridad adecuados, las brechas de seguridad pueden surgir al interactuar con terceros que no cuentan con las mismas medidas de protección (Datos101, 2023).

2.4 Conclusiones del marco teórico

- La auditoría de seguridad física juega un papel fundamental en la protección de los sistemas informáticos, ya que no solo se enfoca en los dispositivos periféricos, sino también en el entorno físico que alberga estos equipos en la infraestructura del Centro de Procesamiento de Datos (CPD). Es esencial que la seguridad física combine aspectos técnicos o humanos para garantizar la operatividad y disponibilidad continua de los sistemas. Este proceso implica un análisis exhaustivo del entorno, desde la disposición de hardware hasta la interconexión del cableado, así como la supervisión de las operaciones diarias para prevenir interrupciones causadas por desastres naturales o acciones humanas.

- La protección efectiva de los activos, individuos e información dentro de una organización requiere una evaluación detallada de los riesgos o vulnerabilidades presentes en el entorno físico. Una auditoría de seguridad física tiene como objetivo identificar estas vulnerabilidades y ofrecer recomendaciones para fortalecer la seguridad de mitigar los posibles riesgos. Este enfoque integral es crucial para asegurar que todos los aspectos del entorno físico contribuyan a la protección robusta, eficiente de los sistemas informáticos permitiendo una operación continúa siendo segura.
- La infraestructura de TI ha avanzado de los modelos tradicionales a soluciones más modernas como la nube de la plataforma definida por software que combina almacenamiento, computación, conectividad de red y virtualización en un solo sistema. Mientras que el modelo tradicional requiere que las empresas gestionen su propio hardware, la infraestructura en la nube permite externalizar estos recursos a proveedores especializados, brindando flexibilidad reduciendo costos. La hiperconvergencia, integra varias funciones tecnológicas en una plataforma única, facilitando la gestión. No obstante, es crucial optimizar tanto en modelos tradicionales como en la nube para mantener una operación eficiente.
- La seguridad de la infraestructura de TI es igualmente crítica, dado que las amenazas cibernéticas pueden poner en riesgo la integridad y disponibilidad de los datos. Para proteger los recursos digitales y asegurar la continuidad del negocio, es indispensable implementar medidas de seguridad robustas manteniendo una vigilancia constante. La formación del personal el adecuado mantenimiento de los sistemas es esenciales para reducir riesgos y asegurar un entorno operativo seguro de manera eficiente.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

El marco investigativo abarca la redacción de los sucesos y eventos necesarios y suficientes para estructurar una investigación de carácter académico. Por lo tanto, debe incluir un marco de antecedentes y contenidos, junto con las respectivas conceptualizaciones e hipótesis. En esencia, el marco investigativo comprende el Marco Teórico, el Marco Referencial y el Marco Conceptual.

En relación con el Marco Teórico, este se define como la sección que presenta la información documental que fundamenta el proyecto, incluyendo contenidos basados en teorías científicas y sus respectivas definiciones, las cuales respaldan el contenido integral del estudio (Caravantes, 2020).

En síntesis, el marco investigativo del presente proyecto establece el procedimiento a seguir para la elaboración de la investigación. Expone las teorías que fundamentan la realización de una auditoría informática aplicada a la infraestructura tecnológica de un laboratorio de cómputo en una unidad educativa. Además, incorpora las referencias documentales y bibliográficas utilizadas, así como las definiciones de conceptos relacionados con las actividades y el mantenimiento de un laboratorio de cómputo. Este marco permite el desarrollo del diseño metodológico de la investigación, tras los análisis preliminares sobre la planificación del uso del tiempo y demás recursos.

3.2 Tipos de investigación

3.2.1 Investigación documental

Para Ruiz y Alvarado (2020), la investigación documental es caracterizada por recolectar, recopilar y seleccionar información de las lecturas de documentos, revistas, libros, artículos científicos, entre otros; es decir utilizar datos secundarios como fuente de información. Su propósito radica en orientar el estudio desde dos perspectivas. En primer lugar, se busca establecer conexiones entre datos preexistentes provenientes de diversas fuentes.

Posteriormente, se pretende ofrecer una visión integral y ordenada acerca de un tema específico que se encuentra disperso en múltiples fuentes.

Con base en este pensamiento, la investigación documental se utilizó para recopilar y analizar diversas fuentes bibliográficas, lo que permitió desarrollar la investigación del marco teórico del presente proyecto.

3.2.2 Investigación descriptiva

La investigación descriptiva se centra en examinar las características particulares de una población o fenómeno específico, sin explorar las relaciones o interacciones entre estas características. Este tipo de investigación suele ser el primer paso en numerosos estudios científicos, ya que ofrece una base fundamental de información sobre la cual se pueden desarrollar investigaciones más detalladas o complejas. Al ofrecer una visión clara y detallada del objeto de estudio (Rus, 2024).

Siguiendo este orden de ideas, la investigación descriptiva permitió establecer un marco de referencia esencial para describir la problemática del proyecto, lo que facilita la realización de análisis más profundos en etapas posteriores.

3.3 Métodos de investigación

3.3.1 Método deductivo

Rodríguez (2020) manifiesta que, el método deductivo se trata del estudio de un fenómeno particular basado en uno general. Este enfoque se caracteriza porque las conclusiones derivadas del razonamiento deductivo son verdaderas siempre que las premisas también lo sean.

Este método fue aplicado en el informe final relacionado con la información de la escuela Simón Bolívar, incorporando los aportes sobre los controles de riesgos, los cuales se emplearon para el desarrollo de hipótesis en el manual de buenas prácticas.

3.3.2 Método inductivo

Según Rodríguez (2020) el método inductivo permite obtener conclusiones generales a partir de premisas particulares, fundamentándose en la observación y experimentación de diversos hechos para llegar a una conclusión que abarque el conjunto de casos estudiados.

Este método fue empleado en la realización de la entrevista a la Coordinadora encargada de la Escuela Simón Bolívar, con el propósito de analizar y evaluar los niveles de riesgo relacionados con la seguridad del laboratorio de cómputo.

3.3.3 Método analítico y sintético

Los métodos analítico y sintético de investigación científica constituyen las estrategias y procedimientos empleados para recolectar información y datos útiles en el desarrollo de una investigación. Su finalidad es garantizar que los datos recopilados sean suficientes y fiables, que los resultados obtenidos sean precisos y que las conclusiones estén en consonancia con los objetivos planteados (Compilatio, 2024).

En este caso, el método fue utilizado para identificar y clasificar las causas del problema presente en el entorno de seguridad informática de la escuela Simón Bolívar. La información procesada se sintetizó en definiciones claras y conceptos precisos, necesarios para abordar los problemas identificados.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias y secundarias

3.4.1.1 Fuentes primarias

Para obtener información directa, se emplearon técnicas de recolección de datos como entrevistas y encuestas dirigidas a la coordinadora y personal docente de la escuela Simón Bolívar. Esto permitió reunir datos estadísticos y cualitativos relevantes para la investigación.

3.4.1.2 Fuentes secundarias

Se consideraron fuentes secundarias de información, libros físicos y digitales, artículos de investigación y páginas web confiables, entre otros, con el fin de construir el marco teórico e identificar los problemas de investigación. Esto permitió analizar y comprender adecuadamente las fuentes primarias de información.

3.5 Estrategia operacional para la recolección de datos

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

3.5.1.1 Población

Veiga (2020) manifiesta que, la población hace referencia a la recopilación de datos en un ámbito estadístico sobre un grupo de personas que forman parte de una investigación, con el único fin de obtener datos estadísticos para el estudio en una determinada área o ubicación geográfica.

Siguiendo esta línea de pensamiento, se delimitó una población compuesta por cinco personas, entre las cuales se incluyen los responsables del uso del laboratorio de cómputo y los directivos encargados de supervisar el área. Este enfoque garantiza que las opiniones y experiencias de los distintos participantes en el laboratorio de cómputo sean consideradas de manera equitativa, proporcionando así una visión integral de la situación actual de la seguridad informática en la Escuela Simón Bolívar.

3.5.1.2 Técnica del muestreo y tamaño de muestra

No se realizó un muestreo debido al reducido número de personas, por lo que se aplicaron los instrumentos directamente al personal docentes.

3.5.2 Análisis de las herramientas de recolección de datos a utilizar

3.5.2.1 Encuesta - Entrevista

3.5.2.1.1 Encuesta

Según Gallejo (2011), la encuesta es un instrumento estructurado para la recopilación de información, lo que puede influir en los datos obtenidos. Este método solo debe emplearse en situaciones específicas donde la información que se requiere recolectar esté organizada y estructurada dentro de la población.

En este caso, la encuesta incluyó una serie de preguntas cerradas (de tipo "Sí" o "No") relacionadas con el laboratorio de cómputo. El cuestionario constó de 10 preguntas, cuyo objetivo fue determinar los problemas de seguridad existentes en el laboratorio de cómputo para identificar posibles soluciones.

3.5.2.1.2 Entrevista

Según Hernández y González (2008), la entrevista es una técnica aplicable a todo tipo de personas, incluso aquellas que puedan presentar limitaciones, como analfabetos, personas con discapacidades físicas o aquellas que enfrenten dificultades para proporcionar respuestas escritas.

La entrevista fue realizada a la Coordinadora, consistiendo en una serie de 10 preguntas estructuradas con respuestas abiertas. Este enfoque facilitó la obtención de información más detallada sobre el establecimiento, centrada en la gestión de las prácticas de seguridad informática en el laboratorio de cómputo. El objetivo fue investigar si la autoridad de la institución está al tanto de los problemas de seguridad existentes en el laboratorio y cómo se procede en relación con estos.

Al permitir respuestas abiertas, se logró captar una visión más completa de los desafíos asociados con los procedimientos actuales, proporcionando una base sólida para identificar áreas de mejora y desarrollar estrategias efectivas para reforzar la seguridad en el entorno educativo de la escuela Simón Bolívar.

3.5.2.2 Estructura de los instrumentos de recolección de datos aplicados

3.5.2.3 Estructura de la entrevista

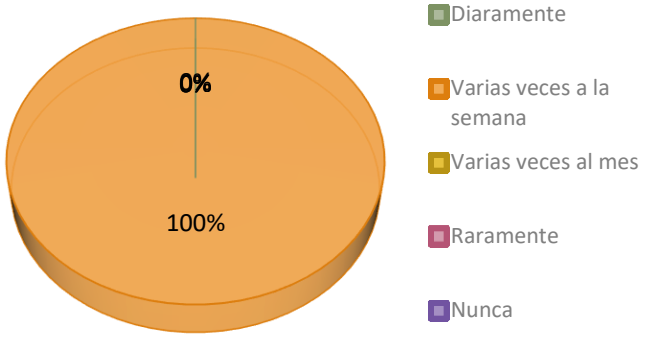
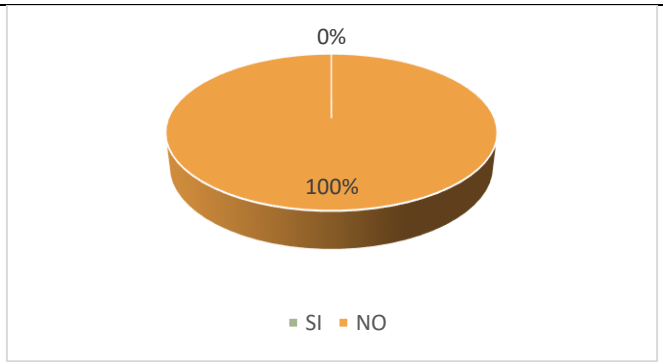
Se elaboró una entrevista compuesta por 10 preguntas abiertas, dirigida a la Coordinadora Lic. Karina Intriago Moreira de la Escuela Simón Bolívar.

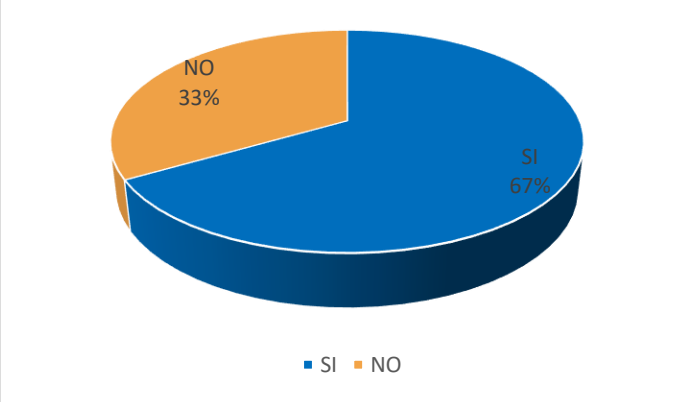
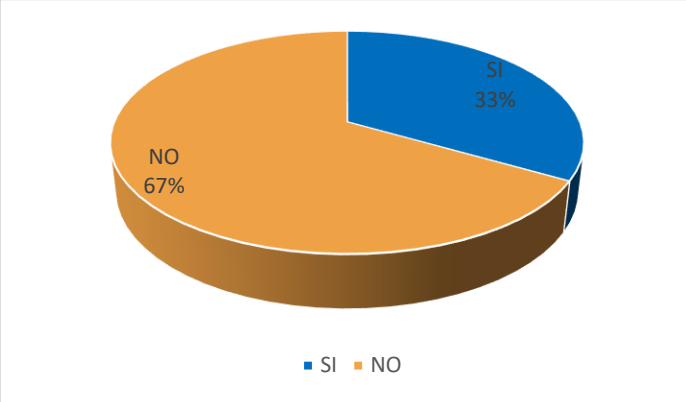
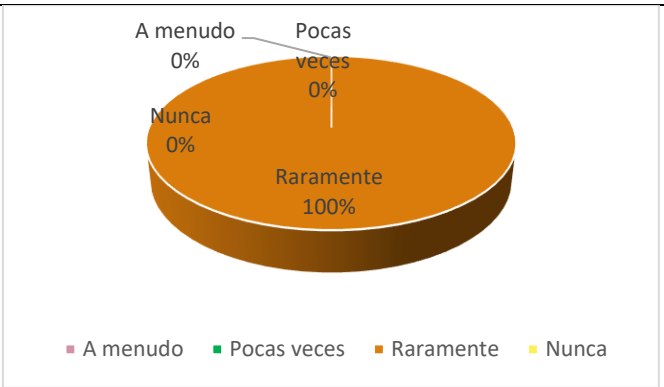
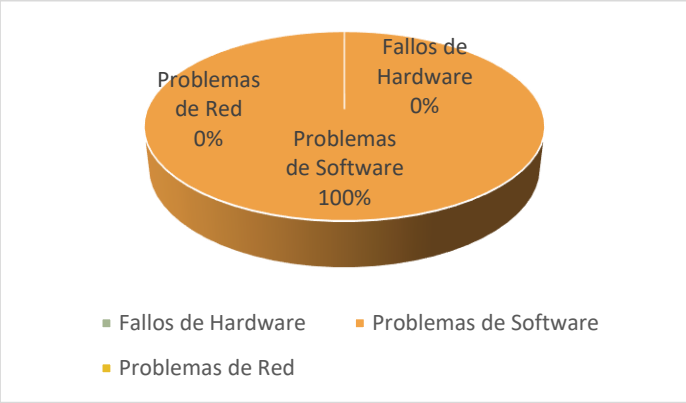
3.5.2.4 Estructura de la encuesta

La información recolectada provino de la Coordinadora y del personal docente de la institución. Se les realizó un total de 10 preguntas, a partir de las cuales se obtuvo la base para implementar el proceso de auditoría. Por tanto, la entrevista se llevó a cabo de manera presencial.

3.6 Análisis y presentación de resultados

3.6.1 Tabulación y análisis de los datos de las encuestas realizadas

Pregunta	Grafico	Interpretación
1. ¿Con que frecuencia utiliza el laboratorio de cómputo en sus clases?		La totalidad de los encuestados manifestó que utiliza el laboratorio varias veces a la semana.
2. ¿Ha tenido dificultades para utilizar el laboratorio de cómputo?		La totalidad de los encuestados manifestó que no tiene dificultad para utilizar el laboratorio.

3. ¿Reportan o informan sobre los problemas encontrados en el laboratorio de cómputo?		Una sexta aparte de los encuestados manifestó que informan los problemas del laboratorio.
4. ¿Hay personal técnico para mantenimiento del laboratorio de cómputo?		Una sexta parte de los encuestados respondió que no hay personal técnico de mantenimiento
5. ¿Con que frecuencia reportan sobre los problemas técnicos de los equipos del laboratorio a los responsables de mantenimiento?		La totalidad de los encuestados raramente reportan problemas técnicos.
6. ¿Qué tipo de problemas técnicos ha experimentado más a menudo en el laboratorio de cómputo?		La totalidad de los encuestados tiene problemas de software.

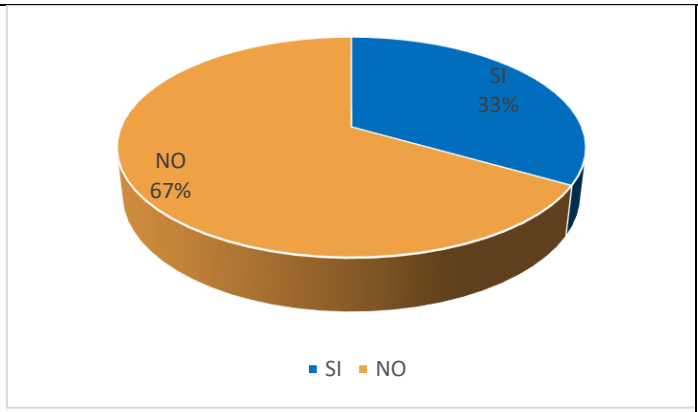
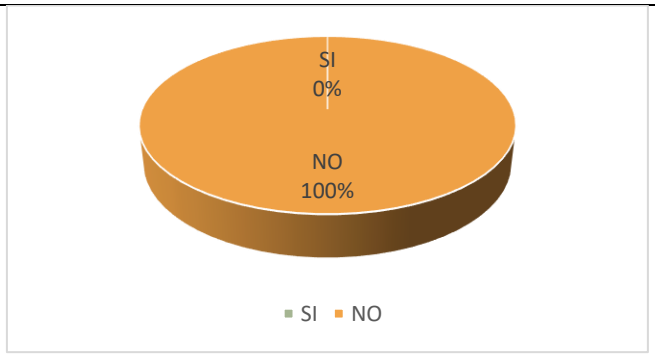
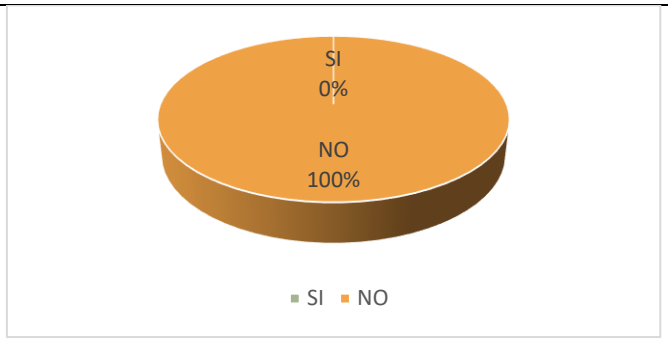
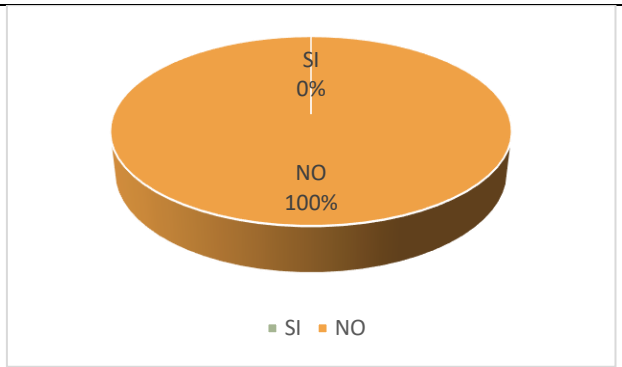
7. ¿Ha recibido capacitación sobre el uso de los equipos?		Una sexta parte de los encuestados respondió que no ha recibido capacitación sobre los equipos.
8. ¿Cuenta con personal de apoyo para el uso del laboratorio?		La totalidad de los encuestados no cuenta con personal de apoyo para el uso de los laboratorios.
9. ¿Conoce usted si el laboratorio ha tenido problemas de humedad durante las épocas de lluvia?		La totalidad de los encuestados no tiene problemas de humedad en épocas de lluvia.
10. ¿Reciben los profesores socialización de las autoridades sobre el Reglamento y políticas sobre el uso del laboratorio?		La totalidad de los encuestados no recibieron la socialización de las autoridades de las políticas sobre el uso del laboratorio.

