PORTADA

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

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

PROYECTO INTEGRADOR

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

TEMA:

SGSI PARA EL ÁREA ACADÉMICA EN LA UNIDAD EDUCATIVA EXCELSO ESPÍRITU SANTO 2023-2024

AUTORA

FUERTES GOMEZ KATTY CAROLINA

TUTORA

ING.POZO HERNÁNDEZ CLARA GUADALUPE MG.

EL CARMEN, AGOSTO 2024

CERTIFICACIÓN DEL TUTOR

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

CERTIFICACIÓN

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

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular bajo la autoría de la estudiante **FUERTES GOMEZ KATTY CAROLINA**, legalmente matriculados en la carrera de Ingeniería en Tecnologías de la Información, período académico 2023(2)-2024(1), cumpliendo el total de 384 horas, cuyo tema del proyecto o núcleo problémico es **"SGSI PARA EL ÁREA ACADÉMICA EN LA UNIDAD EDUCATIVA EXCELSO ESPÍRITU SANTO 2023-2024"**

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

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

El Carmen, 18 de julio del 2024

Lo certifico,

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

TRIBUNAL DE SUSTENTACIÓN

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EL CARMEN

APROBACIÓN DEL TRABAJO DE TITULACIÓN

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con modalidad Proyecto Integrador, titulado "SGSI para el área académica en la Unidad Educativa Excelso Espíritu Santo 2023-2024", cuya autora es Katty Carolina Fuertes Gomez de la Carrera de Ingeniería en Tecnologías de la Información y como Tutora de Trabajo de Titulación la Ing. Clara Guadalupe Pozo Hernández, Mg.

El Carmen, agosto de 2024

Ing. Renelmo Wladimir Minaya Macias, Mg.
Presidente del tribunal de titulación

Ing. Raúl Saed Reascos Pinchao, Mg.
Miembro del tribunal de titulación

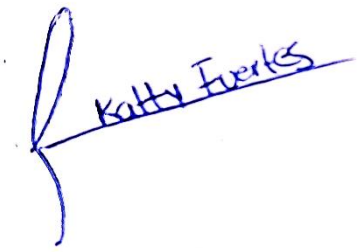
Ing. Jefferson Omar Arca Zavala, Mg.
Miembro del tribunal de titulación

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: SGSI PARA EL ÁREA ACADÉMICA EN LA UNIDAD EDUCATIVA EXCELSO ESPÍRITU SANTO, corresponde exclusivamente a: Fuertes Gomez Katty Carolina con CI. 235074987-1 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.



Fuertes Gomez Katty Carolina

235074987-1

DEDICATORIA

Dedico esta tesis primeramente a Dios, por haberme dado la vida y permitirme haber logrado concluir mi carrera, a mis padres porque sin ellos no hubiera podido lograr esta meta con su amor y apoyo incondicional fueron mi mayor inspiración en mi vida profesional y personal en enseñarme valores desde mi niñez para ser una persona de bien. A mi hermano con su apoyo en cada momento. A mi novio por haberme apoyado y confiar en mí que si podía.

Katty Carolina Fuertes Gomez

AGRADECIMIENTO

A Dios, por acompañarme todos los días. A mi madre Jacoba Gomez y a mi padre Luis Fuertes con su amor incondicional y siempre con unas palabras de apoyo fueron mi mayor inspiración para salir adelante. A mi tía Natalia Gomez con su cariño y apoyo incondicional.

Agradezco a mi tutora de tesis Ing. Clarita Pozo por la dedicación y apoyo que me ha brindado en todo este proceso de titulación. Así como haberme tenido paciencia para guiarme durante todo el desarrollo de la tesis.

Quiero agradecer a los dueños de la Unidad Educativa Excelso Espíritu Santo por haber podido realizar mi trabajo de titulación.

Katty Carolina Fuertes Gomez

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto tiene como objetivo la implementación de un Sistema de Gestión de Seguridad de la Información para el área académica de la Unidad Educativa Excelso Espíritu Santo. Este sistema está diseñado para proteger los equipos informáticos de la institución. Para alcanzar este objetivo, se realizaron entrevistas con el encargado de los equipos informáticos en las aulas y encuestas a los docentes. Estas acciones permitieron identificar la problemática relacionada con la falta de políticas y controles de seguridad informática.

Se llevó a cabo una auditoría siguiendo las cuatro fases de la norma ISO 27001. Primero, se determinó el nivel de madurez del SGSI mediante la aplicación de dos instrumentos: uno para evaluar el cumplimiento de requisitos y otro para evaluar el cumplimiento de controles. Los resultados indicaron que el nivel de madurez en la gestión de seguridad de la información es medio, con un valor porcentual del 67%.

Además, se realizó un análisis de riesgos, para el cual se elaboraron cinco cuestionarios destinados a evaluar controles para prevenir robos, daños en el equipo, incendios, inundaciones y malware. Los resultados mostraron que la seguridad en las aulas de la institución tiene un nivel medio, con un porcentaje del 44%. Se identificaron los riesgos con mayor probabilidad de ocurrencia, siendo el incendio, las inundaciones y el malware los más significativos.

Finalmente, se desarrolló un manual de políticas de seguridad con el propósito de mejorar la protección de los equipos en la Unidad Educativa Excelso Espíritu Santo, brindando a los docentes herramientas y directrices para fortalecer la seguridad en sus actividades educativas diarias.

ABSTRACT

This project aims to implement a Information Security Management System (ISMS) for the academic area of Unidad Educativa Excelso Espíritu Santo. This system is designed to protect the institution's IT equipment. To achieve this goal, interviews were conducted with the person in charge of the IT equipment in the classrooms and surveys were administered to the teachers. These actions helped identify the issue related to the lack of information security policies and controls.

An audit was conducted following the four phases of ISO 27001. First, the maturity level of the ISMS was determined using two instruments: one to assess compliance with requirements and another to assess compliance with controls. The results indicated that the maturity level in information security management is medium, with a percentage value of 67%.

Additionally, a risk analysis was performed, which involved developing five questionnaires to evaluate controls for preventing theft, equipment damage, fire, flooding, and malware. The results showed that the security level in the institution’s classrooms is medium, with a percentage of 44%. The risks with the highest probability of occurrence were identified, with fire, flooding, and malware being the most significant.

Finally, a security policy manual was developed to improve the protection of equipment at Unidad Educativa Excelso Espíritu Santo, providing teachers with tools and guidelines to enhance security in their daily educational activities.

