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 EN SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL DISTRITO DE EDUCACIÓN 13D05 EL CARMEN

MARIA JUDITH ALCIVAR RIVAS

AUTOR

RENELMO WLADIMIR MINAYA MACIAS

TUTOR

EL CARMEN, ENERO 2025

CERTIFICACIÓN DEL TUTOR

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

CERTIFICACIÓN

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

Haber dirigido y revisado el trabajo de investigación, bajo la autoría de la estudiante **ALCIVAR RIVAS MARÍA JUDITH**, legalmente matriculada en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(1)-2024(2), cumpliendo el total de 384 horas, bajo la opción de titulación de proyecto integrador, cuyo tema del proyecto es "Auditoría Informática en la Seguridad Física de los equipos informáticos en el Distrito de Educación 13D05".

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

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

El Carmen, 20 de Diciembre del 2024.

Lo certifico,

Wladimir Minaya Macías, Mg.
Docente Tutor
Área: Sistemas

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

TRIBUNAL DE SUSTENTACIÓN

Universidad Laica Eloy Alfaro de Manabí

Extensión El Carmen

Carrera de Ingeniería en Tecnologías de la Información

TRIBUNAL DE SUSTENTACIÓN

Título del Trabajo de Titulación:
AUDITORÍA INFORMÁTICA EN SEGURIDAD FÍSICA DE LOS EQUIPOS INFORMÁTICOS EN EL DISTRITO DE EDUCACIÓN 13D05 EL CARMEN

Modalidad:
Proyector Integrador.

Autor:
Maria Judith Alcivar Rivas.

Tutor:
Ing. Wladimir Minaya Macías, Mg.

Tribunal de Sustentación:

- **Presidente:** Alex Bladimir Mora Marcillo
- **Miembro:** Clara Guadalupe Pozo Hernández
- **Miembro:** Arturo Patricio Quiroz Valencia

Fecha de Sustentación:
22/1/2025

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este trabajo de titulación, cuyo tema es:
Auditoría Informática en Seguridad Física de los Equipos Informáticos del Distrito de Educación 13D05 El Carmen, corresponde exclusivamente a: Alcivar Rivas Maria Judith con CI. 1718168253, y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Alcivar Rivas Maria Judith

C.I. 171816825-3

DEDICATORIA

A Dios, por darme la fortaleza, sabiduría y salud para culminar este proyecto. A mis padres y abuelita, por su amor incondicional, apoyo constante y enseñarme el valor del esfuerzo y la perseverancia. A mis profesores y mentores, quienes con su guía y conocimiento me inspiraron a superar los retos y alcanzar esta meta. A mis amigos y compañeros, por su comprensión, ánimo y compañía en este camino de aprendizaje.

Judith Alcivar

AGRADECIMIENTO

A Dios, quien me brindó la luz para caminar por este sendero de conocimiento, por darme la fuerza para perseverar en los momentos de duda y por regalarme cada oportunidad de crecimiento. A mi familia, por su apoyo incondicional y su amor constante, por estar a mi lado en cada paso de este viaje. A mis profesores y compañeros de la universidad, por compartir sus conocimientos y experiencias, por contribuir a mi aprendizaje y por ser parte fundamental de mi desarrollo profesional.

Tu corazón late con la fuerza de los vientos, y en tu silencio, encuentro el consuelo que no necesito preguntar.

Judith Alcivar

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

En el contexto de las tecnologías de la información, los datos son un activo valioso que requiere protección para mantener la operatividad y competitividad de las instituciones. Este trabajo de investigación evalúa la seguridad física de los equipos informáticos en el Distrito de Educación 13D05, ubicado en El Carmen, Manabí, utilizando la metodología MAGERIT. La auditoría combinó métodos cuantitativos y cualitativos. El enfoque cuantitativo permitió analizar datos numéricos, mientras que el cualitativo facilitó la interpretación de los resultados y una descripción detallada del objeto de estudio. Para recolectar datos, se aplicaron encuestas al personal administrativo y entrevistas con el encargado del área de TI, Ing. Daniel Carrasco, y la rectora, Ing. Soraida Zambrano. La muestra incluyó a las 23 personas que laboran en la institución. El diagnóstico identificó problemas como acceso no autorizado a áreas de TI, falta de cámaras en puntos críticos y ausencia de políticas claras de seguridad física. Aunque existen medidas de seguridad, estas resultaron insuficientes para garantizar la protección adecuada de los equipos. Las brechas detectadas comprometen la integridad y disponibilidad de los sistemas de información. Como resultado, se elaboró un informe con recomendaciones para fortalecer la seguridad física, incluyendo la implementación de controles de acceso más estrictos, instalación de cámaras de vigilancia y actualización de políticas de seguridad física. Este proyecto subraya la importancia de mejorar las medidas de protección en los equipos informáticos para garantizar un entorno más seguro en el Distrito de Educación 13D05.

ABSTRACT

In the context of information technology, data is a valuable asset that requires protection to maintain the operability and competitiveness of institutions. This research evaluates the physical security of IT equipment at the 13D05 Education District, located in El Carmen, Manabí, using the MAGERIT methodology. The audit combined quantitative and qualitative methods. The quantitative approach enabled the analysis of numerical data, while the qualitative approach facilitated the interpretation of results and provided a detailed description of the subject of study. Data collection involved surveys administered to administrative staff and interviews with the IT manager, Engineer Daniel Carrasco, and the institution's rector, Engineer Soraida Zambrano. The sample consisted of all 23 employees of the institution. The diagnosis identified issues such as unauthorized access to IT areas, a lack of surveillance cameras in critical points, and the absence of clear physical security policies. Although some security measures are in place, they were found to be insufficient to adequately protect the equipment. The identified gaps compromise the integrity and availability of information systems. As a result, a detailed report was prepared with recommendations to enhance physical security, including stricter access controls, the installation of surveillance cameras, and the updating of physical security policies. This project highlights the importance of improving protection measures for IT equipment to ensure a safer environment in the 13D05 Education District.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Introducción

En el presente trabajo de investigación se pretende abordar temas de gran relevancia para la auditoría informática, ya que existen factores de riesgo que pueden afectar el funcionamiento y rendimiento del equipo informático. En la organización, las tecnologías de la información son importantes porque ayudan en gran medida al control. Mediante la auditoría informática, se emplean diversos factores que aseguran el rendimiento y la seguridad de los equipos informáticos. La gestión de riesgos nos permite analizar e identificar posibles vulnerabilidades e inconvenientes que podrían surgir si no se adopta un mantenimiento y cuidado adecuado de estos dispositivos en la Dirección Distrital 13D05, El Carmen.

Este artículo propone estrategias de auditoría informática en la era de la transformación digital, basándose en una revisión bibliográfica exhaustiva. Se identificaron normas como ISO/IEC 27000, ITIL, COBIT y PCI DSS como esenciales para la seguridad y protección de la información. Las estrategias incluyen la adaptación a la transformación digital, la evaluación de riesgos, auditorías periódicas, cumplimiento normativo y mejora continua, permitiendo a las organizaciones enfrentar desafíos y aprovechar oportunidades tecnológicas (Angamarca, 2022). La seguridad física es crucial para proteger a las personas, bienes y activos de una organización contra amenazas como el robo, vandalismo y desastres naturales1. Con la evolución de la tecnología, las medidas de seguridad física y digital se integran cada vez más para ofrecer una protección completa2. Las organizaciones que implementan estas medidas pueden gestionar proactivamente las amenazas y mantener la confianza del mercado (Caburao, 2024).

La auditoría de seguridad informática realiza sus tareas de manera eficaz y eficiente, abordando la seguridad informática desde diferentes ángulos de investigación. Se centra en mejorar la infraestructura y gestionar sus riesgos, así como en detectar y verificar daños en la información. Con el paso del tiempo, la tecnología ha ganado gran importancia debido a su ilimitado crecimiento y las nuevas oportunidades que ofrece en diversos campos. Mientras se desarrollan herramientas de hardware y software que mejoran y automatizan procesos en empresas e instituciones públicas y privadas, a menudo se descuida la inspección de estas. Con

el tiempo, la tecnología se expone a riesgos que pueden causar fallos en los equipos, resultando en reparaciones costosas o pérdida de datos importantes para las instituciones. Por ello, es necesario evaluar y prevenir estos riesgos. El problema es que el distrito de educación no cuenta con un plan de riesgo para proteger sus activos, como los equipos informáticos, que se encuentran en la institución. Para acometer este tema es necesario realizar una auditoría informática de seguridad física enfocada en la protección de los equipos informáticos de esta noble institución.

En el primer capítulo se presenta el tema central del estudio, proporcionando un contexto general y destacando su relevancia en el ámbito actual. A continuación, se plantea la problemática específica que se abordará, subrayando su importancia. Seguidamente, se presentan los objetivos del trabajo, tanto generales como específicos, indicando lo que se espera lograr con la investigación. La justificación del estudio se expone detalladamente, explicando por qué es crucial llevar a cabo esta investigación y mencionando los beneficios potenciales y la contribución al campo de estudio. Finalmente, se describen los impactos esperados, detallando los posibles resultados y efectos a corto y largo plazo

En el segundo capítulo se destacan las definiciones de todos los términos que se utilizarán en la auditoría, proporcionando una comprensión más clara de lo que implica realizar una auditoría informática. Asimismo, al conocer información sobre la infraestructura tecnológica, se aclararon dudas sobre los equipos que conforman un centro informático.

El tercer capítulo profundiza en el estudio de campo, el diseño y los métodos de investigación, describiendo el enfoque inductivo-deductivo. Para fundamentar la información teórica, se aplicó el método bibliográfico. Las técnicas e instrumentos utilizados permitieron la recopilación de datos en una zona específica para su evaluación. Esta recopilación se puede realizar mediante varios instrumentos, como encuestas-cuestionarios y entrevistas-guía, en las cuales participan la autoridad principal de la institución, como la directora distrital, y el personal administrativo del Distrito de Educación 13D05, El Carmen.

En el cuarto capítulo del trabajo de investigación se presenta la propuesta de seguridad informática para el Distrito de Educación 13D05, El Carmen. Se utilizó la metodología Magerit, la cual proporciona recursos informáticos. La auditoría implementada en la institución evaluó cada uno de los activos, identificando las vulnerabilidades y amenazas en los equipos

tecnológicos. Esto permitió concluir con los resultados obtenidos y detectados mediante la investigación en la organización del distrito de educación 13D05. Se determinó que los equipos dentro de la infraestructura tecnológica estaban expuestos a riesgos como incendios, daños, inundaciones, robos y malware. El porcentaje total de seguridad fue del 57% y el nivel de riesgo del 43%. Finalmente, se elaboró un informe de auditoría y se incluyeron varios pasos en la guía de recomendaciones para prevenir dichas vulnerabilidades.

1.2 Presentación del tema

La auditoría informática en seguridad física de los equipos informáticos sirve para evaluar los procesos y controles que se dan dentro de la institución, para así proteger estos equipos de daños, robos entre otras amenazas que pueden estar provocando la exposición de los datos o el deterioro de los equipos informáticos.

Dentro de este contexto, este proyecto está enfocado en identificar las posibles vulnerabilidades y riesgos que acaecen en la infraestructura del distrito. Para ello es preciso, llevar a cabo una auditoria, que permita evaluar los controles y a su vez establecer mejoras para consolidar la seguridad de los mismos.

El objetivo del presente proyecto es certificar que se cumple a cabalidad con las normas y los estándares de seguridad, así mismo detectar y prevenir cualquier amenaza vinculada a la seguridad física. Se debe agregar que este proyecto no solo realiza estas funciones, sino que también establece otras facetas preventivas que pueden ayudar a reducir estas brechas.

La auditoría nace con el fin de analizar y evaluar los procesos que se dan en la institución y de esta manera asegurar la confidencialidad. Integridad y disponibilidad de la información dentro de este órgano colectivo. Para lograr el objetivo planteado es necesario hacer uso de herramientas que nos permitan diagnosticar y encontrar las fallas y vulnerabilidades que se encuentran dentro de la institución.

El tema propuesto es “Auditoria informática en la seguridad física de los equipos informáticos en el distrito 13D05”

1.3 Ubicación y contextualización de la problemática

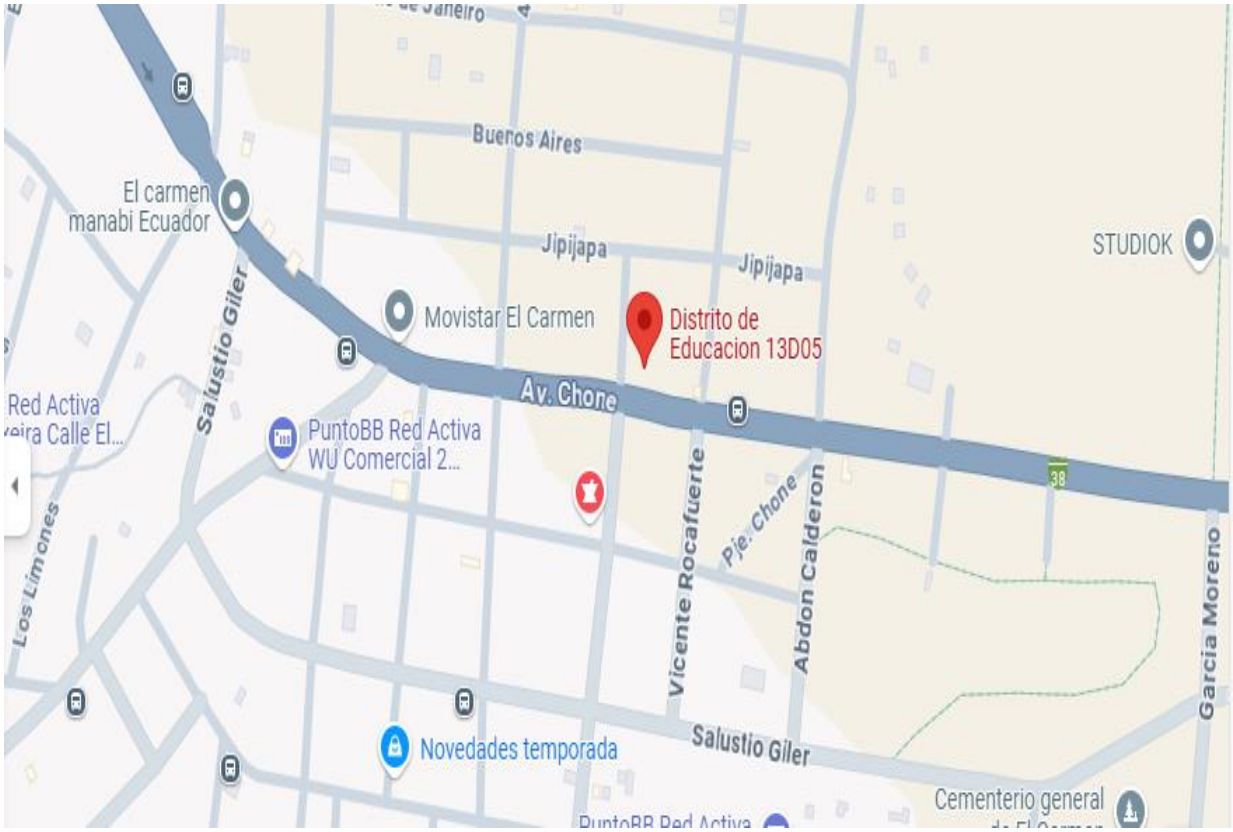


Ilustración 1: Ubicación Distrito de Educación 13D05 El Carmen, Manabí

El Distrito 13D05 se encuentra ubicado en la zona norte de la provincia de Manabí, Ecuador, específicamente en el cantón El Carmen. Su área geográfica comprende aproximadamente 1.422 kilómetros cuadrados, abarcando zonas montañosas, bosques tropicales y áreas agrícolas.El Distrito 13D05 está dirigido por la directora distrital Ing. Soraida Zambrano, quien es la responsable de la gestión administrativa, pedagógica y financiera del distrito.

La estructura organizativa del distrito también incluye jefes departamentales, supervisores educativos, directores de instituciones educativas y docentes.. En cada una de ella se hace uso de equipos informáticos para el total desempeño de sus funciones. En el distrito, se cuenta con un total de 23 computadoras, de las cuales 6 son de la marca Lenovo y 17 de la

marca HP. Todas están equipadas con procesadores Intel Core i5 y 8 GB de RAM. Ninguna de las computadoras posee unidad de CD, pero todas cuentan con CPU y altavoces internos. Los discos duros tienen una capacidad de 120 GB. En cuanto al software, todas operan con el sistema operativo Windows, incluyen la suite ofimática Microsoft Office, el antivirus Defender y el navegador Chrome. Sin embargo, no disponen de reguladores de voltaje. El estado general de estas computadoras se considera medio.

Ilustración 2: Distrito de Educación 13D05 El Carmen, Manabí.

1.4 Planteamiento del problema

1.4.1 Problematización

En esta investigación se realizó una auditoria informática en las instalaciones del distrito de educación 13D05, ubicado en el cantón El Carmen, Manabí. A través de convenio se permitió realizar la auditoria en el Distrito a lo largo del año 2024.

Es importante mencionar que la tecnología ha revolucionado el enfoque de las organizaciones modernas puesto que se logra un mejor desempeño laboral. La falta de medidas adecuadas para mitigar y controlar los riesgos que pueden afectar la seguridad física de los equipos informáticos. Para solventar los diferentes riesgos que existen en el Distrito se busca realizar una guía que asegure el bienestar de los mismos.

Por ello, es importante aplicar una auditoria para prevenir la seguridad dentro de las instalaciones. Identificando y analizando con tiempo para garantizar la seguridad física del equipo de cómputo. Si por alguna causa el equipo de cómputo se llega a dañar esto podría ser fatal de un perjuicio a las personas que hacen uso de ello.

Llevar especial cuidado con los equipos informáticos es importante para evitar que este servicio se suspenda porque ocasiona una gran pérdida de recursos así mismo atrasa las actividades que deben de realizar diariamente. En este contexto, es preciso realizar una pregunta que ayuda a establecer la base principal para este proyecto: ¿Cómo se puede garantizar la seguridad física de los equipos informáticos del Distrito de Educación 13D05?

1.4.2 Génesis del problema

La institución puede ser atacada de diferentes formas, ya sea el robo del equipo informático, ataques cibernéticos o daños por situaciones climatológicas. Por múltiples razones el equipo puede verse comprometido y es necesario captar estas probabilidades para luego evaluar y mitigar estas posibles amenazas que pueden estar perjudicando al activo fijo de la institución.

La tecnología es indispensable para el crecimiento de las organizaciones. Es por ello que se debe de realizar auditorías informáticas para que ayuden a controlar y mitigar los riesgos.

El génesis del problema es: Falta de medidas adecuadas para proteger los equipos informáticos en el Distrito de Educación 13D05 ubicado en el Carmen

1.4.3 Estado actual del problema

Con el fin de satisfacer las necesidades del Distrito de Educación 13D05, ubicado en cantón El Carmen provincia de Manabí se busca realizar una auditoria informática tanto lógica como física de los equipos informáticos con los que cuenta la institución, con el objetico de contribuir en la optimización del uso de la tecnología para el mejor cuidado de los equipos informáticos y de esta manera identificar los riesgos que surgen en estos equipos esenciales para su labor diaria.

En estas áreas puede ocurrir cualquier tipo de evento de manera plausible, que puede ocasionar que los equipos no estén el 100% de su operatividad, estos pueden ser por una mala disposición de las redes, áreas sin organización o poco organizadas, la seguridad de los equipos informáticos es deficiente, errores de actualización, el inventario no está actualizado. En muchas ocasiones estos problemas surgen por la falta de políticas de uso o por el contrario, no se hace el uso adecuado de las políticas y es por ello que los equipos se exponen reducir mucho más si vida útil.

De esta manera se plantea realizar el presente trabajo de investigación, y de esta forma contribuir a la reducción de estos problemas, para que las actividades con los equipos informáticos dentro del distrito se realicen de forma ágil para el personal que labora en esta institución

1.5 Diagrama causa – efecto del problema

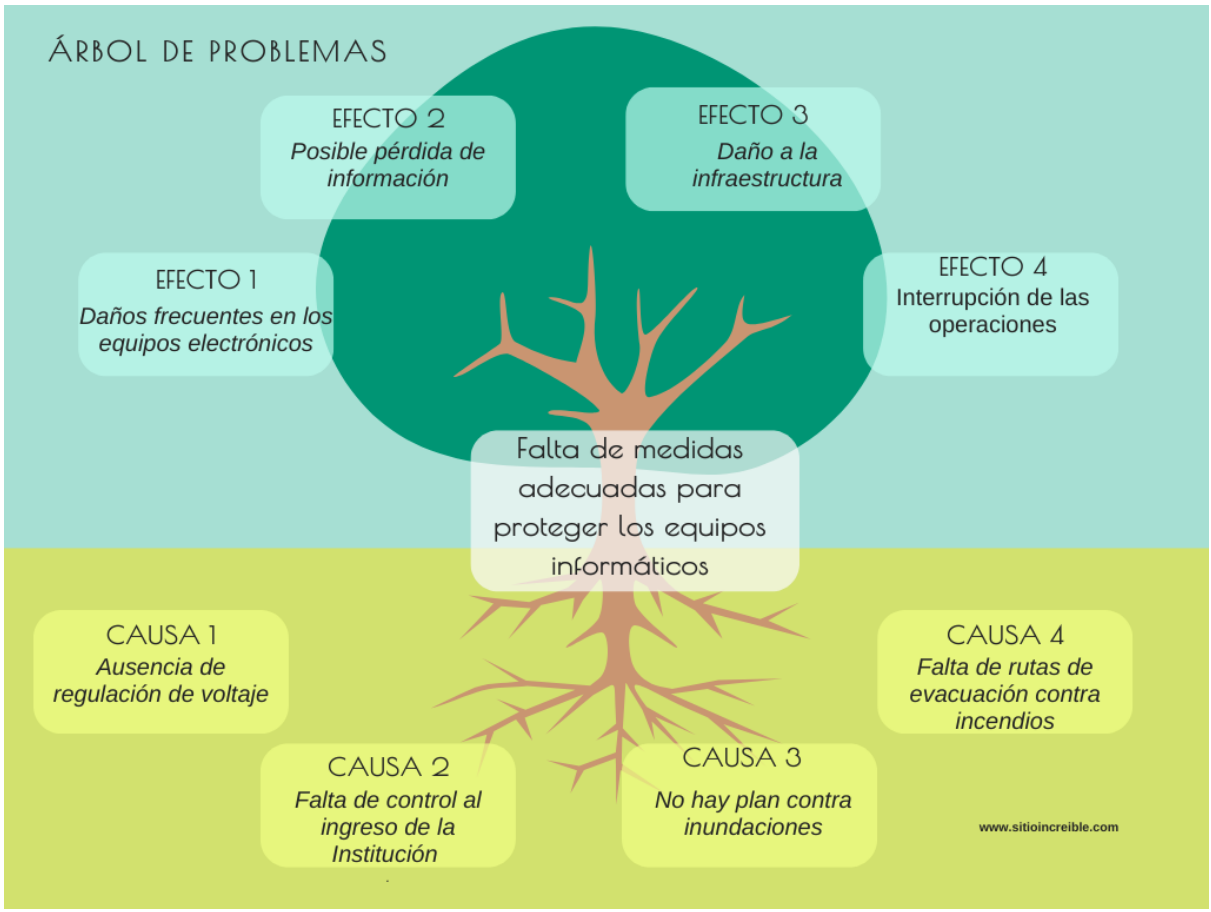


Ilustración 3: Árbol del problema

1.6 Objetivos

1.6.1 Objetivo general

Realizar una Auditoría Informática en Seguridad Física de los Equipos Informáticos del "Distrito de Educación 13D05 El Carmen", con el fin de mejorar procedimientos de seguridad implementados en la institución.

Objetivos específicos

- ✓ Evaluar la situación del Distrito 13D05 El Carmen
- ✓ Realizar una revisión de la literatura sobre auditoria informática y seguridad física

- ✓ Diseñar auditoria con el fin de determinar riesgos de seguridad informática en la institución.
- ✓ Elaborar Guía de la auditoria con sugerencias para la mejora de los procedimientos que se usan en la institución.

1.7 Justificación

El año 2024 ha venido acompañado de fuertes cambios climatológicos, los primeros tres meses se vio afectado por tormentas eléctricas que causaron fuertes devastaciones en varias partes del país. Las consecuencias dentro de varias instalaciones fueron aparatos tecnológicos dañados por la fuerte descarga de los rayos. La auditoría busca realizar un análisis del estado en el que se encuentran las maquinas, de esta forma hallar medidas para la prevención de estas posibles anomalías dentro de la institución. De este modo la institución podrá tomar las decisiones respectivas para mitigar estas amenazas. Toda institución necesita actuar de manera adecuada frente a un incidente de seguridad, la auditoria sirve para aclarar y vislumbrar el camino para realizar un mejor manejo de estos recursos.

1.8 Impactos esperados

Impacto tecnológico

La aplicación de esta auditoria informática incrementará la seguridad física de los equipos informáticos, lo cual ayuda a disminuir las fallas en los dispositivos y que su ciclo de vida sea más duradero. Esto dará permiso a una optimización de la gestión del tiempo laboral en el distrito 13D05.

Impacto social

Un entorno laboral debe de ser armonioso para que este establezca un mejor desempeño laboral, proporcionando a la plantilla un entorno fiable que de fiabilidad para que pueda soportar la jornada laboral. Además, de que la seguridad genera confiabilidad entre los padres de familia y el personal de la plantilla.