Tabla 2 Análisis y presentación de resultados de la encuesta

3.6.2 Presentación y análisis de datos de las entrevistas realizadas

Pregunta	Respuesta	Interpretación
1. ¿Conoce usted la frecuencia con la que los docentes utilizan el laboratorio de cómputo para preparar e impartir sus clases?	Las maestras diariamente y los estudiantes varias veces a la semana.	La coordinadora manifiesta que los estudiantes tienen que recibir más clases y solo se los lleva a los estudiantes al laboratorio cuando hay que despejar la mente.
2. ¿Recibe usted frecuentemente reportes sobre dificultades de los docentes para utilizar el laboratorio de cómputo?	No tengo frecuentemente reportes de las docentes.	No tiene reportes frecuentes de dificultad del laboratorio la coordinadora de la Institución.
3. ¿Qué tipos de problemas son los que los profesores le informan a usted?	Cuando se acaba la tinta de la impresora y cuando se acaba la licencia de Microsoft.	Manifiesta la coordinadora que más información tiene cuando se acabó lo material, más no lo interno del laboratorio.
4. ¿Cuenta la institución con personal técnico para mantenimiento del laboratorio de cómputo?	La institución no cuenta con personal técnico se le comunica al Distrito y envía un encargado en el área de Sistemas.	No cuenta con personal técnico de mantenimiento la Institución.
5. ¿Se realizan frecuentemente labores de mantenimiento al laboratorio de cómputo?	No, es raramente que se le da mantenimiento cuando surge algún inconveniente, en lo que es limpieza sí.	Muy pocas veces se le da mantenimiento al laboratorio.
6. ¿Cuenta la institución con personal de apoyo a los	No cuenta con personal de apoyo la Institución.	No cuenta con personal de apoyo porque no se requiere ya que el

docentes para el uso del laboratorio?		laboratorio es para visualizar más no para utilizarlo.
7. ¿Da la institución capacitación a los docentes sobre los equipos y sobre políticas de seguridad?	No recibe capacitación las docentes, porque lo que se realiza es brindarles videos emotivos a los estudiantes.	No recibe capacitación los docentes, ellos se informan por su propia cuenta lo que desea saber es personal.
8. ¿Qué procedimientos existen para la actualización y reemplazo de equipos obsoletos o dañados en el laboratorio de cómputo?	El procedimiento que se da es que se le reporta al Distrito y ellos tiene el inventario de los equipos obsoletos.	Todo el equipo que ya no se utilice lleva un inventario el Distrito para tener constancia de aquello.
9. ¿Cuenta la institución con algún reporte de humedad en las épocas de lluvia?	En época de lluvia moja una parte de la pared.	Cuando llueve moja la pared, pero solo queda húmeda la pared.
10. ¿Se socializa con los profesores el reglamento y políticas sobre el uso del laboratorio?	Si se socializó los reglamentos, más no políticas.	Los reglamentos fueron socializados, más no políticas de seguridad.

Tabla 3 Resultado entrevista

3.6.3 Presentación y descripción de los resultados obtenidos

El propósito de esta investigación fue identificar los problemas existentes y proponer soluciones para optimizar el manejo del laboratorio de cómputo en la Escuela Simón Bolívar. A través de entrevistas y encuestas, se evaluaron aspectos relacionados con la seguridad y los riesgos presentes en el entorno escolar.

Con base en los resultados obtenidos de las preguntas 1 y 3 de la entrevista, así como la pregunta 1 de la encuesta, se determinó que la mayoría de los usuarios accede al laboratorio varias veces por semana. En este sentido, la coordinadora del establecimiento, la Lic. Karina

Intriago, señaló que los docentes reportan únicamente el material en desuso, sin abordar cuestiones internas del laboratorio.

En relación con las preguntas 4 y 6 de la entrevista y la pregunta 4 de la encuesta, se identificó que existe personal técnico encargado del mantenimiento del laboratorio. Según la coordinadora, los reportes se envían al Distrito de Educación, entidad responsable de revisar el estado de las computadoras y garantizar que estén aptas para su uso por los estudiantes.

Respecto a la pregunta 3 de la encuesta, una sexta parte de los encuestados indicó que informa sobre los problemas encontrados en el laboratorio. Sin embargo, la coordinadora mencionó que recibe reportes únicamente relacionados con el agotamiento de insumos, como la tinta, y no sobre fallos en el funcionamiento del equipo.

En cuanto a la pregunta 4 de la encuesta, una sexta parte de los participantes manifestó la ausencia de personal técnico dentro del laboratorio. No obstante, la coordinadora aseguró que el Distrito de Educación está disponible para resolver cualquier inconveniente que surja.

Finalmente, en la pregunta 7 de la encuesta, una sexta parte de los encuestados indicó no haber recibido capacitación en el uso de los equipos. La coordinadora explicó que no se considera necesaria dicha capacitación, dado que los estudiantes, al ser de nivel inicial, utilizan videos intuitivos como parte de su aprendizaje.

3.6.4 Informe final del análisis de los datos

El análisis de los datos evidencia problemas críticos relacionados con la seguridad y el mantenimiento del laboratorio de informática de la Escuela Simón Bolívar. Aunque el acceso frecuente de los usuarios refleja la importancia del laboratorio, se identificó una falta de políticas claras y reportes efectivos sobre fallos técnicos y necesidades de mantenimiento.

La presencia de personal técnico es limitada y depende del Distrito de Educación, lo que retrasa la solución de problemas, mientras que los riesgos de infraestructura, como cables expuestos y equipos vulnerables a daños por factores climáticos, permanecen sin atención adecuada.

Adicionalmente, se destaca la ausencia de capacitación para el uso óptimo de los equipos, lo que afecta la eficiencia del laboratorio. La coordinación actual prioriza el reporte de materiales en desuso, pero no aborda aspectos internos ni la actualización de los sistemas informáticos, lo que incrementa la exposición a ciberataques y daños físicos.

Por tanto, en base a los resultados obtenidos por parte de la encuesta y entrevista, dejaron en manifiesto que la problemática radica en que la gestión del laboratorio no cuenta con controles de acceso, programas de capacitación, medidas de seguridad para la infraestructura y un plan de mantenimiento preventivo más riguroso y constante.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

El presente proyecto aborda una auditoría informática de la infraestructura del laboratorio de cómputo en la Escuela Básica General Simón Bolívar. El objetivo principal es evaluar los controles relacionados con el nivel de seguridad física dentro de la institución, utilizando la metodología MAGERIT.

Los servicios analizados se encuentra la infraestructura de clave pública, identificando riesgos asociados a ciberataques que podrían comprometer información sensible en el contexto educativo. Dichos riesgos incluyen la pérdida de datos y la retención indebida de información por parte de terceros no autorizados, quienes podrían acceder de manera rápida a la información institucional (Gómez, 2012).

La seguridad física es un elemento esencial para la protección de los equipos tecnológicos, ya que garantiza un entorno seguro para toda la comunidad educativa. Este marco propositivo tiene como finalidad evaluar las medidas de gestión de riesgos presentes en el establecimiento, identificando vulnerabilidades actuales y proponiendo soluciones prácticas para mitigarlas.

El análisis incluye aspectos como el control de acceso, la vigilancia, el mantenimiento de los equipos y la infraestructura en general, con énfasis en la identificación de puntos críticos susceptibles de ser explotados tanto por amenazas externas como internas. Asimismo, se busca asegurar que las políticas y prácticas de seguridad sean comprensibles y aplicables para todos los usuarios, fomentando un entorno colaborativo y seguro.

La implementación de estos principios de auditoría no solo contribuirá a reducir el riesgo de incidentes de seguridad, sino que también fortalecerá la confianza en el uso de las tecnologías dentro del entorno educativo. Una infraestructura física segura resulta fundamental para el correcto funcionamiento y la mejora continua del laboratorio de cómputo, garantizando que los recursos tecnológicos estén siempre disponibles para el proceso de enseñanza-aprendizaje.

Entre las recomendaciones propuestas se incluye la limpieza regular de los dispositivos, la actualización oportuna del software y la instalación de anclajes de seguridad para prevenir robos. Además, se sugiere establecer un sistema de monitoreo continuo que permita detectar y resolver problemas técnicos antes de que generen interrupciones significativas en el uso de los equipos. Finalmente, la realización de capacitaciones regulares sobre cómo responder ante emergencias contribuirá a que todos los usuarios estén preparados para actuar de manera segura y efectiva.

4.2 Descripción de la propuesta

El propósito de este proyecto es desarrollar una aplicación de auditoría que facilite la evaluación de la Institución Educativa Simón Bolívar. Este proyecto pone énfasis en la seguridad, considerándola como un medio de prevención frente a posibles riesgos externos. Además, se abordan aspectos relacionados con desastres naturales que podrían causar daños en el laboratorio, afectando incluso la estructura de la pared adyacente, donde se encuentra asignado otro curso.

4.3 Determinación de recursos

4.3.1 Humanos

El uso del recurso humano, con el apoyo adecuado, permitirá a la investigación agilizar los procesos necesarios para la mejora de la infraestructura.

Cantidad	Recursos	Función	Actividad
1	Domínguez Zambrano Merly Mishelle	Investigadora	Realizar el proyecto integrador.
1	Lic. Karina Intriago Moreira.	Coordinadora de la Institución	Persona que se le realizó la entrevista para el diagnóstico de la investigación.

3	Docentes	Profesoras de nivel, primero de básica	Participaron respondiendo a la encuesta sobre la seguridad del laboratorio.

Tabla 4 Recursos Humanos

4.3.2 Tecnológicos

El uso del recurso tecnológico permitirá la recaudación de los equipos necesarios para desarrollar la actividad propuesta del proyecto.

Cantidad	Recursos	Actividad
1	Computadora portátil	Equipo personal para realizar el proyecto.
1	Teléfono móvil	Utilizado para fotografiar la evidencia de toda el área de investigación.
50	Hojas de impresión	Investigación detallada.
2	Programa de Office	Utilizando Word para le equitación del proyecto.
1	Conexión a Internet	Plan de Claro para cubrir y consultar la información respaldándola a todo momento.

Tabla 5 Recursos Tecnológicos

4.3.3 Económicos

El uso de los recursos económicos facilitará la adquisición de materiales necesarios para la realización del proyecto, satisfaciendo las necesidades de la institución y permitiendo impartir las clases sin inconvenientes.

Cantidad	Descripción	Precio Unitario	Subtotal
1	Laptop portátil, para resguardar la información adquirida.	$ 600	$600
1	Teléfono móvil, para la cámara y audio de información recolectada en la Institución.	$ 200	$200
60	Hojas de impresión, necesarias para documentar toda la información requerida.	$0,20	$12,00
6 meses	Plan de datos, culminar la información recaudada del proyecto.	$25	$150
2	Pasaje, movilidad de la Institución.	$2	$4,00
		TOTAL	**$966,00**

Tabla 6 Recursos Económicos

4.4 Etapas del desarrollo de la propuesta

El control de diversos recursos es necesario para la mejoría de la institución como elemento fundamental en su desarrollo actual y consistente teniendo la cooperación de los recursos humano que facilita su observación dentro de lo planificado equivaliendo la

información de la Coordinadora y de las docentes apoyando con su participación en la información del desarrollo para su crecimiento de reforzar la seguridad de quienes rodean la Institución.

4.4.1 Datos informativos

Nombre de la Institución:	ESCUELA DE EDUCACIÓN GENERAL BÁSICA "SIMÓN BOLÍVAR"
Código Amie	13H01465
Ubicación Geográfica	Rural
Zona	4
Distrito	13D05
Provincia	Manabí – El Carmen
Dirección de ubicación	Recinto San Luis de Cajones
Fundada	1 de octubre de 1973
Niveles Educativos	Educación primaria
Carácter	Fiscal
Jornada	Matutina
Género	Mixto
Número de Estudiantes	63
Número de Docentes	3
E-mail	d13h01465sb@gmail.com

Tabla 7 Datos de la Escuela Simón Bolívar

4.4.1.1 Misión de la Escuela General Básica Simón Bolívar

La Institución Educativa Simón Bolívar del sitio San Luis de Cajones, Provincia Manabí oferta los niveles de Preparatoria, Elemental y Educación General Básica Media, proporcionado una educación de excelencia basada en principios éticos y valores, que fomente el amor por el aprendizaje, la creatividad, la autonomía y la responsabilidad.

4.4.1.2 Visión de la Escuela General Básica Simón Bolívar

La Institución Educativa Simón Bolívar, será una institución líder, reconocida a nivel local y regional formando a través de un enfoque pedagógico innovador y participativo, valorando la diversidad y promoviendo la inclusión, brindando igualdad de oportunidades para que cada estudiante alcance su máximo potencial. Nuestro compromiso es cultivar el desarrollo integral de nuestros estudiantes, preparándolos para ser líderes proactivos y contribuir positivamente a la sociedad.

4.4.1.3 Organigrama

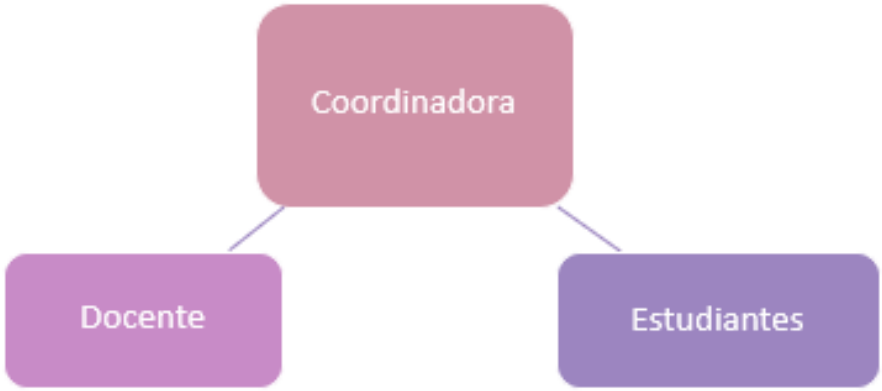


Ilustración 2 Organigrama de la Escuela General Básica Simón Bolívar

4.4.2 Programa de Auditoría Informática

4.4.2.1 Planificación

PROGRAMA DE AUDITORÍA INFORMÁTICA DE SEGURIDAD DE LA INFORMACIÓN		
OBJETIVOS: • Analizar los riesgos de seguridad actual de la Escuela General Básica Simón Bolívar. • Identificar el nivel de seguridad de la infraestructura tecnológica del laboratorio de cómputo que dispone la Escuela.		
TÉCNICAS Y PROCEDIMIENTOS	REFERENCIA	FECHA
1.1 Revisión bibliográfica de seguridad, normas, leyes y políticas.	A1	15/09/2024
1.2 Investigar la metodología Magerit, sus fases ejecutarlas.	A2	15/09/2024
1.3 Identificar o Definir activos y valorarlos.	B1	15/09/2024
1.4 Identificar o Definir amenazas.	B2	01/10/2024
1.5 Realizar el diseño de Instrumento.	C1	03/10/2024
1.6 Ejecución de Auditoría, entrevistar a la Coordinadora, Inspeccionando a la Escuela Simón Bolívar.	C2	03/10/2024
1.7 Tabulación y análisis de datos.	D1	10/10/2024
2 valoración de riesgo (Matriz de riesgo).	F1	24/10/2024
2.1 Políticas de seguridad.	F2	24/10/2024
3 elaborar Informe.	G1	31/10/2024

Tabla 8 Programa de Auditoría

4.4.2.2 Consultar Normas de Seguridad

4.4.2.2.1 ISO 27001

- **A11 Seguridad física y del entorno**

En coordinación con las medidas tecnológicas ISO 27001 se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas.

Áreas seguras	Descripción
11.1.1 Perímetro de seguridad física	Los perímetros y controles previstas deben determinarse en un análisis o evaluación de riesgo. Los requisitos de seguridad física deben tener en cuenta los niveles de protección: • Vallas • Alarmas • Protección de ventanas • cerraduras
11.1.2 Controles de acceso físico	Aquellas áreas que se consideran seguras deben estar protegidas por controles de entrada que permitan solo personal autorizado: • Los visitantes deben autentificarse • Monitorización • Identificaciones
11.1.3 Seguridad de oficinas	Diseñarse para evitar el máximo posible riesgo que la información confidencial sea accesible para los visitantes.
11.1.4 Protección contra amenazas externas y del ambiente	Protección física contra factores externos, asesoramiento especializado; medidas de protección contra inundaciones, incendios y terremotos para mitigar sus efectos.

11.1.5 El trabajo en las áreas seguras	Procedimientos de trabajo: • Prohibición de trabajos sin supervisión por parte de terceros. • Revisión de las zonas a la finalización de las visitas.

Tabla 9 Seguridad física

4.4.3 Metodología Magerit

MAGERIT Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Con su ayuda mejoraremos en lo absoluto los riesgos, brindando una mejor ayuda al momento de utilizar el marco de trabajo. Por tanto, Magerit focaliza su objetivo en el análisis de los riesgos en los sistemas de seguridad informática.