CAPÍTULO
1. INTRODUCCIÓN

1.1 Introducción

Este trabajo de titulación se centra en la implementación de un Sistema de Gestión de Seguridad de la Información en el ámbito académico de la Unidad Educativa Excelso Espíritu Santo. El objetivo fundamental fue realizar un sistema de SI. El objetivo principal fue desarrollar un sistema de seguridad. Para lograrlo, se llevaron a cabo entrevistas con el vicerrector responsable de los salones, y se realizaron encuestas a los maestros donde se pudo identificar las deficiencias en las políticas de seguridad. Como parte de la evaluación, se llevó a cabo una auditoría siguiendo las cuatro fases de la norma ISO 27001, lo que permitió determinar que el nivel de madurez en seguridad es medio, con un valor de 67%. Este resultado se obtuvo mediante la aplicación de un instrumento de medición basado en requisitos y controles específicos. En cuanto a los diferentes aspectos de la seguridad, se determinó un alto nivel de protección contra robos, con un 59%, y un alto nivel de protección frente a daños en los equipos, con un 57%. Sin embargo, se identificó un bajo nivel de seguridad ante riesgos de incendios, con un 24%. La protección frente a inundaciones fue evaluada como media, con un 31%, y la protección contra malware recibió una calificación media del 47%. En resumen, el nivel general de seguridad de la institución se ubicó en un 44%, lo que se clasifica como un nivel medio.

En el primer capítulo, se presenta el tema de titulación a través de un análisis. Se ha elaborado un árbol de problemas basado en la información durante las investigaciones. El segundo capítulo se centra en la aplicación del SGSI, en lo académico y en los equipos informáticos de las aulas. Se identificaron problemas, como la falta de conocimientos sobre el uso de las computadoras y la ausencia de políticas de seguridad. El tercer capítulo describe

los enfoques y métodos de investigación. Se realizaron encuesta a los docentes para adquirir información sobre el uso de los equipos y una entrevista con el responsable de las aulas.

En el cuarto capítulo se detalla la propuesta para el SGSI. Se definieron los recursos, se desarrolló siguiendo las fases de la norma ISO 27001, se diseñó la planificación que abarcó varias etapas claves. Primero, se realizó una auditoría inicial para establecer el punto de partida. Luego, se llevó a cabo un análisis del contexto para comprender el entorno en el que se opera. A continuación, se aplicaron cuestionarios para identificar y evaluar los riesgos. Después, se procedió a la tabulación de los datos y a la evaluación del impacto de estos riesgos.

En el quinto capítulo de mi trabajo tiene todos los resultados. Mediante la evaluación de los requisitos y controles de la norma ISO 27001. El informe tiene un análisis detallado de los riesgos asociados con el daño de equipos, incendios, inundaciones, robo y malware. Además, se incluye el manual de políticas de seguridad implementadas para mitigar estos riesgos.

1.2 Presentación del tema

SGSI para el área académica en la Unidad Educativa Excelso Espíritu Santo 2023-2024

1.3 Ubicación y contextualización de la problemática

El Excelso Espíritu Santo es una institución privada que ofrece formación desde inicial hasta bachiller. Además, ofrecen actividades complementarias y clases de inglés. En este momento, cuenta con 603 alumnos, 32 docentes, 3 administrativos y 12 gestores. También ofrece para que escolares de otras instituciones realicen prácticas. Está ubicada en el kilómetro 8 de la Vía Chone - Santo Domingo. La escuela dispone de 26 equipos, con 32 GB de memoria RAM, discos de estado sólido de 240 GB y monitores de 19.5 pulgadas de las

marcas LG o Samsung. Además, los salones tienen su equipo completo. Todas las aulas de clase, desde inicial hasta bachillerato, el sistema operativo es Windows 10 y utilizan una red de fibra óptica. La gestión de las computadoras de las aulas a cargo del área de Vicerrectorado.

1.4 Planteamiento del problema

1.4.1 Problematización

La ausencia de políticas de seguridad de la información en el EES es un riesgo la privacidad en los ordenados de las aulas. Son utilizados como recurso de enseñanza para los profesores. Se encuentran vulnerables debido a la falta de confidencialidad. Esto incrementa el riesgo de daño al acceder a sitios web con virus o al conectar dispositivos no verificados que puedan contener virus. Además, la falta de restricciones en el uso del hardware permite que los alumnos los utilicen en actividades no relacionadas con el aprendizaje.

Sumando a esto, si no se les brinda el mantenimiento, el computador puede volverse ineficiente. Es decir, afecta el proceso de aprendizaje, ya que los docentes dependen de estos equipos para llevar a cabo actividades. Por otro lado, el uso de contraseñas simples puede llevar a que los estudiantes las compartan con otros, lo que facilita el uso indebido de las CPU, como la instalación de software no autorizado.

1.4.2 Génesis del problema

A nivel mundial, las empresas han adoptado la implementación de un SGSI, con el objetivo de prevenir el uso indebido de datos. En la actualidad, los ataques han crecido, poniendo en riesgo la integridad de las actividades en las empresas. Sin embargo, la falta de conocimiento por parte de la dirección en empresas sobre la importancia del sistema de seguridad resulta en la ausencia de políticas. La falta de comprensión de los avances tecnológicos dificulta la protección contra ataques.

Muchas empresas en la actualidad no cuentan de un SGSI, lo que resulta una falta de protección. Por ello, se deben proteger, estableciendo protocolos que prevengan robos. En respuesta a estos riesgos, Estados Unidos hay un incremento en los ataques y actividades ilegales por hackers en los últimos años. Como resultado, muchas empresas han comenzado a implementar protocolos para salvaguardar sus datos.

En Ecuador, el computador es un recurso de la enseñanza, para alumnos y profesores. Sin embargo, también han aumentado las amenazas en los centros educativos. Por ello, es crucial un Sistema de Gestión que garantice la protección. La ausencia de políticas de seguridad expone a riesgos como virus, robo y fallas en las computadoras. Estos incidentes no solo afectan a las instituciones, sino que también pueden interrumpir los servicios y comprometer la confidencialidad.

En la institución Espíritu Santo, no tienen políticas de seguridad de información para los equipos de clase. Esta falta de políticas compromete la integridad y disponibilidad. La ausencia de mantenimiento, junto con el uso inadecuado de los equipos, debido a la falta de capacitación a los docentes en su funcionamiento. Por lo tanto, se debe implementar un reglamento que prolongue la vida útil de los equipos de TI.

1.4.3 Estado actual del problema

La investigación en la unidad se manifestó la falta de políticas para el uso de los equipos. La ausencia de reglamentos pone en riesgo la confidencialidad, ya que puede ser divulgada a personas desconocidas. Este impacta la calidad de la presentación de contenidos. Además, a ser modificados por personas no autorizadas. La falta de mantenimiento, reduce su vida útil. Por otro lado, el uso de contraseñas débiles, la ausencia de restricciones de acceso a la red y la utilización de dispositivos sin análisis pueden exponer los computadores a virus.