Impacto ecológico

Hacer uso de prácticas sostenibles y amigables con el medio ambiente permitirán la disminución de chatarra electrónica. La disminución de equipos dañados generara una mejor distribución de estos residuos. La distribución adecuada de estos desechos tecnológicos es importante porque permite proteger el medio ambiente.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

La informática es pieza clave a partir de los años 50 porque es una herramienta que facilita las operaciones de auditoria financiera dentro de las entidades. Desde ahí se da inicio a la auditoria con el ordenador puesto que el ordenador es el que realiza la tarea del auditor financiero. Las organizaciones se hicieron dependientes de los sistemas de información lo que provocó que verificaran que estos sistemas funcionen correctamente, en los años 60 se descubrieron varios casos de fraude debido a esto ya no se realiza auditorias alrededor del ordenador si no que se audita el ordenador. Ya no existen dudas de que la información es un principal activo dentro de las empresas ya que, producen a mayor escala y con mejor calidad (Piattinni, Del Peso, & Del Peso, 2007).

Las tecnologías de la información ocasionaron una revolución a la hora de comunicarse a principios de los años 90. Las tecnologías de la información y Comunicación son instrumentos que procesan, almacenan, resumen y recuperan información. Es una agrupación de herramientas que dan nuevas formas para difundir contenidos informacionales (Laborales, 2015).

Las tecnologías de la información son una fuente valiosa para el progreso de la sociedad porque han transformado el funcionamiento económico, cultural. Las TICS son fundamentales y necesarias dentro de las organizaciones por que la información es esencial en cualquier ámbito humano. Muchas organizaciones invierten en tecnologías porque deben de ser resilientes y adaptarse a los cambios que se vienen suscitando. Las compañías tienen a su disposición muchas herramientas tecnológicas, ya que deben integrarse para que este proceso trasgreda límites (Martín, 2016).

2.2 Antecedentes de investigaciones relacionadas al tema presentado

2.2.1 Auditoria informática para el análisis de la seguridad en los recursos informáticos utilizando Normas ISO 27001 en Megakons S.A.

La seguridad de la información es una práctica esencial que se debe llevar a cabo en las organizaciones, es necesario que el análisis sea profundo para afianzar que el uso sea optimo y seguro. En Megakons S.A. se determinó que existe un bajo control de seguridad de la información, por lo tanto, esto ocasiona robo de los bienes de la empresa. Este trabajo tiene como objetivo examinar el proceso de gestión de la seguridad en Megakons S.A. apoyándose en las normas ISO (Organización Internacional de Normalización) 27001 (Balarezo López & Tenezaca Caizabanda, 2024).

2.2.2 Análisis de la incidencia de las políticas y prácticas de seguridad informática en la arquitectura física existente en la dirección de tecnologías y sistemas información de la Universidad Técnica de Babahoyo.

En este caso se realizó el estudio de las políticas y prácticas que existen en la universidad técnica de Babahoyo. La educación superior (IES) afronta varios retos en seguridad de software y hardware. Se hizo un análisis de las políticas que se llevan a cabo en la Institución y se dieron las respectivas recomendaciones para mejorar la seguridad de los equipos (Zobeyda, 2024).

2.2.3 Análisis del nivel de seguridad de la información de la oficina de informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista – 2023

En este caso se utiliza el método de investigación descriptiva proyectada en un marco no experimental, donde se evalúa a fondo el nivel de seguridad de la información en el distrito municipal. Se detalla la población y muestra, los bienes informáticos, elementos físicos y lógicos entre otros aspectos clave. Se determino que existen ciertas vulnerabilidades en cuanto ataques, con varios niveles críticos para pruebas de seguridad (Carmen & Rojas Perleche, 2024).

2.2.4 Comparación de modelos de control COSO y COBIT utilizados para auditorías informáticas para instituciones académicas de educación media de la ciudad de Ibarra.

En las instituciones de formación académica se utilizan varios instrumentos tecnológicos para actividades como: ingreso de notas, matriculas, consultas etc. Es por eso que se recurre a un análisis de seguridad y de este modo verificar el estado de estos sistemas. En cierta medida, es limitado efectuar una auditoria por algunas razones, primordialmente por desconocer la implementación de metodologías, procesos de control. El objetivo en este trabajo es analizar varias fuentes bibliográficas y los modelos COSO y COBIT, estos son comparados para poder determinar cuál de ellos es más adecuado para su uso en la auditoria informática para instituciones de educación media (Guerrero, 2024).

2.2.5 Auditoría Informática a la seguridad física, en los procesos administrativos de la cooperativa interprovincial de transporte manglar alto de la ciudad de Santa Elena.

Esta auditoria se implementó con el fin de evaluar la seguridad física e informática debido a que los procesos se los lleva actualmente de forma automática. Esta investigación es fundamental para determinar que la seguridad de la información y de los equipos informáticos es imprescindible para cumplir a cabalidad con los objetivos de las instituciones, ya que sin la debida atención esto podría ocasionar problemas económicos (Ponce & Ponce Pereira, 2022).

2.1 Antecedentes investigativo-relacionados al tema presentado

2.1.1.1 Auditoria

La auditoría es un ejercicio de bastante relevancia en el sector económico y social, porque permite iniciar conexiones de diferente tipo, a causa de que se confía en el trabajo de los contadores públicos ya que ellos tienen un rol en el pueblo y deben extender su garantía

personal. La auditoría debe de ser continua con las transformaciones que se dan a nivel de cultura y ciencia. La conversión de la auditoria implica un cambio, transformar el cuerpo teórico, para ello es necesario poner en temas de discusión la concesión, impactos, ideas sobre auditoria y formas de dimensionar el entorno (Galvis & Herrera Marchena, 2005).

2.1.1.2 Auditoria informática

En el contexto de la auditoría informática y protección de las organizaciones, es primordial implementar las normas que prevengan la modificación de la información pública. A su vez, es necesario aplicar mecanismos de control para el intercambio de información. Por lo tanto, es de carácter fundamental evitar pérdidas, daños o comprometer los activos de la compañía. Los planes de logística deben tener una constancia para lograr la eficiencia, además, es de vital importancia cumplir a cabalidad con la legislación y así evitar contravenciones y multas (Enrique & García Fernández, 2019).

2.1.1.3 Tipos de auditoría

2.1.1.3.1 *Auditoria de sistemas*

La auditoría en sistemas es la que se ocupa de valorar los recursos informáticos de la empresa, tanto software, hardware, talento humano entre otras funciones, siempre con un objetivo técnico y de seguridad que busca disuadir a la empresa de los riesgos a los que están expuestos. Además de proporcionar recomendaciones y sugerencias a nivel directivo para que exista mayor control interno de la empresa (Alzate, 2001).

2.1.1.3.2 *Auditoria de seguridad informática*

La falta de seguridad se debe al desconocimiento, éste es un factor para que los sistemas sean amenazados y que no se combatan. Hay varios elementos que proteger como los datos, software y hardware. Es por eso que toca realizar inventarios que son la fuente para comprobar los activos que posee la empresa. Estos equipos están expuestos a varios tipos de ataque. No hay organización que pueda asegurar que no haya incidentes con los equipos. A los incidentes se les llama amenazas. Si esta amenaza afecta a un equipo es una vulnerabilidad (Palacios, 2020).

2.1.1.3.3 *Auditoría de cumplimiento*

La auditoría de cumplimiento se enfoca en observar y acatar los principios legales, que se puedan aplicar a los objetivos y que puedan tener relevancia sobre las actividades. Hay que tomar en cuenta que una persona que audita debe comprobar si cumple las normas (Majian, 2020).

2.1.1.4 Metodologías y normativas en auditoría

2.1.1.4.1 *ISO/IEC 27001*

La norma ISO/IEC 27001 es un modelo internacional que define los requisitos a ejecutar, conservar y perfeccionar un sistema de gestión de seguridad de la información. Se establece un código que rige para los SGGI donde el objetivo es determinar los riesgos, fijar planes para evitarlos e implantar garantías (Obregón, 2024).

La norma ISO/IEC 27001 es el canal para disminuir los riesgos que atenten a los sistemas informáticos (Gallejos Manrrique & Lynch Escobar, 2024).

2.1.1.4.2 *COBIT*

Las normas COBIT se distribuyen en 5 y 7 mediadores que dan un respaldo a las empresas en el proceso, ejecución, y supervisión de las buenas prácticas en relación con el gobierno y la gestión de TI. COBIT5 concede un manual para la Asociación de Control y Auditoría de Sistemas de Información. Esta norma lleva vigente hace más de 15 años en empresas y clientes de las alianzas de negocio, riesgo y seguridad (Galeano Gimenéz & González Prieto, 2021).

2.1.1.4.3 MAGERIT

En esta metodología se aplica el proceso de gestión de riesgos para que el consejo de gobierno tome decisiones frente a los riesgos que causa el uso de las Tecnologías de la información. El objetivo principal de este método es evaluar los riesgos que pueden padecer los sistemas. Los métodos a implementar en este método son varios. Esta metodología se utiliza para obtener resultados a través de la aproximación metódica la cual no da pie a la improvisación (Vásquez, 2013).

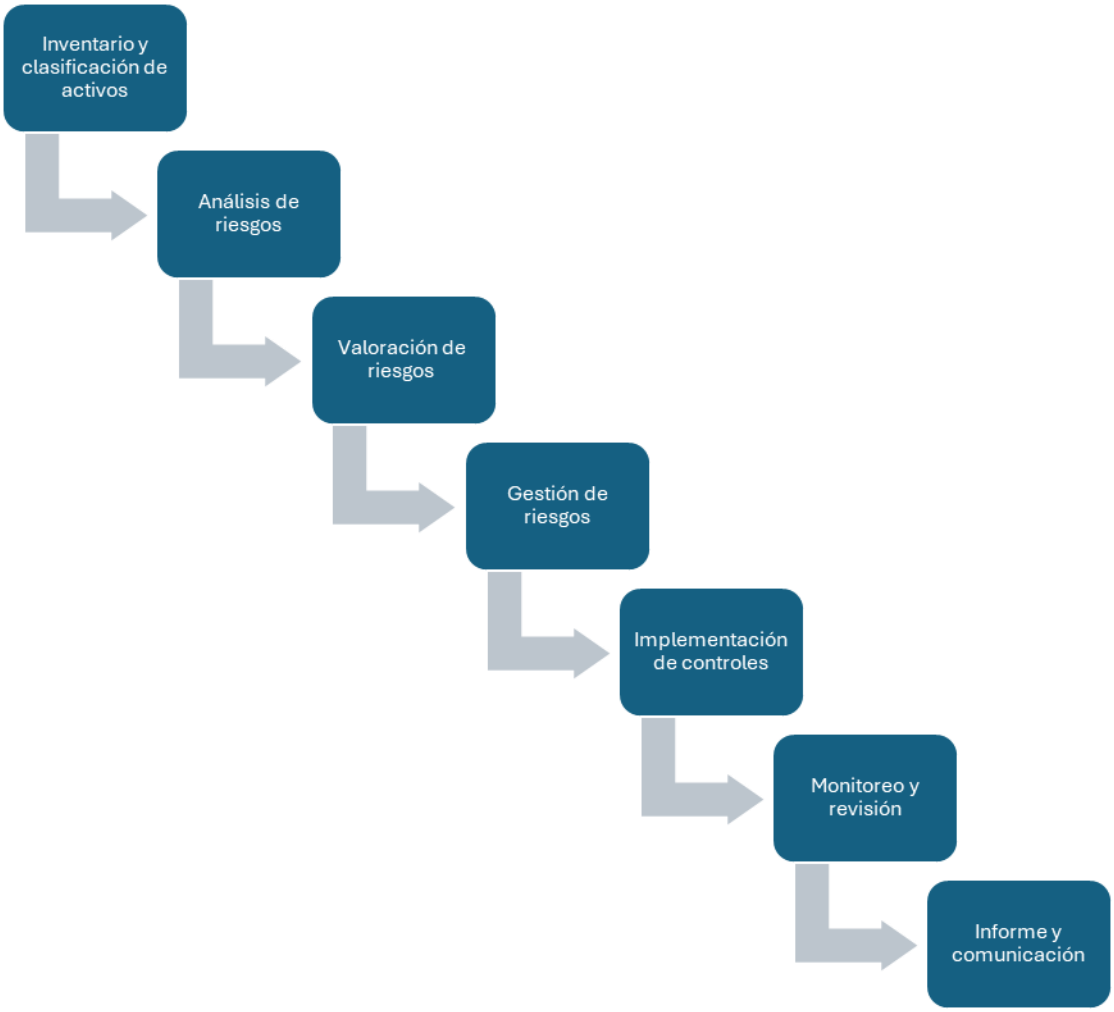


Ilustración 4 fases Metodología Magerit

2.1.1.5 Procesos de auditoría informática

2.1.1.5.1 *Planificación y preparación de la auditoría*

En esta primera fase el auditor debe tener en claro los objetivos y determinar lo que se quiere lograr al final de la auditoría. En primer lugar, hace contacto con el entorno de la institución a auditar para identificar áreas clave. Luego, obtener la información necesaria, como las áreas de riesgo. Por último, dar la relevancia necesaria a cada riesgo ya que no todos tienen la misma importancia. Para la planificación es necesario llevar las fechas con una cronología y contactar con el área que se va a realizar la auditoria.

2.1.1.5.2 *Ejecución de la auditoría*

Es importante considerar que los papeles de trabajo son la principal evidencia del proceso realizado. Para ejecutar una auditoria es necesario realizar pruebas de riesgo, analizar la evidencia y certificarla. Se debe agregar que siempre al final hay que realizar una recomendación.

2.1.1.5.3 *Evaluación y análisis de los resultados*

En esta fase se realiza un análisis de los resultados obtenidos en las etapas anteriores. Donde se encuentran las debilidades en el área a auditar y se establecen áreas de mejora. También se determina cual es el nivel de cumplimiento con las políticas.

2.1.1.5.4 *Presentación de informes y seguimiento*

Finalmente se realiza una guía que detalla los resultados de los hallazgos en la institución y recomendaciones además de las conclusiones pertinentes. Este informe tiene que ser claro, preciso y conciso para que los encargados de las áreas a evaluar tengan en cuenta. Después de que el informe se haya entregado es preciso que se dé seguimiento a las recomendaciones para establecer las mejoras y que permanezcan bastante tiempo.

2.1.1.6 Controles en auditoría informática

2.1.1.6.1 *Identificación de riesgos en sistemas informáticos*

Es evaluar las posibles causas de amenaza que poseen los equipos informáticos. En esta etapa se diseñan los identificadores para que el proceso sea eficaz.

2.1.1.6.2 *Controles internos y externos*

Auditoría interna

La auditoría interna se implementa por el personal que trabaja en la empresa, se organiza para el servicio de la dirección, para controlar y proporcionar un dictamen interno de las actividades que se realizan en ésta (LOZANO, 2014).

Auditoría externa

La auditoría externa es implementada por personal externo para que puedan emitir una opinión técnica de los procesos que se desarrollan en la empresa (LOZANO, 2014).

2.1.1.7 Auditoría informática de la Seguridad Física en las áreas de cómputo

En el siguiente trabajo se realizó el estudio concreto de la auditoria informática en seguridad física donde se muestran las ventajas de implementarla ya que esta permite reducir riesgos los cuales pueden ser inundaciones, terremotos, fuego y daños en el área de cómputo. Además, este trabajo tiene el objetivo de demostrar que es laborioso realizar auditorías informáticas porque muchas de las personas no conocen las ventajas de realizarlas. Por el contrario, desconocen el tamaño del daño al que se enfrentan al no realizar auditorías de seguridad física en las áreas de cómputo (Anabel, 2011).

Ventajas de la auditoria informática en seguridad física

a) Reduce los riesgos en el área, estos pueden ser: inundación, terremoto, fuego y daños en el área.
b) Informa en qué estado se encuentra y cuáles pueden ser las fallas que se pueden presentar a futuro.
c) Mantiene un ambiente y acceso físico controlado.
d) Brinda seguridad al hardware y al personal de la institución.
e) Examina la eficacia y eficiencia que posee la organización para determinar errores y proporcionar las correcciones adecuadas.
f) Detecta fallas que tiene la organización y las toma en cuenta para la toma de decisiones.
g) Reduce en la mayoría de sus casos los riesgos y mejora el área de cómputo mediante soluciones alternas.
h) Acceder a la descripción detallada de la zona que se quiere auditar.

i) Se tiene un mejor control dentro del área de cómputo.

j) Al implementar una metodología se consiguen resultados más óptimos al llevarlos de forma minuciosa.

k) Con la utilización de una metodología dividida en cualitativa y cuantitativa se llega a conocer el alcance y los objetivos de esta (Anabel, 2011).

2.1.1.8 Dificultades e importancia de la Auditoría Informática

El avance de la tecnología en los negocios provoco que emergieran las áreas informáticas las cuales no tenían manera de medir si era correcto o no es por esto que se crea la auditoria informática. El presente trabajo hace una revisión sistemática de las dificultades que tiene en la seguridad de los datos. Aquí se plantean los autores dos preguntas importantes, estas son: ¿Cuáles son los problemas de la auditoria informática?, ¿Importancia de la auditoria informática? Después de la revisión., se concluye que los problemas que hay en la auditoria empieza desde los riesgos personales como la confiabilidad del trabajo del auditor y de como hace para medir la seguridad e integridad de los datos de los servicios en la nube y que su importancia radica en que la actualidad se hace un mayor uso de herramientas de software para el teletrabajo (Moreno & Calvarado Mendoza, 2023).

Variable dependiente

2.1.1.9 Seguridad física

El concepto de seguridad física es un término remoto, hace mucho tiempo que nació la necesidad de protección, debido al incremento de la delincuencia, se moldeó lo que hoy en día se conoce como seguridad física. La seguridad física es un requisito necesario para el ser humano ya que protege la integridad humana y la propiedad (Montejo Suarez, 2014).

La seguridad física es un control que se lleva a cabo en las instalaciones de la empresa ya que, puede afectar a la integridad, confidencialidad, disponibilidad. En esta sección se realizan los controles necesarios para descartar posibles riesgos (Castro Rincón, 2013).

Existen varias amenazas que afectan a los sistemas informáticos estas son los desastres naturales, incendios, inundaciones entre otras causas. Por otro lado, el hombre también es un factor de posibles amenazas por ejemplo puede ocasionar disturbios, sabotajes internos o externos (Oliva, (2013)).

2.1.1.10 Tipos de seguridad informática

Seguridad lógica: este tipo de seguridad se ocupa de consolidar la parte del software es decir todo lo que no es físico, así como son: los programas, los datos que permiten acceder al sistema informático. El sistema debe de realizarse debidamente y por los usuarios autorizados ya sea dentro o fuera en otras palabras desde una red externa usando VPN. Dentro de la seguridad lógica existen programas que se encargan del control de acceso de los procesos de los usuarios a los recursos del programa (Ovalle & Cervantes Sánchez, 2012).

Seguridad Física: se usan para proteger los equipos informáticos a través de los controles utilizando barreras que protejan físicamente la institución de las amenazas que pueden existir por la acción humana ya sea accidental o voluntaria o por desastres naturales. Las amenazas que puede provocar el hombre pueden ser de manera accidental como, por ejemplo: el olvido de la clave de seguridad. De manera voluntaria por ejemplo el robo de la información, la eliminación de la información etc. Y por desastres naturales puede ser inundaciones e incendios (Ovalle & Cervantes Sánchez, 2012).

2.1.1.11 Amenazas en seguridad física

Las amenazas se clasifican en dos estas son las siguientes:

Amenazas informáticas externas: son aquellas que ocurren al exterior de la instalación y no se posee un control del área de TI, estas pueden ser: troyanos, gusanos o virus.

Amenazas informáticas internas: son aquellas que ocurren dentro de las instalaciones y pueden tener un control del departamento de TI, estas pueden ser robo de datos y el ingreso no autorizado al sistema informático (Herrera Mora, 2024).

2.1.1.12 vulnerabilidades en seguridad física

Según (Edwin & Víctor, 2023) Las vulnerabilidades en seguridad física que perjudican el medio son:

Incendios: Son provocados ocasionalmente por colillas de cigarrillos, deterioro de las instalaciones eléctricas, la falta de un uso adecuado de sustancias peligrosas.

Inundaciones: Las inundaciones se generan por la acumulación de agua y la falta de drenaje.

Terremotos: Normalmente a esta amenaza se la clasifica como desastre natural, la tierra ocasiona movimientos leves o intensos que causan la destrucción de edificios y de vidas.

Instalaciones eléctricas: La causa más común de amenazas originada por la incorrecta instalación que pueden ocasionar incendios y electrocución.

2.1.1.13 Origen y evolución de controles de acceso

Los controles de acceso siempre han sido de gran necesidad para las civilizaciones. Se piensa que la primera llave data desde hace 6000 años. Egipto y Babilonia fueron pioneros en su implementación ya que fueron los primeros de la historia en utilizarlos. La cerradura de madera era una herramienta con la que se cerraba las puertas. Eran superiores en volumen comparadas con las cerraduras que se usan hoy en día. La madera era la principal materia prima en la construcción de cerraduras antiguas. Para poder abrir la puerta era necesario utilizar una llave con puntas que al ser introducida levantaba una serie de pines que se ponían en posición para que la puerta pudiera abrirse. Posteriormente los griegos y romanos inventaron el euro cilindro que consistía en una llave de forma cilíndrica que levantaban los pines y los ponían en

la posición necesaria para poder abrir la puerta. Cabe recalcar que estas llaves eran hechas de un material más duradero como lo es el hierro.

En la edad media, usualmente la elaboración de las llaves era realizada por los herreros. Estas consistían en una llave y un cerrojo. Esto ocasionaba que las personas que no tuvieran el acceso a esta llave no podían pasar, y así evitaban el robo de artículos valiosos, cofres, cajas fuertes etc. La revolución industrial permitió avances significativos en cuanto a la fabricación y diseño de las cerraduras y llaves.

El control de acceso a fines del siglo XX restringe el ingreso a los usuarios a algún área a través de varias validaciones. En el año 1960 se desarrolló el primer control de acceso con tarjetas perforadas para acceder a los edificios que implementaban este control. Luego se reemplazó estas por tarjetas con banda magnética. Posteriormente, se inventa los intercomunicadores y los lectores de control de acceso. En 1990, se desarrolla la tecnología RFID que permite la creación de sistemas de control de acceso sin establecer contacto físico. A Finales del siglo XXI se inventó el videoportero IP dando pie a los sistemas de control con más amplitud de funciones (Ashdown, 2023).

2.1.1.14 Tipos de controles de acceso

Existen dos tipos de control de acceso, estos son:

Control de acceso físico: Este tipo de control restringe la entrada a edificios, salas y activos físicos. Normalmente para proteger los activos que poseemos se utilizan llaves y cerraduras. El acceso a la instalación solo se da cuando la persona posee las llaves de la puerta (Klever & Arteaga Zambrano, 2019).

Control de acceso lógico: Este tipo de control al contrario que el primero restringe la entrada a redes de computadoras, archivos del sistema y datos. Además, este tipo de control usa computadoras para solventar los límites que tienen las llaves convencionales (Klever & Arteaga Zambrano, 2019).

2.1.1.15 Protección de Instalaciones y equipos

Las organizaciones poseen barreras de protección contra robos y otras amenazas que atenten contra los equipos tecnológicos. Estas barreras pueden ser: cercados, barreras físicas de protección como materiales en vidrio o iluminación. Los sistemas de seguridad física se dividen en general, natural y estructural. Las barreras naturales son las montañas, lomas cascadas, lugares de difícil acceso. En cambio, las barreras estructurales son aquellas que las elabora el hombre como por ejemplo el techo, cercados, puertas etc (DIAZ, 2019).

2.1.1.16 Políticas y buenas practicas

Las políticas de seguridad aprueban o definen los diferentes protocolos: los métodos, técnicas y herramientas fundamentales para acatar las normas y controles que existen en la institución, las cuales instituyen el conjunto de reglas, leyes y buenas prácticas que generan un modelo para dirigir, amparar y clasificar los recursos en la organización, que van de la mano con los objetivos de seguridad informática dentro de la empresa (López, 2017).

Metodología de desarrollo

En Para llevar a cabo la auditoría informática de la seguridad física en las áreas de cómputo del distrito de educación 13D05 El Carmen, se empleó la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Esta metodología proporciona un marco estructurado y sistemático para identificar, analizar y gestionar los riesgos asociados a los sistemas de información. La aplicación de MAGERIT permitió una evaluación de los controles de seguridad física, identificando vulnerabilidades y proponiendo medidas correctivas para mitigar los riesgos detectados.

El proceso comenzó con la identificación y clasificación de los activos del distrito. Posteriormente, se realizó un análisis detallado de las amenazas potenciales que podrían afectar estos activos, incluyendo riesgos naturales, fallos técnicos y accesos no autorizados. Utilizando las herramientas y técnicas de MAGERIT, se evaluó el impacto y la probabilidad de cada

amenaza, lo que permitió priorizar las áreas de mayor riesgo y enfocar los esfuerzos de mitigación de manera efectiva.

Finalmente, se diseñaron e implementaron medidas de seguridad física específicas para proteger los activos identificados. Estas medidas incluyeron la instalación de sistemas de control de acceso, cámaras de vigilancia, y políticas de seguridad estrictas para el personal. La metodología MAGERIT no solo facilitó la identificación y gestión de riesgos, sino que también promovió una cultura de seguridad dentro del distrito de educación 13D05 El Carmen.

2.2 Conclusiones del marco teórico

En el desarrollo del marco teórico, se muestra que la auditoria informática es fundamental para poder proteger y administrar de forma correcta los recursos tecnológicos en cualquier tipo de organización. El marco teórico propone una base firme para entender la importancia de la seguridad física dentro de las instituciones, específicamente en la protección de los equipos informáticos del distrito de Educación 13D05. La auditoría informática permite el control detallado y constante de los equipos informáticos para de esta manera determinar las debilidades y proporcionar las medidas de seguridad que protejan a los equipos.