4.4.3.1 Gráfico de las fases

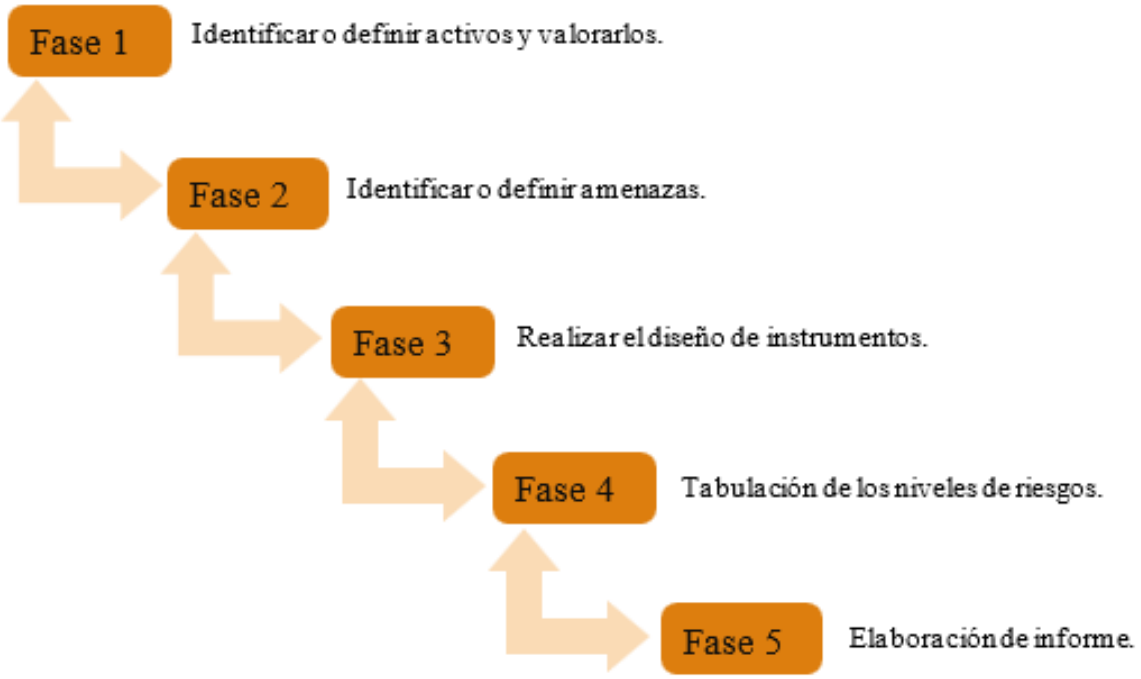


Tabla 10 Fases de Magerit

4.4.4 Aplicación de la metodología Magerit

4.4.4.1 Valor Activo

Tabla que representa los valores de los activos con números representativos de mayor a menor, describiendo que tan seguro puede ser para ubicarlos haciendo referencia al valor de Disponibilidad, Confiabilidad, Integridad que se encuentra en la parte inferior.

VA	Valor del activo	Descripción
5	Muy seguro	Si este activo deja de funcionar, no se puede cumplir con las actividades.
4	Seguro	Si este activo se paraliza temporalmente, las actividades continúan.
3	Riesgo medio	Aunque se paralice no afecta a las actividades, para el desarrollo dentro de lo escolar.
2	Riesgo considerable	Verificar a menudo para las afectaciones entre en el entorno de los activos.
1	Riesgo alto	Tomar medidas para reducir fallas en el activo.

Tabla 11 Valor Activo

4.4.4.1.1 Definir y valorar activos

Los activos físicos y lógicos de Información son los que cuenta la Escuela General Simón Bolívar, están dentro del laboratorio de cómputo.

Código	Nombre	Descripción	Valor			
			D	I	C	V.A
Pc01	Computadora de escritorio	• Monitor Led LG. • Tienen todos los documentos necesarios de los estudiantes.	5	4	4	4

Pc19	Computadora de escritorio	• Monitor Led LG. • CPU Core i3. • El disco duro:1000gb Seagate.	4	3	3	3
Rut01	Router	• Puertos USB Alfanet. • Combatividad con Wifi	4	4	4	4
Ra01	Rack	• 19 pulgadas de ancho. • Accesible y seguro.	5	4	3	4
Br02	Breaker	• Protección termomagnética. • Caja moldeada.	5	4	4	4
LS001	Impresora	• Epson L4260 Series. • Imprime de manera inalámbrica.	3	3	3	3
SO20	Sistema operativo	• Windows 11. • Ofrece paquetes de office. • Interfaz familiar y moderna.	5	4	5	5
Pr20	Programas	• Microsoft. • Canva • YouTube	4	4	4	4
AC001	Aire acondicionado	• 200 voltios.	4	4	3	3,5
Pr002	Proyector	• Espejo • Fuerza de luz Lampara	5	4	4	4

Tabla 12 Aplicación Metodología Magerit

4.4.4.2 Identificación de Amenazas

Activo	Amenaza
PCs	• Robo • Incendio • Daño de equipo • Daño por agua
Impresora	• Robo • Daños
Sistema Operativo	• Malware • Dejar de funcionar • Sin actualizaciones
Programas	• Virus • Dejar de funcionar • Daños

Tabla 13 Identificación de Amenazas

4.4.4.2.1 Analizar Riesgo

El analizar Riesgos y Calcular impactos se detalla en que tanto es confiable el Robo en la Escuela General Básica Simón Bolívar, en tanto la Integridad de Incendio con la Disponibilidad de los Daños en los equipos del laboratorio de cómputo para los estudiantes que integran la Institución.

	Confiable	Integridad	Disponibilidad	Valor de Impacto
Robo	4	4	5	4
Incendio	2	2	5	3
Daño de equipos	4	4	3	3
Daño por agua	3	4	3	3
Malware	5	4	5	4

Tabla 14 Cálculo de Impacto

4.4.4.3 Elaboración de Cuestionarios para analizar riesgos

Se realizó una encuesta a la Coordinadora Lic. Karina Intriago Moreira de la Escuela General Simón Bolívar donde se formuló 25 preguntas por cada parámetro de Robo, Incendio, Inundación, Daño de Equipo y Malware indicando una encuesta con el aplicativo de cuestionario para los riesgos que el laboratorio de computación cuenta con la infraestructura interna y externa del establecimiento.

Cuestionarios para identificar riesgos (Robo). "Controles para robo"		**C1**		
		Pag 1-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Existe personal responsable de la seguridad en la Institución?			
2	¿Existe vigilancia por medio de cámaras de seguridad en el laboratorio?			
3	¿Existe un control biométrico para acceder al laboratorio?			
4	¿Se utilizan tarjetas de autenticación para registrar entrada y salida en el laboratorio?			
5	¿Existe un registro de las personas que ingresan al laboratorio?			
6	¿Los equipos de cómputo están asegurados físicamente con anclajes?			
7	¿Se realizan inventarios regular de los equipos y dispositivos del laboratorio?			
8	¿El personal o usuarios reciben capacitaciones en seguridad física para el laboratorio?			
9	¿Hay sistemas de detección de movimientos instalados en el laboratorio de computación?			
10	¿Cuenta la Institución general Básica Simón Bolívar con el sistema infla rojo?			
11	¿Se utilizan mecanismos de bloqueo automático para las puertas en la Institución General Básica Simón Bolívar?			

12	¿Se han realizado evaluaciones de riesgo de seguridad recientemente en el laboratorio?			
13	¿Se han realizado mantenimiento a las cámaras de seguridad en la Institución General Básica Simón Bolívar?			
14	¿Se cuenta con iluminación adecuada en el laboratorio de cómputo?			
15	¿El laboratorio de cómputo da al exterior de la calle?			
16	¿Existe documentación de políticas contra robos en la Institución General Básica Simón Bolívar?			
17	¿Se han realizado simulacros contra robos en la Institución General Básica Simón Bolívar?			
18	¿Se supervisan las áreas donde almacenan los dispositivos de mantenimiento en el laboratorio?			
19	¿El laboratorio tiene instalado alarmas de seguridad?			
20	¿Qué tipo de alarma de seguridad tiene?			
21	¿Se controla el ingreso a personas no autorizadas al laboratorio?			
22	¿Se cuenta con vigilancia las 24 horas en la Institución General Básica Simón Bolívar?			
23	¿Ha sufrido algún robo el laboratorio de cómputo en algún periodo del año?			
24	¿La puerta del laboratorio de cómputo cuenta con puerta eléctrica?			
25	¿El equipamiento que está con anclaje está 100% seguro en el laboratorio de cómputo?			

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 15 Cuestionario de Robo

Cuestionarios para identificar riesgos (Incendio). "Controles para Incendio"		C1 Pag 2-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Los equipos electrónicos están conectados a tomas de corrientes con protección contra sobretensiones en el laboratorio de cómputo?			
2	¿Se mantiene limpio y libres de obstrucciones los sistemas de ventilación y conductos?			
3	¿Están almacenadas de manera segura y etiquetadas los materiales inflamables?			
4	¿Hay materiales aislantes de incendio en la Institución General Básica Simón Bolívar?			
5	¿Los muebles y equipos están fabricados con materiales retardantes de incendio en el laboratorio?			
6	¿Se realiza una evaluación regular de riesgos de incendio en el laboratorio?			
7	¿Hay personal designado y entrenado para manejar emergencias de incendio?			
8	¿Tiene regulador de voltaje en la Institución General Básica Simón Bolívar?			
9	¿Las instalaciones están en buen estado en el laboratorio de cómputo?			
10	¿Dan mantenimiento a las instalaciones eléctricas en el laboratorio de cómputo?			
11	¿La energía en el sector es estable en la Institución General Básica Simón Bolívar?			
12	¿Se han realizado procedimientos de primeros auxilios en caso de emergencia?			
13	¿Se ha instalado iluminación de emergencia adecuada para guiar la evacuación en caso de apagones en el laboratorio de cómputo?			

14	¿Los equipos quedan apagados al finalizar su labor en el laboratorio de cómputo?			
15	¿Realizan simulacros contra incendio en la Institución General Básica Simón Bolívar?			
16	¿Cuenta con extintor de incendio en la Institución General Básica Simón Bolívar?			
17	¿Se dispone con una alarma de incendio en la Institución General Básica Simón Bolívar?			
18	¿El laboratorio de computación cuenta con aire acondicionado?			
19	¿Existen normativas contra incendio en la Institución General Básica Simón Bolívar?			
20	¿Los cables, los conectores se encuentra en mal estado en el laboratorio de cómputo?			
21	¿Ha encontrado repelados los cables del laboratorio de cómputo?			
22	¿Los conectores están al alcance de los niños en el laboratorio de computación?			
23	¿Los estudiantes tienen opción de encender los equipos en el laboratorio de computación?			
24	¿Se vigila durante la jornada que ningún estudiante manipule los equipos dentro del laboratorio de cómputo?			
25	¿Cuenta con regulador de voltaje en la Institución General Básica Simón Bolívar?			

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 16 Cuestionario de Incendio

Cuestionarios para identificar riesgos (Equipos). "Controles para daño de equipo"		C1 Pag 3-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Hay inventario de los equipos en buen estado en el laboratorio de cómputo?			
2	¿Se realizan inspecciones para comprobar el estado de los equipos en el laboratorio de cómputo?			
3	¿Los equipos cuentan con protección sobre tención eléctrica?			
4	¿Se prohíbe el consumo de alimentos y bebidas cerca de los equipos en el laboratorio de cómputo?			
5	¿Las computadoras del laboratorio de cómputo tienen cierto tiempo al momento de encender?			
6	¿El aire acondicionado lo utilizan cuando están utilizando las computadoras en el laboratorio?			
7	¿Se realizan limpieza de los periféricos periódicamente en el laboratorio de computación?			
8	¿Se realiza mantenimiento preventivo en el laboratorio de cómputo?			
9	¿Existe personal responsable para el mantenimiento de los equipos en el laboratorio de cómputo?			
10	¿El sistema de cableado está correctamente instalado en el laboratorio de cómputo?			
11	¿Los monitores están correctamente sujetados en el laboratorio de computación?			
12	¿Los equipos cuentan con sistemas antivirus en el laboratorio de computación?			
13	¿Los equipos están conectados a una red segura de Internet en la Institución General Básica Simón Bolívar?			
14	¿Los monitores están protegidas con las fundas que esta cubre el antipolvo dentro del laboratorio de computación?			

15	¿Se realizan copias de seguridad de la información de lo realizado día a día en la Institución General Básica Simón Bolívar?			
16	¿Se revisa el estado de funcionamiento de los equipos en el laboratorio de cómputo?			
17	¿Han dañado las etiquetas de identificación de los equipos en el laboratorio de cómputo?			
18	¿Las profesoras encienden las computadoras en el laboratorio de computación para que los niños no tengan dificultad?			
19	¿Los cables de los equipos están organizados dentro del laboratorio de cómputo?			
20	¿Se permite cambiar los equipos de un lado a otro dentro del laboratorio de cómputo?			
21	¿Los niños que ingresan al laboratorio de computación saben las partes de una computadora?			
22	¿El botón de encender los equipos está visiblemente en el laboratorio de cómputo?			
23	¿Los niños al momento de utilizar las computadoras pueden acceder a cualquier aplicación?			
24	¿Hay supervisión al momento de que están utilizando las computadoras en el laboratorio?			
25	¿Los estudiantes mantienen la disciplina adentro del laboratorio de cómputo?			

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 17 Cuestionario de Daño de Equipos

Cuestionarios para identificar riesgos (Agua). "Controles para daño de agua"		C1 Pag 4-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Hay pared con humedad de agua en el laboratorio de cómputo?			
2	¿Alguna vez se ha filtrado agua en el laboratorio de computación?			
3	¿Hacen inspecciones al sistema de drenaje y desagüe en la Institución General Básica Simón Bolívar?			
4	¿El laboratorio de computación tiene protección contra inundación?			
5	¿Hay desagüe en el laboratorio de computación?			
6	¿Las paredes del laboratorio de computación tiene daño por humedad?			
7	¿Existe un plan de emergencia en caso de inundación en la Institución General Básica Simón Bolívar?			
8	¿Las computadoras están a una altura alejada del suelo en el laboratorio de computación?			
9	¿El personal está capacitado en procedimientos de inundación?			
10	¿El sistema eléctrico del laboratorio está protegido contra daños por agua?			
11	¿Los tomacorrientes están altos de algún alcance que este provee en el laboratorio de computación?			
12	¿Anteriormente ha existido daños en los equipos por agua en la Institución General Básica Simón Bolívar?			
13	¿Hay goteras en el laboratorio de cómputo?			
14	¿Los cables tienen protección de cubierta en el laboratorio de computación?			
15	¿Se revisa periódicamente el sistema del aire acondicionado para evitar condensación en el laboratorio de computación?			
16	¿El laboratorio de computación cuenta con seguro contra daños por agua?			

17	¿En la Institución General Básica Simón Bolívar existe un procedimiento para evaluar daños después de un incidente de agua?			
18	¿Si en el caso del que el laboratorio de computación se inunde hay plan de reubicación temporal de los equipos?			
19	¿El sistema de alcantarillado está cerca al laboratorio de cómputo?			
20	¿El laboratorio de cómputo está ubicado en una zona propensa a inundaciones?			
21	¿Tiene medidas de prevención en inundación en el laboratorio de cómputo?			
22	¿Cuándo hay cambios climáticos permanece cerrada la puerta del laboratorio de cómputo?			
23	¿En las ventanas está protegidas contra filtraciones en caso de lluvias en el laboratorio de cómputo?			
24	¿El cielo raso está en buenas condiciones en el laboratorio de cómputo?			
25	¿Hay bidón de agua en el laboratorio de cómputo?			

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 18 Cuestionario de Inundación

Cuestionarios para identificar riesgos (Malware). "Controles para Malware"		C1 Pag 5-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Todos los dispositivos del laboratorio de computación cuentan con un software antivirus actualizado?			
2	¿Se realizan análisis periódicos de malware en todas las computadoras del laboratorio de computación?			
3	¿El personal recibe información sobre cómo identificar y evitar malware en la Institución General Básica Simón Bolívar?			
4	¿Se monitorea sitios de descarga no autorizadas en el laboratorio de cómputo?			
5	¿Está restringido el acceso a páginas en el laboratorio de cómputo?			
6	¿Se realizan copias de seguridad de la información de forma regular en el laboratorio de computación?			
7	¿Los equipos de la red están protegidos con contraseñas seguras en el laboratorio de computación?			
8	¿Se lleva un registro de los equipos informáticos en el laboratorio de cómputo?			
9	¿Se limita el acceso a ciertas funciones de los equipos para prevenir la instalación de software malicioso?			
10	¿Está restringido que puedan instalar cualquier aplicación en el laboratorio de computación?			
11	¿Está restringido que conecten dispositivos de almacenamiento en el laboratorio de computación?			
12	¿Las computadoras tienen contraseña de acceso en el laboratorio de computación?			
13	¿Se permite ingresar a las computadoras cualquier persona sin supervisión?			
14	¿Los niños tienen acceso ilimitado en el laboratorio cómputo?			

15	¿Los niños reciben formación básica sobre los riesgos de seguridad en línea en el laboratorio de cómputo?			
16	¿Tienen instrucciones claras de lo que se realiza el laboratorio de cómputo?			
17	¿Los niños saben que realizar si se encuentra con contenido inapropiado en el laboratorio de cómputo?			
18	¿Los niños saben cómo usar correctamente las aplicaciones autorizadas en las computadoras del laboratorio?			
19	¿Se les ha enseñado a los niños distinguir entre sitios web educativos y aquellos que son peligrosos en el laboratorio de cómputo?			
20	¿Se ha instruido a los niños como apagar correctamente los equipos al finalizar la jornada en el laboratorio de cómputo?			
21	¿Ha realizado recuperación de datos en el laboratorio de cómputo?			
22	¿Se ha infectado la computadora con un USB en el laboratorio de cómputo?			
23	¿Se implementa las políticas de seguridad en el laboratorio de cómputo?			
24	¿Tiene seguridad en la nube en el laboratorio de cómputo?			
25	¿Les enseñan a los niños ciberseguridad en el laboratorio de cómputo?			

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 19 Cuestionario de Malware

4.4.4.4 Aplicación de la Auditoría

Continuando con el desarrollo del proyecto se procedió a la aplicación de los instrumentos diseñados para la auditoría, para ellos se aplicaron diferentes técnicas y procedimientos; en primer lugar, se realizó una entrevista en la Escuela General Simón Bolívar a la Coordinadora la Lic. Karina Intriago Moreira.

Ilustración 3 Entrevista a la Coordinadora de la Escuela Simón Bolívar

Posteriormente se realizó una inspección de las instalaciones para verificar los controles de seguridad implementados por la Institución, brindando su veredicto en cada pregunta mencionada.