1.5 Diagrama causa – efecto del problema

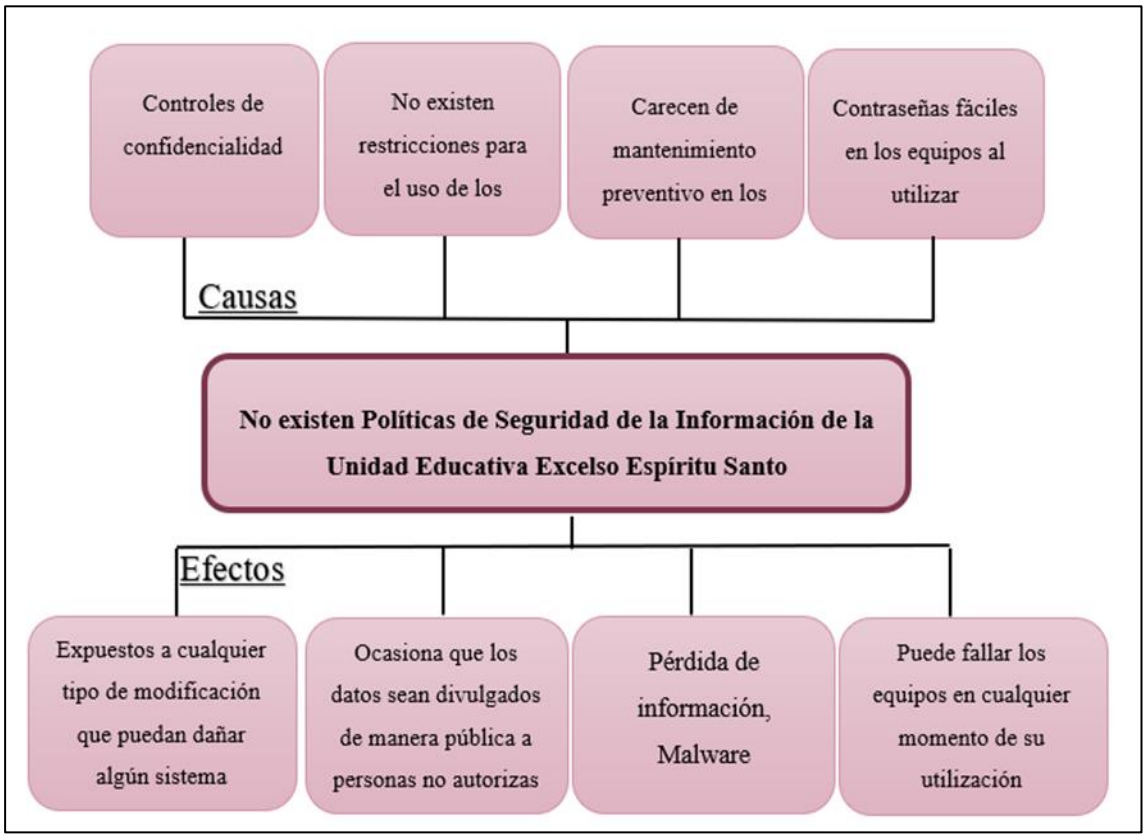


Ilustración 1 Diagrama de causa- efecto del problema

1.6 Objetivos

1.6.1 Objetivo general

Elaborar un SGSI para el área académico en la Unidad Educativa Excelso Espíritu Santo 2023-2024.

1.6.2 Objetivos específicos

- Definir tema de titulación por medio de averiguaciones sobre los problemas de información en el establecimiento.

- Fundamentar teóricamente mediante fuentes bibliográficas de diferentes autores que sea de utilidad sobre SGSI y área académica relacionado a los recursos tecnológicos.
- Diagnosticar el problema mediante la aplicación de encuestas y entrevista en la institución.
- Evaluar las vulnerabilidades de seguridad de los equipos informáticos aplicando la norma ISO 27001 en cada aula de clase de la institución.
- Elaborar un informe de auditoría que incluyan las políticas de informática para la Unidad Educativa Excelso Espíritu Santo agregando conclusiones, recomendaciones.

1.7 Justificación

En la actualidad, vivimos en un mundo donde la tecnología tiene un papel primordial. La información se ha convertido en una herramienta para empresas. Por esta razón, las organizaciones se enfocan en gestionar los datos. Existen amenazas que ponen en riesgo la integridad. Con el avance de la tecnología, los sistemas de seguridad están asumiendo un papel cada vez más relevante. Es fundamental que las empresas gestionen la información, garantizando que los datos estén siempre disponibles.

Es importante las políticas, porque son un instrumento para controlar cómo los docentes utilizan los equipos de la unidad educativa en el proceso de aprendizaje. En el transcurso de la investigación y en consulta con las autoridades. Se constató, a lo largo de los años, no ha implementado un proyecto de auditoría. Por esta razón, el presente trabajo será de gran utilidad. Por lo tanto, es crucial que la institución cuente con políticas de seguridad de información, que permitirá proteger la integridad y disponibilidad.

La UEEES tiene un compromiso al impartir conocimientos a toda su comunidad, abarcando el cuidado de los equipos en las aulas. El objetivo es la seguridad y prolongar la vida de los equipos. Al concluir, presentaré recomendaciones a las autoridades, para que sirvan de apoyo.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

Se busca enseñar a los docentes y alumnos sobre la tecnología que permite tener un título en línea desde cualquier parte del mundo, aprender idiomas. Además, prevenir los peligros asociados con el uso de las tecnologías.

1.8.2 Impacto social

Los alumnos que tienen habilidades en la gestión de riesgos preparados para compartir ese conocimiento. Esto es valioso en los entornos donde la seguridad tecnológica no es un tema importante. De este modo, los jóvenes contribuyen el bienestar de la comunidad, si no que generan un impacto positivo en el uso de las herramientas de la tecnología.