La auditoría informática no solo garantiza la protección de los recursos tecnológicos, sino que también permite optimizar su uso. Al realizar evaluaciones periódicas, se pueden identificar áreas de mejora que aumenten la eficiencia operativa y reduzcan costos asociados a fallos o ineficiencias. Por ejemplo, la detección temprana de hardware obsoleto o software desactualizado evita interrupciones inesperadas, promoviendo un entorno de trabajo más confiable y productivo. Esta herramienta también es esencial para mantener un registro actualizado de los activos tecnológicos, asegurando que estos sean utilizados de manera óptima y que estén disponibles para los usuarios cuando los necesiten.

Se debe agregar que, la auditoria informática ayuda a orientar a la organización en la creación de políticas y protocolos de seguridad. Lo que ayuda a crear un entorno seguro para

desarrollar diariamente las actividades dentro de la institución. El personal del distrito hace uso de los sistemas informáticos de forma diaria entonces realizar una auditoria puede asegurar la operatividad ininterrumpida.

La implementación de una auditoría informática en el distrito no solo se limita a identificar vulnerabilidades, sino que también contribuye al fortalecimiento de las políticas de seguridad existentes. Estas auditorías brindan datos concretos que facilitan la actualización y desarrollo de protocolos más robustos y específicos, adaptados a las necesidades de la institución. Por ejemplo, se pueden establecer medidas estrictas sobre el manejo de contraseñas, acceso físico a los equipos y el uso responsable de redes internas. Al contar con políticas claras, el distrito puede garantizar un marco regulatorio que reduzca riesgos y fomente una cultura de cumplimiento y responsabilidad entre los usuarios.

El uso de esta herramienta para evaluar el control en el distrito tiene sus beneficios para el personal que labora en la institución ya que afianza un acceso seguro a los recursos tecnológicos. Dentro de la institución se impulsa una cultura de seguridad y responsabilidad compartida lo que da a lugar a que los usuarios sean conscientes de las buenas prácticas y el cumplimiento d Un entorno seguro es fundamental para el correcto desarrollo de las actividades en cualquier institución educativa. En el caso del distrito de Educación 13D05, la auditoría informática ayuda a garantizar que los equipos estén protegidos contra accesos no autorizados, fallas técnicas y ataques cibernéticos. Esto no solo protege la información crítica almacenada en los sistemas, sino que también proporciona confianza al personal y estudiantes que dependen de estos recursos para sus labores diarias. Asimismo, un entorno seguro mejora la calidad del trabajo, pues elimina las preocupaciones relacionadas con incidentes de seguridad y permite que las actividades se lleven a cabo sin interrupciones las políticas de seguridad.

La auditoría informática es una herramienta poderosa para fomentar la concienciación entre los usuarios sobre la importancia de seguir buenas prácticas de seguridad. Durante el proceso de auditoría, los empleados tienen la oportunidad de aprender sobre los riesgos asociados al manejo inadecuado de los recursos tecnológicos. Por ejemplo, se pueden organizar sesiones de capacitación basadas en los hallazgos de la auditoría, donde se enseñen conceptos clave como la gestión de datos sensibles o la identificación de correos electrónicos sospechosos. Este enfoque no solo fortalece la seguridad, sino que también crea un sentido de

responsabilidad compartida, donde cada usuario se convierte en un aliado en la protección de los recursos del distrito.

Por último, la auditoría informática desempeña un papel crucial en la sostenibilidad a largo plazo de los recursos tecnológicos del distrito. Al identificar problemas potenciales antes de que se conviertan en fallos críticos, se pueden implementar medidas preventivas que prolonguen la vida útil de los equipos y reduzcan costos de reemplazo. Además, la auditoría permite priorizar las inversiones en tecnología, asegurando que se destinen recursos a áreas críticas y se maximice el retorno de inversión. Esto no solo beneficia al distrito en términos económicos, sino que también refuerza su capacidad para ofrecer un entorno educativo moderno y eficiente, alineado con las demandas tecnológicas actuales.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

En este capítulo se procedió a describir los tipos y metodologías de investigación que se utilizaran para demostrar que es necesario realizar la auditoria informática en las instalaciones del distrito de educación 13D05, El Carmen, por lo tanto, se ejecutaron una serie de interrogantes (entrevista y encuesta) al encargado del área de Tecnologías de la información y la directora del distrital además del personal administrativo.

De esta forma se recolectaron datos para poder cumplir con el objetivo del siguiente capitulo y a su vez con los datos de la encuesta y entrevista podremos conocer a partir de donde empezar la auditoria informática para ayudar a el correcto funcionamiento de los equipos informáticos e instalaciones del distrito.

La recolección de datos a través de entrevistas y encuestas fue fundamental para identificar las necesidades específicas del distrito en términos de seguridad informática. Estas herramientas permitieron obtener información de primera mano sobre las debilidades percibidas, los riesgos recurrentes y las prácticas actuales del personal. Por ejemplo, una

encuesta al personal administrativo puede revelar hábitos inseguros como el uso de contraseñas débiles, mientras que una entrevista con el encargado de TI puede ofrecer una visión técnica más detallada sobre las áreas críticas que requieren atención inmediata.

3.2 Tipos de investigación

Investigación descriptiva

Este enfoque trata de realizar un análisis de contenido para que sea útil en la investigación. La investigación descriptiva es un proceso que se debe llevar a cabo para que ésta sea completa y legible. El fenómeno a investigar cada vez será más complejo y es por ello que mediante el uso de la investigación descriptiva podremos realizar con más detalle y precisión la investigación. Esta metodología parte desde el inicio en el que aparece el objeto a investigar e indaga en las diversas fuentes de investigación previas para lograr ser un referente para futuras investigaciones sobre el tema.

La investigación descriptiva se utilizó para detallar el estado actual del Distrito de educación 13D05 mediante el uso de instrumentos de recolección de datos como son: encuestas, entrevistas además de observaciones que se realizaron en las instalaciones. Esto ayudara en la investigación ya que gracias a ello se puede recabar información sobre las falencias en seguridad física que tiene la institución.

Investigación bibliográfica

La investigación bibliográfica es toda aquella información que se va recaudando sobre el tema a investigar. En la investigación bibliográfica es importante la validez de la información ya que con las fuentes como libros, revistas e informes se realiza un análisis para una posterior síntesis de dicha información recopilada.

Esta recopilación de información fue primordial porque contiene las bases del conocimiento de investigaciones anteriores, esta investigación fue realizada en el marco teórico amparando la teoría de la auditoria informática física como una disciplina más de las tecnologías de la información.

Investigación de campo

La investigación de campo se refiere a la observación del entorno a investigar en el tiempo en el que suceden los fenómenos. Este tipo de investigación se usa para poder recopilar información y dar respuesta a las preguntas de investigación. Consecuentemente, se obtendrá información cualitativa y cuantitativa.

Este tipo de investigación se llevó a cabo para observar directamente las instalaciones y determinar los puntos de control de acceso y los mecanismos para la seguridad de los equipos informáticos.

3.3 Métodos de investigación

Analítico – Sintético

En esta investigación se aplicó el método analítico-sintético, el análisis es el proceso que trata de extraer los elementos de un fenómeno e inspeccionar cada uno por separado (Somano & Medina León, 2020).

Este método se utilizó para descomponer el fenómeno de la auditoría informática en sus componentes básicos, permitiendo un análisis detallado de cada uno de ellos. Posteriormente, se integraron los elementos analizados para comprender las relaciones entre ellos y cómo contribuyen al funcionamiento general del sistema de seguridad informática.

Inductivo – Deductivo

La inducción puede ser entendida como el razonamiento que intenta establecer enunciados universales ciertos a partir de la experiencia. La deducción el tipo de inferencia que, partiendo de enunciados generales o universales, nos conduce a enunciados particulares, singulares. (Somano & Medina León, 2020).

Se usó inducción para analizar datos observados y extraer conclusiones generales sobre la seguridad. La deducción permitió evaluar estas conclusiones frente a normas y derivar recomendaciones específicas.

Dentro del estudio de campo se realizó para conocer más a fondo la seguridad física del Distrito de educación y en la auditoria se hizo un análisis de riesgo para probar los parámetros de la seguridad lo que logro realizar una guía para dar una solución a la problemática de la seguridad informática en el Distrito 13D05 El Carmen.

3.4 Fuentes de información de datos

Encuestas

La técnica de encuesta trata de recopilar información interactuando con el entrevistado a través de un interrogatorio a favor del entrevistador. La encuesta se realiza mediante un cuestionario, está dirigido a las personas de establecimiento para conocer sus opiniones, recomendaciones o comportamientos y su finalidad es obtener resultados mayormente numéricos (Gonzáles, 2020).

Primero, se elaboró 13 preguntas relacionadas con la seguridad física de los equipos informáticos, diseñadas para identificar riesgos potenciales. Estas preguntas fueron aplicadas al personal administrativo del distrito educativo con el objetivo de recopilar información sobre las condiciones y posibles amenazas que afectan la institución.

Entrevista

Es un procedimiento donde se recauda información a través de una conversación cara a cara, dando la oportunidad de que el entrevistado se exprese libremente, donde el entrevistador debe ir dirigiendo la entrevista hacia los objetivos pretendidos. Su objetivo principal es dar una connotación de expresión libre donde la recogida de información la proporciona el discurso del entrevistado. (Rodríguez, 2011)

En la entrevista se aplicó 16 preguntas dirigidas al encargado de TI y a la directora distrital. Con el fin de conocer riesgos que afecten a la institución y proceder a elaborar la auditoria.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

La población es el conjunto de elementos de estudio. El investigador debe especificar los elementos a investigar. Estos elementos se denominan individuo o unidad estadística estos pueden ser personas, animales, registros. (Pino, 2008)

El Distrito de educación 13D05 cuenta con 23 personas que utilizan los equipos informáticos donde el responsable es el Ing. Daniel Carrasco, encargado del departamento de TI. Estos equipos se utilizan dentro del horario laboral, es decir, de 8 de la mañana hasta las cinco de la tarde.

3.5.2 Segmentación

3.5.2 Muestra

La muestra es el subconjunto de la población es decir un tamaño limitado de individuos extraídos de la población o universo. Se tiene como objeto disminuir el número de muestras. (Pino, 2008)

La población en este caso es de 23 personas, se tomó la decisión de utilizar una muestra censal, para ello es necesario considerar a la población en su totalidad ya que esto asegura que los resultados sean representativos.

3.5.4 Tamaño de la muestra

3.5.5 Análisis de las herramientas de recolección de datos a utilizar

3.5.1.1 Encuesta

Encuesta Dirigida a: Personal que labora en el Distrito 13D05 El Carmen.

Objetivo: Conocer el estado en cuanto seguridad física desde la perspectiva del personal que labora en la institución.

Nombre de la empresa: Distrito de Educación 13D05 El Carmen.

¿Conoce usted si la institución cuenta con seguridad física?

Si No

¿Seleccione el tipo de seguridad física con la que cuenta la institución?

Guardia Cámaras

Ruta de evacuación

Botón de pánico

No cuenta con seguridad física

¿En su lugar de trabajo, existe una señalética para evacuar el edificio en caso de emergencia?

Si___ No___

¿Ha recibido capacitación sobre riesgos laborales?

Si___ No___

¿Si la respuesta anterior es sí, cuando fue la última vez que lo capacitaron?

Hace 6 meses

Hace 1 año

Hace más de un año

¿Tiene conocimiento de un manual o guía de buen uso de equipos informáticos?

Si ___ No ___

¿Se hace mantenimiento frecuente de los computadores o se espera a que estos se dañen?

Una vez al año

Dos veces al año Cuando se dañan Nunca

¿El cableado de la red de computadoras, se encuentra correctamente conectado al equipo?

Si___ No___

¿El servicio de guardianía esta todo el tiempo disponible?

Si___ No___

¿Existe alarma contra incendio?

Si___ No___

¿Existen extintores?

Si___ No___

¿Existe un inventario físico en la Institución?

Si___ No___

¿Se realizan auditorías físicas en la Institución?

Si___ No___

3.5.1.2 Entrevista

Objetivo: Conocer el estado en cuanto seguridad física con el fin de conocer si es preciso realizar una auditoria informática en la institución.

Entrevista dirigida a: Directora Distrital y el encargado del área de TI en la institución.

Nombre de la empresa: Distrito de Educación 13D05 El Carmen.

¿Con que tipo de seguridad física cuenta el Distrito de Educación?

¿Qué tipo de señalética informativa existe para evacuar el edificio en caso de emergencia?

¿En la institución, los servidores públicos reciben periódicamente capacitación en riesgos laborales?

¿Los usuarios de computadoras, cuentan con un reglamento de buen uso?

¿Los equipos cuentan con un regulador de voltaje?

¿Alguna vez los equipos informáticos se han averiado por cuestiones de lluvia?

¿Los mantenimientos se realizan en base a una planificación adecuada?

¿Cree usted que la infraestructura física es la adecuada para los equipos de cómputo?

¿Se tiene alarmas contra incendio?

¿Se controla el acceso a la institución?

¿Si se tiene guardianía estos están las 24 horas y en algún momento han dejado de dar servicios por falta de pago o renovación de contratos?

¿Los usuarios conocen el uso que se les debe dar a los ciclos de carga de las portátiles?

¿Si existen extintores se ha procedido a recargar estos cómo lo exige el manejo de los mismos?

¿En la institución existe un inventario físico?

¿Se realizan Auditorias físicas en la institución?

3.5.6 Estructura de los instrumentos de recolección de datos aplicado

En este caso se hizo uso de una entrevista dirigida a el encargado del área de Tecnologías de la información en el distrito de educación 13D05 El Carmen y a la directora distrital con el fin de conocer la situación en la que se encuentran los equipos informáticos dentro de la institución y conocer si es preciso realizar la auditoria informática. Esta entrevista tuvo un total de 15 preguntas abiertas donde la persona pudiera responder de forma maleable y con tranquilidad.

Por otro lado, también se aplicó una encuesta, en este caso contaba con un total de 14 preguntas, con la gran diferencia de que sus preguntas serian del tipo cerradas, pues la intención de esta encuesta fue recoger datos cuantitativos los cuales se puedan contabilizar, la encuesta fue aplicada al personal que labora en el distrito de educación 13D05 El Carmen, con el fin de conocer el estado en cuanto a seguridad física dentro de la institución, desde el punto de vista del personal de la institución.

3.5.7 Plan de recolección de datos

Para la recolección de los datos se procedió a realizar un diagnóstico del estado del distrito de educación 13D05 El Carmen en el cual se revisó el estado físico de las instalaciones, revisando si existen vulnerabilidades que puedan implicar amenazas en la institución. Esto se

aplicó por la investigadora durante el año 2024. Los instrumentos que se utilizaron fueron la encuesta y entrevista las cuales se aplicaron para poder recoger datos, estos instrumentos se aplicaron una sola vez. Las preguntas dirigidas al personal que labora en la institución se aplicaron de forma presencial. Se escogió un día miércoles para lograr empatía con el horario del personal para realizar con tranquilidad y de forma descansada, logrando así una mejor sintonía para responder de manera adecuada.

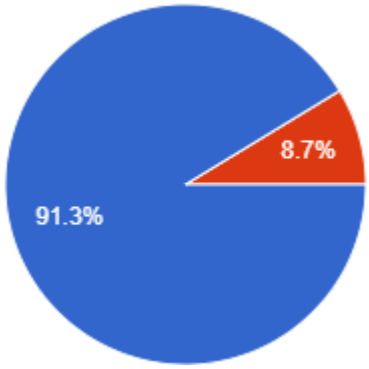
3.5.6 Análisis y presentación de resultados

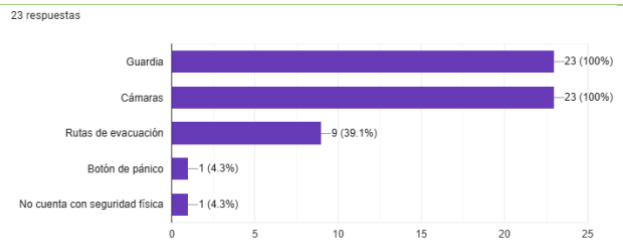
3.5.2 Tabulación y análisis de los datos

3.5.3 Encuesta aplicada al personal que labora en el distrito de educación 13D05 El Carmen.

Tabla 1: Tabulación y análisis de datos

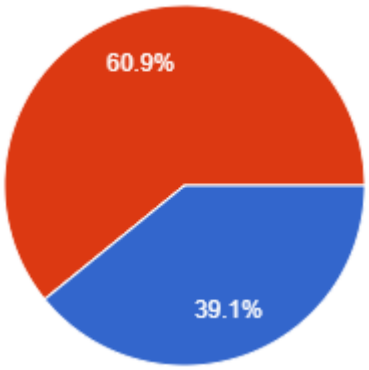
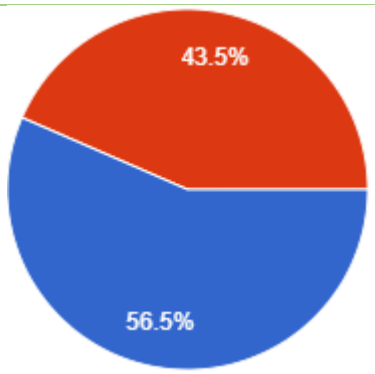
<table>
<tr><th>Pregunta</th><th>Gráfico</th></tr>
<tr><td>¿Conoce usted si la institución cuenta con seguridad física?

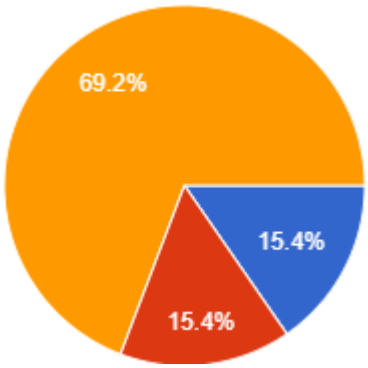
Si
No</td><td> 
</td></tr>
<tr><td colspan="2">Interpretación: En esta pregunta podemos ver que la mayoría (91.3%) del personal conoce sobre las medidas de seguridad física en la institución, lo que significa que existe una buena conciencia general sobre este ámbito.</td></tr>
<tr><td>¿Seleccione el tipo de seguridad física con la que cuenta la institución?

Si
No</td><td> 
</td></tr>
<tr><td colspan="2">Interpretación: En esta pregunta podemos observar que hay un porcentaje de 39.1% de los encuestados que mencionan que existe la presencia de guardias, y otro de 4,3 que determina que la institución cuenta con cámaras rutas de evacuación y botón de pánico. Los siguientes datos demuestran que existe una dependencia representativa en la vigilancia humana, con escasas medidas adicionales de seguridad.</td></tr>
</table>

Fuente 1: Elaboración propia

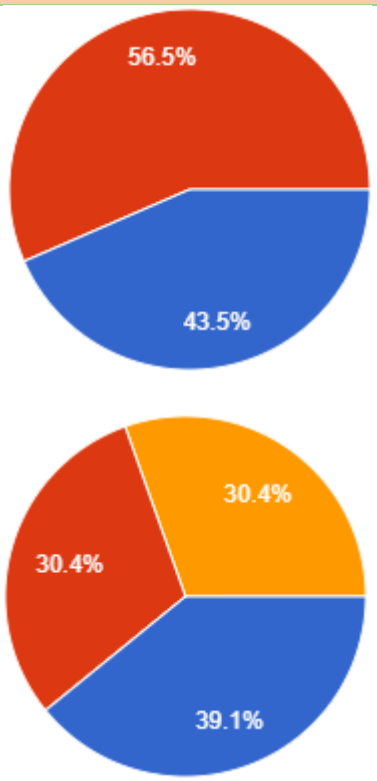
Tabla 2: Tabulación y análisis de datos

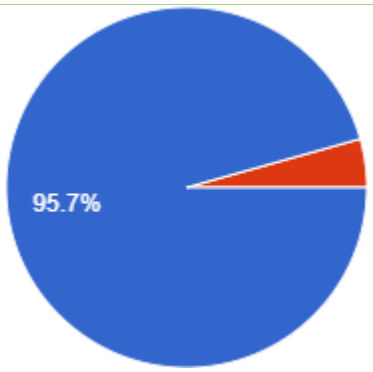
<table>
<tr><th>Pregunta</th><th>Gráfico</th></tr>
<tr><td>¿En su lugar de trabajo, existe una señalética para evacuar el edificio en caso de emergencia?
Si
No</td><td> 
</td></tr>
<tr><td colspan="2">Interpretación: En la pregunta sobre si existen señaléticas en el lugar el 60,9% respondió que si existen señaléticas para evacuar el edificio, esto de cierta manera es positivo para la seguridad de la institución en situaciones de peligro, aunque un 39, 1% dicen que no observan estas indicaciones, lo cual se convierte en un área para mejorar.</td></tr>
<tr><td>¿Ha recibido capacitación sobre riesgos laborales?
Si
No
¿Si la respuesta anterior es sí, cuando fue la última vez que lo capacitaron?
Hace 6 meses
Hace 1 año
Hace mas de un año</td><td> 


</td></tr>
<tr><td colspan="2">Interpretación: En este caso podemos observar que solo el 56.5% han recibido capacitación en riesgos laborales, y el 43.5 no cuenta con este tipo de capacitación. Además de que los que, si están capacitados, un 69.2% lo hace más de un año, en consecuencia, indica que les falta una actualización periódica en esta área.</td></tr>
</table>

Fuente 2: Elaboración propia

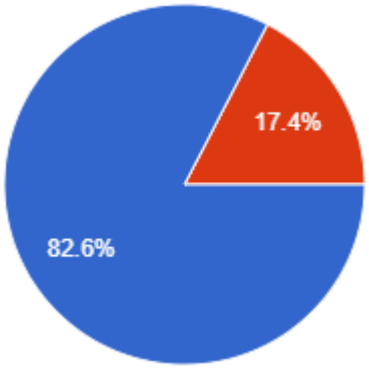
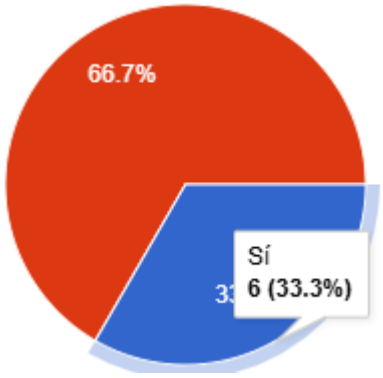
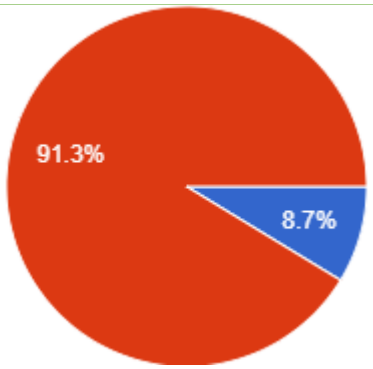
Tabla 3: Tabulación y análisis de datos

<table>
<tr><th>Pregunta</th><th>Gráfico</th></tr>
<tr><td>¿Tiene conocimiento de un manual o guía de buen uso de equipos informáticos?
Si
No
¿Se hace mantenimiento frecuente de los computadores o se espera a que estos se dañen?
Una vez al año
Dos veces al año
Cuando se dañan
Nunca</td><td> 

</td></tr>
<tr><td colspan="2">Interpretación: Aquí podemos concluir con que la mayoría de conocer sobre el manual con un porcentaje de 56.5, solo el 30.4% recibe un mantenimiento anual, entretanto el 39.1% espera que se dale el equipo para realizar las respectivas reparaciones. Esto da a lugar a un enfoque reactivo en lugar de preventivo en cuanto al mantenimiento.</td></tr>
<tr><td>¿El cableado de la red de computadoras, se encuentra correctamente conectado al equipo?
Si
No</td><td> 
</td></tr>
<tr><td colspan="2">Interpretación: En este caso podemos presenciar que casi por completo responden que si se encuentra bien conectado, esto genera positividad en términos de infraestructura.</td></tr>
</table>

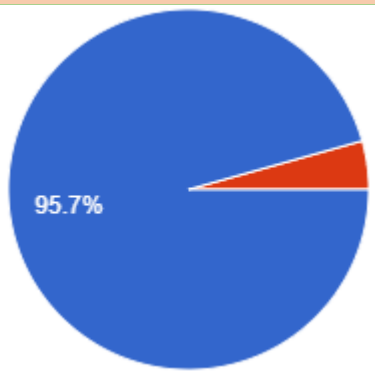
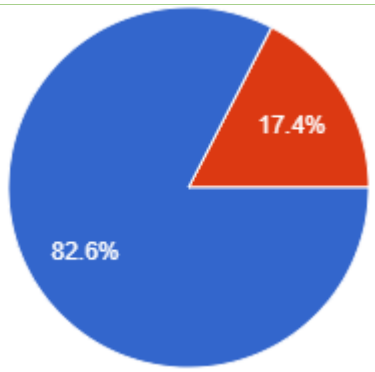
Fuente 3: Elaboración propia

Tabla 4: Tabulación y análisis de datos

Pregunta	Gráfico
¿El servicio de guardianía esta todo el tiempo disponible? Si No	
Interpretación: En este caso el 82,6% informo que el servicio de guardianía se encuentra disponible lo que indica que existe menor incidencia a que los equipos se expongan a cualquier tipo de peligro.	
¿Conoce el uso correcto de los ciclos de carga de la batería de las portátiles? Si No	
Interpretación: En este caso se puede observar que el 66.7% indico no conocer el uso de los ciclos de carga de las portátiles, entretanto que el 33,3% indica afirmativamente que conocen su ciclo, lo que demuestra que existe una falta de conocimiento en general en este sentido.	
¿Existe alarma contra incendio? Si No	
Interpretación: El 91,3% respondieron que no existen alarma contra incendios lo cual revela que existe gran vulnerabilidad en la protección contra emergencias. Las alarmas son esenciales para la institución ya que detectan de modo rápido si existe alguna emergencia.	