4.4.4.4.1 Ejecución

Cuestionarios para identificar riesgos (Robo). "Controles para robo"		C1 Pag 1-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Existe personal responsable de la seguridad en la Institución?	X		
2	¿Existe vigilancia por medio de cámaras de seguridad en el laboratorio?	X		
3	¿Existe un control biométrico para acceder al laboratorio?		X	
4	¿Se utilizan tarjetas de autenticación para registrar entrada y salida en el laboratorio?		X	
5	¿Existe un registro de las personas que ingresan al laboratorio?		X	
6	¿Los equipos de cómputo están asegurados físicamente con anclajes?	X		
7	¿Se realizan inventarios regular de los equipos y dispositivos del laboratorio?	X		
8	¿El personal o usuarios reciben capacitaciones en seguridad física para el laboratorio?	X		
9	¿Hay sistemas de detección de movimientos instalados en el laboratorio de computación?		X	
10	¿Cuenta la Institución general Básica Simón Bolívar con el sistema infla rojo?		X	
11	¿Se utilizan mecanismos de bloqueo automático para las puertas en la Institución General Básica Simón Bolívar?		X	
12	¿Se han realizado evaluaciones de riesgo de seguridad recientemente en el laboratorio?	X		
13	¿Se han realizado mantenimiento a las cámaras de seguridad en la Institución General Básica Simón Bolívar?	X		
14	¿Se cuenta con iluminación adecuada en el laboratorio de cómputo?	X		
15	¿El laboratorio de cómputo da al exterior de la calle?		X	

16	¿Existe documentación de políticas contra robos en la Institución General Básica Simón Bolívar?	X		
17	¿Se han realizado simulacros contra robos en la Institución General Básica Simón Bolívar?	X		
18	¿Se supervisan las áreas donde almacenan los dispositivos de mantenimiento en el laboratorio?	X		
19	¿El laboratorio tiene instalado alarmas de seguridad?	X		
20	¿Qué tipo de alarma de seguridad tiene?	X		Sirena
21	¿Se controla el ingreso a personas no autorizadas al laboratorio?	X		
22	¿Se cuenta con vigilancia las 24 horas en la Institución General Básica Simón Bolívar?	X		Cámara de Seguridad
23	¿Ha sufrido algún robo el laboratorio de cómputo en algún periodo del año?		X	
24	¿La puerta del laboratorio de cómputo cuenta con puerta eléctrica?		X	
25	¿El equipamiento que está con anclaje está 100% seguro en el laboratorio de cómputo?		X	

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 20 Diseño de Instrumento de Robo

Cuestionarios para identificar riesgos (Incendio). "Controles para Incendio"		C1 Pag 2-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Los equipos electrónicos están conectados a tomas de corrientes con protección contra sobretensiones en el laboratorio de cómputo?	X		
2	¿Se mantiene limpio y libres de obstrucciones los sistemas de ventilación y conductos?	X		
3	¿Están almacenadas de manera segura y etiquetadas los materiales inflamables?	X		
4	¿Hay materiales aislantes de incendio en la Institución General Básica Simón Bolívar?		X	
5	¿Los muebles y equipos están fabricados con materiales retardantes de incendio en el laboratorio?		X	
6	¿Se realiza una evaluación regular de riesgos de incendio en el laboratorio?	X		Por año
7	¿Hay personal designado y entrenado para manejar emergencias de incendio?		X	
8	¿Tiene regulador de voltaje en la Institución General Básica Simón Bolívar?	X		
9	¿Las instalaciones están en buen estado en el laboratorio de cómputo?	X		
10	¿Dan mantenimiento a las instalaciones eléctricas en el laboratorio de cómputo?	X		
11	¿La energía en el sector es estable en la Institución General Básica Simón Bolívar?	X		
12	¿Se han realizado procedimientos de primeros auxilios en caso de emergencia?	X		
13	¿Se ha instalado iluminación de emergencia adecuada para guiar la evacuación en caso de apagones en el laboratorio de cómputo?		X	

14	¿Los equipos quedan apagados al finalizar su labor en el laboratorio de cómputo?	X		
15	¿Realizan simulacros contra incendio en la Institución General Básica Simón Bolívar?	X		
16	¿Cuenta con extintor de incendio en la Institución General Básica Simón Bolívar?	X		
17	¿Se dispone con una alarma de incendio en la Institución General Básica Simón Bolívar?	X		
18	¿El laboratorio de computación cuenta con aire acondicionado?	X		
19	¿Existen normativas contra incendio en la Institución General Básica Simón Bolívar?	X		
20	¿Los cables, los conectores se encuentra en mal estado en el laboratorio de cómputo?		X	
21	¿Ha encontrado repelados los cables del laboratorio de cómputo?		X	
22	¿Los conectores están al alcance de los niños en el laboratorio de computación?		X	
23	¿Los estudiantes tienen opción de encender los equipos en el laboratorio de computación?		X	
24	¿Se vigila durante la jornada que ningún estudiante manipule los equipos dentro del laboratorio de cómputo?	X		
25	¿Cuenta con regulador de voltaje en la Institución General Básica Simón Bolívar?	X		

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 21 Diseño de Instrumento de Incendio

Cuestionarios para identificar riesgos (Equipos). "Controles para daño de equipo"		C1 Pag 3-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Hay inventario de los equipos en buen estado en el laboratorio de cómputo?	X		
2	¿Se realizan inspecciones para comprobar el estado de los equipos en el laboratorio de cómputo?	X		
3	¿Los equipos cuentan con protección sobre tención eléctrica?	X		
4	¿Se prohíbe el consumo de alimentos y bebidas cerca de los equipos en el laboratorio de cómputo?	X		
5	¿Las computadoras del laboratorio de cómputo tienen cierto tiempo al momento de encender?		X	
6	¿El aire acondicionado lo utilizan cuando están utilizando las computadoras en el laboratorio?	X		
7	¿Se realizan limpieza de los periféricos periódicamente en el laboratorio de computación?	X		
8	¿Se realiza mantenimiento preventivo en el laboratorio de cómputo?	X		
9	¿Existe personal responsable para el mantenimiento de los equipos en el laboratorio de cómputo?	X		Docentes
10	¿El sistema de cableado está correctamente instalado en el laboratorio de cómputo?	X		
11	¿Los monitores están correctamente sujetados en el laboratorio de computación?	X		
12	¿Los equipos cuentan con sistemas antivirus en el laboratorio de computación?	X		
13	¿Los equipos están conectados a una red segura de Internet en la Institución General Básica Simón Bolívar?	X		
14	¿Los monitores están protegidas con las fundas que esta cubre el antipolvo dentro del laboratorio de computación?	X		

15	¿Se realizan copias de seguridad de la información de lo realizado día a día en la Institución General Básica Simón Bolívar?		X	
16	¿Se revisa el estado de funcionamiento de los equipos en el laboratorio de cómputo?	X		
17	¿Han dañado las etiquetas de identificación de los equipos en el laboratorio de cómputo?	X		Algunas
18	¿Las profesoras encienden las computadoras en el laboratorio de computación para que los niños no tengan dificultad?	X		
19	¿Los cables de los equipos están organizados dentro del laboratorio de cómputo?	X		
20	¿Se permite cambiar los equipos de un lado a otro dentro del laboratorio de cómputo?		X	
21	¿Los niños que ingresan al laboratorio de computación saben las partes de una computadora?	X		
22	¿El botón de encender los equipos está visiblemente en el laboratorio de cómputo?	X		
23	¿Los niños al momento de utilizar las computadoras pueden acceder a cualquier aplicación?		X	
24	¿Hay supervisión al momento de que están utilizando las computadoras en el laboratorio?	X		
25	¿Los estudiantes mantienen la disciplina adentro del laboratorio de cómputo?	X		

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 22 Diseño de Instrumento de Controles para daño de equipo

Cuestionarios para identificar riesgos (Agua). "Controles para daño de agua"		C1 Pag 4-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Hay pared con humedad de agua en el laboratorio de cómputo?	X		
2	¿Alguna vez se ha filtrado agua en el laboratorio de computación?		X	
3	¿Hacen inspecciones al sistema de drenaje y desagüe en la Institución General Básica Simón Bolívar?	X		
4	¿El laboratorio de computación tiene protección contra inundación?		X	
5	¿Hay desagüe en el laboratorio de computación?		X	
6	¿Las paredes del laboratorio de computación tiene daño por humedad?	X		
7	¿Existe un plan de emergencia en caso de inundación en la Institución General Básica Simón Bolívar?		X	
8	¿Las computadoras están a una altura alejada del suelo en el laboratorio de computación?	X		
9	¿El personal está capacitado en procedimientos de inundación?		X	
10	¿El sistema eléctrico del laboratorio está protegido contra daños por agua?	X		
11	¿Los tomacorrientes están altos de algún alcance que este provee en el laboratorio de computación?	X		
12	¿Anteriormente ha existido daños en los equipos por agua en la Institución General Básica Simón Bolívar?		X	
13	¿Hay goteras en el laboratorio de cómputo?		X	
14	¿Los cables tienen protección de cubierta en el laboratorio de computación?	X		
15	¿Se revisa periódicamente el sistema del aire acondicionado para evitar condensación en el laboratorio de computación?	X		Por año
16	¿El laboratorio de computación cuenta con seguro contra daños por agua?		X	

17	¿En la Institución General Básica Simón Bolívar existe un procedimiento para evaluar daños después de un incidente de agua?	X		
18	¿Si en el caso del que el laboratorio de computación se inunde hay plan de reubicación temporal de los equipos?	X		
19	¿El sistema de alcantarillado está cerca al laboratorio de cómputo?		X	
20	¿El laboratorio de cómputo está ubicado en una zona propensa a inundaciones?		X	
21	¿Tiene medidas de prevención en inundación en el laboratorio de cómputo?	X		
22	¿Cuándo hay cambios climáticos permanece cerrada la puerta del laboratorio de cómputo?	X		
23	¿En las ventanas está protegidas contra filtraciones en caso de lluvias en el laboratorio de cómputo?	X		
24	¿El cielo raso está en buenas condiciones en el laboratorio de cómputo?		X	
25	¿Hay bidón de agua en el laboratorio de cómputo?		X	

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 23 Diseño de Instrumento de Inundación

Cuestionarios para identificar riesgos (Malware). "Controles para Malware"		C1 Pag 5-5		
Preguntas		**SI**	**NO**	**Observación**
1	¿Todos los dispositivos del laboratorio de computación cuentan con un software antivirus actualizado?	X		
2	¿Se realizan análisis periódicos de malware en todas las computadoras del laboratorio de computación?	X		Por año
3	¿El personal recibe información sobre cómo identificar y evitar malware en la Institución General Básica Simón Bolívar?		X	
4	¿Se monitorea sitios de descarga no autorizadas en el laboratorio de cómputo?	X		
5	¿Está restringido el acceso a páginas en el laboratorio de cómputo?	X		
6	¿Se realizan copias de seguridad de la información de forma regular en el laboratorio de computación?		X	
7	¿Los equipos de la red están protegidos con contraseñas seguras en el laboratorio de computación?		X	
8	¿Se lleva un registro de los equipos informáticos en el laboratorio de cómputo?	X		
9	¿Se limita el acceso a ciertas funciones de los equipos para prevenir la instalación de software malicioso?	X		
10	¿Está restringido que puedan instalar cualquier aplicación en el laboratorio de computación?	X		
11	¿Está restringido que conecten dispositivos de almacenamiento en el laboratorio de computación?	X		
12	¿Las computadoras tienen contraseña de acceso en el laboratorio de computación?		X	
13	¿Se permite ingresar a las computadoras cualquier persona sin supervisión?		X	
14	¿Los niños tienen acceso ilimitado en el laboratorio cómputo?	X		
15	¿Los niños reciben formación básica sobre los riesgos de seguridad en línea en el laboratorio de cómputo?	X		

16	¿Tienen instrucciones claras de lo que se realiza el laboratorio de cómputo?	X		
17	¿Los niños saben que realizar si se encuentra con contenido inapropiado en el laboratorio de cómputo?	X		
18	¿Los niños saben cómo usar correctamente las aplicaciones autorizadas en las computadoras del laboratorio?	X		
19	¿Se les ha enseñado a los niños distinguir entre sitios web educativos y aquellos que son peligrosos en el laboratorio de cómputo?	X		
20	¿Se ha instruido a los niños como apagar correctamente los equipos al finalizar la jornada en el laboratorio de cómputo?	X		
21	¿Ha realizado recuperación de datos en el laboratorio de cómputo?	X		
22	¿Se ha infectado la computadora con un USB en el laboratorio de cómputo?	X		
23	¿Se implementa las políticas de seguridad en el laboratorio de cómputo?	X		
24	¿Tiene seguridad en la nube en el laboratorio de cómputo?		X	
25	¿Les enseñan a los niños ciberseguridad en el laboratorio de cómputo?	X		

Realizado por: Mishelle Domínguez **Fecha:** 03/10/2024	**Revisado por:** Ing. Clara Guadalupe Pozo **Observación:**

Tabla 24 Diseño de Instrumento de Malware

4.4.4.5 Tabla de riesgos en el establecimiento Simón Bolívar

Riesgo de Robo	
En la puerta del laboratorio de cómputo de dicho establecimiento no cuenta con una puerta segura, es metálica tiene acceso a disponibilidad de que dañen fácilmente.	En el exterior del laboratorio de cómputo, ubicado junto a la dirección, se encuentra instalada una sirena destinada a activarse en caso de que personas no autorizadas intenten ingresar al recinto.
	

Tabla 25 Riesgo de Robo

Riesgo de Incendio	
La alarma que detecta humo dentro del laboratorio de cómputo, por si pasa algo éste da un sonido que alerta a todos.	El laboratorio de cómputo cuenta con un sólo extintor, dentro del establecimiento por si se presenta alguna novedad.
	

Tabla 26 Riesgo de Incendio

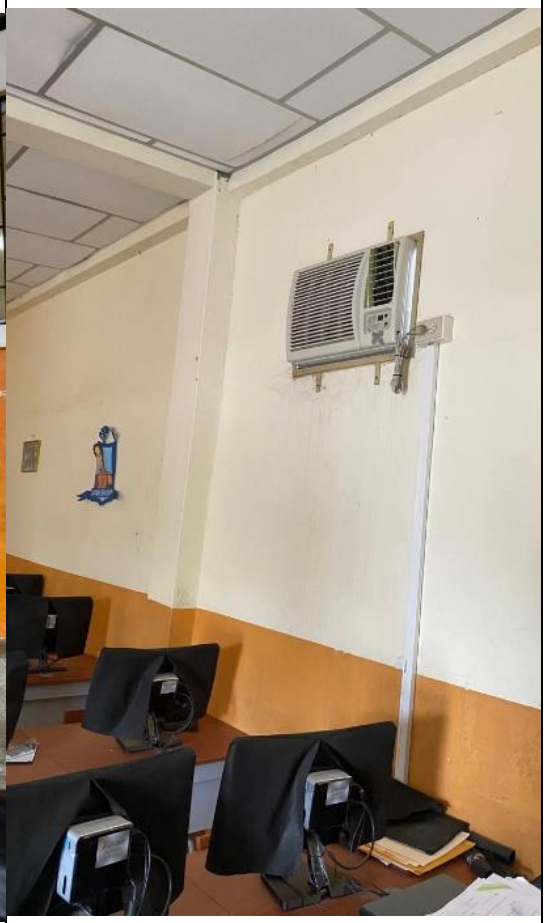
Riesgo de Inundación	
El laboratorio de computación de la Escuela Simón Bolívar tiene un alto de escalón, que hace no ingrese fácilmente agua por si hay demasiada lluvia.	El aire acondicionado está en una mala ubicación porque debajo tiene las computadoras, que están conectadas a tomas corrientes que puede afectar con un corto circuito.
	

Tabla 27 Riesgo de Inundación

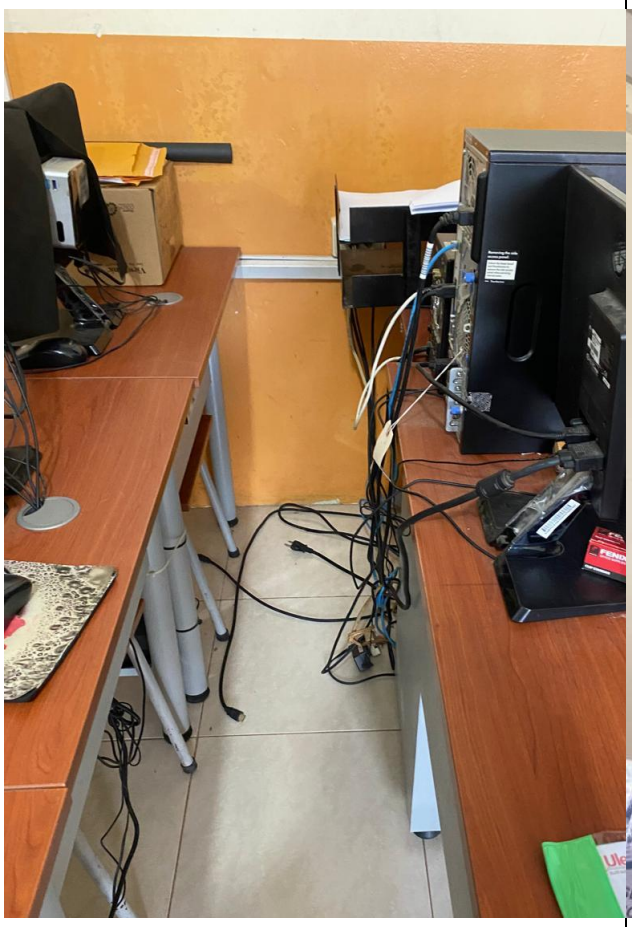
Riesgo de Daño de Equipos	
El sistema de cableado no está 100% asegurado, con anclaje puede ocasionar molestia de parte de alumno.	El Rack permanece con la llave en el seguro, puede que manipulen los cables que están dentro.
	

Tabla 28 Riesgo de Daño de Equipos

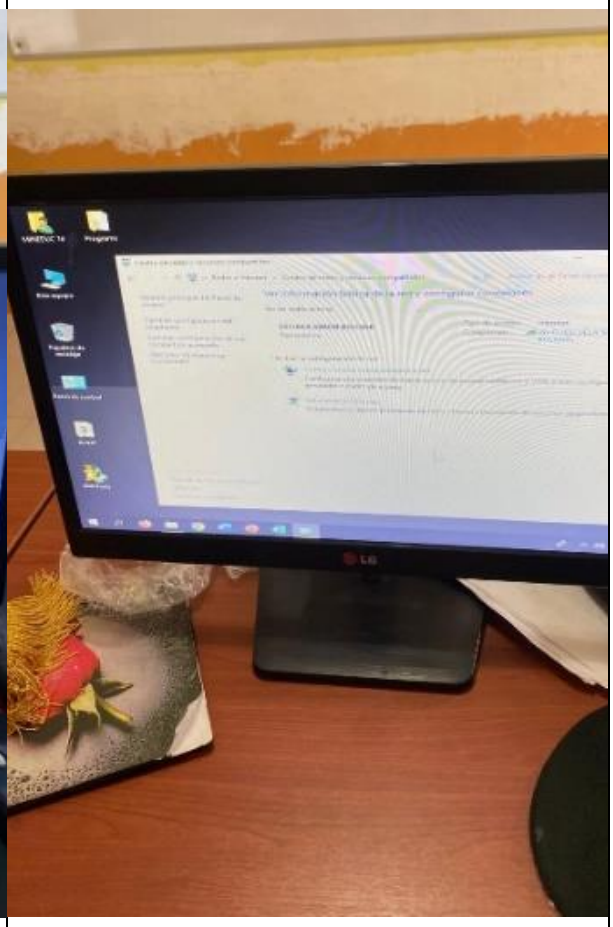
Riesgo de Malware	
Al iniciar sesión no cuenta con contraseña, impidiendo que tenga protección de información de datos.	El Internet de la Red es pública en el laboratorio de cómputo.
	

Tabla 29 Riesgo de Malware

4.4.4.6 Tabulación

Se utilizó la herramienta de Excel para tabular los datos obtenidos en el checklist de controles de seguridad en la Escuela General Simón Bolívar a docente y Coordinadora de dicha Institución.