1.8.3 Impacto ecológico

Es fundamental educar a los usuarios con acceso a un equipo, el mantenimiento, tanto el aspecto tecnológico y la parte del computador. Las precauciones permiten un buen estado, prolongando su vida útil. Además, la protección del medio ambiente al reducir la necesidad de reemplazar o reparar equipos, lo que a su vez disminuye los desechos.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes históricos

2.1.1 Sistema de gestión de seguridad de la información (SGSI)

La norma ISO 27001, creada el 15 de octubre de 2005, fue inspeccionada el 25 de septiembre de 2013 y actualizada el 15 de febrero de 2022. Se caracteriza por su estructura de controles, para su correcta implementación. Es reconocida por su enfoque en la gestión de riesgos, lo que contribuye a mejorar la seguridad de la información. (Ruiz et al., 2018)

Con el tiempo, esta norma ha avanzado hasta convertirse en una certificación que cumple con todas sus condiciones. Además, ha sido de revisiones y actualizaciones para los riesgos en las empresas. (López A. , 2005)

La SI comenzó adquirir en la década de 1980, cuando se empezaron a utilizar sistemas informáticos para almacenar datos en los negocios. En esta época, no existían normas de proteger los archivos. En la actualidad, la seguridad de la información ha crecido, y se han desarrollado leyes que deben cumplirse para garantizar la protección de la información. (Romero al., 2018)

2.1.2 Área Académica

La gestión académica surge como respuesta a la necesidad de organizar las tareas. Está basada en la tecnología en su evolución y se enfoca en los alumnos. Su propósito es gestionar y regular las operaciones dentro de las entidades. (Cavassa, 2005)

El origen de la educación en la Antigua Grecia, donde Platón fundó la primera academia con el guía de estudio. Durante la Edad Media, en Europa, como las universidades de Bolonia y París se formalizaron la educación. En el siglo XIX, con la Revolución Industrial, se produjo una transformación en el ámbito educativo. (Morán al., 2017)

2.2 Antecedentes de investigaciones relacionadas al tema presentado

2.2.1 Propuesta de Sistema de Gestión de Seguridad de la Información utilizando la norma ISO 27001 par la Unidad Educativa Nuestra Señora de Fátima.

Este trabajo aborda diversas problemáticas relacionadas con la falta de seguridad informática en el uso de los computadores. Uno de los principales problemas es el riesgo de hurto de información y el mal uso, por parte de los niños. Dado que no cuentan con cámaras de vigilancia. La ausencia de un sistema informático robusto o de normas de seguridad de la información representa un peligro. Los riesgos incluyen ataques como malware, problemas técnicos, y robo de los equipos, lo cual puede afectar a la institución. La implementación de un SI permitirá proteger la integridad y disponibilidad. (Acurio, 2019)

2.2.2 Implementación de un SGSI basado en la norma ISO 27001 para la Unidad Educativa "El libertador"

En la entidad escolar se encuentran ataques con la seguridad en el inicio de sesión de las herramientas de Office 365. La falta de acceso de personal y los ataques de phishing, debido a su desconocimiento de la SI. Además, la ausencia de políticas ha facilitado el hurto de archivos, afectando en el proceso. La implementación del SGSI ha mejorado la protección. Este sistema ha garantizado la confidencialidad para adaptarse a la tecnología. Gracias a la implementación del sistema, se realiza una auditoría para los riesgos de la entidad. (Guachamin, 2023)

2.2.3 Sistema de Gestión de Seguridad de la Información en la Universidad Estatal Amazónica

Se evidenció que la entidad no cuenta con un SGSI. La ausencia de reglamentos que aseguren la protección de los datos de los CPU. Esta situación ha facilitado delitos, como la

manipulación de notas y finanzas incorrectas, la falta de confidencialidad e integridad en la gestión de la información. La implementación de SI, basado en políticas, contribuirá a que la información sea más confiable. Esto permitirá mitigar los riesgos internos como externos, fortaleciendo la conservación de los datos sensibles y evitando su pérdida. (Morales, 2023)

2.2.4 Elaboración de una Guía de implementación de un SGSI para la corporación ecuatoriana para el desarrollo de la investigación y la Academia-Cedia

Este estudio es la deficiencia en el conocimiento de los procesos tecnológicos. En la actualidad, carece de estrategias para protegerse de ataques, lo que pone en riesgo sus recursos. Además, no cuentan con procedimientos para la Gestión de la Información, lo que incluye la falta de bases sólidas en seguridad. Esto incrementa el riesgo de que la información sea manipulada. (Toledo, 2022)

2.2.5 Elaboración de un SGSI usando 27001:2013 en la Unidad Educativa Adventista Gedeón.

Este trabajo destaca que, debido al desconocimiento por el personal sobre el SGSI. La falta de controles de protección permitía que los datos estuvieran expuestos a cualquier persona, y en algunos casos, los datos eran manipulados. Por ello, surge la necesidad de implementar una guía que permita medir de manera eficaz la gestión de áreas. (Cuvi, 2019)

2.3 Sistema Gestión De La Seguridad De La Información (SGSI)

2.3.1 Definición de SGSI

El SGSI es un conjunto de controles para proteger sus ámbitos. Su implementación por parte del personal garantiza la confidencialidad, integridad y disponibilidad. (López R. A., 2017)

Es importante destacar que un conjunto de documentos tiene un valor al de la estructura, preservando su relevancia desde la fecha de su creación. (LISOT, 2018)

2.3.2 Importancia de SGSI

El SGSI en la actualidad se basa en su capacidad para salvaguardar las empresas. Se encuentra la evaluación de los controles, que se estructura en procesos, objetivos y fases, abarcando desde su implementación hasta la restauración del sistema. (Pérez, 2020)

2.3.3 Características del SGSI

Las características de custodia de los activos es la gestión eficaz de fallos de seguridad en los negocios y la realización de análisis de protección para impulsar una transformación en las mejoras. Es esencial que los líderes aseguren los recursos en el desarrollo. En las compañías, los objetivos. Esto implica definir competencias y la responsabilidad en la mejora de los recursos. (Paniagua, 2021)

2.3.4 Elementos de SGSI

- Política de seguridad de la información
- Planificación
- Implementación
- Evaluación y revisión
- Mejor continua
- Gestión de incidentes
- Documentación y registros
- Comunicación y concienciación
- Cumplimiento legal y contractual
- Supervisión y revisión de la dirección

2.3.5 Fases de SGSI

Según Arroyo Guardeño (2020) Las fases son las siguientes:

Planificar: En esta fase son los objetivos y se desarrolla el SGSI. Se identifican los riesgos en la seguridad, se definen las políticas y se asignen responsabilidades y se programan acciones.

Hacer: Se procede a la ejecución del sistema. Esto incluye la implementación de controles, la capacitación del personal sobre las medidas, y la documentación.

Comprobar: En esta fase se realiza un seguimiento de los procesos. Se recopila información y se llevan a cabo auditorías para verificar el cumplimiento.

Actuar: Basándose en los resultados de la fase, se toman medidas para corregir inconvenientes en las políticas. Esto asegura que el SGSI se mantenga actualizado y preparado.