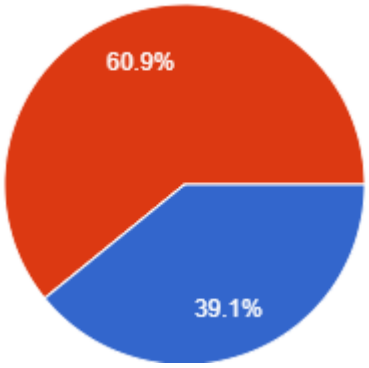
Fuente 4: Elaboración propia

Tabla 5: Tabulación y análisis de datos

Pregunta	Gráfico
¿Existen extintores? Si No	
Interpretación: Aquí podemos observar que el 95.7% responde que si existen extintores dentro de la institución lo cual es favorable porque la institución ha tomado medidas para responder de manera directa en caso de existir alguna emergencia.	
¿Existen un inventario físico en la institución? Si No	
Interpretación: En este grafico podemos observar que existe un 82.6% de los encuestados indica que si existe un inventario físico y refleja que dentro de la institución existe un esfuerzo para amparar el control sobre los activos y recursos de la institución.	

Fuente 5: Elaboración propia

Tabla 6: Tabulación y análisis de datos

Pregunta	Gráfico
¿Se realizan auditorias físicas en la Institución? Si No	
Interpretación: En este grafico se puede observar que el 60.9% de los encuestados afirmo que no se realizan auditorias físicas en la institución y un 39.1% responde que sí. Lo que evidencia de que no se hacen auditorias físicas.	

Fuente 6: Elaboración propia

3.6.3 Entrevista dirigida a la directora distrital y el encargado del área de Tecnologías de la información del distrito de educación 13D05 El Carmen.

Tabla 7: Análisis de la Encuesta

Pregunta	Respuesta directora	Respuesta del encargado de TI	Análisis
¿Con qué tipo de seguridad física cuenta el Distrito de Educación?	Guardias. Guardias y unas que otras cámaras instaladas internamente. Sí tiene cámaras, pero dentro de la oficina no, aparte en los pasillos.	Bueno, siempre hay servicio de guardianía, el Distrito cuenta con servicio de guardianía, también el de cámaras. Pero es un circuito cerrado, porque son los internos, no es así afuera. Solo el circuito es interno, nada más. Esas seguridades tiene el Distrito.	Ambas partes coinciden en que el distrito tiene guardias y cámaras, sin embargo, estas solo son internas, lo que limita la cobertura en áreas exteriores y puede exponer la infraestructura a áreas de monitoreo.
¿Qué tipo de señalética informativa existe para evacuar el edificio en caso de emergencia?	Todo, todo lo que exige el cuerpo de bomberos. Puntos de encuentro, todas esas cosas que exigen.	Te comento que ahorita creo que no hay, lo que sí hubo, pero... Estas se habían pintado en las aceras por donde tenían que salir	Da como evidencia que existe una contradicción porque la directora asiente que dentro de la institución se cumple con los requisitos que establece el cuerpo de bomberos. No obstante, el encargado de TI transmite duda sobre la existencia de señaléticas en la institución.

Fuente 7: Elaboración propia

Tabla 8: Tabulación y análisis de datos

Pregunta	Respuesta directora	Respuesta del encargado de TI	Análisis
¿En la institución, los servidores públicos reciben periódicamente capacitación en riesgos laborales?	Sí, todos, en las unidades educativas también.	Casi no, como una vez al año.	La directora afirma que se hacen capacitaciones regulares, entretanto el encargado de TI dice que se llevan a cabo una vez al año. En este caso existe discrepancia en la percepción de la frecuencia de la capacitación, es decir que esto afecta en la preparación del personal frente a los riesgos.
¿Los usuarios de computadoras, cuentan con un reglamento de buen uso?	Bueno, la mayoría tienen computadoras personales y otras son del Estado. Si son del Estado existe un compromiso de por medio, no, del buen uso	Sí, se les pasa así**.**	Ambos coinciden que se cuenta con el compromiso de buen uso para los equipos en la institución, sin embargo, no existe ningún seguimiento del reglamento del uso correcto de los equipos.
¿Los equipos cuentan con un regulador de voltaje?	Ninguno.	Bueno, la mayoría no, porque son equipos portátiles, entonces casi no se utilizan ahorita ya los que son los equipos principales del servidor y los del internet. Ellos sí tienen un UPS que dura varias horas de almacenamiento de la energía.	Los equipos no poseen reguladores de voltaje salvo los equipos principales como los servidores y los de internet. Empero evidencia de que sin estos equipos la mayoría de los equipos sufren un riesgo de daño por fluctuaciones eléctricas.

Fuente 8: Elaboración propia

Tabla 9: Tabulación y análisis de datos

Pregunta	Respuesta directora	Respuesta del encargado de TI	Análisis
¿Cree usted que la infraestructura física es la adecuada para los equipos de cómputo?	¿Qué te puedo decir yo?, todos tenemos una expectora, sí, lo considero que sí, la infraestructura física también, porque todos tienen su aire acondicionado, todos están en un lugar limpio, buena humedad, todo eso.	Sí, sí es adecuada.	Ambos coinciden en que la infraestructura es adecuada. Esto sugiere que el lugar de trabajo es propicio para la operación de los equipos.
¿Se tiene alarmas contra incendio?	No.	No.	En ambos casos coinciden en que no se cuenta con una alarma contra incendios lo que significa carencia en la seguridad física del lugar.
¿Se controla el acceso a la institución?	Si.	Si.	En este caso los entrevistados coinciden con que si se da un control de acceso para el ingreso a la institución, esto da indicios de una medida de seguridad efectiva en el control de ingreso al área.

Fuente 9: Elaboración propia

Tabla 10: Tabulación y análisis de datos

Pregunta	Respuesta directora	Respuesta del encargado de TI	Análisis
¿Si se tiene guardianía estos están las 24 horas y en algún momento han dejado de dar servicios por falta de pago o renovación de contratos?	24-7. ¿O renovación de contrato? No, 24-7, antes de que se termine el contrato ya se está o renovándola ella misma o contratando una nueva empresa, pero sin guardianía no nos quedamos nunca.	Más bien por renovación de contrato. O sea, a veces el recurso no llega enseguida cuando ya se le finaliza a la empresa el contrato que tiene. Porque a veces llega para seis meses, a veces un año, a veces ocho meses. Entonces ya cuando se le cumple la fecha a veces no llega enseguida el recurso nuevo para contratar. Entonces ahí sí se queda el distrito sin servicio.	La directora sostiene que el servicio de guardianía se da constantemente y se renueva de manera anticipada. En cambio, el encargado de TI dice que, en ciertas ocasiones, se quedan sin guardias debido a atrasos con la renovación de los contratos, lo que da a entender que existe vulnerabilidad en la continuidad del servicio.

Fuente 10: Elaboración propia

Tabla 11: Tabulación y análisis de datos

Pregunta	Respuesta directora	Respuesta del encargado de TI	Análisis
¿Los usuarios conocen el uso que se les debe dar a los ciclos de carga de las portátiles?	No	No.	Ambas partes coinciden con que los usuarios no conocen el uso idóneo de los ciclos de carga de las portátiles, esto representa una oportunidad para dar capacitaciones en cuanto al cuidado de los equipos informáticos.
¿Si existen extintores se ha procedido a recargar estos cómo lo exige el manejo de los mismos?	Sí, eso se encarga el Estado.	Exacto, sí. Sí existe.	Los dos coinciden en que el estado se ocupa de la recarga de los extintores, en este sentido la seguridad esta bajo control.
¿En la institución existe un inventario físico?	Sí, bien correcto.	Si. Eso lo maneja el área administrativa. Ella tiene un sistema que es el ministerio donde están todos los bienes que tiene el ministerio de educación por distrito.	En este caso ambas partes coinciden que en la institución si existe un inventario físico.

Fuente 11: Elaboración propia

Tabla 12: Tabulación y análisis de datos

Pregunta	Respuesta directora	Respuesta del encargado de TI	Análisis
¿Se realizan Auditorias físicas en la institución?	Sí. Bueno. Sí, todo eso se realiza.	Te comento que no. Hasta el momento no.	La directora menciona que se realizan auditorias físicas y el encargado de TI muestra que no se han realizado. En este caso existe discrepancia ya que la respuesta indica falta de claridad en el manejo de los inventarios a su vez esto puede afectar a la gestión de los activos.

Fuente 12: Elaboración propia

3.6.4 Presentación y descripción de los resultados obtenidos

En la siguiente sección, se realizó la triangulación de datos recogidos en la encuesta y entrevista con el propósito de recolectar los resultados, esto con el objetivo de balancear en base de fundamentos teóricos y de esta forma confirmar los hallazgos.

Siendo que en la pregunta 6 de la encuesta donde el 56.5% de los encuestados respondieron que no tienen conocimiento del buen uso de los equipos informáticos, sin embargo, hay que tener presente que en la entrevista en la pregunta 4 ambos tanto la directora como el encargado del área de TI, indican que los usuarios si cuentan con el compromiso del buen uso de los equipos en la institución. En contraste con lo anterior, en la pregunta 7 sobre si se realiza un mantenimiento frecuente a los computadores el 39.1% de los encuestados responden que esperan a que el equipo se dañe para realizar las respectivas reparaciones, a su vez, en la pregunta 7 de la entrevista la directora dijo que los mantenimientos se los realiza cuando el equipo se avería, esto nos lleva a concluir y a verificar lo dicho por la directora y encuestados ya que no se está realizando un mantenimiento preventivo y así mismo no se da un buen uso a las computadoras.

En la pregunta 3, en la que se cuestiona a los encuestados sobre si existen señaléticas para evacuar el edificio en caso de emergencia el 60.9 % responde que no, hay que tener en cuenta que en la pregunta 2 de la entrevista el encargado hace saber que en la institución antes el piso tenía franjas que señalaban la ruta de evacuación, pero en el momento de la entrevista no las hay, lo cual ayuda a concluir que hacen falta más señaléticas que ayuden a evacuar el edificio en caso de emergencia.

Además de que en la pregunta 4 se cuestiona a los encuestados si han realizado algún tipo de capacitación sobre riesgos laborales en la institución, el 56.5% responden que si han realizado capacitaciones sobre esta área. En contraste a la pregunta anterior, se despliega si la respuesta es sí cuándo fue la última vez que lo capacitaron el 69.2% lo realizaron hace más de un año, el 15.4% hizo la capacitación hace 6 meses y el 15.4% restante hizo la capacitación hace 1 año. En lo cual se concluyó que en la institución no existe una actualización periódica en esta área importante para la prevención de los riesgos que pueden coexistir en el área de labores.

Por otra parte, se llega a observar que en la pregunta 14, se pregunta a los encuestados si se realizan auditorias físicas en la institución el 60.9% respondieron que no se realizan auditorias física, lo cual concuerda con el encargado en la pregunta 15 de la entrevista que responde que hasta el momento no se han realizado auditorias físicas en la institución. Esto ayuda a concluir que no se tiene conocimiento claro sobre el inventario y en consecuencia esto puede afectar a la gestión de los activos.

3.6.5 Informe final del análisis de los datos

Se puede concluir que, los resultados obtenidos en los instrumentos que se aplicaron desvelan la realidad sobre la gestión de riesgos y datos en el distrito de educación objeto de estudio, ta que no existe un control exhaustivo que pueda mitigar los riesgos sobre seguridad física. Adicionalmente, se pudo evidenciar que en su mayoría desconocen de estas prácticas, a su vez se da importancia a la auditoria informativa para realizar mejoras en cuanto a la gestión del control de riesgos.

Los hallazgos de la auditoria informática desarrollada en el distrito de educación, con base a los resultados de los instrumentos han sido adecuados para la obtención de resultados que dan a notar vulnerabilidades en cuanto a seguridad física, y en efecto manifiestan el análisis y gestión de riesgos de los equipos informáticos en el distrito de educación objeto de estudio.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

El presente capítulo describe la ejecución de la auditoría inicial en el Distrito de Educación, aplicando los principios de la metodología Magerit para detectar brechas existentes en la seguridad física relacionada con los equipos informáticos. Habrá de realizarse un análisis de los sistemas de seguridad vigentes en el Distrito para detectar eventuales vulnerabilidades, analizando las amenazas que pueden afectar tanto la integridad de los equipos como de la información que se procesa en el distrito. Este análisis será el adecuado para detectar los niveles de riesgo y las medidas a adoptar para conseguir un adecuado estatus de protección de os recursos informáticos.

En primer lugar, se llevó a cabo una revisión de la infraestructura física del Distrito. Esto incluyó la inspección de las instalaciones, la verificación de los controles de acceso y la evaluación de los sistemas de vigilancia. Se identificaron varias áreas críticas que requieren mejoras, como la instalación de cámaras adicionales en puntos ciegos y la actualización de los sistemas de control de acceso para incluir tecnologías biométricas.

Además, se realizó un análisis detallado de las políticas y procedimientos de seguridad física existentes. Se encontró que, aunque existen directrices claras, la implementación de estas políticas no siempre es consistente. Por ejemplo, se observó que algunos empleados no siguen los protocolos de acceso establecidos, lo que podría comprometer la seguridad de los equipos. Se recomienda la realización de sesiones de capacitación periódicas para asegurar el cumplimiento de estas políticas.

4.2 Descripción de la propuesta

El presente trabajo tiene como objetivo evaluar la seguridad física actual en el Distrito de Educación. Se parte de un análisis de las instalaciones y de las medidas de seguridad implementadas para proteger el distrito de posibles amenazas, el cual tiene como objetivo la

identificación de eventuales vulnerabilidades que podría comprometer la integridad de la institución. Este análisis inicial es crucial para establecer una línea base sobre la cual se puedan medir las mejoras y la efectividad de las medidas de seguridad implementadas

Por medio de las técnicas de recolección de datos, se realizarán actividades donde va implicado el personal administrativo y técnico del Distrito de Educación. Se aplicarán encuestas con preguntas concretas sobre herramientas utilizadas en equipos de trabajo y medidas de seguridad ejecutadas en las instalaciones. Y además se realizarán entrevistas con la persona responsable del área tecnológica del distrito para conocer el nivel de cumplimiento con la normativa de seguridad y los controles de acceso utilizados en el entorno donde residen y se gestionan los equipos de cómputo. Estas actividades permitirán obtener una visión integral de la situación actual y las prácticas de seguridad en el distrito.

Con base en estos datos, se realizará un análisis considerando criterios establecidos en normativas internacionales como la Magerit, para tratar de asegurar una gestión correcta de los medios informáticos. Este análisis incluirá la identificación de riesgos potenciales y la evaluación de la efectividad de las medidas de seguridad existentes. A continuación, se llevará a cabo un informe del estado actual respecto a los equipos auditados y medidas de seguridad establecidas. Este informe servirá como una herramienta fundamental para la toma de decisiones y la planificación de futuras acciones de mejora.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recurso	Función	Actividad

1	Maria Judih Alcivar Rivas	Investigadora	Consultar sobre las bases teóricas que sustentan el proyecto.
1	Ing. Soraida Zambrano	Directora distrital	Contribuyó en la entrevista como máxima autoridad de la institución.
1	Ing. Daniel Carrasco	Responsable del área de TIC de la institución	Contribuyo en la entrevista como líder del área informática de la institución.
23	Personal administrativo del Distrito	Personal administrativo de la institución	Fueron parte de la muestra discrecional de la encuesta para la obtención de datos.

Tabla 13: Recursos Humanos

4.3.2 Tecnológicos

Cantidad	Recurso	Actividad
1	Computadora portátil	Equipo implementado para el desarrollo de la investigación.
1	Teléfono con cámara	Dispositivo utilizado para la toma de evidencias durante el proceso de la investigación.

1	Microsoft Office	Herramienta utilizada para el desarrollo de la documentación y tabulación de datos.
1	Microsoft Forms	Herramienta utilizada para la aplicación de las encuestas al personal administrativo.
1	Impresora	Equipo utiñizado para la impresión de la documentación e instrumentos de evaluación.
1	Conexión a internet	Utilización de los servicios de internet para la investigación teórica.

Tabla 14: Recursos tecnológicos

4.3.3 Económicos

Cantidad	Descripción	Precio Unitario	Subtotal
9	Viáticos en servicios de transportación para llegar a la institución.	$ 0,40	$ 3,60
50	Hojas de instrumentos de evaluación	$0,05	$ 2,50

1	Computadora portátil hp	$ 431.00	$ 431.00
1	Cámara fotográfica	$ 140.00	$ 140.00
1	Internet	$ 0,55 por hora	$ 55.00
		Total	$ 632,10

Tabla 15: Recursos Económicos

4.4 Etapas de acción para el desarrollo de la propuesta

4.4.1 Información de la institución

El Distrito de Educación 13D05 también ha implementado programas de apoyo para estudiantes con necesidades educativas especiales. Estos programas están diseñados para garantizar que todos los estudiantes, independientemente de sus capacidades, tengan acceso a una educación de calidad. Se han creado aulas de recursos y se ha capacitado a los docentes en técnicas de enseñanza inclusivas, lo que ha permitido una mayor integración y participación de estos estudiantes en el entorno escolar.

Además, se han establecido alianzas con organizaciones locales y nacionales para fortalecer los recursos educativos disponibles en el distrito. Estas alianzas han facilitado la obtención de materiales didácticos, la organización de talleres y seminarios para docentes, y la implementación de proyectos educativos innovadores. Gracias a estas colaboraciones, el Distrito de Educación 13D05 ha podido ofrecer una educación más enriquecedora y diversa a sus estudiantes.

La tecnología ha jugado un papel crucial en la modernización del Distrito de Educación 13D05. Se han instalado laboratorios de computación en varias escuelas y se ha promovido el uso de herramientas digitales en el aula. Esto no solo ha mejorado las habilidades tecnológicas de los estudiantes, sino que también ha facilitado el acceso a información y recursos educativos en línea. La integración de la tecnología en la educación ha sido un factor clave para preparar a los estudiantes para el futuro.

4.4.1 Misión

Garantizar el acceso y calidad de la educación inicial, básica y bachillerato a los y las habitantes del territorio nacional, mediante la formación integral, holística e inclusiva de niños, niñas, jóvenes y adultos, tomando en cuenta la interculturalidad, la plurinacionalidad, las lenguas ancestrales y género desde un enfoque de derechos y deberes para fortalecer el desarrollo social, económico y cultural, el ejercicio de la ciudadanía y la unidad en la diversidad de la sociedad ecuatoriana.

4.4.1.2 Visión

El Sistema Nacional de Educación brindará una educación centrada en el ser humano, con calidad, calidez, integral, holística, crítica, participativa, democrática, inclusiva e interactiva, con equidad de género, basado en la sabiduría ancestral, plurinacionalidad, con identidad y pertinencia cultural que satisface las necesidades de aprendizaje individual y social, que contribuye a fortalecer la identidad cultural, la construcción de ciudadanía, y que articule los diferentes niveles y modalidades del sistema de educación.

4.4.1.3 Valores

Honestidad, para tener comportamientos transparentes –honradez, sinceridad, autenticidad, integridad-– con nuestros semejantes y permitir que la confianza colectiva se transforme en una fuerza de gran valor.

Justicia, para reconocer y fomentar las buenas acciones y causas, condenar aquellos comportamientos que hacen daño a los individuos y a la sociedad, y velar por la justicia a fin de que no se produzcan actos de corrupción.

Respeto, empezando por el que nos debemos a nosotros mismos y a nuestros semejantes, al ambiente, a los seres vivos y a la naturaleza, sin olvidar las leyes, normas sociales y la memoria de nuestros antepasados.

Paz, para fomentar la confianza en nuestras relaciones con los demás, para reaccionar con calma, firmeza y serenidad frente a las agresiones, y para reconocer la dignidad y los derechos de las personas.

Solidaridad, para que los ciudadanos y ciudadanas colaboren mutuamente frente a problemas o necesidades y se consiga así un fin común, con entusiasmo, firmeza, lealtad, generosidad y fraternidad.

Responsabilidad, para darnos cuenta de las consecuencias que tiene todo lo que hacemos o dejamos de hacer, sobre nosotros mismos o sobre los demás, y como garantía de los compromisos adquiridos.

Pluralismo, para fomentar el respeto a la libertad de opinión y de expresión del pensamiento, y para desarrollar libremente personalidad, doctrina e ideología, con respeto al orden jurídico y a los derechos de los demás.

4.4.1.4 Organigrama Institucional

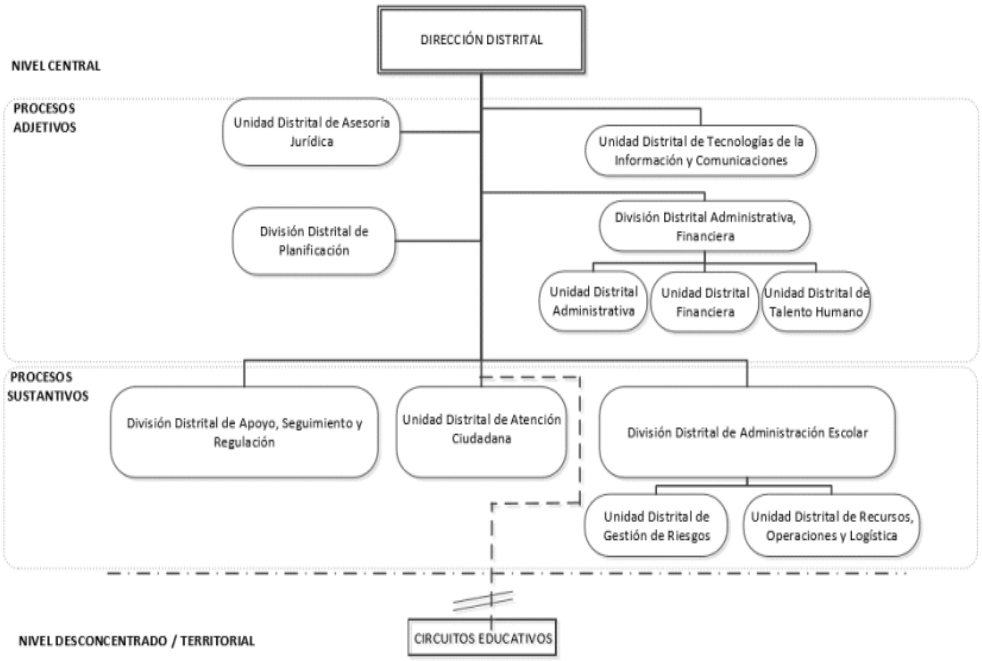


Ilustración 5: Organigrama institucional/ Fuente: Página del distrito de Educación

4.4.1 Fase 1 Planificar

Tabla 16: Programa de auditoría

AUDITORÍA INFORMATICA EN SEGURIDAD FISICA DE LOS EQUIPOS INFORMÁTICOS DEL DISTRITO DE EDUCACIÓN 13D05.
Objetivo General: Realizar una auditoría informática en seguridad física de los equipos informáticos del distrito de educación 13D05. **Objetivo Específico:** ● Evaluar el nivel de seguridad informática en el Distrito de educación 13D05. ● Identificar riesgos de seguridad informática en el Distrito de educación 13D05.
Procedimientos

1. Introducción a metodología Magerit.	**AuMaT 1**
2. Definir activos	**AuMaT 2**
3. Definir amenazas	**AuMaT 3**
4. Diseñar instrumentos de auditoría basándose las normas.	**AuMaT 4**
5. Aplicar instrumentos de investigación.	**AuMaT 5**
6. Tabulación y análisis de datos.	**AuMaT 6**
7. Análisis de los riesgos.	**AuMaT 7**
8. Elaboración de un informe que contenga observaciones, riesgos, recomendaciones.	**AuMaT 8**

Fuente: Elaboración propia

4.4.1.1 Introducción a metodología Magerit. (AuMaT 1)

Magerit es una metodología que se implementa como respuesta ante la adaptación de la tecnología en la administración pública. Estas nuevas tecnologías han sido pieza clave para su desarrollo, en contraste con lo anterior, también supone ciertos riesgos que se deben administrar de forma que den confianza a los usuarios de los servicios. En otras palabras, Magerit utiliza el proceso de gestión de riesgos para que los gobiernos a la hora de tomar decisiones tengan en cuenta los riesgos derivados de la utilización de las tecnologías de la información.

En este contexto, es oportuno utilizar esta metodología en el distrito de educación 13D05 El Carmen, porque es una metodología que identifica los riesgos que pueden malograr el equipo o los recursos que se implementan por el personal del distrito. Es por ello que se elaborará una guía para las buenas prácticas de los equipos y su correcta utilización. Esta guía no solo ayudará a mitigar los riesgos identificados, sino que también proporcionará un marco de referencia para el manejo seguro y eficiente de los recursos tecnológicos.

La implementación de Magerit en el Distrito de Educación 13D05 permitirá una evaluación sistemática de los riesgos asociados con el uso de tecnologías de la información. Este proceso incluirá la identificación de amenazas potenciales, la evaluación de la vulnerabilidad de los sistemas y la determinación del impacto de posibles incidentes. Con esta información, se podrán desarrollar estrategias efectivas para minimizar los riesgos y proteger los activos tecnológicos del distrito.

Además, la metodología Magerit fomenta la creación de un entorno de trabajo seguro y confiable. Al seguir las recomendaciones y buenas prácticas establecidas en la guía, el personal del distrito podrá manejar los equipos de manera más segura y eficiente. Esto no solo reducirá la probabilidad de incidentes de seguridad, sino que también mejorará la confianza de los usuarios en los sistemas tecnológicos del distrito.