4.4.4.6.1 Representación de los números para tabular

- 1 = Representa Seguridad, evaluando la respuesta si brinda seguridad.
- 2 = No aplica, cuando hay respuesta que no va acorde con la seguridad ni riesgo.
- 0 = Representa Riesgo, para el laboratorio de cómputo.

Fórmula	
1	Seguridad
2	No Aplica
0	Riesgo

Tabla 30 Fórmula de Tabulación

4.4.4.6.2 Evidencia de la Tabulación

	Riesgo de Robo	
Nro	**Pregunta**	**Respuesta**
1	¿Existe personal responsable de la seguridad en la Institución?	1
2	¿Existe vigilancia por medio de cámaras de seguridad en el laboratorio?	1
3	¿Existe un control biométrico para acceder al laboratorio?	0
4	¿Se utilizan tarjetas de autenticación para registrar entrada y salida en el laboratorio?	0
5	¿Existe un registro de las personas que ingresan al laboratorio?	0
6	¿Los equipos de cómputo están asegurados físicamente con anclajes?	1
7	¿Se realizan inventarios regular de los equipos y dispositivos del laboratorio?	1
8	¿El personal o usuarios reciben capacitaciones en seguridad física para el laboratorio?	1
9	¿Hay sistemas de detección de movimientos instalados en el laboratorio de computación?	0
10	¿Cuenta la Institución general Básica Simón Bolívar con el sistema inflarojo?	0
11	¿Se utilizan mecanismos de bloqueo automático para las puertas en la Institución General Básica Simón Bolívar?	0
12	¿Se han realizado evaluaciones de riesgo de seguridad recientemente en el laboratorio?	1
13	¿Se han realizado mantenimiento a las cámaras de seguridad en la Institución General Básica Simón Bolívar?	1
14	¿Se cuenta con iluminación adecuada en el laboratorio de cómputo?	1
15	¿El laboratorio de cómputo da al exterior de la calle?	1
16	¿Existe documentación de políticas contra robos en la Institución General Básica Simón Bolívar?	1
17	¿Se han realizado simulacros contra robos en la Institución General Básica Simón Bolívar?	1
18	¿Se supervisan las áreas donde almacenan los dispositivos de mantenimiento en el laboratorio?	1
19	¿El laboratorio tiene instalado alarmas de seguridad?	1
20	¿Qué tipo de alarma de seguridad tiene?	1
21	¿Se controla el ingreso a personas no autorizadas al laboratorio?	1
22	¿Se cuenta con vigilancia las 24 horas en la Institución General Básica Simón Bolívar?	1
23	¿Ha sufrido algún robo el laboratorio de cómputo en algún periodo del año?	1
24	¿La puerta del laboratorio de cómputo cuenta con puerta eléctrica?	0
25	¿El equipamiento que está con anclaje está 100% seguro en el laboratorio de cómputo?	0
	Total controles no aplica (2)	0
	Total de controles Evaluados	25
	Seguridad (1)	17
	Riesgo (0)	8
	Porcentaje de seguridad	68%
	Porcentaje de Riesgo	32%
		100%

Ilustración 4 Tabulación de Riesgo

	Riesgo de Incendio	
Nro.	**Pregunta**	**Respuesta**
1	¿Los equipos electrónicos están conectados a tomas de corrientes con protección contra sobretensiones en el laboratorio de cómputo?	1
2	¿Se mantiene limpio y libres de obstrucciones los sistemas de ventilación y conductos?	1
3	¿Están almacenadas de manera segura y etiquetadas los materiales inflamables?	1
4	¿Hay materiales aislantes de incendio en la Institución General Básica Simón Bolívar?	0
5	¿Los muebles y equipos están fabricados con materiales retardantes de incendio en el laboratorio?	0
6	¿Se realiza una evaluación regular de riesgos de incendio en el laboratorio?	1
7	¿Hay personal designado y entrenado para manejar emergencias de incendio?	0
8	¿Tiene regulador de voltaje en la Institución General Básica Simón Bolívar?	1
9	¿Las instalaciones están en buen estado en el laboratorio de cómputo?	1
10	¿Dan mantenimiento a las instalaciones eléctricas en el laboratorio de cómputo?	1
11	¿La energía en el sector es estable en la Institución General Básica Simón Bolívar?	1
12	¿Se han realizado procedimientos de primeros auxilios en caso de emergencia?	1
13	¿Se ha instalado iluminación de emergencia adecuada para guiar la evacuación en caso de apagones en el laboratorio de cómputo?	0
14	¿Los equipos quedan apagados al finalizar su labor en el laboratorio de cómputo?	1
15	¿Realizan simulacros contra incendio en la Institución General Básica Simón Bolívar?	1
16	¿Cuenta con extintor de incendio en la Institución General Básica Simón Bolívar?	1
17	¿Se dispone con una alarma de incendio en la Institución General Básica Simón Bolívar?	1
18	¿El laboratorio de computación cuenta con aire acondicionado?	1
19	¿Existen normativas contra incendio en la Institución General Básica Simón Bolívar?	1
20	¿Los cables, los conectores se encuentra en mal estado en el laboratorio de cómputo?	1
21	¿Ha encontrado repelados los cables del laboratorio de cómputo?	1
22	¿Los conectores están al alcance de los niños en el laboratorio de computación?	1
23	¿Los estudiantes tienen opción de encender los equipos en el laboratorio de computación?	1
24	¿Se vigila durante la jornada que ningún estudiante manipule los equipos dentro del laboratorio de cómputo?	1
25	¿Cuenta con regulador de voltaje en la Institución General Básica Simón Bolívar?	1
	Total controles no aplica (2)	0
	Total de controles Evaluados	25
	Seguridad (1)	21
	Riesgo	4
	Porcentaje de seguridad	84%
	Porcentaje de Riesgo	16%
		100%

Ilustración 5 Tabulación de Incendio

	Riesgo de Inundación	
Nro.	**Pregunta**	**Respuesta**
1	¿Hay pared con humedad de agua en el laboratorio de cómputo?	0
2	¿Alguna vez se ha filtrado agua en el laboratorio de computación?	1
3	¿Hacen inspecciones al sistema de drenaje y desagüe en la Institución General Básica Simón Bolívar?	1
4	¿El laboratorio de computación tiene protección contra inundación?	0
5	¿Hay desagüe en el laboratorio de computación?	1
6	¿Las paredes del laboratorio de computación tiene daño por humedad?	0
7	¿Existe un plan de emergencia en caso de inundación en la Institución General Básica Simón Bolívar?	0
8	¿Las computadoras están a una altura alejada del suelo en el laboratorio de computación?	1
9	¿El personal está capacitado en procedimientos de inundación?	1
10	¿El sistema eléctrico del laboratorio está protegido contra daños por agua?	1
11	¿Los tomacorrientes están altos de algún alcance que este provee en el laboratorio de computación?	1
12	¿Anteriormente ha existido daños en los equipos por agua en la Institución General Básica Simón Bolívar?	1
13	¿Hay goteras en el laboratorio de cómputo?	1
14	¿Los cables tienen protección de cubierta en el laboratorio de computación?	1
15	¿Se revisa periódicamente el sistema del aire acondicionado para evitar condensación en el laboratorio de computación?	1
16	¿El laboratorio de computación cuenta con seguro contra daños por agua?	0
17	¿En la Institución General Básica Simón Bolívar existe un procedimiento para evaluar daños después de un incidente de agua?	1
18	¿Si en el caso del que el laboratorio de computación se inunde hay plan de reubicación temporal de los equipos?	1
19	¿El sistema de alcantarillado está cerca al laboratorio de cómputo?	1
20	¿El laboratorio de cómputo está ubicado en una zona propensa a inundaciones?	1
21	¿Tiene medidas de prevención en inundación en el laboratorio de cómputo?	1
22	¿Cuándo hay cambios climáticos permanece cerrada la puerta del laboratorio de cómputo?	1
23	¿En las ventanas está protegidas contra filtraciones en caso de lluvias en el laboratorio de cómputo?	1
24	¿El cielo raso está en buenas condiciones en el laboratorio de cómputo?	0
25	¿Hay bidón de agua en el laboratorio de cómputo?	1
	Total controles no aplica (2)	0
	Total de controles Evaluados	25
	Seguridad (1)	19
	Riesgo	6
	Porcentaje de seguridad	76%
	Porcentaje de Riesgo	24%
		100%

Ilustración 6 Tabulación de Inundación

	Riesgo de Daño de Equipo	
Nro.	**Pregunta**	**Respuesta**
1	¿Hay inventario de los equipos en buen estado en el laboratorio de cómputo?	1
2	¿Se realizan inspecciones para comprobar el estado de los equipos en el laboratorio de cómputo?	1
3	¿Los equipos cuentan con protección sobre tención eléctrica?	1
4	¿Se prohíbe el consumo de alimentos y bebidas cerca de los equipos en el laboratorio de cómputo?	1
5	¿Las computadoras del laboratorio de cómputo tienen cierto tiempo al momento de encender?	2
6	¿El aire acondicionado lo utilizan cuando están utilizando las computadoras en el laboratorio?	1
7	¿Se realizan limpieza de los periféricos periódicamente en el laboratorio de computación?	1
8	¿Se realiza mantenimiento preventivo en el laboratorio de cómputo?	1
9	¿Existe personal responsable para el mantenimiento de los equipos en el laboratorio de cómputo?	1
10	¿El sistema de cableado está correctamente instalado en el laboratorio de cómputo?	1
11	¿Los monitores están correctamente sujetados en el laboratorio de computación?	1
12	¿Los equipos cuentan con sistemas antivirus en el laboratorio de computación?	1
13	¿Los equipos están conectados a una red segura de Internet en la Institución General Básica Simón Bolívar?	1
14	¿Los monitores están protegidas con las fundas que esta cubre el antipolvo dentro del laboratorio de computación?	1
15	¿Se realizan copias de seguridad de la información de lo realizado día a día en la Institución General Básica Simón Bolívar?	0
16	¿Se revisa el estado de funcionamiento de los equipos en el laboratorio de cómputo?	1
17	¿Han dañado las etiquetas de identificación de los equipos en el laboratorio de cómputo?	1
18	¿Las profesoras encienden las computadoras en el laboratorio de computación para que los niños no tengan dificultad?	1
19	¿Los cables de los equipos están organizados dentro del laboratorio de cómputo?	1
20	¿Se permite cambiar los equipos de un lado a otro dentro del laboratorio de cómputo?	1
21	¿Los niños que ingresan al laboratorio de computación saben las partes de una computadora?	1
22	¿El botón de encender los equipos está visiblemente en el laboratorio de cómputo?	1
23	¿Los niños al momento de utilizar las computadoras pueden acceder a cualquier aplicación?	1
24	¿Hay supervisión al momento de que están utilizando las computadoras en el laboratorio?	1
25	¿Los estudiantes mantienen la disciplina adentro del laboratorio de cómputo?	1
	Total controles no aplica (2)	1
	Total de controles Evaluados	24
	Seguridad (1)	23
	Riesgo	1
	Porcentaje de seguridad	96%
	Porcentaje de Riesgo	4%
		100%

Ilustración 7 Tabulación de Daño de Equipo

	Riesgo de Malware	
Nro.	**Pregunta**	**Respuesta**
1	¿Todos los dispositivos del laboratorio de computación cuentan con un software antivirus actualizado?	1
2	¿Se realizan análisis periódicos de malware en todas las computadoras del laboratorio de computación?	1
3	¿El personal recibe información sobre cómo identificar y evitar malware en la Institución General Básica Simón Bolívar?	0
4	¿Se monitorea sitios de descarga no autorizadas en el laboratorio de cómputo?	1
5	¿Está restringido el acceso a páginas en el laboratorio de cómputo?	1
6	¿Se realizan copias de seguridad de la información de forma regular en el laboratorio de computación?	0
7	¿Los equipos de la red están protegidos con contraseñas seguras en el laboratorio de computación?	0
8	¿Se lleva un registro de los equipos informáticos en el laboratorio de cómputo?	1
9	¿Se limita el acceso a ciertas funciones de los equipos para prevenir la instalación de software malicioso?	1
10	¿Está restringido que puedan instalar cualquier aplicación en el laboratorio de computación?	1
11	¿Está restringido que conecten dispositivos de almacenamiento en el laboratorio de computación?	1
12	¿Las computadoras tienes contraseña de acceso en el laboratorio de computación?	0
13	¿Se permite ingresar a las computadoras cualquier persona sin supervisión?	1
14	¿Los niños tienen acceso ilimitado en el laboratorio cómputo?	1
15	¿Los niños reciben formación básica sobre los riesgos de seguridad en línea en el laboratorio de cómputo?	1
16	¿Tienen instrucciones claras de lo que se realiza el laboratorio de cómputo?	1
17	¿Los niños saben que realizar si se encuentra con contenido inapropiado en el laboratorio de cómputo?	1
18	¿Los niños saben cómo usar correctamente las aplicaciones autorizadas en las computadoras del laboratorio?	1
19	¿Se les ha enseñado a los niños distinguir entre sitios web educativos y aquellos que son peligrosos en el laboratorio de cómputo?	1
20	¿Se ha instruido a los niños como apagar correctamente los equipos al finalizar la jornada en el laboratorio de cómputo?	1
21	¿Ha realizado recuperación de datos en el laboratorio de cómputo?	1
22	¿Se ha infectado la computadora con un USB en el laboratorio de cómputo?	0
23	¿Se implementa las políticas de seguridad en el laboratorio de cómputo?	1
24	¿Tiene seguridad en la nube en el laboratorio de cómputo?	0
25	¿Les enseñan a los niños ciberseguridad en el laboratorio de cómputo?	1
	Total controles no aplica (2)	0
	Total de controles Evaluados	25
	Seguridad (1)	19
	Riesgo	6
	Porcentaje de seguridad	76%
	Porcentaje de Riesgo	24%
		100%

Ilustración 8 Tabulación de Malware

4.4.4.7 Análisis de resultados

Se realizó un análisis de riesgo utilizando la matriz de riesgos.

MATRIZ DE RIESGOS				
		IMPACTO		
RIESGO	Impacto	Gravedad	Valor Riesgo	Nivel de Riesgo
Robo	4	3	12	IMPORTANTE
Incendio	3	2	6	APRECIABLE
Inundación	3	2	6	APRECIABLE
Daño de equipos	3	1	3	APRECIABLE
Malware	4	2	8	APRECIABLE

Ilustración 9 Matriz de Riesgo

Se aplicó la matriz de riesgo, considerándose el Impacto con los valores que se detallan a continuación:

Valor del impacto	Descripción
1	No se paralizan las actividades y continúan.
2	Afecta las operaciones, pero no se paralizan.
3	Cuando se paralice, pero no por tiempo prolongado.
4	Cuando se paraliza las operaciones temporalmente y afecte económicamente.
5	Cuando el riesgo paralice totalmente las actividades de la Escuela, ocasione daños a terceros.

Tabla 31 Valoración de Impacto de la Matriz de Riesgo

Se realizó un análisis de riesgo utilizando la matriz de riesgo para ello se calculó el impacto y el valor de riesgo, para la valoración de impacto se consideró desde la menor gravedad, cuando no ocasiona mayores inconvenientes en el funcionamiento de la Escuela Simón Bolívar y el quinto cuando los efectos sean altamente negativos y paralicen el tiempo prolongado las operaciones de la Institución. Para el cálculo de impacto se analizaron las dimensiones de la información calificándole con los valores anteriores.

	Confiable	Integridad	Disponibilidad	Valor de Impacto
Robo	4	4	5	4
Incendio	2	2	5	3
Daño de equipos	4	4	3	3
Daño por agua	3	4	3	3
Malware	5	4	5	4

Tabla 32 Dimensiones de Seguridad

En cuanto a la valoración de riesgo se consideró los porcentajes de los controles de riesgos Robo, Incendio, Inundación, Daño de Equipo y Malware, evaluados en cada cuestionario y se procedió a valorar con la siguiente tabla:

Valoración de Riesgo		
Valor		**Rango (riesgo)**
1	MAS BAJO	1-10%
2		11%-30
3		31%-50
4		51-75
5	MÁS ALTO	75-

Ilustración 10 Valoración de Riesgo del cuestionario

LEYENDA

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

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

Ilustración 11 Gravedad impacto

CAPÍTULO V

5 EVALUACIÓN DE RESULTADOS

5.1 Introducción

El presente capítulo corresponde al Informe detallado de la Auditoría realizada a la infraestructura tecnológica del laboratorio de cómputo en la Escuela Simón Bolívar con su respectiva guía de recomendación.

5.2 INFORME DE AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN

Tipo de Auditoría

Auditoría Informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar.

Dirigido a: Lic. Karina Intriago Moreira, Coordinadora y Docente de la Escuela Simón Bolívar.

Motivo: Trabajo de Titulación.

Objetivos:

- Analizar los riesgos de seguridad actual de la Escuela General Básica Simón Bolívar.
- Identificar el nivel de seguridad de la infraestructura tecnológica del laboratorio de cómputo que dispone la Escuela.

Personal Relacionado:

- Coordinadora
- Docente

Alcance:

Para el desarrollo de la Auditoría se aplicaron los siguientes técnicas y procedimientos:

- Revisión bibliográfica de seguridad, normas, leyes y políticas.
- Investigar la metodología Magerit, sus fases ejecutarlas.
- Identificar o Definir activos y valorarlos.
- Identificar o Definir amenazas.
- Realizar el diseño de Instrumentos.
- Ejecución de Auditoría, entrevistar a la Coordinadora, Inspeccionando a la Escuela Simón Bolívar.
- Tabulación y análisis de datos.
- Valoración de riesgo (Matriz de riesgo).
- Políticas de seguridad.
- Elaborar Informe.

5.3 Hallazgos

Como resultado relevante de la presente Auditoría se puede encontrar lo siguiente:

5.3.1 Nivel de Seguridad General

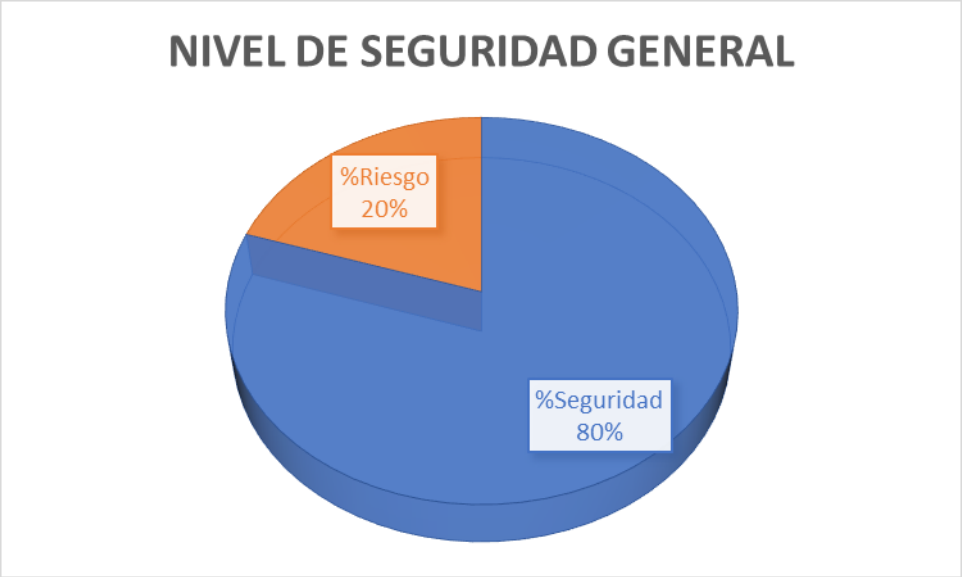


Ilustración 12 Nivel de Seguridad general

Interpretación:

El ochenta por ciento corresponde a la seguridad, indica que las condiciones evaluadas cumplen con los estándares de seguridad establecidas, lo que significa que la Escuela General

básica Simón Bolívar cumple con los criterios. El veinte por ciento corresponde a los riesgos que representa las áreas que tiende a ser problema dentro de la Escuela en seguridad física.