2.3.6 Ventajas y Desventajas de SGSI

Ventajas es la protección de la información frente a amenazas. Internas y externas. Sin embargo, también presenta desventaja. Los costos de implementación pueden ser elevados. Además, es posible que no todos los empleados acepten las normas (Berrueta , 2022)

2.3.7 SGSI según ISO 27001

El SGSI basado en la norma, en el marco de una gestión integral, ayuda a la entidad a identificar los riesgos. Implementa medidas para proteger los activos, garantizando la confidencialidad, integridad y disponibilidad de la información. El SGSI controla los riesgos como en la tecnología utilizada en el negocio. A través de prácticas de seguridad, demuestra a su entorno con la protección de los recursos. (Tonysé de la Rosa, 2021)

2.3.8 Implementación de SGSI según la ISO 27001

2.3.8.1 Fases del proyecto

Las siguientes fases constituyen componentes del ciclo continuo de gestión de la seguridad de la información. (Briceño , 2021)

2.3.8.2 Documentación del SGSI

La documentación juega un papel crucial en la implementación efectiva y en la mejora de las prácticas de seguridad. (Herrero , 2022)

2.3.8.3 Política de seguridad

Las políticas de seguridad delinean las directrices a seguir y se formalizan en un documento que debe ser firmado por un encargado de la dirección. Esto manifiesta el compromiso en los negocios con la protección a la información. (Barría , 2020)

2.3.8.4 Identificar a los propietarios de los riesgos y tratamientos de los riesgos

Una vez obtenidos todos los valores de riesgos, se determina cómo tratar cada uno de ellos, ya sea eliminándolos. Esto requiere llegar a un acuerdo con el propietario para minimizar los riesgos. Además, es importante recordar que en los negocios existe un grupo de control encargado de reducir los riesgos mediante políticas. (Tejerina & Beltrán, 2020)

2.3.8.5 Determinar las medidas de seguridad

Se identifica los activos del SGSI y se evalúan los peligros externos a los que están expuestos. Los riesgos se reducen a niveles asumibles mediante la implementación de medidas de seguridad. Una vez establecidos los controles, se utiliza el anexo como referencia para asegurarse de no omitir ningún aspecto. (Martín & Fernández, 2020)

Algunos controles son obligatorios y están requeridos por las normas. Además, es crucial evaluar los costos asociados al funcionamiento y mantenimiento de estos controles. No existe un número fijo de controles, ya que se deben aplicar de manera gradual con el tiempo, a medida que se avanza en la mejora continua del sistema. (Menéndez , 2022)

2.3.8.6 Plan de tratamiento del riesgo

Se debe definir las tareas a realizar y los controles a establecer para cada actividad, asegurando que estén alineados con el plan. Es fundamental asignar responsabilidades y evaluar la eficacia de los controles. Para ello, se revisan los métodos que se ajusten a las necesidades de la empresa. Es recomendable comenzar con un número reducido de controles y, con el tiempo, ir expandiéndolos para mejorar el beneficio. (Postigo, 2020)

2.3.8.7 Información documentada sobre procesos

Según Hernández Bejarno (2020) Es crucial establecer normas que permitan la creación de documentos que describan las funciones del sistema. Estos documentos deben dividirse en políticas, procedimientos e instrucciones técnicas. Es posible que surjan dudas sobre los detalles y la información que debe incluirse en cada uno de estos documentos, por lo que es fundamental mantener un enfoque claro.

Se debe considerar los siguientes aspectos:

- **Políticas**
- **Normas**
- **Instrucciones**

2.3.8.8 Formación y concienciación

Todas las personas involucradas en el SGSI tienen que ser consciente de como desarrollan su trabajo aplicando las normas de seguridad por esto debemos realizar una formación general, sean capacitados en los aspectos específicos que ejercen los actos de concienciación, permiten hacer un seguimiento y una valoración de su eficacia. (Palacio, 2021)

2.3.8.9 Auditoría Interna

La auditoría interna es una herramienta para identificar deficiencias en el sistema y detectar riesgos. Su propósito es asegurar que la GSI cumpla con las normativas, mediante la revisión de las actividades de la empresa y a la evaluación del SGSI. (Cienfuegos et., 2021)

Durante la auditoría, recopilan tipos de evidencias para evaluar la efectividad de los controles. Estas pruebas deben documentarse en un informe, el cual la empresa debe revisar para tomar las acciones que sean necesarias. (Gómez, 2015)

2.3.8.10 Revisión por la dirección

El responsable de la SI debe garantizar la implementación y funcionamiento del Sistema de Gestión de Seguridad de la Información. Su labor es crucial y debe abarcar no solo un informe sobre las acciones realizadas hasta la fecha y la situación actual, sino también incluir los planes de mejora que se hayan establecidos. (Minaya et., 2023)

2.3.8.11 Evidencias

La evidencia debe estar en un formato y resguardada para evitar cualquier daño. Es recomendable la correcta conservación, facilitando su revisión y garantizando su integridad durante el tiempo de custodia, ya que existe el riesgo de perder datos. (Heredero et., 2019)

2.4 Recursos Tecnológicos

2.4.1 Definición de Recursos tecnológicos educativos

Son un factor importante para mantenerse al día con los acontecimientos, lo que puede influir en el éxito de cualquier proyecto. Los recursos tecnológicos desempeñan funciones en diversas áreas. (López E. , 2020)

Además, un recurso tecnológico es fundamental para el avance de los sistemas existentes. En el contexto, tanto el personal técnico como los usuarios de los sistemas informáticos participan en los procesos. Estos recursos pueden ser tanto tangibles como intangibles y son el medio para lograr los objetivos planteados. (Quintas, 2020)

2.4.2 Importancia de los recursos tecnológicos en el proceso educativo

La educación en entornos de aprendizaje con recursos que busca desarrollar habilidades mediante el uso de medios. Mejorando la calidad de vida de las personas, en la educación para que los profesores transmitan conocimientos de manera más eficaz. Los recursos tecnológicos refuerzan el aprendizaje, lo que exige que estén preparados para diseñar unidades que incorporen estas herramientas. En este contexto, las unidades gestionen la integridad de recursos. (Vázquez, 2021)

2.4.3 Tipos de recursos tecnológicos

Según Allueva y Alejandre (2020) en la actualidad, les permiten desarrollar su intelecto. Estos recursos, que incluyen herramientas prácticas de diversas tecnologías, pueden ser clasificados de manera precisa como tangibles o intangibles, dependiendo si pueden ser manipulados o son abstractos y no se puede cuantificar.

Estos recursos se dividen en dos tipos:

- **Recursos tecnológicos tangibles:** Son los elementos físicos que realizan tareas, como CPU.
- **Recursos tecnológicos intangibles**: Se refieren a los elementos no físicos, como el software.