La capacitación y concienciación del personal son componentes clave en la implementación de Magerit. Es esencial que todos los empleados comprendan la importancia de la seguridad de la información y estén familiarizados con las prácticas recomendadas. La formación continua y las campañas de concienciación ayudarán a mantener un alto nivel de seguridad y a garantizar que las medidas implementadas sean efectivas a largo plazo.

Finalmente, la adopción de Magerit en el Distrito de Educación 13D05 contribuirá a la mejora continua de la gestión de riesgos. La metodología incluye la realización de auditorías periódicas y la revisión de las políticas de seguridad para adaptarse a nuevas amenazas y cambios tecnológicos. Este enfoque proactivo permitirá al distrito mantenerse a la vanguardia en la protección de sus recursos tecnológicos y en la prestación de servicios educativos de calidad.

4.5 Introduccion

Este informe se focaliza en el análisis de los resultados adquiridos por medio de la auditoria informática efectuada en el Distrito de Educación 13D05, El Carmen. Se realizaron varios procesos que nos ayudaron a recolectar los datos para su posterior análisis del estado actual de los equipos en el distrito en cuanto a la seguridad física de los mismos, esta información es de vital importancia porque ayudan a sugerir los cambios a realizar para solventar estos riesgos.

Su objetivo principal es comprender como puede ser mejorado el distrito de educación para garantizar el uso más eficiente de los equipos informáticos. El posterior análisis permitirá presentar recomendaciones basadas en nuestros hallazgos.

4.6 Informe de auditoría

El presente documento detalla los hallazgos obtenidos al realizar la auditoria informática llevada a cabo en las instalaciones del Distrito de Educación 13D05, El Carmen.

4.6.1 DIRIGIDO A:

Persona encargada del área de Tecnologías de la Información en el Distrito de Educación 13D05, El Carmen. Ing Daniel Carrasco. Este informe va dirigido al distrito de educación 13D05.

4.6.2 MOTIVO:

Proyecto integrador previo a la obtención del título de ingeniero en tecnologías de la información

4.6.3 OBJETIVO:

Para llevar a cabo la auditoría, se definieron objetivos que proporcionaron una orientación mucho más clara sobre lo que se evaluaría dentro de la institución.

- Evaluar el nivel de seguridad informática en el Distrito de educación 13D05.
- Identificar riesgos de seguridad informática en el Distrito de educación 13D05.

4.6.5 PERSONAL RELACIONADO:

En esta sección se presenta el personal compuesto por diferentes actores los cuales están relacionados con los recursos de Tecnologías de la información en el Distrito de Educación, El Carmen. Donde se contó con la participación de la Ing, Soraida Zambrano, quien contribuyo en el desarrollo de esta auditoría dando su perspectiva institucional durante la entrevista.

El Ing, Daniel Carrasco, es el responsable del área de TI, el cual desarrollo un papel fundamental como el líder del área informática, aportando en la entrevista para poder identificar riesgos especifico en los activos auditados. Además, del personal administrativo del Distrito comprendido por 23 personas, fueron incluidos como parte de la muestra discrecional en la aplicación de encuestas para obtener los datos que nos permitan tener una visión mas clara de los riesgos y necesidades dentro del distrito de educación.

Nombre	**Función**

Maria Judih Alcivar Rivas	**Investigadora**
Ing. Soraida Zambrano	**Directora distrital**
Ing. Daniel Carrasco	**Responsable del área de TIC de la institución**
Personal administrativo del Distrito	**Personal administrativo de la institución**

Tabla 17: Personal relacionado

4.6.4 ALCANCE:

Como parte esencial de esta auditoría de seguridad informática física, se utilizó la metodología de análisis de Riesgo Magerit. Este enfoque de gestión de riesgos nos permitió identificar las vulnerabilidades y amenazas en la tecnología de la información, siguiendo cinco pasos clave en la investigación: determinar los activos a evaluar en la institución, identificar las amenazas y riesgos a los que están expuestos dichos activos, evaluar el impacto, y obtener un resultado efectivo. El objetivo principal es concienciar a los responsables de la institución distrital 13D05 sobre la existencia de los riesgos y analizar las amenazas presentes en cada uno de los equipos informáticos, ayudando a planificar y aplicar el tratamiento adecuado para mantener los riesgos bajo control.

Esta metodología incluye etapas que fueron fundamentales para evaluar el nivel de seguridad de cada uno de los riesgos presentes en el laboratorio informático de la institución. Además, se utilizaron dos herramientas para analizar los posibles riesgos en los dispositivos informáticos. La primera herramienta fue una encuesta con un cuestionario compuesto por 25 preguntas sobre el riesgo de robo, daño de equipos e incendio, 24 preguntas sobre inundación y 20 preguntas sobre malware, sumando un total de 119 preguntas. Esta encuesta fue dirigida al encargado del área de TI del distrito de educación.

4.6.1.1 Fase 2 Identificar activos

4.6.1.2 Definir activos (AuMaT 2)

Para comenzar, se realizó un inventario detallado de todos los equipos de hardware presentes en las instalaciones del distrito de educación 13D05 El Carmen. Este inventario incluyó computadoras de escritorio, laptops, servidores, impresoras, proyectores y otros dispositivos periféricos. Cada equipo fue catalogado con su respectiva marca, modelo, número de serie y estado actual de funcionamiento. Esta información es crucial para tener un control preciso de los recursos disponibles y para planificar futuras adquisiciones o reemplazos.

Además del hardware, se llevó a cabo un análisis del software utilizado en la institución. Se identificaron los sistemas operativos instalados en cada equipo, así como las aplicaciones y programas específicos que se utilizan para las actividades administrativas. Este análisis permitió detectar la necesidad de actualizaciones de software y la implementación de licencias adecuadas para asegurar el cumplimiento legal y el óptimo rendimiento de los sistemas.

La infraestructura de red también fue evaluada durante la auditoría. Se revisaron los puntos de acceso a internet, la configuración de los routers y switches, y la calidad de las conexiones de red. Se identificaron áreas con problemas de conectividad y se propusieron soluciones para mejorar la cobertura y la velocidad de la red.

En cuanto a la seguridad de la información, se revisaron las medidas de protección de datos implementadas en la institución. Se evaluaron los sistemas de antivirus y firewall, así como las políticas de seguridad para el acceso a los equipos y la información sensible. Se recomendó la implementación de protocolos adicionales de seguridad, como la autenticación de dos factores y la encriptación de datos, para proteger mejor la información contra posibles amenazas cibernéticas.

Finalmente, se realizaron entrevistas con el encargado de área de TI para entender mejor cómo se utilizan los recursos tecnológicos en el día a día. Estas entrevistas revelaron áreas donde se podría mejorar la capacitación del personal en el uso de ciertas aplicaciones y herramientas tecnológicas. También se identificaron oportunidades para optimizar el uso de los recursos existentes y para implementar nuevas tecnologías que puedan apoyar mejor las actividades educativas y administrativas.

Formato 1: Ficha de levantamiento de información

DISTRITO DE EDUCACIÓN 13D05 EL CARMEN					
AREA DE INFORMÁTICA	**AUDITORIA INFORMATICA**				
AUDITOR: _____		**FECHA:**			
		HORA:			
HARDWARE					
N° DE SERIE					
PROCESADOR					
RAM	2GB 4GB	4GB	8GB	16GB	Otra:
DISCO DURO	CAPACIDAD:				
UNIDAD DE CD/DVD	SI		NO		
CPU	SI		NO		
REGULADOR	SI		NO		
PERIFÉRICOS					

ALTAVOCES INTERNOS	SI		NO	
SOFTWARE				
SO	Windows Versión: _____	Linux Versión: _____	MacOS Versión: _____	Android Versión: _____
OFIMATICA	Microsoft office Versión: _____	Libre office Versión: _____	WPS office Versión: _____	Otros _____ Versión: _____
ANTIVIRUS	W. defender	Avast		Otros: _____
NAVEGADORES	Chrome	Edge	Firefox	Otros: _____
OTROS	_____			
EN GENERAL				
ESTADO	Bueno	Medio	Regular	Malo
OBSERVACIONES	_____			

Fuente: Elaboración propia

Tabla 18: : Identificación de activos

IDENTIFICAR LOS ACTIVOS				
Nombre del activo	**Descripción del activo**	**Tipo de activo**	**Nivel de confidencialidad**	**Propietario del activo**
CPU	Unidad central de procesamiento	Físico	Confidencial del Distrito de Educación.	Responsable de TI

Puertos E/S	Periférico de salida de datos.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Batería	Componente de hardware.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Mouse	Periférico de entrada de comandos.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Proyector	Dispositivo de salida de imagen	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Routers	Equipo de control para la circulación de datos.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Switch	Equipo de red para la conexión de dispositivos.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Sistema operativo	Aplicación responsable de gestionar los recursos de un ordenador.	Lógico	Confidencial del Distrito de Educación.	Responsable de TI

Programas de ofimática	Aplicación que mejora y automatiza las actividades de oficina.	Lógico	Confidencial del Distrito de Educación.	Responsable de TI
Antivirus	Software encargado de detectar y eliminar virus.	Lógico	Confidencial del Distrito de Educación.	Responsable de TI
Navegadores	Aplicación responsable de la conexión a internet.	Lógico	Confidencial del Distrito de Educación.	Responsable de TI
Escritorios y sillas	Mobiliario para los dispositivos informáticos y usuarios.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Cableado, toma corrientes **Interruptores**	Instalaciones eléctricas.	Físico	Confidencial del Distrito de Educación.	Responsable de TI
Aire acondicionado	Aparato eléctrico que regula la temperatura en el área.	Físico	Confidencial del Distrito de Educación.	Responsable de TI

Fuente 13: Elaboración propia

4.6.1.3 Fase 3 Análisis de riesgos

4.6.1.4 Definir amenazas (AuMaT 3)

En el distrito de educación 13D05, El Carmen las amenazas que pueden afectar a los activos son perdidas, daños en equipos, amenazas naturales como inundaciones o errores humanos como incendios, amenazas cibernéticas como malware o software malicioso.

4.6.1.5 Diseñar instrumentos de auditoría (AuMaT 4)

Se realizó una encuesta al encargado del área de TI del distrito de educación donde se realizaron 25 preguntas en los siguientes riesgos: robo, daños a equipos e incendio.20 peguntas en el riesgo por inundación, y 24 preguntas para malware.

Tabla 19: Cuestionario para medir el nivel de riesgo en robo

CUESTIONARIO PARA IDENTIFICAR RIESGOS		
ROBO	**SI**	**NO**
1. ¿El perímetro de la instalación está adecuadamente cercado?		
2. ¿Hay sistemas de vigilancia cubriendo todo el perímetro?		
3. ¿Hay controles de acceso en todas las entradas y salidas?		
4. ¿Se registran todas las personas que ingresan y salen del establecimiento?		
5. ¿Se realiza una inspección de seguridad antes de abrir y cerrar las puertas de la institución?		
6. ¿Existen alarmas antirrobo instaladas y operativas?		
7. ¿Existen controles de acceso físico como tarjetas?		
8. ¿Existe un sistema de vigilancia por cámara en las zonas críticas?		
9. ¿Se realizan patrullas regulares por las instalaciones?		
10. ¿Lleva un registro de todas las personas que entran o salen?		
11. ¿Se realizan verificaciones de antecedentes para el personal de seguridad?		
12. ¿Están las áreas sensibles, como las salas de servidores o almacenes, protegidas con cerraduras adicionales?		
13. ¿Están las alarmas conectadas a una central de monitoreo?		
14. ¿Existen políticas claras sobre el manejo de visitantes?		
15. ¿Se realizan simulacros de emergencia y respuesta a incidentes de seguridad?		
16. ¿Se monitorean en tiempo real las cámaras de seguridad?		
17. ¿Están las puestas y ventanas aseguradas?		
18. ¿Existen procedimientos para reportar y documentar incidentes de seguridad?		
19. ¿Se realizan un control de inventario regular de los bienes y equipos?		
20. ¿Se realizan sistemas de rastreo y localización?		

21. ¿Existen mecanismos para asegurar que los empleados y contratistas devuelvan las credenciales de acceso cuando dejan de trabajar para la organización?		
22. ¿Existe un sistema de gestión de acceso para controlar y monitorear el ingreso de empleados?		
23. ¿El perímetro del edificio está adecuadamente iluminado durante la noche?		
24. ¿Se llevan a cabo auditorias de seguridad físicas?		
25. ¿Hay guardias presentes en todas las entradas?		
ELABORADO POR: Maria Judith Alcivar Rivas FECHA: 26-06-2024 *OBSERVACIONES:*	*REVISADO POR:* *FECHA:*	

Fuente 14: Elaboración propia

Tabla 20: Cuestionario para medir el nivel de riesgo en daños de equipos

CUESTIONARIO PARA IDENTIFICAR RIESGOS		
DAÑOS DE EQUIPOS	**SI**	**NO**
1. ¿Están todos los equipos etiquetados correctamente con números de inventario y códigos de identificación?		
2. ¿Se realiza un inventario regular de los equipos del laboratorio?		
3. ¿Existen procedimientos documentados para la instalación y el mantenimiento de los equipos?		
4. ¿Los equipos están ubicados en áreas designadas y adecuadas para su uso y almacenamiento?		
5. ¿Los equipos están protegidos contra fluctuaciones de energía con sistemas de alimentación ininterrumpida?		
6. ¿Hay alarmas de seguridad instaladas para detectar instrucciones no autorizadas?		
7. ¿Se restringe el acceso físico al laboratorio?		
8. ¿Se utilizan cámaras de vigilancia para monitorear las áreas críticas del laboratorio?		
9. ¿Los equipos están debidamente protegidos contra daños por agua, fuego y otros aspectos?		
10. ¿Se han implementado controles ambientales (temperatura, humedad) adecuados en el laboratorio?		
11. ¿Se realizan inspecciones regulares de los sistemas de protección contra incendios?		
12. ¿Se mantienen los equipos en condiciones limpias y libres de polvo?		
13. ¿Hay protocolos de apagado seguro y desconexión para equipos electrónicos?		
14. ¿El personal está capacitado en el manejo y uso adecuado de los equipos?		
15. ¿Se registran y analizan los incidentes de daños a equipos costosos?		
16. ¿Existen políticas de seguro para cubrir los daños a equipos costosos?		
17. ¿Los cables y conexiones están organizados y protegidos contra daños físicos?		
18. ¿Se realizan auditorías periódicas de seguridad física en el laboratorio?		
19. ¿Se emplean sistemas de bloqueo y etiquetado para equipos fuera de servicio?		
20. ¿Existen procedimientos de emergencia que incluyan la protección de los equipos?		
21. ¿Los equipos están sujetos a programas regulares de mantenimiento preventivo?		
22. ¿Hay registros de mantenimiento y reparación de todos los equipos?		
23. ¿Se utilizan protectores contra tensiones en todos los equipos?		
24. ¿Las instalaciones cuentan con señalización adecuada para advertir sobre el peligro y restricciones?		
25. ¿Se revisan y actualizan regularmente las políticas y procedimientos de seguridad física?		

ELABORADO POR: Maria Judith Alcivar Rivas FECHA: 26-06-2024 *OBSERVACIONES:*	*REVISADO POR:* *FECHA:*

Fuente 15: Elaboración propia

Tabla 21: Cuestionario para medir el nivel de riesgo de incendio

CUESTIONARIO PARA IDENTIFICAR RIESGOS		
INCENDIO	**SI**	**NO**
1. ¿Existe un plan de prevención de incendios documentado y actualizado?		
2. ¿Se han identificado y evaluado los riesgos de incendio en la institución?		
3. ¿Están disponibles los planos de evacuación y están claramente visibles en todas las áreas?		
4. ¿Están los sistemas de detección de incendio conectado a una alarma central?		
5. ¿Están los equipos de cómputo alejados de materiales inflamables?		
6. ¿Se dispone detectores de humo y alarma de incendios en las áreas de equipos de cómputo?		
7. ¿Se revisan y mantienen regularmente los detectores de humo y calor?		
8. ¿Están las salidas de emergencia libres de objetos que obstaculicen?		
9. ¿Se han realizado pruebas en los sistemas de extinción?		
10. ¿Se capacita al personal en el uso de extintores de incendio?		
11. ¿Se encuentra señalizada todas las áreas de salida de emergencia?		
12. ¿Están las salas de servidores y áreas con equipos informáticos protegidos contra el acceso no autorizado?		
13. ¿Se ha revisado y actualizado los planes contra evacuación en caso de incendios?		
14. ¿Se han implementado medidas para evitar el sobre calentamiento?		
15. ¿Se han inspeccionado los cables y conexiones eléctricas para detectar posibles incendios?		
16. ¿Existen procedimientos documentados para la respuesta ante incendios en el área de cómputo?		
17. ¿Se realiza mantenimiento preventivo regular de los equipos de aires acondicionados?		
18. ¿Se han tomado medidas para minimizar la acumulación de polvo en las áreas con equipos informáticos?		
19. ¿Existen sistemas de monitoreo de temperatura y humedad en las áreas con equipos informáticos?		
20. ¿Se han identificado y documentado todos los riesgos potenciales de incendio en las áreas con equipos informáticos?		
21. ¿Se realizan inspecciones regulares de las áreas con equipos informáticos para detectar posibles riesgos de incendio?		
22. ¿Existen procedimientos para la gestión segura de materiales inflamables en las áreas con equipos informáticos?		
23. ¿Se revisan y actualizan periódicamente los planes de contingencia y de respuesta ante incendios?		
24. ¿Se han implementado sistemas de respaldo de datos y recuperación ante desastres?		
25. ¿Hay un equipo de respuesta de emergencia designado y capacitado para manejar incidentes de incendio en las áreas con equipos informáticos?		
ELABORADO POR: Maria Judith Alcivar Rivas FECHA: 26-06-2024 *OBSERVACIONES:*	*REVISADO POR:* *FECHA:*	

Fuente 16: Elaboración propia

Tabla 22: Cuestionario para medir el nivel de riesgo de inundación

CUESTIONARIO PARA IDENTIFICAR RIESGOS		
INUNDACIÓN	**SI**	**NO**
1. ¿Existe un plan de contingencia documentado para inundaciones?		
2. ¿Se realizan inspecciones regulares de los equipos de drenaje y desagüe de las instalaciones?		
3. ¿Se utilizan Rac elevados para servidores y otros equipos?		
4. ¿Están claramente señaladas y accesibles los puntos de corte de agua de emergencia?		
5. ¿Se han implementado barreras o sellos impermeables en áreas críticas para evitar la entrada de agua?		
6. ¿Se realizan simulacros de inundación para asegurar que el personal este preparado para una emergencia de agua?		
7. ¿Existen sensores y alarmas de detección de agua instalados en áreas de alto riesgo?		
8. ¿Se mantiene un inventario de equipos como bombas portátiles y suministros de emergencia?		
9. ¿Los equipos electrónicos y de TI están elevados del suelo o protegidos contra posibles inundaciones?		
10. ¿Se revisan y mantienen regularmente los techos y sistemas de canalización para prevenir filtraciones?		
11. ¿Se han identificado y evaluado las áreas de mayor riesgo de inundación dentro de las instalaciones?		
12. ¿Hay planes específicos para la protección de documentos y registros importantes en caso de inundación?		
13. ¿El personal está capacitado para responder adecuadamente a situaciones de inundación?		
14. ¿Se cuenta con un seguro adecuado que cubra los daños causados por inundaciones de agua?		
15. ¿Existe un protocolo de comunicación para informar al personal y a las autoridades en caso de una inundación?		
16. ¿Se inspeccionan y mantienen regularmente las fuentes de agua internas (como tuberías y tanques) para prevenir fugas?		
17. ¿Están los equipos de HVAS (calefacción, ventilación y aire acondicionado) protegidos contra daños por agua?		
18. ¿Se han implementado medidas de prevención de inundaciones en el diseño del paisaje exterior, como zanjas y desagües?		
19. ¿Se realizan auditorias periódicas y se actualizan los planes de riesgo de contingencia en caso de inundación?		
20. ¿Se documentan y revisan incidentes previos de inundación para mejorar las medidas preventivas y la respiuesta?		
ELABORADO POR: Maria Judith Alcivar Rivas FECHA: 26-06-2024 *OBSERVACIONES:*	*REVISADO POR:* *FECHA:*	

Fuente 17: Elaboración propia

Tabla 23: Cuestionario para medir el nivel de riesgo en malware

CUESTIONARIO PARA IDENTIFICAR RIESGOS		
MALWARE	**SI**	**NO**
1. ¿El sistema operativo y todas las aplicaciones están actualizados con los últimos parches de seguridad?		
2. ¿Se utilizan soluciones antivirus y antimalware confiables y están actualizadas?		
3. ¿Se realiza un análisis regular del sistema en busca de malware?		
4. ¿Existen alertas o notificaciones de actividad inusual en el sistema?		
5. ¿Hay programas o procesos desconocidos ejecutándose en el sistema?		
6. ¿El sistema está experimentando una ralentización inexplicable?		

7. ¿Se han detectado cambios en archivos o configuraciones sin autorización?		
8. ¿Se han recibido correos electrónicos sospechosos o con archivos adjuntos desconocidos?		
9. ¿Hay protección contra la redirección de las búsquedas en el navegador a sitios web no deseados?		
10. ¿Hay protección contra pop-ups o anuncios emergentes inusuales al navegar por la web?		
11. ¿Se han observado conexiones a direcciones IP sospechosas?		
12. ¿Hay protección extra en el cortafuego para que no realicen configuración sin autorización?		
13. ¿Los usuarios han informado de problemas de acceso a sus cuentas?		
14. ¿Se han detectado intentos de inicio de sesión fallidos o no autorizados?		
15. ¿Existen registros de actividad inusual en los logs del sistema?		
16. ¿Se ha realizado una copia de seguridad reciente de los datos importantes?		
17. ¿Se están aplicando políticas de contraseñas fuertes y de renovación regular?		
18. ¿Los permisos de usuario están correctamente configurados y limitados según el principio de menor privilegio?		
19. ¿Se han revisado y analizado las aplicaciones y programas instalados recientemente?		
20. ¿El tráfico de red muestra patrones de comportamiento anómalo?		
21. ¿Se han instalado y configurado adecuadamente las herramientas de monitoreo de red?		
22. ¿Se han revisado las políticas de seguridad y se han aplicado correctamente?		
23. ¿Existen procedimientos definidos para la respuesta a incidentes de seguridad?		
24. ¿Los usuarios han recibido capacitación en concienciación sobre seguridad informática?		
ELABORADO POR: Maria Judith Alcivar Rivas FECHA: 26-06-2024 OBSERVACIONES:	*REVISADO POR:* *FECHA:*	

Fuente 18: Elaboración propia

”’

4.6.1.6 Fase 4 Aplicación y pruebas

4.6.1.7 Aplicación (AuMaT 5)

Para realizar la investigación, se utilizó un instrumento de recolección de datos mediante un cuestionario, con el objetivo de determinar los riesgos existentes en la institución distrital. Dependiendo del tipo de riesgo, como robo, daños a equipos e incendios, se aplicaron 25 preguntas. Para el riesgo de inundación se aplicaron 20 preguntas, y para el riesgo de malware, 24 preguntas.