5.3.2 Nivel General de todos los riesgos

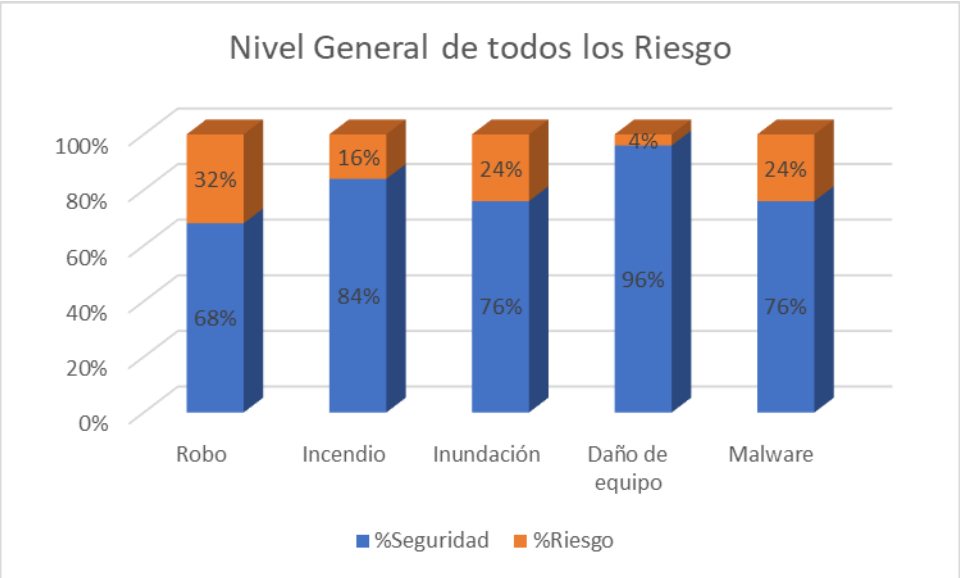
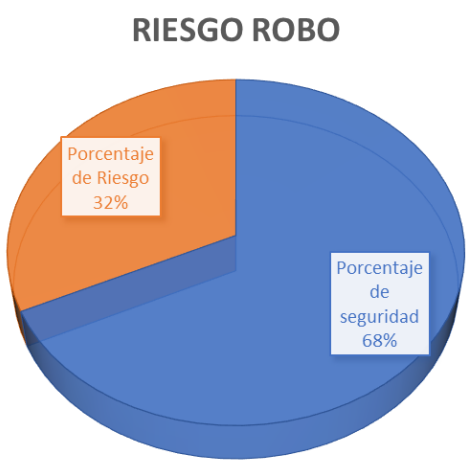


Ilustración 13 Gráfica de los controles de Riesgos

Interpretación:

De los riesgos evaluados, el laboratorio de computación presenta mayor porcentaje de exposición a sufrir un robo, puesto que se encontró un treinta y dos por ciento de incumpliendo de medidas y controles para evitarlo por otra parte, se destaca que se cumple de forma eficiente normas y políticas para evitar el daño de equipos con un noventa y seis por ciento.

5.3.3 Los riesgos identificados fueron

<table>
<tr>
<td> 
</td>
<td>Debido a:
No existe un control biométrico para acceder al laboratorio.
No se utilizan tarjetas de autenticación para registrar entrada y salida en el laboratorio.
No existe un registro de las personas que ingresan al laboratorio.
No hay sistemas de detección de movimientos instalados en el laboratorio de computación.
No cuenta la Institución General básica Simón Bolívar con el sistema infrarrojo.
No se utilizan mecanismos de bloqueo automático para las puertas en la Institución General Básica Simón Bolívar.
No cuenta con puerta eléctrica el laboratorio de cómputo.
No está el equipamiento con anclaje está 100% seguro en el laboratorio de cómputo.</td>
</tr>
<tr>
<td colspan="2">Interpretación:

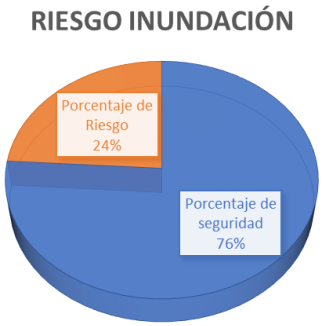
Mas de la mitad de los controles contra Robo porque cuenta la Escuela con alarma y con cámaras de seguridad teniendo en cuenta que se cumple con un 68% de seguridad, viendo que lo que es en falta de riesgo es el ingreso hacia el laboratorio de computación con un 32% obteniendo un valor de Riesgo Importante.</td>
</tr>
</table>

Tabla 33 Riesgo identificado Robo

<table>
<tr>
<td> 
</td>
<td>Debido a:
No hay materiales aislantes de incendio en la Institución General Básica Simón Bolívar.
Los muebles y equipos no están fabricados con materiales retardantes de incendio en el laboratorio.
No hay personal designado y entrenado para manejar emergencias de incendio.
No se ha instalado iluminación de emergencia adecuada para guiar la evacuación en caso de apagones en el laboratorio de cómputo.</td>
</tr>
<tr>
<td colspan="2">Interpretación:

El laboratorio de cómputo cuenta con la mayoría de seguridad dentro de la Escuela porque tiene extintor y regulador de voltaje lo que permite que al momento de que se presente una situación pueda dar respuesta rápido, mientras que lo que hace vulnerable al laboratorio es que lo inmuebles no están fabricados con material retardantes es así que se obtuvo un valor de Riesgo Apreciable.</td>
</tr>
</table>

Tabla 34 Riesgo identificado Incendio

<table>
<tr>
<td> 
</td>
<td>Debido a:
Tiene una pared con humedad de agua en el laboratorio de cómputo.
El laboratorio de computación No tiene protección contra inundación.
Las paredes de computación No tienen daño por humedad.
No existe un plan de emergencia en caso de inundación en la Institución General Básica Simón Bolívar.
El laboratorio de computación No cuenta con seguro contra daños por agua.
El cielo raso No está en buenas condiciones en el laboratorio de cómputo.</td>
</tr>
<tr>
<td colspan="2">Interpretación:

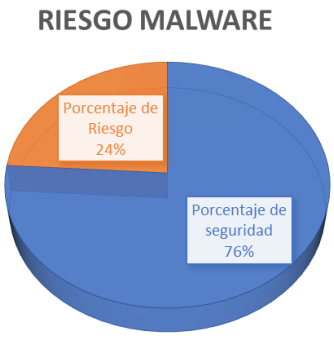
Identificando la seguridad cumple con una mayoría de seguridad lo que respalda es el escalón que cuenta para ingresar al laboratorio, mientras que, si el aire acondicionado perdure en un lugar que cause daño, la protección no será tan segura es así es un valor de Riesgo Apreciable.</td>
</tr>
</table>

Tabla 35 Riesgo identificado Inundación

<table>
<tr>
<td> 
</td>
<td>Debido a:
No se realizan copias de seguridad de la información de lo realizado día a día en la Institución general Básica Simón Bolívar.</td>
</tr>
<tr>
<td colspan="2">Interpretación:

Es muy notable el porcentaje de seguridad que el laboratorio de cómputo les brinda a los estudiantes de la Escuela Simón Bolívar teniendo un noventa y seis por ciento en tanto que el riesgo se da por no tener una información de lo que se realiza día a día con un cuatro por ciento obteniendo un valor de Riesgo Apreciable.</td>
</tr>
</table>

Tabla 36 Riesgo identificado Daño de equipo

<table>
<tr>
<td> 
</td>
<td>Debido a:
El personal No recibe información sobre cómo identificar y evitar malware en la Institución General Básica Simón bolívar.
No se realizan copias de seguridad de la información de forma regular en el laboratorio de cómputo.
Los equipos de la red No están protegidos con contraseñas seguras en el laboratorio de computación.
Las computadoras tienen contraseñas de acceso en el laboratorio de computación.
Se ha infectado la computadora con un USB en el laboratorio de cómputo.
Tiene seguridad en la nube en el laboratorio de cómputo.</td>
</tr>
</table>

Interpretación:

El control de malware constituye más de la mitad de las medidas de seguridad, ya que al restringir sitios web, se logra un 76% de protección. Sin embargo, en situaciones de riesgo, la falta de precaución al insertar cables o dispositivos USB en computadoras infectadas genera un 24% de vulnerabilidad, lo que resulta en un nivel de **Riesgo Apreciable.**

Tabla 37 Riesgo identificado Malware

5.4 Opinión

5.4.1 Los Riesgos identificados

Riesgo	Nivel
Robo	Importante
Incendio	Apreciable
Inundación	Apreciable
Daño de equipo	Apreciable
Malware	Apreciable

Tabla 38 Nivel de Riesgo General

5.4.2 Nivel de Seguridad General

El nivel de Seguridad General representa un 80% de Seguridad lo que está entendido que en la Escuela Simón Bolívar está respaldado por un Nivel Alto.

5.4.3 Recomendación

Se recomienda tener en consideración el manual de buenas prácticas de seguridad que se adjunta a continuación:

5.4.3.1 Manual de buenas prácticas

San Luis de Cajones –
El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

MANUAL DE POLÍTICAS DE SEGURIDAD DE BUENAS PRÁCTICAS

PARA LA

ESCUELA GENERAL BÁSICA SIMÓN BOLÍVAR

San Luis de Cajones –
El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

INDICE

Contenido

San Luis de Cajones – El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

INTRODUCCIÓN

Un plan de seguridad informática es una estrategia que define las medidas digitales para proteger los datos recopilados a través de plataformas, aplicaciones o software especializado. La implementación adecuada de este plan asegura la protección de la información valiosa de los estudiantes en el campo de la informática. (Duran, 2023)

Lo importante de brindar seguridad en la Institución y dentro del laboratorio de cómputo es que al momento de realizarlas podemos ver ciertos cambios que antes no se consideraba como implemento necesario, pero con el pasar el tiempo te vas dando cuenta que, si mi Misión como institución es crecer tengo que asegurar mejores adecuaciones en el plantel. Estas prácticas son fundamentales para proteger la Institución pueden incluir pautas básicas, como cambiar las contraseñas regularmente y seguir procedimientos específicos para añadir o eliminar información o empleados de manera segura en la infraestructura interna.

A continuación, se presentan algunas acciones que garantizan el adecuado funcionamiento de los servicios informáticos:

- Evaluación de riesgos de seguridad.
- Actualización de equipos.
- Sistemas de control de acceso.
- Protección de datos.
- Políticas de seguridad.

OBJETIVO

Plantear las normas básicas de seguridad en el laboratorio de cómputo de la Escuela General Básica Simón Bolívar.

ALCANCE

Está orientado a todos los miembros de la comunidad educativa que utilicen el laboratorio de cómputo en la Escuela Simón Bolívar, para que conlleve un ambiente armonioso para las Docentes, alumnos y padres de familia teniendo un enfoque familiar para quienes conforman la Institución.

San Luis de Cajones – El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

DEFINICIONES

Laboratorio de Cómputo:

Es un ambiente confortable está ubicado en medio del paralelo de 7° grado y la Oficina de la Coordinadora, diseñados para los Alumnos y Docentes que cuenta la Escuela Simón Bolívar.

5.1 Equipo de Cómputo:

Cuenta la Escuela Simón Bolívar en el laboratorio de cómputo con 20 equipos uno de ellos no está en funcionamiento por ahora, para uso de medidas de prevención.

5.2 Periféricos:

Son dispositivos conectados a la computadora en el laboratorio de cómputo teniendo interacción entre el usuario y los equipos de cómputo: el mouse, teclado, impresora, etc.

5.4 Componente Técnico:

En cierto tiempo se le brinda de parte del Ministerio de Educación un mantenimiento al laboratorio d cómputo de la Escuela Simón Bolívar.

RESPONSABLES

6.1 Docente de la Asignatura:

Es responsable desde el momento que ingresan al laboratorio de cómputo, en como imparte la clase teniendo el orden a su cargo, además es responsable de hacer cumplir las normas establecidas por el Reglamento.

6.2 El alumno:

Tiene que comportarse en el laboratorio de cómputo porque hay cosas que se pueden dañar fácilmente con solo dar un clic o moviendo los periféricos de lugar.

TIPOS DE RIESGO EN EL USO DE LOS AMBIENTES

7.1 Riesgos electrónicos:

Son aquellos que se originan por contacto eléctrico o exposición de cables que conllevan a: incendios, shock eléctrico, quemaduras de la piel y en circunstancias graves que pueden originar la muerte de la persona.

7.2 Riesgos físicos:

Puede ser molestoso para una persona el ruido, iluminación directa a los ojos, temperatura o humedad que puede ocasionar irritación ocular frente al monitos o enfermedades de origen auditivo.

7.3 Riesgos ergonómicos:

La postura de una persona de permanecer una hora en el laboratorio de cómputo con una silla que no le lleguen los pies al suelo, dando lesión en la espalda.

POLÍTICA DE SEGURIDAD

8.1 Contactos de Emergencia:

Los teléfonos en caso de accidente se muestran a continuación:

- Cuerpo de Bombero: *0981918757*
- Ambulancia: ECU 911
- Policía: *2 661 – 857*

San Luis de Cajones – El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

Prevenir o Evitar Riesgos:

RIESGO	PREVENCIÓN
Robo	• Se sugiere implementar puerta eléctrica en el laboratorio de cómputo. • Instalar un biométrico para restringir el ingreso y visualizar la hora al laboratorio de cómputo. • Mantener cerrada la puerta del laboratorio de cómputo. • Se propone instalar un sistema infla rojo, detector de calor. • Se necesita vigilancia física en la Escuela Simón Bolívar dos veces a la semana. • Instalar una cámara de seguridad dentro del laboratorio de cómputo. • Tiene una alarma tipo sirena.
Incendio	• El laboratorio de cómputo debe contar con un extintor para las medidas de precaución. • Tiene que contar con una varilla de cobre para la conexión a tierra. • Tener en cuenta que cada equipo esté conectado a su regulador de voltaje. • Establecer rutas de evacuación, salidas de emergencia y puntos de encuentro. • Antes de salir del laboratorio de cómputo cerciorarse de que los equipos estén completamente apagados.
Daño de equipos	• Revisar los periféricos de entrada y salida. • Cerciorarse que el cableado esté correctamente anclado en su respectivo casillero. • Tener poster de no consumir alimentos, ni bebidas dentro del laboratorio de cómputo. • Precaución al momento de insertar en un computador la memoria USB. • Se recomienda realizar un cronograma de actividades del día que se utilizó el laboratorio de cómputo y que actividad se desarrolló en ésta.

Riesgo	Prevención
Inundación	• Instalar un desagüe en el laboratorio de cómputo. • Se sugiere que se tome medidas de prevención con la pared húmeda que existe dentro del laboratorio de cómputo. • Contar con un plan de emergencia en caso de Inundación. • Revisar una vez al mes la condensación del aire acondicionado, siendo esta una precaución importante. • Procurar que el alcantarillado funcione adecuadamente y pueda fluir el agua sin inconveniente.
Malware	• Los Docentes necesitan recibir capacitación para evitar malware. • Realizar copias de seguridad por si se pierde archivos. • Tener contraseñas, en todas las computadoras para el inicio de sesión.

MANUAL DE POLÍTICAS DE SEGURIDAD DE BUENAS PRÁCTICAS PARA EL LABORATORIO DE CÓMPUTO DE LA ESCUELA SIMÓN BOLÍVAR.

Código AMIE: 13H01465

San Luis de Cajones – El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

ANEXOS

- ANEXO 1: MATRIZ DE HERRAMIENTAS BÁSICAS DE SEGURIDAD EN EL ALBORATORIO.
- ANEXO 2: FORMATO DE RESPORTES DE INCIDENCIA.

ANEXO 1

MATRIZ DE HERRAMIENTAS BÁSICAS DE SEGURIDAD EN EL ALBORATORIO

Ambiente:
Encargado de Inspección:
Fecha de Inspección:

Ítems	Herramienta de Seguridad	Disponible	Observación
1	Botiquín de emergencia		
2	Detector de humo y alarma		
3	Equipos eléctricos conectados a sistemas de puesta a tierra (pozo de tierra)		
4	Extintor Tipo CO_2		
5	Luz de emergencia		
6	Manual de seguridad vigente		
7	Señales visibles de aforo		
8	Señalética (señales de emergencia y salida)		

Firma de la Coordinadora

San Luis de Cajones –
El Carmen – Manabí
Telf.: 0990503641
E-mail: d13h01465sb@gmail.com

ANEXO 2

FORMATO DE REPORTES DE INCIDENCIAS

Del: Encargado
Al: Ministerio de Educación 13D05
Asunto: Alumno sufre contusión por paso a desnivel

Informo del incidente ocurrido el día XX de XX del 20XX en los ambientes de XX, de la Escuela General Básica Simón Bolívar.

A continuación, se detalla los hechos ocurridos:

a.
b.
c.
...
z.

La Coordinadora, XX de XX 20XX

Encargada de la Institución
Escuela Simón Bolívar

Ilustración 14 Manual de buenas prácticas

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Al realizar el análisis de la problemática se pudo determinar que existen pocas medidas de seguridad implementadas las cuales como sugerencia acorde a la Institución se reforma por el bien de su seguridad establecer medidas de prevención por ser una zona rural, que presenta vulnerabilidades desde el ingreso para posteriormente sus impactos esperados por la tecnología de sus equipos del laboratorio de cómputo en su vida útil.

Fue de suma importancia la base de información que brindaron los libros de auditoría informática, reestableciendo los conocimientos que estos difunde en la infraestructura teniendo una conectividad y prevención del laboratorio de cómputo como proteger el hardware y software maliciosos que se pueden encontrar a lo largo de las redes, evitándolas en no ser víctimas de sucesos que se dan a diarios.

Al aplicar el proceso de investigación mediante encuesta y entrevistas a las docentes y Coordinadora de la Escuela Simón Bolívar, se verificó la problemática que se había planteado que realmente existía deficiencia de seguridad, siendo así vulnerable a Robo por medio de la puerta del laboratorio de cómputo y por no tener autenticación ni permiso al momento de ingresar, en tanto Malware por utilizar una red pública que en cuestiones de minutos se podrían filtrar los datos de quienes pertenecen a la Institución.