2.4.4 Características de las tecnologías para el aprendizaje y el conocimiento

El rendimiento en el ámbito dinámico se refiere al proceso de aprendizaje con la capacidad y el esfuerzo que el alumno demuestra. En su aspecto estático, el rendimiento se manifiesta como el resultado del aprendizaje, evidenciando a través de una buena disciplina y comprobando en diversas evaluaciones y trabajos. Además, el rendimiento está vinculado con factores y expectativas, siendo que se ajuste al modelo social vigente. (Salazar et., 2019)

2.4.5 Funciones de recursos tecnológicos en la educación

Los recursos tecnológicos desempeñan un papel importante en lo escolar, ya que mejoran el aprendizaje al hacerlo más accesible. Su función principal es facilitar el acceso a una amplia gama de archivos y recursos. Además, los recursos tecnológicos permiten un aprendizaje, adaptándose a las necesidades individuales de los alumnos mediante actividades. Esto prepara a los estudiantes para el mundo laboral con el uso de innovación. (Murcia, 2020)

2.4.6 Beneficios de la tecnología en la educación

La integración de la tecnología en los salones va más allá del uso de computadoras y software, implica la participación activa de los alumnos, la relación entre maestros y estudiantes. Incorporar estos instrumentos en la educación ofrece numerosos beneficios, aumentando la eficiencia y la productividad. (Hinojo et., 2019)

Los recursos tecnológicos facilitan el aprendizaje de diferentes idiomas mediante herramientas digitales, permitiendo acceder a cursos y materiales de instituciones que, de otro modo no contarían con docentes en estos idiomas. Gracias a la tecnología, como los cursos en línea y los programas gratuitos, los estudiantes pueden mejorar sus habilidades lingüísticas. (González, 2019)

La tecnología también ofrece la oportunidad de acceder a una educación en línea para aquellos que no pueden asistir debido a compromisos laborales u otras circunstancias. Esta modalidad de aprendizaje contribuye al progreso educativo, garantizando que todos tengamos la posibilidad de prepáranos. (Quitian, 2019)

2.4.7 El uso de los recursos tecnológicos en el proceso de enseñanza educativa

La incorporación de nuevas tecnologías ofrece a los docentes enriquecer su práctica educativa. Estas herramientas permiten un enfoque, creativo en el aprendizaje, facilitando una metodología innovadora apoyada por ordenadores. Esta transformación promueve un modelo de enseñanza abierto que fomenta la interacción. (Fernández, 2019)

Brinda a los docentes la posibilidad de conectarse con los estudiantes a través de plataformas en línea y herramientas educativas. Esto facilita la realización de tareas, la obtención de información y el apoyo en la preparación de los estudiantes. (Reynoso et., 2020)

Además, la tecnología juega un papel crucial en la solución de problemas educativos. Por ejemplo, permite la continuidad del aprendizaje, como enfermedades, evitando retrasos en el plan de estudios y mitigando el impacto de fenómenos ambientales, como el fenómeno del Niño. Por tanto, la evolución tecnológica en el ámbito educativo resulta esencial para enfrentar estos desafíos. (Móran et., 2021)

2.4.8 Ventajas del uso de los recursos tecnológicos

La tecnología ha permitido que los seres humanos accedan a la educación a través de medios, generando así formas de conocimiento. Uno de los grandes avances que la tecnología ha traído son las aulas virtuales, las cuales facilitan el aprendizaje y la enseñanza al permitir el intercambio de conocimientos entre alumnos y docentes. (Batanero, 2019)

Gracias a los recursos tecnológicos, tanto docentes como estudiantes cuentan con herramientas que facilitan la investigación sobre los temas tratados en clase, utilizan plataformas en línea para compartir información y los alumnos pueden gestionar sus trabajos, monitorear su rendimiento académico. (Heredia et., 2020)

2.4.9 Desventajas del uso de los recursos tecnológicos

Una de las principales desventajas es la falta de equipos, acceso a internet o la carencia de conocimientos necesarios para utilizar los recursos tecnológicos. El exceso de información puede convertirse en un problema, ya que puede generar distracción y confusión si no se tiene una guía clara o si se presentan definiciones contradictorias, dificultando la identificación de información verdadera o falsa. (Silva, 2021)

Además, el uso inadecuado de los recursos tecnológicos por parte de estudiantes y docentes puede dar lugar a problemas como el aislamiento social durante los recreos y el acoso escolar (bullying). También existen riesgos asociados con el uso incorrecto de las redes sociales. (Catagua & Cevallos, 2019)

2.4.10 Hardware y dispositivos tecnológicos en el ámbito académico

Según Bohórquez Gómez y García González (2022) los dispositivos de hardware desempeñan un papel crucial en la enseñanza y el aprendizaje dentro de las instituciones educativas. Es fundamental que estos dispositivos se utilicen de manera adecuada y con fines académicos. A continuación, se presentan algunos de los dispositivos tecnológicos relevantes en el ámbito académico:

- Computadoras de escritorio
- Computadoras portátiles
- Tabletas
- Pizarras interactivas
- Proyectores
- Impresoras

2.4.11 Los recursos tecnológicos y los docentes

Los recursos tecnológicos ofrecen numerosos beneficios en el ámbito educativo, facilitando el aprendizaje de los estudiantes. Estos recursos proporcionan una amplia variedad de materiales, como textos, videos y contenido audiovisual, que permiten a los alumnos comprender y asimilar las asignaturas de manera atractiva, divertida y práctica, lo que contribuye a mejorar sus resultados académicos. (Fabre et., 2021)

Los docentes también se benefician del uso de recursos tecnológicos en sus prácticas educativas. Utilizan herramientas digitales para compartir tareas, proporcionar videos explicativos, difundir información sobre la clase, notas de evaluaciones y comunicados institucionales. Durante la pandemia, muchos profesores tuvieron que adaptarse a la educación en línea y utilizar computadoras, enfrentando dificultades debido al desconocimiento del uso de estos dispositivos. (Unesco, 2019)

Los recursos tecnológicos enriquecen la enseñanza en diversas materias. Los profesores emplean aplicaciones y software de manera visual y práctica, facilitando una mejor comprensión de las clases por parte de los estudiantes. Es fundamental que los docentes cuenten con dispositivos actualizados y programas de seguridad para prevenir la infección por virus. (Ortega, 2019)

2.5 Metodología de desarrollo.

Fases de la Norma ISO 27001

Ilustración 2 Fases Norma ISO 27001

2.6 Conclusiones del marco teórico

- La revisión de la literatura indica que el SGSI son primordiales para las empresas. Estas políticas son para proteger los datos, resguardar los activos contra amenazas y permitir la evaluación de riesgos.