La encuesta fue aplicada al encargado de TI de la institución, donde las preguntas solo tenían dos opciones de respuesta: sí o no. De esta manera, se obtuvieron los resultados de los riesgos, que incluyeron robo, daño de equipos, inundación, incendio y malware, sumando un total de 119 preguntas

4.6.1.8 Fase 4 Evaluación y pruebas

4.6.1.9 Tabulación (AuMaT 6)

Para lograr la respectiva tabulación de datos se lo realiza mediante la herramienta de Excel para alcanzar de forma ordenada la información obtenida mediante la indagación al encargado del área de TI del distrito dentro del laboratorio de TI del distrito de educación 13D05, El Carmen,

RIESGO DE ROBO			
PREGUNTA	SI	NO	valoración
1. ¿El perimetro de la instalación está adecuadamente cercado?		x	0
2. ¿Hay sistemas de vigilancia cubriendo todo el perimetro?		x	0
3. ¿Hay controles de acceso en todas las entradas y salidas?	x		1
4. ¿Se registran todas las personas que ingresan y salen del establecimiento?		x	0
5. ¿Se realiza una inspección de seguridad antes de abrir y cerrar las puertas de la institución?		x	0
6. ¿Existen alarmas antirrobo instaladas y operativas?		x	0
7. ¿Existen controles de acceso físico como tarjetas?		x	0
8. ¿Existe un sistema de vigilancia por cámara en las zonas criticas?		x	0
9. ¿Se realizan patrullas regulares por las instalaciones?	x		1
10. ¿Lleva un registro de todas las personas que entran o salen?	x		1
11. ¿Se realizan verificaciones de antecedentes para el personal de seguridad?	x		1
12. ¿Están las áreas sensibles, como las salas de servidores o almacenes, protegidas con cerraduras adicionales?	x		1
13. ¿Están las alarmas conectadas a una central de monitoreo?		x	2
14. ¿Existen políticas claras sobre el manejo de visitantes?	x		1
15. ¿Se realizan simulacros de emergencia y respuesta a incidentes de seguridad?	x		1
16. ¿Se monitorean en tiempo real las cámaras de seguridad?	x		1
17. ¿Están las puestas y ventanas aseguradas?	x		1
18. ¿Existen procedimientos para reportar y documentar incidentes de seguridad?	x		1
19. ¿Se realizan un control de inventario regular de los bienes y equipos?	x		1
20. ¿Se realizan sistemas de rastreo y localización?		x	0
21. ¿Existen mecanismos para asegurar que los empleados y contratistas devuelvan las credenciales de acceso cuando dejan de trabajar para la organización?	x		1
22. ¿Existe un sistema de gestión de acceso para controlar y monitorear el ingreso de empleados?	x		1
23. ¿El perimetro del edificio está adecuadamente iluminado durante la noche?	x		1
24. ¿Se llevan a cabo auditorias de seguridad físicas?	x		1
25. ¿Hay guardias presentes en todas las entradas?	x		1
total de controles evaluados			24
total seguridad(contar 1s)			16
total riesgo (contar 0s)			8
%seguridad(total seguridad/total controles evaluados)			67%
%riesgo (total riesgo/total controles evaluados)			33%

Ilustración 6: Tabulación de datos riesgo robo

RIESGO DE DAÑOS A EQUIPOS			
PREGUNTA	SI	NO	valoración
1. ¿Están todos los equipos etiquetados correctamente con números de inventario y códigos de identificación?	x		1
2. ¿Se realiza un inventario regular de los equipos del laboratorio?	x		1
3. ¿Existen procedimientos documentados para la instalación y el mantenimiento de los equipos?	x		1
4. ¿Los equipos están ubicados en áreas designadas y adecuadas para su uso y almacenamiento?	x		1
5. ¿Los equipos están protegidos contra fluctuaciones de energía con sistemas de alimentación ininterrumpida?		x	0
6. ¿Hay alarmas de seguridad instaladas para detectar instrucciones no autorizadas?		x	2
7. ¿Se restringe el acceso físico al laboratorio?	x		1
8. ¿Se utilizan cámaras de vigilancia para monitorear las áreas críticas del laboratorio?		x	0
9. ¿Los equipos están debidamente protegidos contra daños por agua, fuego y otros aspectos?		x	0
10. ¿Se han implementado controles ambientales (temperatura, humedad) adecuados en el laboratorio?		x	0
11. ¿Se realizan inspecciones regulares de los sistemas de protección contra incendios?	x		1
12. ¿Se mantienen los equipos en condiciones limpias y libres de polvo?	x		1
13. ¿Hay protocolos de apagado seguro y desconexión para equipos electrónicos?	x		1
14. ¿El personal está capacitado en el manejo y uso adecuado de los equipos?	x		1
15. ¿Se registran y analizan los incidentes de daños a equipos costosos?	x		1
16. ¿Existen políticas de seguro para cubrir los daños a equipos costosos?		x	0
17. ¿Los cables y conexiones están organizados y protegidos contra daños físicos?		x	0
18. ¿Se realizan auditorías periódicas de seguridad física en el laboratorio?	x		1
19. ¿Se emplean sistemas de bloqueo y etiquetado para equipos fuera de servicio?	x		1
20. ¿Existen procedimientos de emergencia que incluyan la protección de los equipos?	x		1
21. ¿Los equipos están sujetos a programas regulares de mantenimiento preventivo?	x		1
22. ¿Hay registros de mantenimiento y reparación de todos los equipos?	x		1
23. ¿Se utilizan protectores contra tensiones en todos los equipos?		x	0
24. ¿Las instalaciones cuentan con señalización adecuada para advertir sobre el peligro y restricciones?	x		1
25. ¿Se revisan y actualizan regularmente las políticas y procedimientos de seguridad física?	x		1
total de controles evaluados			24
total seguridad(contar 1s)			17
total riesgo (contar 0s)			7
%seguridad(total seguridad/total controles evaluados)			71%
%riesgo (total riesgo/total controles evaluados)			29%

Ilustración 7: Ilustración 6: Tabulación de datos riesgo daños a equipos

RIESGO DE INCENDIO			
PREGUNTA	SI	NO	valoración
1. ¿Existe un plan de prevención de incendios documentado y actualizado?		x	0
2. ¿Se han identificado y evaluado los riesgos de incendio en la institución?		x	0
3. ¿Están disponibles los planos de evacuación y están claramente visibles en todas las áreas?		x	0
4. ¿Están los sistemas de detección de incendio conectado a una alarma central?		x	0
5. ¿Están los equipos de cómputo alejados de materiales inflamables?	x		1
6. ¿Se dispone detectores de humo y alarma de incendios en las áreas de equipos de cómputo?		x	0
7. ¿Se revisan y mantienen regularmente los detectores de humo y calor?		x	2
8. ¿Están las salidas de emergencia libres de objetos que obstaculicen?	x		1
9. ¿Se han realizado pruebas en los sistemas de extinción?	x		1
10. ¿Se capacita al personal en el uso de extintores de incendio?	x		1
11. ¿Se encuentra señalizada todas las áreas de salida de emergencia?	x		1
12. ¿Están las salas de servidores y áreas con equipos informáticos protegidos contra el acceso no autorizado?	x		1
13. ¿Se ha revisado y actualizado los planes contra evacuación en caso de incendios?	x		1
14. ¿Se han implementado medidas para evitar el sobre calentamiento?		x	0
15. ¿Se han inspeccionado los cables y conexiones eléctricas para detectar posibles incendios?		x	0
16. ¿Existen procedimientos documentados para la respuesta ante incendios en el área de cómputo?		x	0
17. ¿Se realiza mantenimiento preventivo regular de los equipos de aires acondicionados?	x		1
18. ¿Se han tomado medidas para minimizar la acumulación de polvo en las áreas con equipos informáticos?	x		1
19. ¿Existen sistemas de monitoreo de temperatura y humedad en las áreas con equipos informáticos?		x	0
20. ¿Se han identificado y documentado todos los riesgos potenciales de incendio en las áreas con equipos informáticos?		x	0
21. ¿Se realizan inspecciones regulares de las áreas con equipos informáticos para detectar posibles riesgos de incendio?		x	0
22. ¿Existen procedimientos para la gestión segura de materiales inflamables en las áreas con equipos informáticos?		x	0
23. ¿Se revisan y actualizan periódicamente los planes de contingencia y de respuesta ante incendios?		x	0
24. ¿Se han implementado sistemas de respaldo de datos y recuperación ante desastres?	x		1
25. ¿Hay un equipo de respuesta de emergencia designado y capacitado para manejar incidentes de incendio en las áreas con equipos informáticos?		x	0
total de controles evaluados			24
total seguridad(contar 1s)			10
total riesgo (contar 0s)			14
%seguridad(total seguridad/total controles evaluados)			42%
%riesgo (total riesgo/total controles evaluados)			58%

Ilustración 8: Ilustración 6: Tabulación de datos riesgo de incendio

RIESGO DE INUNDACIÓN			
PREGUNTA	SI	NO	valoración
1. ¿Existe un plan de contingencia documentado para inundaciones?		x	0
2. ¿Se realizan inspecciones regulares de los equipos de drenaje y desagüe de las instalaciones?		x	0
3. ¿Se utilizan Rac elevados para servidores y otros equipos?	x		1
4. ¿Están claramente señaladas y accesibles los puntos de corte de agua de emergencia?		x	0
5. ¿Se han implementado barreras o sellos impermeables en áreas críticas para evitar la entrada de agua?		x	0
6. ¿Se realizan simulacros de inundación para asegurar que el personal este preparado para una emergencia de agua?		x	0
7. ¿Existen sensores y alarmas de detección de agua instalados en áreas de alto riesgo?		x	2
8. ¿Se mantiene un inventario de equipos como bombas portátiles y suministros de emergencia?		x	0
9. ¿Los equipos electrónicos y de TI están elevados del suelo o protegidos contra posibles inundaciones?		x	0
10. ¿Se revisan y mantienen regularmente los techos y sistemas de canalización para prevenir filtraciones?	x		1
11. ¿Se han identificado y evaluado las áreas de mayor riesgo de inundación dentro de las instalaciones?		x	0
12. ¿Hay planes específicos para la protección de documentos y registros importantes en caso de inundación?		x	0
13. ¿El personal está capacitado para responder adecuadamente a situaciones de inundación?		x	0
14. ¿Se cuenta con un seguro adecuado que cubra los daños causados por inundaciones de agua?	x		1
15. ¿Existe un protocolo de comunicación para informar al personal y a las autoridades en caso de una inundación?	x		1
16. ¿Se inspeccionan y mantienen regularmente las fuentes de agua internas (como tuberías y tanques) para prevenir fugas?	x		1
17. ¿Están los equipos de HVAS (calefacción, ventilación y aire acondicionado) protegidos contra daños por agua?		x	0
18. ¿Se han implementado medidas de prevención de inundaciones en el diseño del paisaje exterior, como zanjas y desagües?		x	0
19. ¿Se realizan auditorias periódicas y se actualizan los planes de riesgo de contingencia en caso de inundación?	x		1
20.¿Se documentan y revisan incidentes previos de inundación para mejorar las medidas preventivas y la respuesta?	x		1
total de controles evaluados			19
total seguridad(contar 1s)			7
total riesgo (contar 0s)			12
%seguridad(total seguridad/total controles evaluados)			37%
%riesgo (total riesgo/total controles evaluados)			63%

Ilustración 9: Ilustración 6: Tabulación de datos riesgo de inundación

RIESGO DE MALWARE			
PREGUNTA	SI	NO	valoración
1. ¿El sistema operativo y todas las aplicaciones están actualizados con los últimos parches de seguridad?	x		1
2. ¿Se utilizan soluciones antivirus y antimalware confiables y están actualizadas?	x		1
3. ¿Se realiza un análisis regular del sistema en busca de malware?	x		1
4. ¿Existen alertas o notificaciones de actividad inusual en el sistema?	x		1
5. ¿Hay programas o procesos desconocidos ejecutándose en el sistema?		x	1
6. ¿El sistema está experimentando una ralentización inexplicable?		x	1
7. ¿Se han detectado cambios en archivos o configuraciones sin autorización?		x	2
8. ¿Se han recibido correos electrónicos sospechosos o con archivos adjuntos desconocidos?	x		0
9. ¿Hay protección contra la redirección de las búsquedas en el navegador a sitios web no deseados?		x	0
10. ¿Hay protección contra pop-ups o anuncios emergentes inusuales al navegar por la web?		x	0
11. ¿Se han observado conexiones a direcciones IP sospechosas?	x		1
12. ¿Hay protección extra en el cortafuego para que no realicen configuración sin autorización?		x	1
13. ¿Los usuarios han informado de problemas de acceso a sus cuentas?	x		0
14. ¿Se han detectado intentos de inicio de sesión fallidos o no autorizados?		x	0
15. ¿Existen registros de actividad inusual en los logs del sistema?		x	0
16. ¿Se ha realizado una copia de seguridad reciente de los datos importantes?	x		1
17. ¿Se están aplicando políticas de contraseñas fuertes y de renovación regular?	x		1
18. ¿Los permisos de usuario están correctamente configurados y limitados según el principio de menor privilegio?	x		1
19. ¿Se han revisado y analizado las aplicaciones y programas instalados recientemente?	x		1
20. ¿El tráfico de red muestra patrones de comportamiento anómalo?	x		0
21. ¿Se han instalado y configurado adecuadamente las herramientas de monitoreo de red?	x		1
22. ¿Se han revisado las políticas de seguridad y se han aplicado correctamente?	x		1
23. ¿Existen procedimientos definidos para la respuesta a incidentes de seguridad?	x		1
24. ¿Los usuarios han recibido capacitación en concienciación sobre seguridad informática?	x		1
total de controles evaluados			23
total seguridad(contar 1s)			16
total riesgo (contar 0s)			7
%seguridad(total seguridad/total controles evaluados)			70%
%riesgo (total riesgo/total controles evaluados)			30%

Ilustración 10: Ilustración 6: Tabulación de datos riesgo de malware

Para realizar la tabulación en Excel se utilizó una hoja de códigos para de esta forma identificar los riesgos que hay en la institución el cual el numero 1 corresponde a la seguridad, 2 es igual a no aplica y por ultimo el 0 representa un riesgo para poder identificar y analizar cada respuesta.

hoja de códigos	
1	si la respuesta significa seguridad
0	si la respuesta significa peligro
2	no aplica

4.6.1.10 Análisis de los riesgos (AuMaT7)

Por medio del análisis de riesgos se obtuvieron como resultados que el principal riesgo es el riesgo de incendio, reflejado en la imagen, indica un nivel de riesgo significativo del 58%, mientras que el nivel de seguridad se mantiene en un 42%. Este resultado evidencia la

necesidad de implementar medidas inmediatas para mitigar las posibles amenazas de incendios dentro del distrito educativo. Factores como la falta de sistemas adecuados de detección de incendios, el uso de materiales inflamables o la ausencia de planes de evacuación podrían estar contribuyendo a este porcentaje.

Por otra parte, el riesgo de inundación, representado en la imagen, muestra un riesgo aún más alto, alcanzando el 68%, mientras que el nivel de seguridad se reduce al 37%. Este hallazgo sugiere que el distrito educativo está altamente expuesto a posibles daños por inundaciones, que podrían afectar tanto la infraestructura física como los equipos informáticos esenciales para las operaciones.

4.7 Matriz de riesgo

MATRIZ DE RIESGOS				
RIESGO	**Aparición**	**Gravedad**	**Valor del Riesgo**	**Nivel de Riesgo**
Robo	3	4	12	Importante
Daños a equipos	2	4	8	Apreciable
Incendio	4	3	12	Importante
Inundación	4	3	12	Importante
Malware	2	4	8	Apreciable

Ilustración 11: Matriz de Riesgos

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	10
	MUY BAJA	1	1	2	3	4	5

COLOR	RANGO	NIVEL DE RIESGO	MEDIDAS
	DE15 A 25	MUY GRAVE	Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo
	DE 9 A 12	IMPORTANTE	Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	DE 3 A 8	APRECIABLE	Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas
	DE 1 A 2	MARGINAL	Se vigilará aunque no requiere medidas preventivas de partida

Ilustración 12: Leyenda

ESCALA PARA ASIGNAR VALOR DE APARICIÓN		
NIVEL DE APARICIÓN (PROBABILIDAD)		
1	MAS BAJO	1%-10%
2		11%-30%
3		31%-50%
4		51%-75%
5	MÁS ALTO	76%-100%

Ilustración 13: Escala de aparición

GRAVEDAD (IMPACTO)		CONSIDERACIONES
1	MAS BAJO	Las instalaciones quedan temporalmente cerrada o no puede operar, pero puede continuar su actividad. La interrupcion es menor a 8 horas. Existe un daño limitado de activos. La mayoría de las instalaciones no se verán afectadas
2		
3		
4		
5	MÁS ALTO	Daños irreparables en instalaciones / afectada más allá del uso habitable. La mayoría de los datos y activos se pierden, destruyen o dañan sin posibilidad de reparación o restauración.

4.7.1 Fase 5 Informe de resultados

4.7.1.1 Hallazgos

Nivel de seguridad general

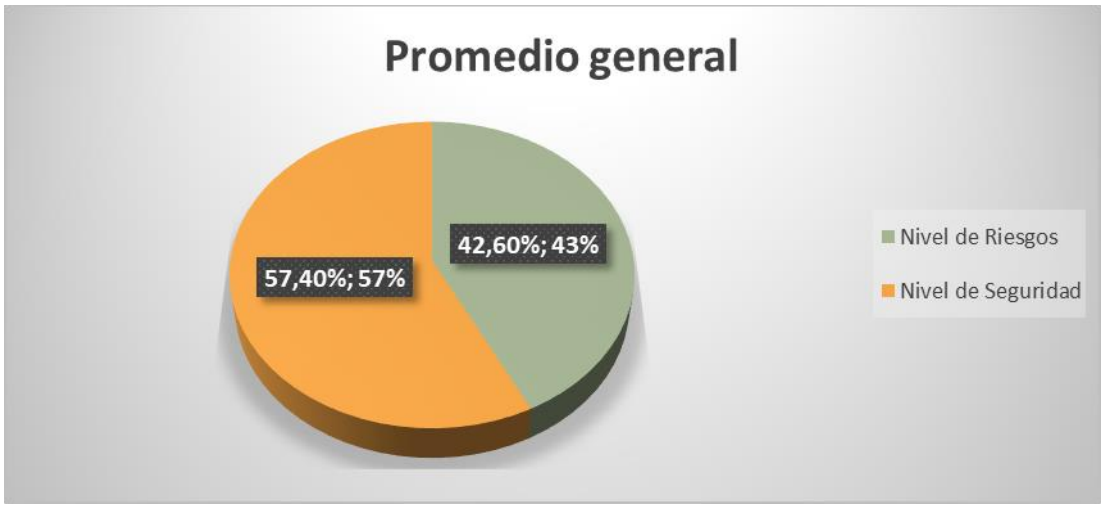


Ilustración 14: Promedio general

Interpretación:

Con un nivel de seguridad del 57,4% y un nivel de riesgo del 42,6%, se puede concluir que la protección general es moderada, pero aún presenta riesgos significativos. Este equilibrio sugiere que, aunque se han implementado medidas de seguridad efectivas, todavía existen vulnerabilidades que podrían ser explotadas. Para mejorar la seguridad general, es crucial identificar y abordar estas áreas de riesgo mediante la implementación de medidas adicionales y la mejora continua de las prácticas de seguridad.

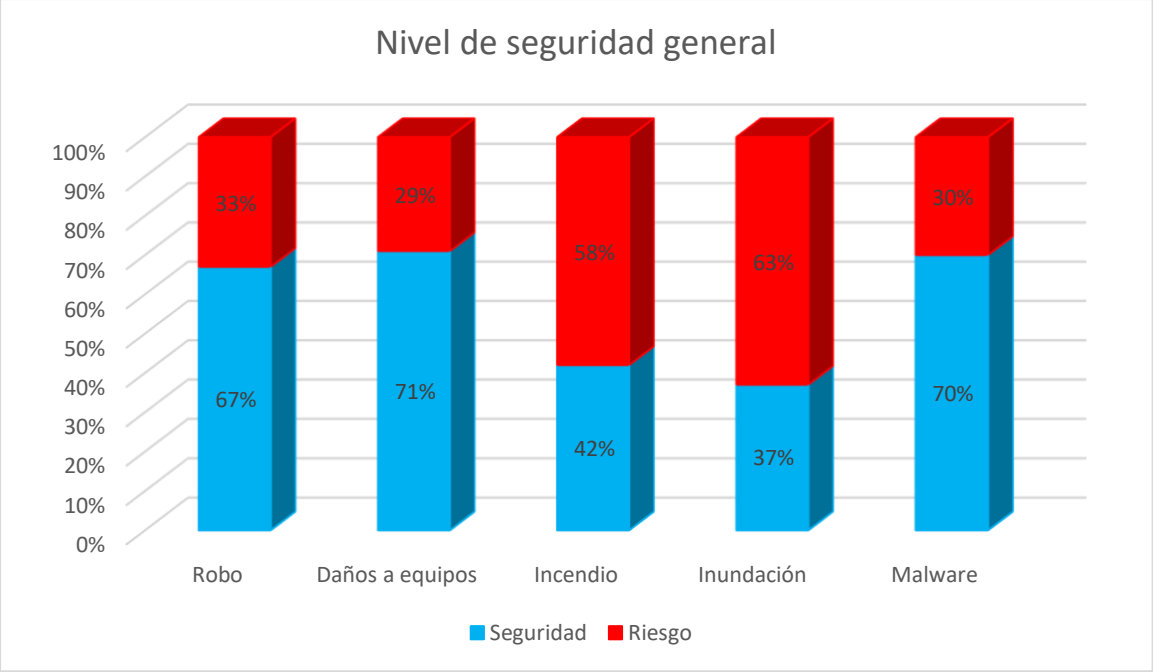


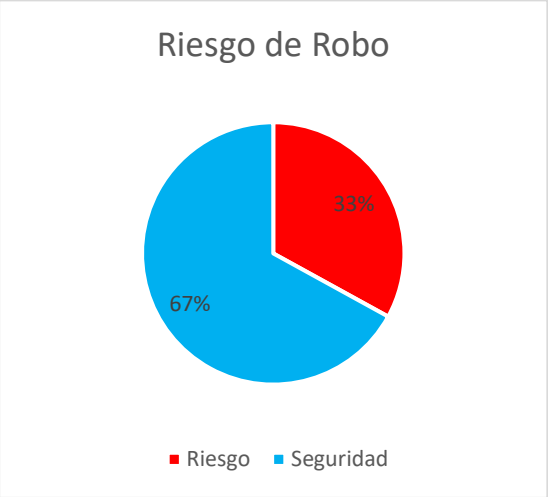
Ilustración 15: Nivel de seguridad general

Interpretación

Teniendo en cuenta el nivel de seguridad general, se obtiene dos niveles de importancia estos se dan en inundación e incendios. Ambos tienen un riesgo alto y un porcentaje de seguridad bajo, esto podría incidir en la seguridad física de nuestros equipos informáticos. Otro riesgo que refleja su importancia es el de robos, sin embargo, en este caso el nivel de seguridad es mayor. Cabe recalcar que, se necesita de medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.

Nivel de riesgo Robo

Gráfico:	**Causas:**

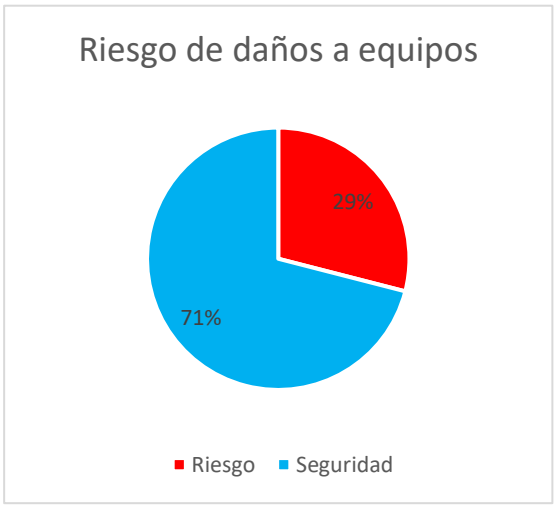


- No existe un perímetro adecuadamente cercado.
- No hay un sistema de vigilancia que cubra todo el perímetro.
- No se registra a las personas al entrar y salir del establecimiento.
- No se realiza una inspección de seguridad al abrir y cerrar las puertas de la institución.
- No hay alarmas antirrobo
- No hay controles de accesos como tarjetas
- Las zonas críticas no tienen cámaras de vigilancia.
- No hay alarmas conectadas a la central de monitoreo.
- No existen políticas sobre el manejo de visitantes.
- No hay un sistema que rastree y localice el aparato tecnológico.

Interpretación: Con un nivel de seguridad del 67% y un nivel de riesgo del 33%, se puede concluir que, aunque la seguridad contra el robo es relativamente alta, todavía existe un riesgo significativo que no debe ser ignorado. Este 33% de riesgo indica que hay vulnerabilidades que podrían ser explotadas, lo que podría resultar en incidentes de robo. Para reducir este riesgo, es crucial implementar medidas adicionales de seguridad, como sistemas de vigilancia más avanzados, controles de acceso más estrictos y capacitación continua para el personal en prácticas de seguridad.

Ilustración 16: Nivel de riesgo de robo

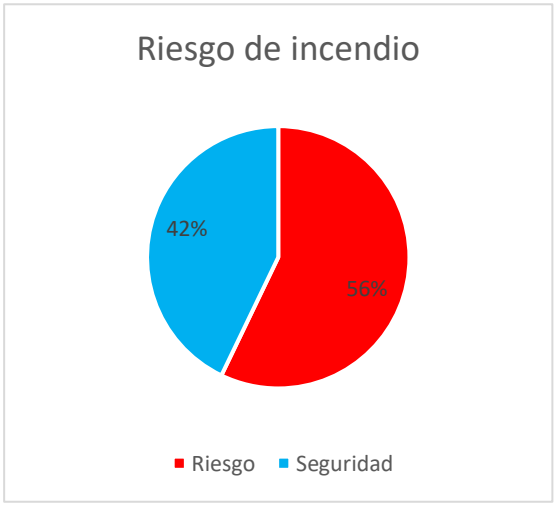
Nivel de riesgo daños a equipos

Gráfico:	**Causas:**
	• No existen equipos para regular el voltaje. • No existen alarmas para detectar accesos no autorizados. • No existen cámaras de vigilancia que monitoreen áreas críticas. • Los equipos no poseen protección contra daños por agua o fuego y otros aspectos. • No se han implementado controles ambientales (temperatura, humedad) adecuados en el laboratorio.

	• No hay políticas de seguro para cubrir daños a equipos costosos. • Los cables no están organizados ni protegidos contra daños físicos. • No se utilizan protectores contra tensiones en todos los equipos.
Interpretación: Con un nivel de seguridad del 71% y un nivel de riesgo del 29%, se puede concluir que la protección contra daños a equipos es bastante sólida. Este alto nivel de seguridad indica que se han implementado medidas efectivas para proteger los equipos. Sin embargo, el 29% de riesgo restante sugiere que aún hay margen para mejorar. Para fortalecer aún más la seguridad, es recomendable continuar con el mantenimiento preventivo, mejorar los sistemas de protección contra sobretensiones y asegurar que el personal esté bien capacitado en el manejo adecuado de los equipos	

Ilustración 17: Nivel de riesgo daños a equipos

Nivel de riesgo incendio

Gráfico:	**Causas:**
	• No existe un plan de prevención de incendio. • No se han hecho evaluaciones de los riesgos de incendio. • No cuentan con señalizaciones claras y visibles de los planes de evacuación.

	• No cuenta con sistemas de detección de incendios conectados a una alarma central • No se cuenta con detectores de humo ni sistemas de detección de incendios en áreas de cómputo. • No se han implementado medidas para evitar el sobre calentamiento. • No se realizan inspecciones a los cables de conexión eléctrica para la detección de posibles incendios. • No existen procedimientos documentados para la respuesta ante incendios en el área de cómputo. • No existen sistemas de monitoreo de temperatura y humedad en las áreas de equipos. • No se han identificado y documentado todos los riesgos potenciales de incendio. • No se realizan inspecciones regulares de las áreas con equipos informáticos para la detección de posibles riesgos.