Mediante la aplicación de auditoría se pudo identificar los riesgos reales en su dimensión a los que está expuesto el laboratorio de cómputo tanto que se optó por la metodología Magerit, como referencias valorando los activos físicos para conseguir los porcentajes generales y así descartar ciertos desbalances como el daño de equipo siendo el más cuidado dentro de la Institución con un promedio casi perfecto.

Para concluir se receptó información a quién iba dirigido el informe final, debido a que se estaría proporcionando los riesgos de los niveles de seguridad con un plan de buenas prácticas, para inconveniente en el establecimiento por falta de simulacros o aprendizajes de la utilización de las herramientas Tics, tomando consideraciones medidas de prevención y

protocolo de ayudas de emergencia, conservando dos matrices, una de botiquín en la Escuela y la segunda en presentación que pueden suscitarse eventualidades dentro o fuera del laboratorio de cómputo.

6.2 Recomendaciones

Para el mejoramiento de una infraestructura tecnológica del laboratorio de cómputo se recomienda a las demás Instituciones Provinciales, Cantonales e incluso Nacionales que se tomen medidas de prevención en su establecimiento de los niveles de seguridad, que se presentan siguiendo un plan de buenas prácticas para revisar lo físico y lógico en los equipos informáticos.

La Universidad Laica Eloy Alfaro de Manabí como parte Institucional de tercer grado referente al proceso de titulación, tiene asociación con todas las Escuelas para implementaciones de red, desarrollo de software y realizar evaluación de auditoría, gestionando las estrategias como sugerir y recomendar mejoras de su proyecto a un futuro que se requieran estas medidas de salvaguardar los controles de seguridad en ciertos períodos académicos.

Contando con el manual de buenas prácticas desarrollado por parte de su laboralista de que se implemente en la Escuela Simón Bolívar cuando lo requieran necesario, teniendo en consideración sus niveles de riesgos, aportando lo considerable en funciones de los controles evaluados como lo son Robo, Incendio, Inundación y Malware, siguiendo el mejoramiento para un laboratorio de cómputo en mejor seguridad de riesgo dentro o fuera del plantel.

BIBLIOGRAFÍA

Ambit. (9 de Febrero de 2021). *Ambit 20 years*. Obtenido de Tipos y fases de una seguridad informatica: https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases

Aredes, J. P., Rosi, B., & Tirimaco, S. (27 de Diciembre de 2022). *Campus educativo Santa Fe*. Obtenido de Campus educativo ministerio de educacion: https://campuseducativo.santafe.edu.ar/el-laboratorio-como-recurso-educativo/

Atico34. (19 de Agosto de 2022). *Proteccion de datos LOPD*. Obtenido de Desastres Informaticos: https://protecciondatos-lopd.com/empresas/plan-recuperacion-ante-desastres-informaticos/

Barreto, A. (2021). AUDITORIA INFORMÁTICA APLICANDO METODOLOGÍA COBIT EN LOS LABORATORIOS DE COMPUTO DE LA FACULTAD DE CIENCIAS TÉCNICAS DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABI. 1-107. Obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/3058/1/TESIS%20%20DE%20-BARRETO%20TOALA%20%20%20ALEXANDRA%20GISSELA.pdfhttps://repositorio.unesum.edu.ec/bitstream/53000/3058/1/TESIS%20%20DE%20-BARRETO%20TOALA%20%20%20ALEXANDRA%20GISSELA.pdf

Bolaños, N., & Muñoz , L. (2024). *Seguridad en el laboratorio informatico.* Valle del Cauca: Servicio Nacional de Aprendizaje SENA.

Brown, L., & Miller, T. (2023). *Advances in IT Auditing: Standards and Practices.* IT Governance Publishing.

C2H. (9 de Octubre de 2023). *C2H SOLUTIONS*. Obtenido de Sistemas de seguridad: https://c2hsolutions.com.br/es/llevar-a-cabo-una-evaluacion-de-riesgos-de-seguridad-fisica-para-edificios-y-oficinas/

Calderon, P. (10 de Julio de 2023). *https://editorialalema.org/*. Obtenido de Diseño de infraestructura tecnológica para fortalecer la conectividad en el Malecón de Puerto Cayo: https://editorialalema.org/index.php/pentaciencias/article/view/763

Callejo Gallejo, J. (2011). *Cuadernos Metodológicos.* Espña: Centro de Investigaciones Sociológicas.

Caravantes, B. (25 de Septiembre de 2020). *MARCOS DE INVESTIGACIÓN*. Obtenido de Sitio Web de issuu: https://issuu.com/beverlyncaravantes/docs/marcos_de_investigacion

Castillo, G. (30 de Agosto de 2023). *Innovacion Digital 360*. Obtenido de Infraestructura tecnológica: Qué es, tipos y características: https://www.innovaciondigital360.com/industria-4-0/infraestructura-tecnologica-que-es-tipos-y-caracteristicas/

Chen, Y., & Wang, J. (2022). *Cloud Computing and Virtualization: Transforming IT Infrastructure.* Springer.

Chicano, E. (2024). *Auditoría de Seguridad Informatica.* Antequera, Malaga, España: IC EDITORIAL. Obtenido de https://elibro.net/es/ereader/uleam/232692?page=11

Cobeña, D., & Mendoza, J. (2021). AUDITORÍA INFORMÁTICA INTERNA DE LOS MÓDULOS DE AUDITORÍA INFORMÁTICA INTERNA DE LOS MÓDULOS DE ACADÉMICA DE LA ESPAM MFL. 1-122. Obtenido de https://repositorio.espam.edu.ec/bitstream/42000/1566/1/TTC13D.pdf

Compilatio. (04 de Junio de 2024). *Realizar una investigación académica eficaz: 9 métodos de investigación que debe conocer*. Obtenido de Elija la metodología de investigación más adecuada a su situación: https://www.compilatio.net/es/noticias/metodo-investigacion-academica

CompuSoluciones. (4 de Abril de 2022). *Compu Soluciones*. Obtenido de Hiperconvergencia, ¿qué es y qué beneficios tiene?: https://www.compusoluciones.com/blog/convergencia-e-hiperconvergencia/

Darling, R. (26 de Septiembre de 2020). *C3NTRO Telecom*. Obtenido de c3ntro.com: https://www.c3ntro.com/es-mx/blog/importancia-seguridad-infraestructura-ti

Datos101. (19 de Enero de 2023). *Datos 101*. Obtenido de Las 9 medidas de seguridad informática: https://www.datos101.com/blog/medidas-de-seguridad-informatica/

Delgado, O. (2 de Febrero de 2023). *SGC LAB*. Obtenido de 10 consejos de buenas prácticas para garantizar la seguridad de la información en tu laboratorio: https://www.google.com/search?q=seguirdad+en+un+laboratorio+informatico&sca_esv=f911e4bfb540ceed&sca_upv=1&rlz=1C1UEAD_esEC1080EC1080&biw=1366&bih=641&ei=QXmOZuCVMaiYwbkPrOCyqAc&ved=0ahUKEwiguvHNt5yHAxUoTDABHSywDHUQ4dUDCA8&uact=5&oq=seguirdad+en+un+labora

Duran, M. (3 de Agosto de 2023). *Hubspot*. Obtenido de Plan de seguridad informática: qué es, elementos clave y ejemplo: https://blog.hubspot.es/website/plan-de-seguridad-informatica

Gallo, K. (10 de Enero de 2020). *UTPL*. Obtenido de Noticias Utpl: https://noticias.utpl.edu.ec/uso-de-la-tecnologia-en-la-prevencion-de-desastres

Ginzo. (1 de Junio de 2022). *Ginzo Tech*. Obtenido de ginzo.com: https://ginzo.tech/infraestructura-tecnologica-servicios-informaticos/

Gómes, A. (4 de Julio de 2023). *DELTA PROTEC*. Obtenido de Auditoria de seguridad informatica: https://www.deltaprotect.com/blog/auditoria-de-seguridad-informatica

Gómez, M. (2012). *MAGERIT*. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Gòmez, V. (2020). Control y monitoreo en tiempo real de los equipos informáticos para los laboratorios 1-2-3 de informática de la Universidad Estatal Península de Santa ElenaSanta Elena. 1-73.

GRCTools. (16 de Febrero de 2024). *GRCTools Software*. Obtenido de GRCTools.Software: https://grctools.software/2024/02/16/riesgos-en-infraestructura-ti-protegiendo-la-tecnologia-empresarial/

Guerrón, A., Yumbo, A., & Montenegro, F. (2020). *Auditoria Fisica.* Ambato: Universidad Tecnica de Ambato.

Hernández León, R. A., & Coello González, S. (2008). *El paradigma cuantitativo de la investigación científica.* Habana: Editorial Universitaria del Ministerio de Educación Superior.

Itsqmet. (10 de Mayo de 2024). *Itsqmet*. Obtenido de itsqmet.edu.ec: https://itsqmet.edu.ec/descubre-los-riesgos-informaticos-protege-tu-empresa/

ITSQMET. (23 de Julio de 2024). *ITSQMET*. Obtenido de https://itsqmet.edu.ec/importancia-de-la-auditoria-ambiental/#:~:text=Superior%20en%20Contabilidad-,%C2%BFQu%C3%A9%20Hace%20la%20Auditor%C3%ADa%20Ambiental?,su%20compromiso%20con%20la%20sostenibilidad.

Kvam, R. (2018). *Evaluación del impacto social.* América: Evolución del impacto social.

Laedu. (7 de Septiembre de 2021). *LAEDU.DIGITAL*. Obtenido de Auditoria informatica: https://laedu.digital/2021/09/07/auditoria-informatica-objetivos-metodologia-e-importancia/

MegaPractical. (2017). *Metodologías de Desarrollo de Software.* hubspot. doi:https://cdn2.hubspot.net/hubfs/371274/Desarrollo%20de%20Software/metodologias%20de%20desarrollo%20de%20software.pdf

Menéndez, S. (2024). *Auditoría de Seguridad Informatica: Curso practico.* Madrid: RA-MA EDITORIAL.

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

Paladines, L. (2023). AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA INFRAESTRUCTURA TECNOLÓGICA EN LA UNIDAD EDUCATIVA ANTONIO JOSÉ DE SUCRE EN EL PERIODO 2022. 1-98. Obtenido de https://repositorio.uleam.edu.ec/bitstream/123456789/4583/1/ULEAM-INFOR-0108.pdfhttps://repositorio.uleam.edu.ec/bitstream/123456789/4583/1/ULEAM-INFOR-0108.pdf

Parra, J. (04 de mayo de 2023). *Corporación BI*. Obtenido de Corporación BI: https://blog.corporacionbi.com/productos-servicios/el-impacto-del-cambio-tecnologico-en-la-sociedad

Pesantez, C. (2023). *Analisis de la ciberseguridad a la infraestructura tecnologica de la empresa SEÑAL X*. Cuenca: Universidad Politecnica Salesiana Ecuador.

Pulsar. (30 de Junio de 2023). *Pulsar Tecnologjes*. Obtenido de pulsartec.es: https://pulsartec.es/7-amenazas-comunes-de-seguridad-de-la-infraestructura-de-red-que-debes-conocer/

Quezada, G. D. (3 de Abril de 2019). *Dialogemos la academia de la humanidad*. Obtenido de diaolegemos.ec: https://dialoguemos.ec/2019/04/que-importancia-tienen-los-laboratorios-en-la-educacion/

RedHat. (27 de Febrero de 2020). *Red Hat*. Obtenido de ¿Qué es la infraestructura hiperconvergente?: https://www.redhat.com/es/topics/hyperconverged-infrastructure/what-is-hyperconverged-infrastructure

RedHat. (4 de Agosto de 2023). *Red Hat*. Obtenido de Qué es la infraestructura de TI: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

Reyes Ruíz, & Carcoma Alvarado. (2020). *La investigación documental para la comprensión ontológica del objeto de estudio.* Manabí: Ediciones Universidad Simón Bolívar.

Riveros, A. (8 de Abril de 2021). *EALDE BUSINESS SCHOOL*. Obtenido de Auditoria de Seguridad Fisica: https://www.ealde.es/auditoria-de-seguridad-informatica/

Robalino, P., Yanza, W., & Montoya, J. (2022). *Auditoria Informatica.* Riobamba, Chimborazo, Ecuador: ISBN: 978-9942-42-606-2. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://cimogsys.espoch.edu.ec/direccion-publicaciones/public/docs/books/2023-09-27-175154-2.%20LIBRO_AUDITORIA%20INFORMA%CC%81TICA%20digital.pdf

Rodríguez Sánchez, Y. (2020). *Metodología de la Investigación.* México: klik soluciones educativas.

Rodríguez, A., & Gómez, M. (2023). *Modern IT Infrastructure: Hardware, Software, and NetworkinG.* Wiley.

Rus, E. (19 de Marzo de 2024). *Economipedia*. Obtenido de Definciones investigaciones: https://economipedia.com/definiciones/investigacion-descriptiva.html

Salinas, J. (5 de Mayo de 2021). *blogvisionarios*. Obtenido de Hiperconvergencia. ¿Qué es y cómo funciona?: https://blogvisionarios.com/articulos-sistemas/hiperconvergencia-que-es-y-como-funciona/

Santos, J. (20 de Abril de 2023). *Delta Protec*. Obtenido de deltaprotec.com: https://www.deltaprotect.com/blog/amenazas-de-ciberseguridad

Smith, J., & Johnson, R. (2022). *Trends in IT Auditing: Challenges and Innovation.* TechAudit Publications.

Solano, O., & Riasco, S. (2021). *Sistema de información contable en la era digital, Marco de referencia para su administración y control.* Cali: Facultad de Ciencias de la Administración de la Universidad del Valle. Obtenido de https://www.google.com.ec/books/edition/Sistema_de_informaci%C3%B3n_contable_en_la_e/74hAEAAAQBAJ?hl=es&gbpv=1

TecnologiaLC. (20 de Julio de 2021). *Tecnologia LC*. Obtenido de Proteccion de datos: https://lc-tech.com/es/how-to-protect-data-from-disasters/

Tirescue. (8 de Enero de 2024). *Tirescue Seguridad Informatica*. Obtenido de tirescue.com: https://tirescue.com/por-que-es-necesaria-la-infraestructura-en-la-seguridad-informatica/

Unir. (21 de Noviembre de 2022). *UNIR Formación profesional*. Obtenido de Auditoria de seguridad informatica: https://unirfp.unir.net/revista/ingenieria-y-tecnologia/auditoria-seguridad-informatica/

Vazquez, F. (26 de Abril de 2024). *Icorp*. Obtenido de ¿Qué es Infraestructura de TI y cuáles son sus componentes?: https://icorp.com.mx/blog/infraestructura-de-ti-componentes/

VidaEscolar. (26 de Septiembre de 2023). *Colegio Bertolt Brecht*. Obtenido de cbb.edu.pe: https://cbb.edu.pe/descubriendo-los-laboratorios-escolares-espacios-de-innovacion-y-aprendizaje/

ViewSonic. (23 de Diciembre de 2023). *View Sonic*. Obtenido de Educacion: https://www.viewsonic.com/library/es/educacion/5-razones-por-las-que-los-laboratorios-de-informatica-de-la-escuela-siguen-siendo-importantes/

Wrobel, M. (22 de Agosto de 2023). *https://blog.invgate.com/*. Obtenido de Explorando los componentes principales de la infraestructura de IT: https://blog.invgate.com/es/infraestructura-de-it

Yumbillo, E. (2020). AUDITORÍA INFORMÁTICA AL DEPARTAMENTO DE SISTEMAS DE LA UNIDAD EDUCATIVA “SAN FELIPE NERI” SISTEMAS DE LA UNIDAD

EDUCATIVA “SAN FELIPE NERI” PERÍODO 2018.”. 1-170. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/16338/1/82T01081.pdf

ANEXOS

Anexo A: Aprobación del tema

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

NT NOTIFICACIONES TITULACION

Para: POZO HERNANDEZ CLARA GUADALUPE

CC: DOMINGUEZ ZAMBRANO MERLY MISHELLE

Sáb 27/04/2024 0:24

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Universidad Laica Eloy Alfaro de Manabí

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

Estimad@
Docente y Estudiante
Uleam

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

Tema: AUDITORÍA INFORMÁTICA A LA INFRAESTRUCTURA TECNOLÓGICA DEL LABORATORIO DE CÓMPUTO EN LA UNIDAD EDUCATIVA SIMÓN BOLÍVAR

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: DOMINGUEZ ZAMBRANO MERLY MISHELLE

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2024-2025(1)

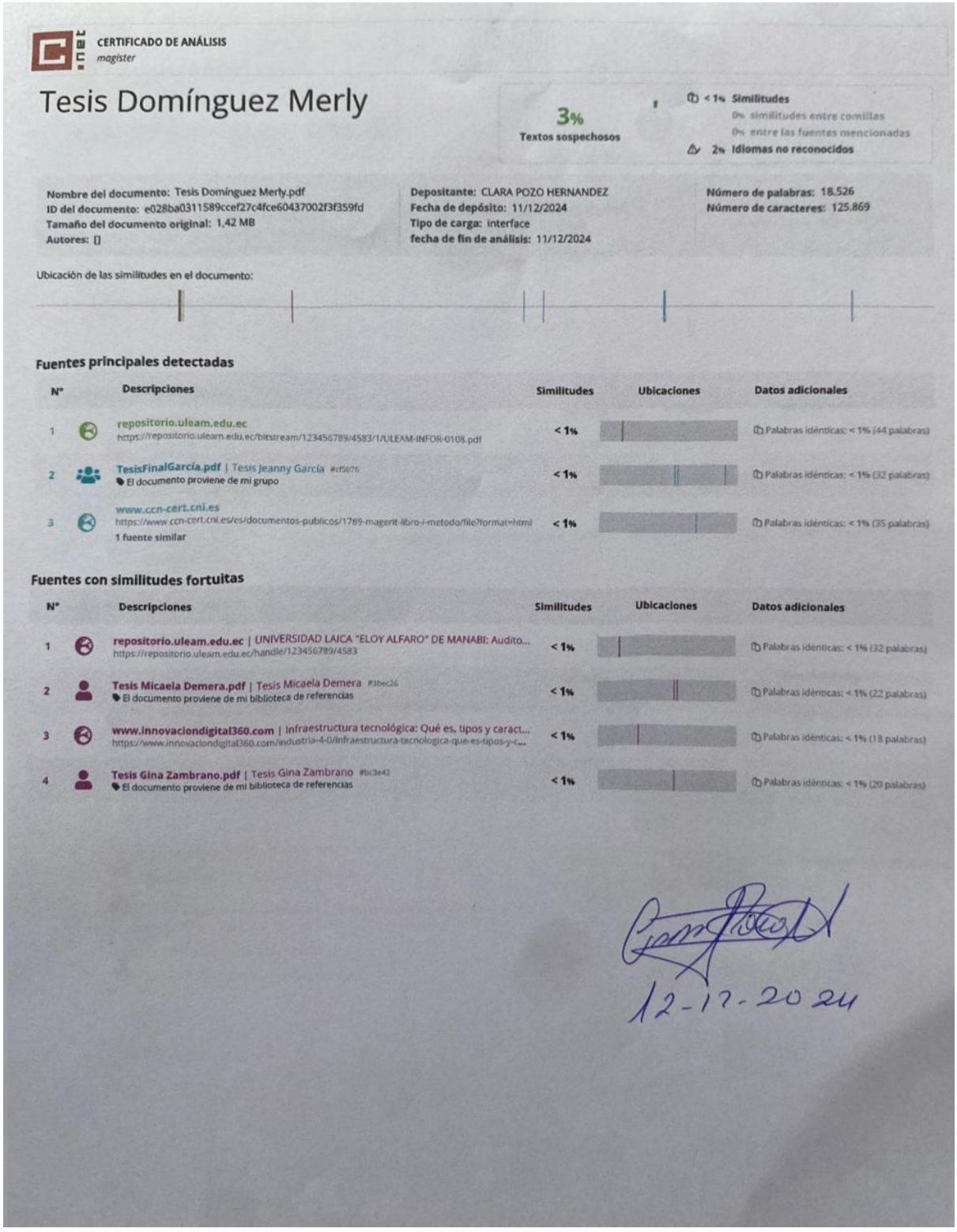
Sírvasen cumplir con lo dispuesto en el Manual de Procedimientos de TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR: https://departamentos.uleam.edu.ec/gestion-aseguramiento-calidad/files/2023/04/Titulacion-de-Est.-Grado-Bajo-la-Unidad-Integr.-Curri.-V.2-1-1.pdf.