- Se ha comprobado que la implementación de estas normativas es esencial para garantizar el funcionamiento de los equipos. En lo académico, esto es aún mayor, ya que el uso seguro de estas CPU por parte de maestros y alumnos para el buen desarrollo del entorno.

CAPÍTULO III

3. MARCO INVESTIGATIVO

3.1 Introducción

En este capítulo se presenta una evaluación informática basada en tres tipos de información: cualitativa, cuantitativa y descriptiva. A través de la investigación, se definieron los estudios pertinentes y se emplearon métodos de análisis inductivo, deductivo, analítico y sintético para determinar la existencia de políticas de SI en las aulas que albergan equipos.

Se utilizaron herramientas para recopilar datos, incluyendo encuestas dirigidas a los docentes de la UEEES, quienes fueron el foco principal de la auditoría. Ellos proporcionaron información para el análisis. Además, se realizó una entrevista al vicerrector encargado de las aulas con equipos. Finalmente, se presentó el informe de análisis, obtenido mediante la tabulación de las encuestas, lo cual permitió diagnosticar el problema.

3.2 Tipos de investigación

3.2.1 Investigación cualitativa

La investigación cualitativa implica la recopilación y el análisis de datos no numéricos para comprender conceptos y comportamientos, así como las personas asignan a estos elementos. Este enfoque puede ser útil para investigar cómo ocurrieron ciertos incidentes y para detallar las acciones a tomar en tales situaciones. (Santander Becas, 2021)

Se empleó para desarrollar del marco teórico y para comprender los conceptos relacionados. Además, se realizó una entrevista al vicerrector de la unidad, para recopilar datos y analizar sobre la problemática de la inexistencia de políticas en la entidad donde se encuentran las CPU.

3.2.2 Investigación cuantitativa

Se trata de un método que se encuentra en diversos ámbitos cuyo propósito es obtener datos. Se centra en reunir y analizar datos conceptuales. (Alan Neill & Cortez Suárez, 2018)

En este trabajo, se utilizó la investigación para realizar cuestionarios a los 32 maestros de la unidad. El objetivo fue obtener datos sobre la problemática, tabular y generar gráficos que reflejen el porcentaje de las respuestas, así como la interpretación de los hallazgos.

3.2.3 Investigación descriptiva

Se utiliza para examinar componentes, permitiendo un análisis. Este enfoque facilita la identificación de las características del fenómeno, mostrando modelos de comportamiento. Con base en los objetivos, el analista determina el tipo de descripción. (Guevara Alban et., 2020)

En este caso, se empleó para identificar las características de la unidad. Este método resultó para examinar la problemática. Se llevó a cabo la recolección de datos mediante instrumentos, lo cual facilitó la interpretación de los resultados en el desarrollo del SGSI.

3.3 Métodos de investigación

3.3.1 Método inductivo

Es un enfoque científico que permite llegar a conclusiones a partir de observaciones y suposiciones. Este método se basa en la recolección y análisis de datos y eventos concretos para formular teorías. En otras palabras, el proceso va de lo específico a lo general. (Cabrerizo, 2019)

En el contexto del análisis del problema en la unidad, el método resultó ser una herramienta clave. Gracias a este enfoque, fue posible identificar variables cruciales y

mediante razonamiento inductivo, el problema principal en la unidad radica en la ausencia de políticas de SI en las aulas de clase donde se encuentran las CPU.

3.3.2 Método deductivo

La reflexión lógica, caracterizada por el hecho de que el resultado se deriva de varios métodos, permite obtener conclusiones a partir de la resolución válida de documentos basados en uno o más permisos de tipo general. (Segundo, 2018)

En este trabajo, se empleó el método deductivo para analizar los datos obtenidos de encuestas y entrevistas. Los resultados con el fin de extraer conclusiones y avanzar.

3.3.3 Método analítico

Es un método de investigación que radica en clasificar el todo, desintegrando en partes a factores, sus causas y efectos. El análisis es el examen de un hecho particular. Para comprender su naturaleza es necesario el fenómeno y el elemento. Este método nos da la oportunidad de conocer más sobre el objeto de estudio, que a su vez puede exponer la analogía comprendida. (Ruiz, 2006)

En el método analítico se clasificó la metodología norma ISO 27001 analizando paso a paso de sus fases donde se aplicó la evaluación de la seguridad de los equipos informáticos de la Unidad Educativa Excelso Espíritu Santo.

3.3.4 Método sintético

Es un proceso busca restaurar información utilizando diversos bloques de construcción derivados del progreso. Este enfoque permite a las personas resumir y consolidar sus conocimientos, funcionando como un proceso mental que almacena información en la memoria. Este procedimiento demuestra la capacidad del ser humano para reconocer lo conocido y extraer los elementos. (Piña & Novoa, 2014)

En el método sintético, se seleccionaron investigaciones relevantes del marco teórico para redactar de manera más inclusiva y concreta, con el fin de obtener variables precisas para el estudio.

3.4 Fuentes de información de datos

3.4.1 Fuente primaria

Las fuentes primarias ofrecen información clara y de primera mano, facilitando su interpretación. En este contexto, las empresas serán la fuente de estos datos, los cuales se obtendrán mediante entrevistas para recopilar datos. Se obtendrán a través de entrevistas para recopilar detalles.

En particular, se realizó una entrevista con el encargado de la entidad para determinar la existencia de políticas de SI para obtener detalles sobre las medidas de protección implementadas en las CPU en los salones.

3.4.2 Fuente secundaria

Las fuentes secundarias se emplean para obtener datos recopilados por otras personas. Estas fuentes pueden incluir encuestas y detalles de fuentes de libros, ofreciendo así una visión general del tema en cuestión.

En este caso, se realizó una encuesta a los 32 maestros con el objetivo de evaluar su conocimiento sobre la existencia de políticas de seguridad de la información en la unidad, así como su familiaridad con las CPU que utilizan en sus aulas.

3.4.3 Entrevista

Las entrevistas se realizaron con el objetivo de recopilar datos a través de un proceso que abarca varios aspectos de la comunicación. Su propósito principal es conocer el comportamiento y las opiniones de los entrevistados, permitiendo así la recolección de datos. (Grados & Sánchez, 2017))

En este caso, se implementó una entrevista con el vicerrector, responsable de las aulas de clase donde se encuentran los equipos. El propósito fue obtener datos que permitiera evaluar si se están cumpliendo las políticas de SI.