	• No existen procedimientos para la gestión segura de materiales inflamables en las áreas con equipos. • No se revisan y actualizan periódicamente los planes de contingencia y de respuesta ante incendio. • No hay un equipo de emergencia designado y capacitado para manejar incidentes de incendio en las áreas con equipos informáticos.
Interpretación: Con un nivel de seguridad del 42% y un nivel de riesgo del 56%, se puede concluir que la protección contra incendios es insuficiente y presenta un riesgo significativo. Este alto nivel de riesgo indica que existen vulnerabilidades críticas que podrían resultar en incidentes de incendio. Para reducir este riesgo, es esencial implementar medidas adicionales, como sistemas de detección y extinción de incendios más avanzados, realizar inspecciones regulares y capacitar al personal en procedimientos de emergencia y prevención de incendios.	

Ilustración 18: Nivel de riesgo incendio

Nivel de riesgo de inundación

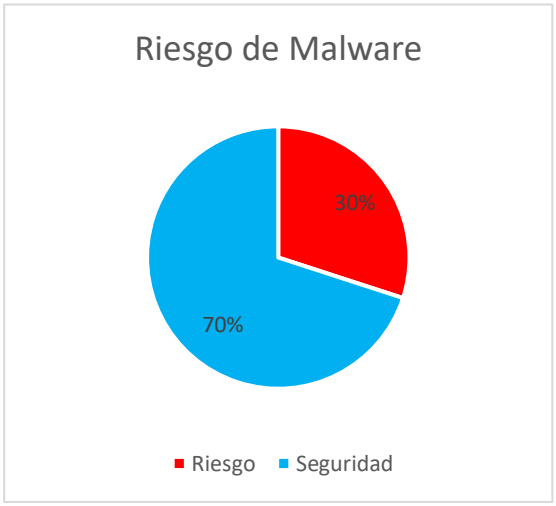
Gráfico:	**Causas:**
	• No existe un plan de contingencia documentado para inundaciones. • No se realizan inspecciones regulares de los sistemas de drenaje y desagüe de las instalaciones. • No se encuentra claramente señalados y accesible a los trabajadores los puntos de corte de agua de emergencia. • No se han implementado barreras o sellos impermeables en áreas críticas para evitar la entrada de agua. • No se realizan simulacros de inundación para una inundación para asegurar que el personal esté preparado para una emergencia de agua. • No Existen sensores y alarmas de detección de agua instalados en áreas de alto riesgo.

	• No se realiza control de inventario de equipos como bombas portátiles y suministros de emergencia. • Los equipos electrónicos y de TI no están elevados del suelo o protegidos contra posibles inundaciones. • No se han identificado y evaluado las áreas de mayor riesgo de inundación dentro de las instalaciones. • No existe un plan en específico para la protección de documentos y registros importantes en caso de inundación. • El personal no está debidamente capacitado para responder ante un riesgo de inundación. • No están los equipos de HVAS debidamente protegidos contra daños por agua. • No se han implementado medidas de prevención de inundaciones en el diseño del paisaje exterior.

Interpretación: Con un nivel de seguridad del 37% y un nivel de riesgo del 63%, se puede concluir que la protección contra inundaciones es muy deficiente y presenta un riesgo considerable. Este alto nivel de riesgo indica que existen vulnerabilidades significativas que podrían resultar en daños por inundación. Para mitigar este riesgo, es crucial implementar medidas adicionales, como sistemas de drenaje mejorados, barreras contra inundaciones y planes de emergencia específicos para inundaciones.

Ilustración 19: Nivel de riesgo inundación

Nivel de riesgo Malware

Gráfico:	**Causas:**
	• No hay protección contra la redirección de las búsquedas en el navegador a sitios web no deseados. • No hay protección contra pop-ups o anuncios emergentes inusuales al navegar por la web. • No hay protección extra en el cortafuego para que no realicen configuración sin autorización.

Interpretación: Con un nivel de seguridad del 70% y un nivel de riesgo del 30%, se puede concluir que la protección contra malware es bastante robusta. Este alto nivel de seguridad indica que se han implementado medidas efectivas para prevenir infecciones de malware. Sin embargo, el 30% de riesgo restante sugiere que aún existen algunas vulnerabilidades que podrían ser explotadas. Para reducir este riesgo, es importante mantener actualizados los sistemas de seguridad, realizar análisis regulares de malware y capacitar al personal en prácticas seguras de navegación y manejo de correos electrónicos.

Ilustración 20: Nivel de riesgo malware

4.7.1.1 Conclusiones- Opinión de la auditoria

- Según el objetivo establecido, se identificó que los principales riesgos de seguridad presentes en la instalación informática fueron incendio, robo, inundación, daño de equipos y malware. Es esencial implementar estrategias de gestión de riesgos y planes de contingencia para minimizar el impacto de estos eventos y asegurar la continuidad operativa.

- Al concluir el análisis de riesgos de seguridad informática durante la auditoría, se identificó un nivel importante de riesgo en cuanto a inundaciones, incendios y robos, debido al grado de exposición de los datos e información.

- La evidencia presentada nos permite concluir que el departamento de informática de la Dirección Distrital 13D05 El Carmen no está completamente protegido contra muchas de las amenazas previamente identificadas. Según la investigación, su nivel de seguridad es del 57,4%, mientras que el riesgo se sitúa en el 42,6%. La distribución de los riesgos es bastante uniforme, con algunas variables significativas. Por lo tanto, es necesario considerar medidas adicionales para gestionar estos riesgos de manera efectiva

- En conclusión, con base en toda la información recopilada, se elaboró una guía de recomendaciones destinada a prevenir desastres en la infraestructura tecnológica del distrito de Educación 13D05, El Carmen.

4.7.1.2 Recomendaciones de la auditoría

- A partir de los resultados de la auditoría de seguridad informática, se insta al personal administrativo de la institución a adoptar medidas preventivas de seguridad al utilizar los equipos informáticos y a implementar las siguientes buenas prácticas.

- Se sugiere seguir las indicaciones de la guía de buenas prácticas formulada para reducir la probabilidad de ocurrencia de los riesgos previamente citados. Es fundamental contar con la colaboración del personal administrativo que labora en la institución para implementar estas medidas de manera efectiva.

4.3 Guía de las buenas prácticas informáticas (AuMaT 6)

En función a las amenazas, riesgos y vulnerabilidades que fueron detallados en el transcurso de la auditoria informática elaborada en el Distrito de Educación 13D05, El Carmen. Por lo tanto, se desarrolló la siguiente guía para el adecuado uso, manejo y conservación de los equipos informáticos e instalaciones del distrito, garantizando su funcionalidad y prolongando su vida útil.

Tabla 24: Guía de recomendaciones para el distrito de educación 13D05

<table>
<tr><td rowspan="3">Guía de recomendaciones para el distrito de Educación 13D05, El Carmen

Universidad Laica Eloy Alfaro de Manabí extensión en el Carmen</td><td rowspan="3">Distrito de Educación 13D05, El Carmen.</td><td colspan="3">Fecha</td><td>PT1</td></tr>
<tr><td>17</td><td>01</td><td>2025</td><td rowspan="2"></td></tr>
<tr><td colspan="3">MARIA JUDITH ALCIVAR RIVAS</td></tr>
<tr><td colspan="6">Guía de recomendaciones para el distrito de Educación 13D05, El Carmen</td></tr>
<tr><td colspan="6">Objetivo:</td></tr>
</table>

• Establecer medidas preventivas para garantizar el funcionamiento seguro de los equipos informáticos en el distrito.	
Riesgos	**Recomendación**
ROBOS	• Instalar cercos eléctricos en las instalaciones • Instalar sistema de vigilancia que cubra todo el perímetro • Realizar registro a las personas al ingreso y salida de la institución • Realizar inspecciones de seguridad al inicio y cese de las actividades • Instalar alarmas antirrobo • Instalar un sistema de acceso con tarjetas • Instalar cámaras de vigilancia en las zonas vulnerables • Instalar alarmas que se conecten a la central de monitoreo • Establecer políticas para el ingreso de visitantes • Instalar sistema de rastreo y localización de aparatos tecnológicos

Fuente 19: Elaboración propia

Tabla 25: Guía de recomendaciones para el distrito de educación 13D05

Guía de recomendaciones para el distrito de Educación 13D05, El Carmen **Universidad Laica Eloy Alfaro de Manabí extensión en el Carmen**	**Distrito de Educación 13D05, El Carmen.**	**Fecha**			**PT1**
		17	**01**	**2025**	
		MARIA JUDITH ALCIVAR RIVAS			
Guía de recomendaciones para el distrito de Educación 13D05, El Carmen					

Objetivo: • Establecer medidas preventivas para garantizar el funcionamiento seguro de los equipos informáticos en el distrito.	
Riesgos	**Recomendación**
DAÑOS A EQUIPOS	• Comprar equipos para regular voltaje • Instalar alarmas para el control de acceso no autorizados • Instalar cámaras de vigilancia para el monitoreo de las zonas criticas • Compra de protección de equipos contra daños ocasionados por agua, fuego y otros aspectos • Compra de controles ambientales (temperatura, humedad) • Establecer políticas de seguro para daños de los equipos costosos • Organizar cables mediante bandeja de cables con múltiples orificios • Instalar protección contra la tensión a todos los equipos

Fuente 20: Elaboración propia

Tabla 26: Guía de recomendaciones para el distrito de educación 13D05

Guía de recomendaciones para el distrito de Educación	**Distrito de Educación 13D05, El Carmen.**	**Fecha**			**PT1**
		17	**01**	**2025**	

13D05, El Carmen **Universidad Laica Eloy Alfaro de Manabí extensión en el Carmen**		**MARIA JUDITH ALCIVAR RIVAS**

Guía de recomendaciones para el distrito de Educación 13D05, El Carmen

Objetivo:

- Establecer medidas preventivas para garantizar el funcionamiento seguro de los equipos informáticos en el distrito.

Riesgos	Recomendación
INCENDIO	
	• Crear un plan de prevención de incendio • Gestionar evaluaciones de los riesgos de incendio • Gestionar señalizaciones claras y visibles de los planes de evacuación • Compra de un sistema de detección de incendios conectados a una alarma central • Comprade un sistema de detección de humo • Gestionar la implementación de medidas para evitar el sobre calentamiento • Realizar inspección de cables de conexión eléctrica para la detección de posibles incendios • Gestión de procedimientos documentados para la respuesta ante incendios en el área de cómputo • Comprar un sistema de monitoreo de temperatura y humedad en las áreas de equipos

	• Gestión de identificación y documentación de todos los riesgos potenciales de incendio • Gestión de planes de inspecciones regulares de las áreas con equipos informáticos para la detección de posibles riesgos • Documentar los procedimientos para la gestión segura de materiales inflamables en las áreas con equipos • Gestionar y actualizan periódicamente los planes de contingencia y de respuesta ante incendio • Capacitar al personal para manejar incidentes de incendio en las áreas con equipos informáticos

Fuente 21: Elaboración propia

Tabla 27: Guía de recomendaciones para el distrito de educación 13D05

Guía de recomendaciones para el distrito de Educación 13D05, El Carmen **Universidad Laica Eloy Alfaro de Manabí extensión en el Carmen**	**Distrito de Educación 13D05, El Carmen.**	**Fecha**			**PT1**
		17	**01**	**2025**	
		MARIA JUDITH ALCIVAR RIVAS			
Guía de recomendaciones para el distrito de Educación 13D05, El Carmen					
Objetivo: • Establecer medidas preventivas para garantizar el funcionamiento seguro de los equipos informáticos en el distrito.					
Riesgos	**Recomendación**				

INUNDACIONES	• Gestionar y crear un plan de contingencia documentado para inundaciones de agua • Documentar horarios de inspecciones regulares de los sistemas de drenaje y desagüe de las instalaciones • Gestionar los puntos señalados y accesible a los trabajadores los puntos de corte de agua de emergencia • Compra de barreras o sellos impermeables en áreas críticas para evitar la entrada de agua • Gestionar los horarios de simulacros de inundación para asegurar que el personal esté preparado para una emergencia de agua • Comprar sensores y alarmas de detección de agua instalados en áreas de alto riesgo • Gestionar y documentar los controles de inventario de equipos como bombas portátiles y suministros de emergencia • Documentar y gestionar la movilización de los equipos electrónicos y de TI no están a lugares elevados • Documentar e identificar las áreas de mayor riesgo de inundación dentro de las instalaciones • Gestionar la implementación de planes en específico para la protección de documentos y registros importantes en caso de inundación • Capacitar al personal para responder ante un incendio • Comprar protectores para los equipos de HVAS (calefacción, ventilación y aire acondicionado) para la protección contra daños por agua • Gestionar medidas de prevención de inundaciones en el diseño del paisaje exterior

Fuente 22: Elaboración propia

Tabla 28: Guía de recomendaciones para el distrito de educación 13D05

<table>
<tr><td rowspan="2">Guía de recomendaciones para el distrito de Educación 13D05, El Carmen

Universidad Laica Eloy Alfaro de Manabí extensión en el Carmen</td><td rowspan="2">Distrito de Educación 13D05, El Carmen.</td><td colspan="3">Fecha</td><td>PT1</td></tr>
<tr><td>17</td><td>01</td><td>2025</td></tr>
<tr><td colspan="5">MARIA JUDITH ALCIVAR RIVAS</td></tr>
<tr><td colspan="6">Guía de recomendaciones para el distrito de Educación 13D05, El Carmen</td></tr>
<tr><td colspan="6">Objetivo:
• Establecer medidas preventivas para garantizar el funcionamiento seguro de los equipos informáticos en el distrito.</td></tr>
<tr><td>Riesgos</td><td colspan="5">Recomendación</td></tr>
<tr><td rowspan="2">MALWARE</td><td colspan="5"></td></tr>
<tr><td colspan="5">• Comprar un software para la protección de redirección de las búsquedas en el navegador a sitios web no deseados
• Comprar un software para la protección contra pop-ups o anuncios emergentes inusuales al navegar por la web
• Comprar un software para la protección extra en el cortafuego para que no realicen configuración sin autorización</td></tr>
</table>

Fuente 23: Elaboración propia

CAPÍTULO V

5 EVALUACIÓN DE RESULTADOS

En este capítulo se presentan los resultados obtenidos tras la implementación de la propuesta, evaluando la efectividad de las acciones y su impacto en la seguridad física de los equipos informáticos.

5.2 Informe detallado

El presente documento detalla los hallazgos obtenidos al realizar la auditoria informática llevada a cabo en las instalaciones del Distrito de Educación 13D05, El Carmen.

Dirigido a: Persona encargada del área de Tecnologías de la Información en el Distrito de Educación 13D05, El Carmen. Ing Daniel Carrasco. Este informe va dirigido al distrito de educación 13D05.

Motivo:

Proyecto integrador previo a la obtención del título de ingeniero en tecnologías de la información

Objetivo:

Para llevar a cabo la auditoría, se definieron objetivos que proporcionaron una orientación mucho más clara sobre lo que se evaluaría dentro de la institución.

- Evaluar el nivel de seguridad informática en el Distrito de educación 13D05.
- Identificar riesgos de seguridad informática en el Distrito de educación 13D05.

Personal relacionado:

Nombre	Función
Maria Judih Alcivar Rivas	**Investigadora**
Ing. Soraida Zambrano	**Directora distrital**
Ing. Daniel Carrasco	**Responsable del área de TIC de la institución**
Personal administrativo del Distrito	**Personal administrativo de la institución**

Tabla 29: Personal relacionado

Alcance:

El informe de auditoría de seguridad informática física del Distrito de Educación 13D05 identifica y evalúa riesgos en varias áreas, incluyendo robo, daño de equipos, incendios, inundaciones, y malware. Se encontraron deficiencias significativas en la seguridad contra incendios y daños por agua, así como en la protección contra fluctuaciones de energía y malware. Se recomienda implementar medidas como sistemas de detección de incendios, barreras impermeables, y capacitación en seguridad informática para mitigar estos riesgos y mejorar la seguridad general de la institución.

5.2.1 Resumen de hallazgos

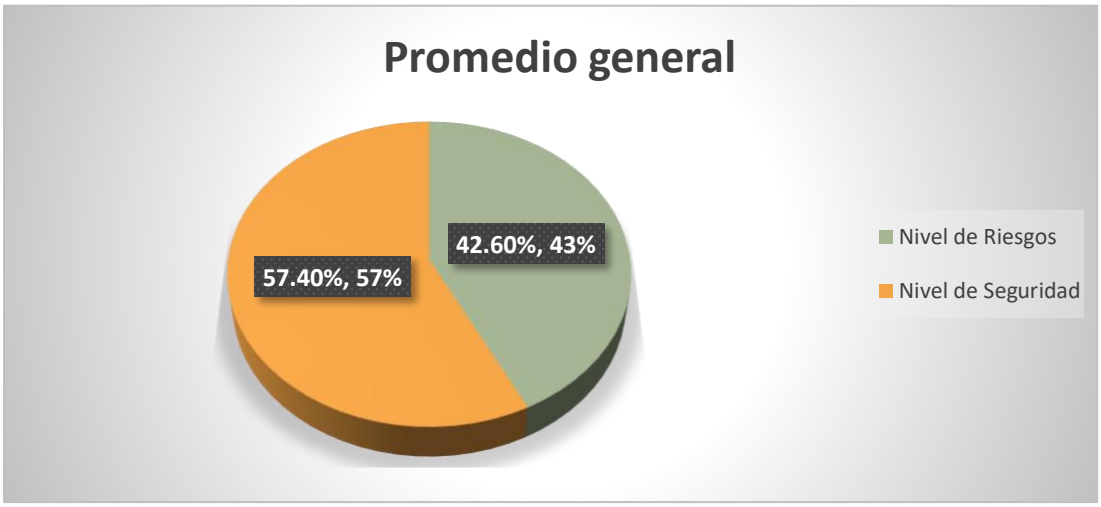


Ilustración 21: Promedio general

Interpretación:

Existe un porcentaje de seguridad del 57,4% y un 42,6% de riesgo. Dado que la distribución de los riesgos es bastante uniforme, aunque con algunas variables significativas, es imperativo implementar medidas adicionales para gestionar estos riesgos de manera efectiva y garantizar la protección integral de la infraestructura tecnológica.

Interpretación:

En este gráfico de barras, las medidas de mitigación de riesgos indican una alta seguridad en todas las áreas, excepto en las de incendios e inundaciones, que presentan niveles críticos. Es crucial abordar estas áreas con urgencia para fortalecer la protección general y minimizar los riesgos asociados.

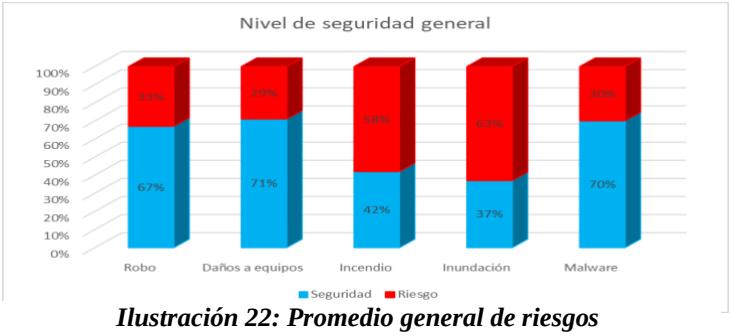
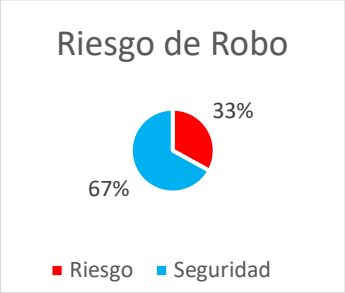
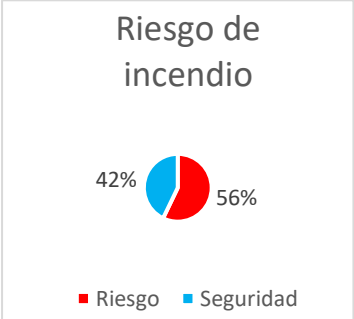


Ilustración 22: Promedio general de riesgos



Nivel de Riesgo de Robo: Importante

Aunque la seguridad contra el robo es del 67%, el 33% de riesgo indica vulnerabilidades significativas. Es crucial implementar medidas adicionales, como sistemas de vigilancia.



Nivel de Riesgo de Incendio: Importante

Con un nivel de seguridad del 42% y un riesgo del 56%, la protección contra incendios es insuficiente y presenta vulnerabilidades críticas.

Nivel de Riesgo de Inundación: Importante

Con un nivel de seguridad del 37% y un riesgo del 63%, la protección contra inundaciones es muy deficiente y presenta vulnerabilidades significativas.

Conclusión-opinión de la auditoría

Según el objetivo establecido, se identificó que los principales riesgos de seguridad presentes en la instalación informática fueron incendio, robo, inundación, daño de equipos y malware.

Al concluir el análisis de riesgos de seguridad informática durante la auditoría, se identificó un nivel importante de riesgo en cuanto a inundaciones, incendios y robos, debido al grado de exposición de los datos e información.

Recomendación

A partir de los resultados de la auditoría de seguridad informática, se insta al personal administrativo de la institución a adoptar medidas preventivas de seguridad.

Se sugiere seguir las indicaciones de la guía de buenas prácticas formulada para reducir la probabilidad de ocurrencia de los riesgos previamente citados.

CAPÍTULO VI

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Conforme a lo desarrollado en esta auditoria pude observar que la literatura tiene un papel fundamental y de gran repercusión social, por tanto, se ejecuta una recapitulación acerca del uso de estos recursos informáticos que posee la institución para luego expedir un informe sobre la situación en la que se administran estos recursos, el análisis crítico de los auditores permite suministrar un análisis, evaluaciones y recomendaciones de las actividades.

Se evaluó la situación actual del Distrito de educación 13D05 por medio de una auditoria informática y apoyándose en la metodología Magerit se logró analizar los riesgos asignados en cada activo del distrito, lo que pudo ampliar más el enfoque de los diferentes acontecimientos que pueden ocurrir y de esta manera poder solventarlas con varias medidas.

El informe de la auditoria fue elaborado con el fin de encontrar y analizar las debilidades procedimientos y controles existentes en la institución. Esto permitirá implementar medidas para el mejor desempeño de los usuarios que laboran en la institución. A través de la guía generada a partir de este informe es posible reducir o mitigar los riesgos relacionados con la seguridad física en el Distrito de Educación 13D05 El Carmen.

La guía ofrece recomendaciones basadas en los hallazgos de la auditoria, las cuales, con el enfoque de fortalecer los sistemas de control, optimizar el uso de los recursos y minimizar la probabilidad de incidentes que puedan afectar las actividades del distrito.

6.2 Recomendaciones

Es recomendable desarrollar políticas claras para el uso adecuado y el propio mantenimiento preventivo de los equipos informáticos. Al cual se le añade capacitar al personal que labora en la institución sobre las mejores prácticas para el cuidado de los dispositivos, reportar cuando ocurre alguna falla técnica es oportuno además de que garantiza que los recursos este disponibles para las actividades correspondientes, se podría aplicar normas del buen uso de los equipos en cada área del distrito para su mejor implementación. Así mismo, los equipos deben de estar sujetos a controles que eviten interrupciones en el servicio y ampliar su vida útil.

Las auditorias informáticas son importantes por las razones que se detallan a continuación. Es necesario realizar evaluaciones iterativas aplicando la metodología Magerit con el fin de identificar posibles amenazas y priorizar en acciones correctivas. Para luego, establecer un plan de contingencia que ayude a la institución a seguir los procedimientos en caso de ocurrir incidentes. Es por ello que hay que motivar a las instituciones a implementar auditorias informáticas.

Hay que destacar que es necesario realizar copias de seguridad para los datos del distrito, esto permitirá almacenar copias en ubicaciones seguras. Lo que permitirá recuperar la información en casi de fallos técnicos, ataques cibernéticos o desastres naturales, minimizando el impacto en las operaciones.

BIBLIOGRAFÍA

7 Bibliografía

Alzate, A. T. (2001). AUDITORÍA DE SISTEMAS Una visión práctica. En A. T. Alzate, *AUDITORÍA DE SISTEMAS Una visión práctica* (pág. 16). Colombia: Universidad Nacional de Colombia Sede Manizales.

Anabel, H. P. (19 de 03 de 2011). *http://ri.uaemex.mx/*. Obtenido de http://ri.uaemex.mx/: http://hdl.handle.net/20.500.11799/99917

Angamarca, L. (2022). Estrategias de auditoría informática en la era de la transformación digital. *Technology Rain Journal*, 11.

Ashdown, C. (04 de 05 de 2023). *https://www.2n.com/es-ES/blog/la-historia-de-los-sistemas-de-control-de-acceso*. Obtenido de https://www.2n.com/es-ES/blog/la-historia-de-los-sistemas-de-control-de-acceso: https://www.2n.com/es-ES/blog/la-historia-de-los-sistemas-de-control-de-acceso

Balarezo López, J. E., & Tenezaca Caizabanda, M. (2024). *Auditoria informática para el análisis de la seguridad en los recursos informáticos utilizando Normas ISO 27001 en Megakons S.A.* Ambato: Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Tecnologías de la Información.

Caburao, E. A. (2024). Seguridad Física: Estrategias Esenciales para Proteger los Activos Críticos de una Organización. *SafetyCulture*.

Carmen, D. S., & Rojas Perleche, C. (2024). *Análisis del nivel de seguridad de la información de la oficina de informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista – 2023.* San Juan Bautista: Universidad Científica del Perú.