Particular que se informa para los fines consiguientes.

Atentamente,

Comisión Académica y Responsable de Titulación.

Anexo B: Certificado de análisis Compilatio



CERTIFICADO DE ANÁLISIS
magister

Tesis Domínguez Merly

3% Textos sospechosos

< 1% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos

Nombre del documento: Tesis Domínguez Merly.pdf
ID del documento: e028ba0311589ccef27c4fce60437002f3f359fd
Tamaño del documento original: 1,42 MB
Autores: []

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 11/12/2024
Tipo de carga: interface
fecha de fin de análisis: 11/12/2024

Número de palabras: 18.526
Número de caracteres: 125.869

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uleam.edu.ec https://repositorio.uleam.edu.ec/bitstream/123456789/4583/1/ULEAM-INFOR-0108.pdf	< 1%		Palabras idénticas: < 1% (44 palabras)
2	TesisFinalGarcía.pdf | Tesis Jeanny García #cf5676 El documento proviene de mi grupo	< 1%		Palabras idénticas: < 1% (32 palabras)
3	www.ccn-cert.cni.es https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html 1 fuente similar	< 1%		Palabras idénticas: < 1% (35 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.uleam.edu.ec | UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABI: Audito... https://repositorio.uleam.edu.ec/handle/123456789/4583	< 1%		Palabras idénticas: < 1% (32 palabras)
2	Tesis Micaela Demera.pdf | Tesis Micaela Demera #3bec26 El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (22 palabras)
3	www.innovaciondigital360.com | Infraestructura tecnológica: Qué es, tipos y caract... https://www.innovaciondigital360.com/industria-4-0/infraestructura-tecnologica-que-es-tipos-y-c...	< 1%		Palabras idénticas: < 1% (18 palabras)
4	Tesis Gina Zambrano.pdf | Tesis Gina Zambrano #bc3e42 El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (20 palabras)

12-12-2024

Anexo C: Certificado de la empresa

Ministerio de Educación del Ecuador

Escuela de Educación General Básica
"SIMON BOLIVAR"
Código AMIE: 13H01465
San Luis de Cajones - El Carmen – Manabí
Telf.: 0990503641 E-mail: d13h01465sb@gmail.com

ESCUELA

El Carmen, 10 de febrero del 2024

CARTA DE ACEPTACIÓN DE LA INSTITUCIÓN

Lcda. Karina Intriago Moreira.
Coordinadora de la Escuela Educativa General Básica "Simón Bolívar" de San Luís de Cajones del Cantón El Carmen.
Ciudad – Manabí.

Presente. -

Tengo el agrado de dirigirme a usted, con la finalidad de hacer de su conocimiento que la estudiante: **DOMINGUEZ ZAMBRANO MERLY MISHELLE** con **C.I 1315108421** de la Universidad Laica Eloy Alfaro de Manabí Extensión El Carmen, ha sido admitida para realizar su Proyecto Integrador en la Institución, teniendo como fecha de inicio el 31 de enero del 2024 y como fecha de culminación el 15 de diciembre del 2024 en el área de Investigación y Análisis del laboratorio de cómputo.

Aprovecho la oportunidad para expresarle mi consideración y estima personal.

Atentamente.

Lcda. Karina Intriago Moreira
Coordinadora

ESCUELA DE EDUCACIÓN BÁSICA FISCAL "SIMON BOLÍVAR" Recto. San Luis de Cajones • El Carmen - Manabí • DIRECCION

RECIBIDO 11-02-24 10:00 am

Anexo D: Fotografías

Ilustración 15 La puerta de ingreso a la Escuela General Simón Bolívar

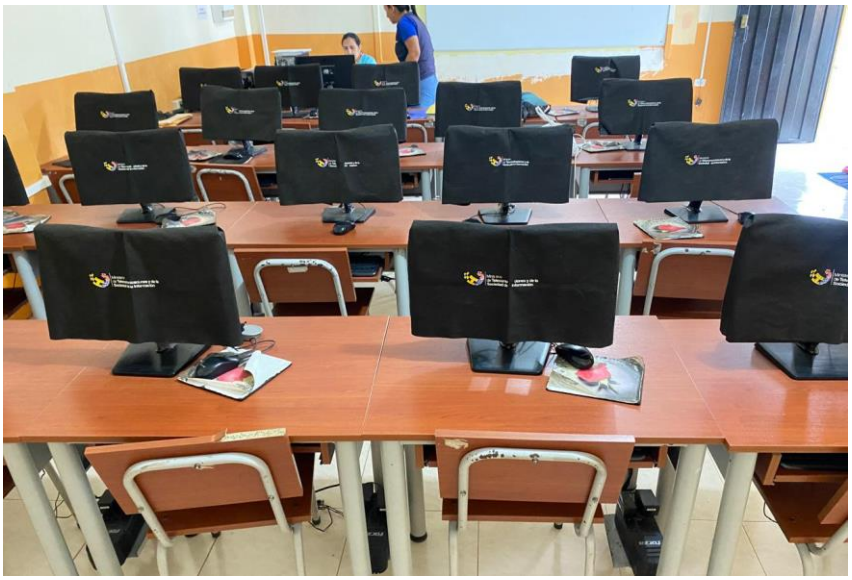
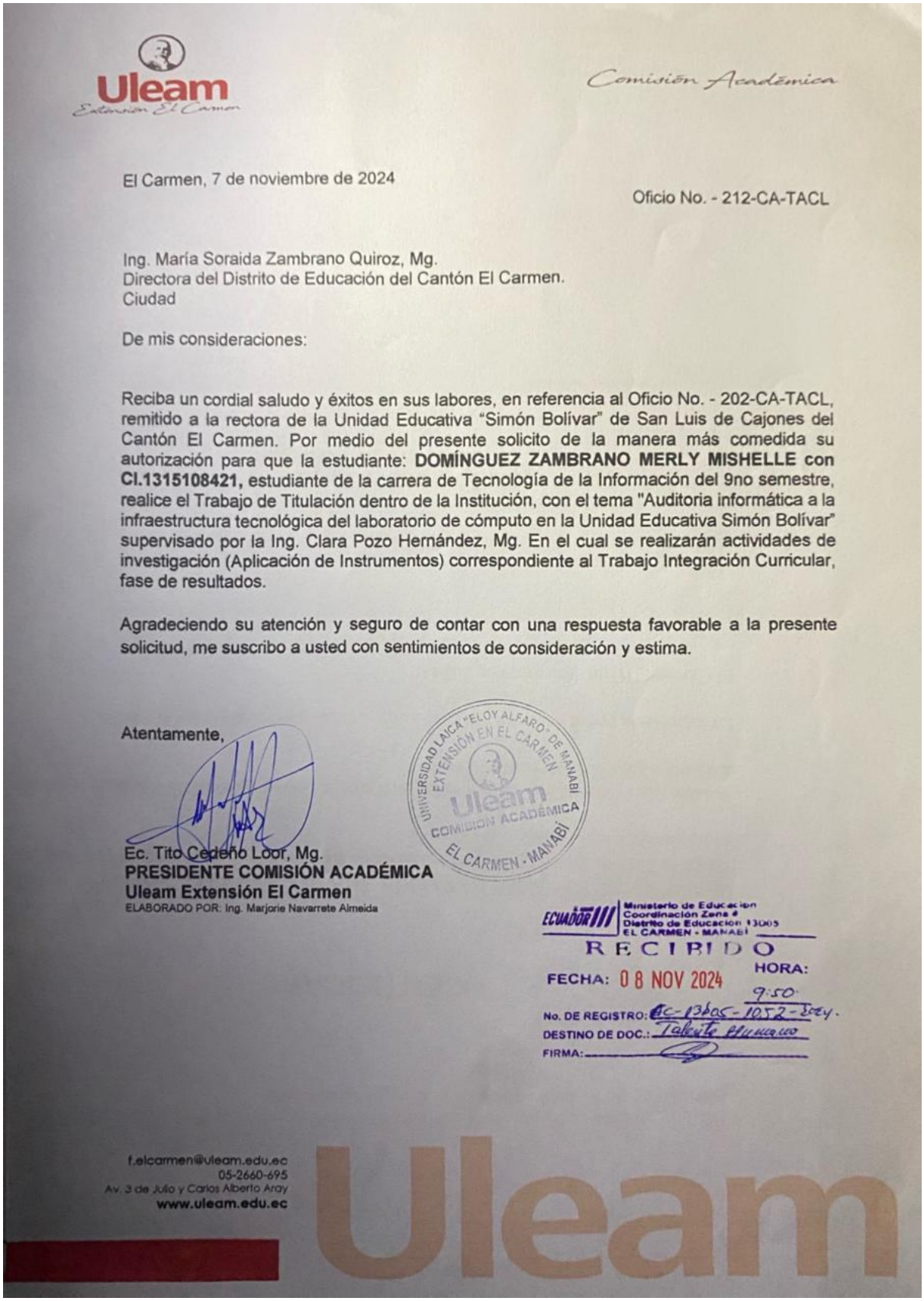


Ilustración 16 Supervisión del laboratorio de cómputo

Ilustración 17 Tutorías con la Ing. Clara Pozo Hernández



Uleam
Extensión El Carmen

Comisión Académica

El Carmen, 7 de noviembre de 2024

Oficio No. - 212-CA-TACL

Ing. María Soraida Zambrano Quiroz, Mg.
Directora del Distrito de Educación del Cantón El Carmen.
Ciudad

De mis consideraciones:

Reciba un cordial saludo y éxitos en sus labores, en referencia al Oficio No. - 202-CA-TACL, remitido a la rectora de la Unidad Educativa "Simón Bolívar" de San Luis de Cajones del Cantón El Carmen. Por medio del presente solicito de la manera más comedida su autorización para que la estudiante: **DOMÍNGUEZ ZAMBRANO MERLY MISHELLE con CI.1315108421,** estudiante de la carrera de Tecnología de la Información del 9no semestre, realice el Trabajo de Titulación dentro de la Institución, con el tema "Auditoria informática a la infraestructura tecnológica del laboratorio de cómputo en la Unidad Educativa Simón Bolívar" supervisado por la Ing. Clara Pozo Hernández, Mg. En el cual se realizarán actividades de investigación (Aplicación de Instrumentos) correspondiente al Trabajo Integración Curricular, fase de resultados.

Agradeciendo su atención y seguro de contar con una respuesta favorable a la presente solicitud, me suscribo a usted con sentimientos de consideración y estima.

Atentamente,

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

Ec. Tito Cedeño Loor, Mg.
PRESIDENTE COMISIÓN ACADÉMICA
Uleam Extensión El Carmen
ELABORADO POR: Ing. Marjorie Navarrete Almeida

ECUADOR
Ministerio de Educación
Coordinación Zonal 4
Distrito de Educación 13D05
EL CARMEN - MANABÍ
RECIBIDO
FECHA: 08 NOV 2024
HORA: 9:50
No. DE REGISTRO: 0C-13D05-1052-2024.
DESTINO DE DOC.: Talento Humano
FIRMA:

f.elcarmen@uleam.edu.ec
05-2660-695
Av. 3 de Julio y Carlos Alberto Aray
www.uleam.edu.ec

Uleam

Ilustración 18 Carta de permiso al Distrito de Educación 13D05

Anexo E: Evidencia de aplicación de encuestas y entrevistas

Ilustración 19 Encuesta y Entrevista

ENCUESTA

Universidad Lacia Eloy Alfaro de Manabí

Extensión "El Carmen"

Cuestionario para encuesta a las Docentes de la Unidad Educativa Simón Bolívar de San Luís de Cajones del Cantón El Carmen provincia de Manabí sobre los riesgos de seguridad en el laboratorio de cómputo.

Cuestionario estructurado para respuestas de tipo cerradas (Sí o No) y abiertas para que las profesoras hagan comentarios libremente

Objetivo: Determinar los problemas de seguridad existentes en el laboratorio de cómputo para poder hallar las soluciones.

1. **¿Con qué frecuencia utiliza el laboratorio de cómputo en sus clases?**

a. Diariamente ……
b. Varias veces a la semana:
c. Varias veces al mes:
d. Raramente ……
e. Nunca ……

2. **¿Ha tenido dificultades para utilizar el laboratorio de cómputo?**

Sí …. No ….

3. **Reportan o informan sobre los problemas encontrados en el laboratorio de cómputo:**

Sí ……. No …....

4. **¿Hay personal técnico para mantenimiento del laboratorio de cómputo?**

Sí …. No ….

5. **¿Con qué frecuencia reportan sobre los problemas técnicos de los equipos del laboratorio a los responsables de mantenimiento?**

a. A menudo ….
b. Pocas veces ….
c. Raramente ….
d. Nunca ….

6. **¿Qué tipo de problemas técnicos ha experimentado más a menudo en el laboratorio de cómputo?**

a. Fallos de hardware (computadoras, impresoras, etc.) ….
b. Problemas de software (sistema operativo, aplicaciones, etc.) ….
c. Problemas de red (conexión a Internet, red local, etc.) ….

7. **¿Ha recibido capacitación sobre uso de los equipos?**

Sí. ….. No. …

8. **¿Cuentan con personal de apoyo para el uso del laboratorio?**

Sí. ….. No. …

9. **¿Conoce usted si el laboratorio ha tenido problemas de humedad durante las épocas de lluvia?**

Sí …. No ….

10. **¿Reciben los profesores socialización de las autoridades sobre el Reglamento y políticas sobre el uso del laboratorio?**

Sí. ….. No. …

ENTREVISTA

Universidad Lacia Eloy Alfaro de Manabí

Extensión "El Carmen"

Guía para entrevista a la Coordinadora de la Unidad Educativa Simón Bolívar de San Luís de Cajones del cantón El Carmen provincia de Manabí sobre los problemas de seguridad en el laboratorio de cómputo.

Cuestionario estructurado para respuestas de tipo abiertas para que la autoridad exponga libremente sus respuestas, comentarios u opiniones.

Objetivo: Investigar si la Autoridad de la Institución conoce de los problemas de seguridad existentes en el laboratorio de cómputo y como proceden al respecto de eso.

1. **¿Conoce usted la frecuencia con la que los docentes utilizan el laboratorio de cómputo para preparar e impartir sus clases?**
   Si la respuesta es afirmativa continúa la pregunta
   a. Diariamente ……
   b. Varias veces a la semana. ….
   c. Raramente ……

Comentario:

……

……

2. **¿Recibe usted frecuentemente reportes sobre dificultades de los docentes para utilizar el laboratorio de cómputo?**

……..

3. **¿Qué tipos de problemas son los que los profesore le informan a usted?**

Comentario.

……..……
……..

……

4. **¿Cuenta la institución con personal técnico para mantenimiento del laboratorio de cómputo?**

……

5. **¿Se realizan frecuentemente labores de mantenimiento al laboratorio de cómputo?**

…….

6. **¿Cuenta la institución con personal de apoyo a los docentes para el uso del laboratorio?**

……

7. **¿Da la institución capacitación a los docentes sobre capacitación a los docentes sobre los equipos y sobre políticas de seguridad?**

……..…….

8. **¿Qué procedimientos existen para la actualización y reemplazo de equipos obsoletos o dañados en el laboratorio de cómputo?**

…….

9. **¿Cuenta la institución con algún reporte de humedad en las épocas de lluvia?**

…….

10. ***¿Se socializa con los profesores el reglamento y políticas sobre uso del laboratorio?***

……..…

GLOSARIO

Salvaguardas. – medidas de políticas implementadas para proteger sistemas, datos e infraestructura contra amenazas de vulnerabilidades.

Riesgo. – Probabilidad de que ocurra un evento que pueda causar daño o pérdida a una organización.

Preámbulos. – Introducciones o declaraciones iniciales que explican el contexto y los objetivos de un documento o estudio.

Disco Duro. – Dispositivo de almacenamiento que utiliza discos magnéticos para guardar o recuperar datos digitales.

HCI. – Interacción persona-computador, campo de estudio que analiza cómo los seres humanos interactúan con las computadoras.

ISACA. – Asociación global que proporciona conocimientos, certificaciones, defensa, educación formación en gobernanza, riesgo y control de sistemas de información.

Hiperconvergente. – Infraestructura de TI que combina almacenamiento, computación de red en una sola solución gestionada a través de una única interfaz.

Software. – Conjunto de programas, instrucciones, datos que permiten a las computadoras realizar tareas específicas.

Hardware. – Componente físicos de un sistema informático, como la CPU, la RAM y los dispositivos de almacenamiento.

PYMES. – Pequeñas y medianas empresas con un tamaño reducido en cuanto a números de empleados.

Startups. – Empresas emergentes que buscan desarrollar un modelo de negocio innovador o escalable.

Ciberseguridad. – Práctica de proteger sistemas, redes de programas contra ataques digitales, daños o acceso no autorizado.

CPD. – Centro de Procesamiento de Datos instalación que aloja sistemas informáticos de componentes asociados.

TI. – Tecnología de la Información uso de sistemas computacionales, software y redes para el procesamiento de distribución de datos.

Clústeres. – Conjunto de computadoras que trabajan juntas como un sistema único para mejorar el rendimiento la disponibilidad de recursos informáticos,

HCI. – Interfaz de comunicación Humano-Computador sistema de hardware y software que permite la interacción entre usuario y las computadoras.

CPD. – Centro de proceso de datos, instalación que alberga sistemas de información de almacenamiento de datos.

Firewall. – Sistema de seguridad de red diseñado para monitorear y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas.

Penetration Testing. – Prueba de seguridad en la que se simulan ciberataques para identificar y corregir vulnerabilidades en un sistema informático.

Criptografía. – Técnica de protección de la información mediante la codificación de datos para que solo los usuarios autorizados puedan acceder a ella.

ISO 27001. – Norma internacional para la gestión de seguridad de la información, que proporciona requisitos para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

Backup. – Copia de seguridad de los datos que se realiza para garantizar su recuperación en caso de pérdida, daño o ataque cibernético.