Castro Rincón, C. A. (29 de 04 de 2013). *UNIVERSIDAD MILITAR Nueva Granada.* Obtenido de UNIVERSIDAD MILITAR Nueva Granada: http://hdl.handle.net/10654/3431

DIAZ, R. A. (2019). *UNIVERSIDAD MILITAR NUEVA GRANADA.* Obtenido de UNIVERSIDAD MILITAR NUEVA GRANADA: https://repository.unimilitar.edu.co/

Edwin, R. C., & Víctor, A. D. (24 de 06 de 2023). *Análisis y Mitigación de Riesgos que afectan la Seguridad Física: una revisión.* Obtenido de Análisis y Mitigación de Riesgos que afectan la Seguridad Física: una revisión: https://revistas.universu.com.co/index.php/rices/article/view/5

Enrique, C. d., & García Fernández, F. (02 de 2019). *GREDOS*. Obtenido de GREDOS: https://gredos.usal.es/handle/10366/139644

Galeano Gimenéz, R., & González Prieto, O. M. (24 de Agosto de 2021). *FPUNE Scientific.* Obtenido de FPUNE Scientific: http://servicios.fpune.edu.py:83/fpunescientific/index.php/fpunescientific/article/view/207

Gallejos Manrrique, L. A., & Lynch Escobar, C. D. (2024). *Universidad Politécnica Salesiana.* Obtenido de Universidad Politécnica Salesiana: http://dspace.ups.edu.ec/handle/123456789/28028

Galvis, O. D., & Herrera Marchena, L. G. (30 de 8 de 2005). *Scielo*. Obtenido de Scielo: http://www.scielo.org.co/scielo.php?pid=S0123-59232006000100004&script=sci_arttext

Gonzáles, J. L. (Diciembre de 2020). *https://gc.scalahed.com/.* Obtenido de https://gc.scalahed.com/: https://gc.scalahed.com/recursos/files/r161r/w26118w/Tecnicas%20e%20instrumentos.pdf

Guerrero, B. A. (2024). *Comparación de modelos de control COSO y COBIT utilizados para auditorías informáticas para instituciones académicas de educación media de la ciudad de Ibarra.* Ibarra: Universidad Técnica del Norte.

Herrera Mora, A. Z. (2024). *Universidad Técnica de Babahoyo.* Obtenido de Universidad Técnica de Babahoyo: http://dspace.utb.edu.ec/handle/49000/15678

Klever, M. P., & Arteaga Zambrano, J. A. (1 de 2019). *UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ.* Obtenido de UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ: http://repositorio.unesum.edu.ec/handle/53000/1519

Laborales, P. d. (2015). *Modelos de las Nuevas Tecnologías aplicadas a las PRL.* Jaén : CEJ.

López, R. (2017). *https://repositorio.usam.ac.cr/*. Obtenido de https://repositorio.usam.ac.cr/: localhost/xmlui/handle/11506/2036

LOZANO, L. C. (2014). *Academia.edu.* Obtenido de Academia.edu: https://d1wqtxts1xzle7.cloudfront.net/54176062/Importancia_de_las_Auditorias-libre.pdf?1503074883=&response-content-disposition=inline%3B+filename%3DLA_IMPORTANCIA_DE_LAS_AUDITORIAS_INTERNA.pdf&Expires=1721103155&Signature=CrAwvMg3kELe1GLoZh9yAf1vFQMqbcFh

Majian, A. (Noviembre de 2020). *Universidad Nacional de San Martín.* Obtenido de Universidad Nacional de San Martín: https://ri.unsam.edu.ar/handle/123456789/1482

Martín, S. d. (2016). *El uso de las TICs para la gestión empresarial.* Soria: CET.

Martínez, L. C. (Diciembre de 2017). *https://repository.ucc.edu.co/.* Obtenido de https://repository.ucc.edu.co/: https://repository.ucc.edu.co/server/api/core/bitstreams/6122fd2b-e1a9-49cd-94d9-feb17a4ee3e4/content

Martínez, Y. A., Blanco Alfonso, B., & Loy Marichal, L. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería*, 14.

Montejo Suarez, J. C. (17 de 04 de 2014). *Importancia de la seguridad física en Colombia como mecanismo de seguridad en el sector privado.* Obtenido de Importancia de la seguridad física en Colombia como mecanismo de seguridad en el sector privado: http://hdl.handle.net/10654/11169

Moreno, V. M., & Calvarado Mendoza, A. (31 de 07 de 2023). *Revista Científica: BIOTECH AND ENGINEERING*. Obtenido de Revista Científica: BIOTECH AND ENGINEERING: https://doi.org/10.52248/eb.Vol3Iss2.78

Obregón, M. A. (Marzo de 2024). *Universidad Israel.* Obtenido de Universidad Israel: http://repositorio.uisrael.edu.ec/handle/47000/4071

Oliva, M. D. ((2013)). *Seguridad física, prevención y detección.* Obtenido de Seguridad física, prevención y detección.: Seguridad física, prevención y detección

Ovalle, S. O., & Cervantes Sánchez, O. (07 de 2012). *https://www.eumed.net/rev/cccss/21/oocs.html*. Obtenido de https://www.eumed.net/rev/cccss/21/oocs.html: https://www.eumed.net/rev/cccss/21/oocs.html

Palacios, A. P. (2020). Seguridad Informática. En A. P. Palacios, *Seguridad Informática* (págs. 2-3). Madrid: Parainfo, SA.

Piattinni, M., Del Peso, E., & Del Peso, M. (2007). *Auditoría de Tecnilogías y Sistemas de Información.* Madrid: Ra-Ma.

Pino, S. B. (Diciembre de 2008). *https://archivos.csif.es/.* Obtenido de https://archivos.csif.es/: https://archivos.csif.es/archivos/andalucia/ensenanza/revistas/csicsif/revista/pdf/Numero_12/SILVIA_BORREGO_1.pdf

Ponce, W. P., & Ponce Pereira, R. L. (2022). *Auditoría Informática a la seguridad física, en los procesos administrativos de la cooperativa interprovincial de transporte manglar alto de la ciudad de Santa Elena.* Santa Elena: Jijpijapa.UNESUM.

Rodríguez, F. A. (01 de Julio de 2011). *https://redined.educacion.gob.es/*. Obtenido de https://redined.educacion.gob.es/: https://redined.educacion.gob.es/xmlui/bitstream/handle/11162/14880/00720113000433.pdf?seq

Somano, A. K., & Medina León, C. A. (2020). *http://monografias.umcc.cu/*. Obtenido de http://monografias.umcc.cu/: http://monografias.umcc.cu/monos/2020/IngInd/mo2076.pdf

Tacuri, G. Y., & Narvaez Zurita, C. (2024). Auditoría forense en el contexto latinoamericano: comparación de prácticas y normativas. *Gestio Et Productio. Revista Electrónica De Ciencias Gerenciales* , 16.

Vásquez, K. d. (Octubre de 2013). *https://dspace.ups.edu.ec/*. Obtenido de https://dspace.ups.edu.ec/: https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

Zobeyda, H. M. (2024). *Análisis de la incidencia de las políticas y prácticas de seguridad informática en la arquitectura física existente en la dirección de tecnologías y sistemas información de la universidad técnica de Babahoyo.* Babahoyo: Universidad Tecnica de Babahoyo.

ANEXOS

Anexo A: Asignación de tutor

Anexo A: Asignación de tutor

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

CERTIFICACIÓN

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

Haber dirigido y revisado el trabajo de investigación, bajo la autoría de la estudiante **ALCIVAR RIVAS MARÍA JUDITH**, legalmente matriculada en la carrera de Ingeniería en Tecnologías de la Información, período académico 2024(1)-2024(2), cumpliendo el total de 384 horas, bajo la opción de titulación de proyecto integrador, cuyo tema del proyecto es "Auditoría Informática en la Seguridad Física de los equipos informáticos en el Distrito de Educación 13D05".

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

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

El Carmen, 20 de Diciembre del 2024.

Lo certifico,

Wladimir Minaya Macías, Mg.
Docente Tutor
Área: Sistemas

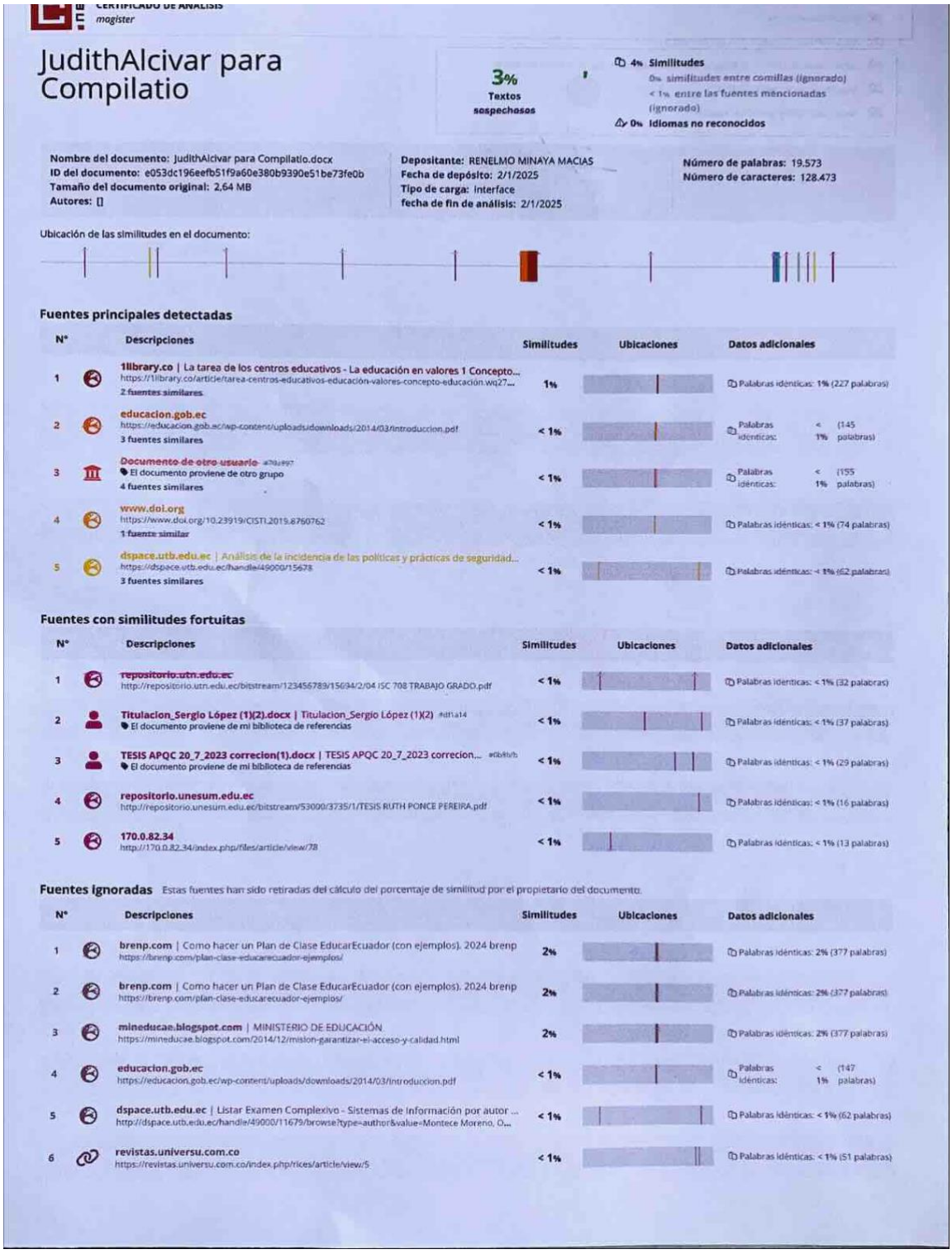
UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ EXTENSIÓN EN EL CARMEN
Uleam
COMISIÓN ACADÉMICA
EL CARMEN - MANABÍ

Anexo B: Certificado de la empresa

Anexo B: Certificado de la empresa

Anexo D: Reporte del sistema antiplagio

Anexo C: Reporte del sistema antiplagio



CERTIFICADO DE ANÁLISIS
magister

JudithAlcivar para Compilatio

3%
Textos sospechosos

4% Similitudes
0% similitudes entre comillas (ignorado)
< 1% entre las fuentes mencionadas (ignorado)
0% Idiomas no reconocidos

Nombre del documento: JudithAlcivar para Compilatio.docx
ID del documento: e053dc196eefb51f9a60e380b9390e51be73fe0b
Tamaño del documento original: 2,64 MB
Autores: []

Depositante: RENELMO MINAYA MACIAS
Fecha de depósito: 2/1/2025
Tipo de carga: Interface
fecha de fin de análisis: 2/1/2025

Número de palabras: 19.573
Número de caracteres: 128.473

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**1library.co** | La tarea de los centros educativos - La educación en valores 1 Concepto... https://1library.co/article/tarea-centros-educativos-educación-valores-concepto-educación.wq27... 2 fuentes similares	1%		Palabras idénticas: 1% (227 palabras)
2	**educacion.gob.ec** https://educacion.gob.ec/wp-content/uploads/downloads/2014/03/Introduccion.pdf 3 fuentes similares	< 1%		Palabras idénticas: < 1% (145 palabras)
3	**Documento de otro usuario** El documento proviene de otro grupo 4 fuentes similares	< 1%		Palabras idénticas: < 1% (155 palabras)
4	**www.doi.org** https://www.doi.org/10.23919/CISTI.2019.8760762 1 fuente similar	< 1%		Palabras idénticas: < 1% (74 palabras)
5	**dspace.utb.edu.ec** | Análisis de la incidencia de las políticas y prácticas de seguridad... https://dspace.utb.edu.ec/handle/49000/15673 3 fuentes similares	< 1%		Palabras idénticas: < 1% (62 palabras)

Fuentes con similitudes fortuitas

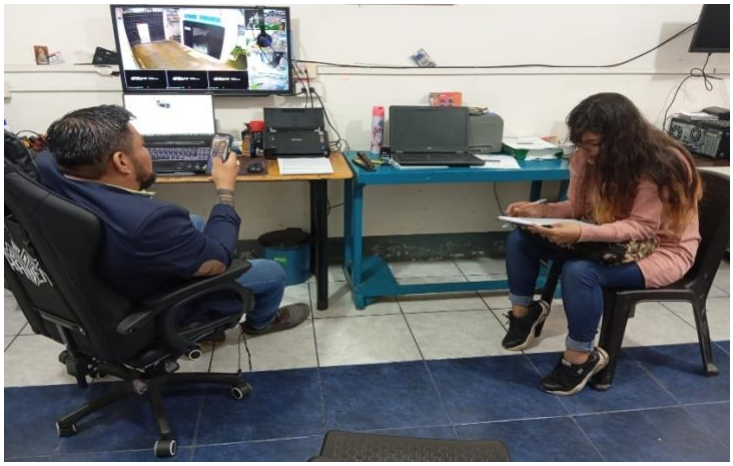
N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**repositorio.utn.edu.ec** http://repositorio.utn.edu.ec/bitstream/123456789/15034/2/04 ISC 708 TRABAJO GRADO.pdf	< 1%		Palabras idénticas: < 1% (32 palabras)
2	**Titulacion_Sergio López (1)(2).docx** | Titulacion_Sergio López (1)(2) El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (37 palabras)
3	**TESIS APQC 20_7_2023 correcion(1).docx** | TESIS APQC 20_7_2023 correcion... El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (29 palabras)
4	**repositorio.unesum.edu.ec** http://repositorio.unesum.edu.ec/bitstream/53000/3735/1/TESIS RUTH PONCE PEREIRA.pdf	< 1%		Palabras idénticas: < 1% (16 palabras)
5	**170.0.82.34** http://170.0.82.34/index.php/files/article/view/78	< 1%		Palabras idénticas: < 1% (13 palabras)

Fuentes ignoradas

Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

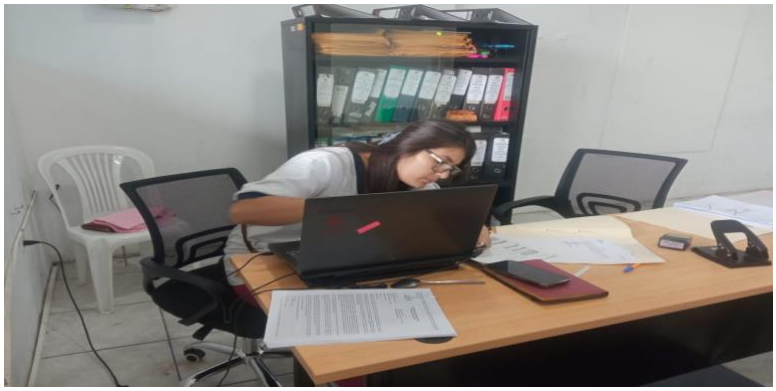
N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**brenp.com** | Como hacer un Plan de Clase EducarEcuador (con ejemplos). 2024 brenp https://brenp.com/plan-clase-educarecuador-ejemplos/	2%		Palabras idénticas: 2% (377 palabras)
2	**brenp.com** | Como hacer un Plan de Clase EducarEcuador (con ejemplos). 2024 brenp https://brenp.com/plan-clase-educarecuador-ejemplos/	2%		Palabras idénticas: 2% (377 palabras)
3	**mineducae.blogspot.com** | MINISTERIO DE EDUCACIÓN https://mineducae.blogspot.com/2014/12/mision-garantizar-el-acceso-y-calidad.html	2%		Palabras idénticas: 2% (377 palabras)
4	**educacion.gob.ec** https://educacion.gob.ec/wp-content/uploads/downloads/2014/03/Introduccion.pdf	< 1%		Palabras idénticas: < 1% (147 palabras)
5	**dspace.utb.edu.ec** | Listar Examen Complexivo - Sistemas de Información por autor ... http://dspace.utb.edu.ec/handle/49000/11679/browse?type=author&value=Montece Moreno, O...	< 1%		Palabras idénticas: < 1% (62 palabras)
6	**revistas.universu.com.co** https://revistas.universu.com.co/index.php/rices/article/view/5	< 1%		Palabras idénticas: < 1% (51 palabras)

Anexo E: Fotografías



Entrevista a encargado del área de Tecnologías de la Información en el Distrito de Educación 13D05.

Evidencia de aplicación de encuesta al personal administrativo del Distrito.



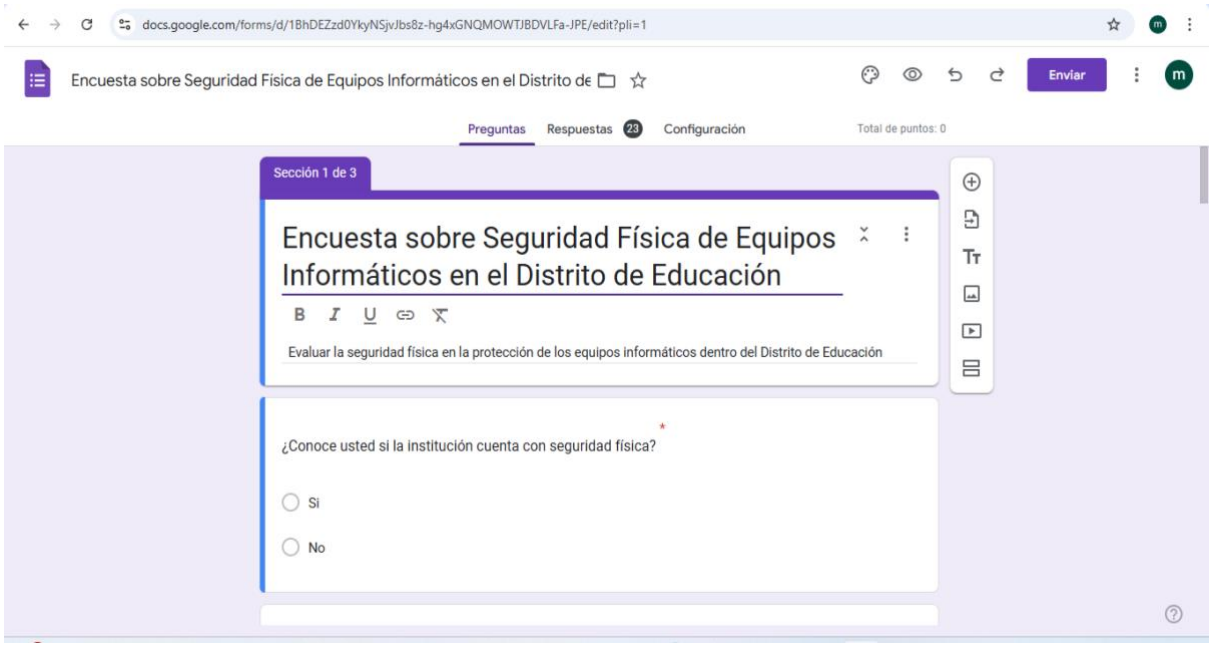
Evidencia de ejecución de auditoría

Entrada principal al distrito de educación.

Entrada secundaria del Distrito de Educación.

Estanterías

Anexo F: Evidencia de aplicación de encuestas y entrevistas


docs.google.com/forms/d/1BhDEZzd0YkyNSjvJbs8z-hg4xGNQMOWTJBDVLFa-JPE/edit?pli=1
Encuesta sobre Seguridad Física de Equipos Informáticos en el Distrito de
Enviar
Preguntas
Respuestas 23
Configuración
Total de puntos: 0
Sección 1 de 3
Encuesta sobre Seguridad Física de Equipos Informáticos en el Distrito de Educación
Evaluar la seguridad física en la protección de los equipos informáticos dentro del Distrito de Educación
¿Conoce usted si la institución cuenta con seguridad física?
Si
No

Glosario

Definiciones:

A

Acceso restringido: Área o recurso que solo puede ser utilizado por personal autorizado.
Actualización: Proceso mediante el cual se mejora o renueva un sistema, software o hardware para optimizar su funcionamiento.
Almacenamiento: Espacio o capacidad para guardar datos en dispositivos físicos o digitales.

B

Backup (Copia de seguridad): Proceso de duplicar información importante para evitar su pérdida en caso de fallos.
Base de datos: Conjunto de datos organizados y almacenados de manera que puedan ser consultados y gestionados fácilmente.
Bios (Sistema Básico de Entrada/Salida): Software preinstalado en una computadora que controla las funciones básicas de hardware.

C

Configuración: Conjunto de ajustes o parámetros establecidos para que un sistema funcione de manera específica.
Conmutador: Dispositivo de red que conecta múltiples dispositivos para permitir la comunicación entre ellos.

CPU (Unidad Central de Procesamiento): Parte principal de un computador encargada de procesar las instrucciones y ejecutar los programas.

D

Disco duro: Dispositivo de almacenamiento permanente donde se guardan los datos de un sistema.

Dominio: Nombre único que identifica a un sitio web en Internet.

Driver: Software que permite a un sistema operativo interactuar con un hardware específico.

E

Encriptación: Proceso de codificar información para protegerla contra accesos no autorizados.

Escritorio remoto: Tecnología que permite controlar un computador a distancia a través de una red.

Extranet: Red privada que permite el acceso controlado a usuarios externos.

F

Firewall (Cortafuegos): Sistema de seguridad que controla el tráfico de datos entre redes, bloqueando accesos no autorizados.

Firmware: Software preinstalado en dispositivos de hardware que permite su funcionamiento básico.

Formato: Proceso de preparación de un dispositivo de almacenamiento eliminando todo el contenido existente.

G

Gestión de datos: Administración de información para su organización, almacenamiento y análisis.
Gigabyte (GB): Unidad de medida de datos equivalente a 1,024 megabytes.
GPU (Unidad de Procesamiento Gráfico): Componente que se encarga de renderizar imágenes, videos y gráficos en una computadora.

H

Hardware: Componentes físicos de un sistema informático, como monitores, discos duros y procesadores.
Host: Computador o servidor que provee recursos o servicios en una red.
HTTP (Protocolo de Transferencia de Hipertexto): Protocolo utilizado para la comunicación de datos en la web.

I

Interfaz: Medio a través del cual los usuarios interactúan con un sistema o dispositivo.
IP (Protocolo de Internet): Dirección única asignada a cada dispositivo conectado a una red.

TI (Tecnologías de la Información): Conjunto de recursos y herramientas tecnológicas utilizadas para el manejo de información.

M

Malware: Software malicioso diseñado para dañar sistemas informáticos o robar información.
Monitor: Dispositivo de salida que muestra imágenes generadas por un sistema informático.
Memoria RAM: Componente que almacena temporalmente los datos y programas que utiliza el sistema operativo para funcionar.

P

Password (Contraseña): Cadena de caracteres utilizada para autenticar el acceso a un sistema.
Phishing: Técnica de fraude que busca engañar a los usuarios para obtener información personal.
Procesador: Componente encargado de interpretar y ejecutar las instrucciones de un programa.

R

Red: Conjunto de dispositivos interconectados que comparten recursos e información.
Router: Dispositivo que conecta redes y dirige el tráfico de datos entre ellas.
RAM (Memoria de Acceso Aleatorio): Memoria temporal utilizada por los sistemas para ejecutar programas y procesos.

S

Servidor: Computadora o sistema que provee servicios y recursos a otros dispositivos en una red.
Sistema operativo: Software que actúa como intermediario entre el hardware y el usuario.
Software: Conjunto de programas y aplicaciones que ejecutan tareas específicas en un sistema informático.

T

Tecnologías de soporte: Herramientas diseñadas para facilitar el trabajo colaborativo y la gestión organizacional.
Token: Elemento de seguridad que verifica la autenticidad de un usuario o transacción.
Troyano: Tipo de malware que se oculta en un programa legítimo para infiltrarse en un sistema.

U

Unidad de almacenamiento: Dispositivo físico o virtual utilizado para guardar datos.
URL (Localizador Uniforme de Recursos): Dirección web que permite acceder a recursos en Internet.
Usuario: Persona o entidad que interactúa con un sistema informático.

V

VPN (Red Privada Virtual): Tecnología que establece conexiones seguras entre redes públicas y privadas.
Velocidad de transmisión: Tasa a la cual se transfieren datos en una red.
Virus: Programa malicioso diseñado para replicarse y dañar sistemas o datos.

W

WAN (Red de Área Amplia): Red que conecta múltiples redes locales a través de grandes distancias.
Wi-Fi: Tecnología de conectividad inalámbrica que permite a los dispositivos acceder a redes.