3.4.4 Encuestas

La encuesta es una técnica que permite recolectar datos a través de la aplicación de un cuestionario a una persona. Este método facilita la obtención de datos sobre actitudes y comportamientos relacionados con uno o varios temas, siguiendo un enfoque científico para asegurar que las respuestas representen a la población de interés. (Pobea, 2015)

En este caso, la encuesta se aplicó a los 32 docentes de la UEEES con el propósito de evaluar si la unidad cuenta con políticas de SI.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

Una población se refiere a un conjunto de elementos con atributos que son objeto de estudio. Dependiendo de la exploración, la población puede ser accesible y limitada en tamaño, o amplia, lo que dificulta el acceso del investigador a todos sus integrantes. (Ventura León, 2017)

En este caso, la población está conformada por 32 maestros de la UEEES, donde se implementaron los instrumentos.

3.5.2 Muestra

Es una parte de la población con la que se lleva a cabo en la investigación, existe un número de componentes de mostrarios, lo que muestra son un número de representantes de la población a la cual se le puede dar a conocer el objetivo. (Lopez, 2004)

No se aplicó un muestreo debido a que la población de la UEEES no se prestaba para ello. En lugar de realizar un muestreo, se seleccionó a los maestros y al vicerrector como sujetos para el desarrollo de las encuestas y entrevistas, con el fin de obtener información.

El vicerrector de la entidad se le realizo una entrevista, mientras que a los docentes se les aplicaron encuestas para recopilar los datos.

3.5.3 Análisis de las herramientas de recolección de datos a utilizar

3.5.3.1 Cuestionario

Encuesta Dirigida a: Docentes de la institución

Objetivo: Determinar el conocimiento sobre las políticas de seguridad de la información en el manejo de los equipos informáticos del aula de clase.

Nombre de la empresa: Unidad Educativa Excelso Espíritu Santo.

1. **¿Conoce usted en que consiste la seguridad de la información?**

   Si ( ) No ( )

2. **¿Conoce usted sobre las políticas de seguridad de la información?**

   Si ( ) No ( )

3. **¿Conoce usted si la institución cuenta con políticas de seguridad de la información?**

   Si ( ) No ( )

4. **¿La institución ha socializado con usted las políticas de seguridad de la información?**

   Si ( ) No ( )

5. **¿En el aula de clase existe restricciones para el uso de los equipos?**

   Si ( ) No ( )

6. **¿Ha recibido alguna capacitación sobre las mejores prácticas para el uso seguro de equipos en el entorno educativo?**

   Si ( ) No ( )

7. **¿Está al tanto de los controles de confidencialidad implementados en los equipos informáticos que utiliza en clase?**

   Si ( ) No ( )

8. **¿Se realiza mantenimiento en el equipo informático que utiliza en el aula de clase?**

   Si ( ) No ( )

9. **¿Utiliza contraseña para acceder a su equipo informático del aula de clase?**

   Si ( ) No ( )

10. **¿Existen en el aula un lugar visible de las instrucciones de cómo utilizar los equipos informáticos si sucede algún tipo de problema?**

    Si ( ) No ( )

Ilustración 3 Encuestas de los docentes

3.5.3.2 Guía de entrevista

Entrevista dirigida a: Vicerrector encargado del área académica de los equipos informáticos

Objetivo: Determinar el conocimiento sobre las políticas de seguridad de la información en el manejo de los equipos informáticos del aula de clase.

Nombre de la Empresa: Unidad Educativa Excelso Espíritu Santo

1. **La institución cuenta con políticas de seguridad de la información**
2. **La institución ha socializado con sus docentes las políticas de seguridad de la información.**
3. **¿Por qué medios ha realizado la socialización?**
4. **¿Cuál es su opinión sobre si la implementación de políticas de seguridad de la información sería beneficioso para el entorno educativo?**
5. **¿Podría compartir si existen restricciones específicas para el uso de equipos informáticos en las aulas de clase de la institución?**
6. **¿Qué capacitaciones se han desarrollado sobre los controles de confidencialidad de los equipos informáticos del aula de clase?**
7. **La institución cuenta con un Sistema de Gestión de Seguridad de la información (SGSI).**
8. **¿En relación con los equipos informáticos en las aulas, ¿se realiza algún tipo de mantenimiento regular para garantizar su funcionamiento y seguridad?**
9. **¿Se proporciona información regular a los profesores sobre la importancia de utilizar contraseñas seguras en los equipos informáticos del aula de clase?**
10. **¿Los docentes han reportado algún incidente de seguridad con los equipos informáticos?**

Ilustración 4 Entrevista al encargado

3.5.3.3 Estructura de los instrumentos de recolección de datos aplicados

La encuesta se compone de 10 preguntas, cada una con dos opciones de respuesta. Una de las preguntas clave es la número 3, que indaga si la institución cuenta con un SSI. Además, se incluyen preguntas para evaluar el conocimiento sobre el SGSI.

Se llevó a cabo una entrevista, también compuesta por 10 preguntas, con el objetivo de recopilar datos sobre la implementación de políticas de SI en la institución. Estas preguntas fueron dirigidas al vicerrector de la Unidad Educativa Excelso Espíritu Santo, considerando la relevancia de la información que se necesita obtener.

3.5.4 Plan de recolección de datos

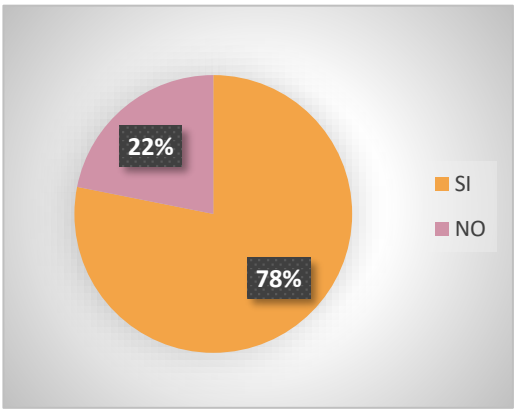
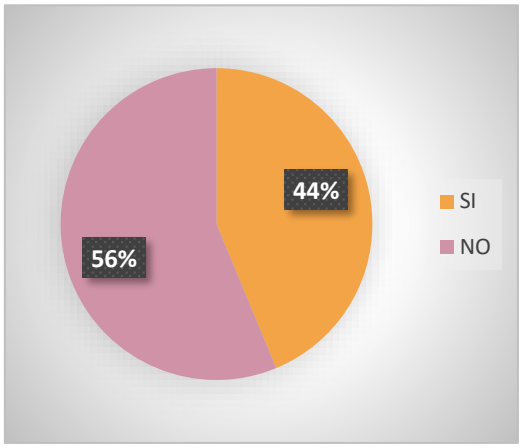
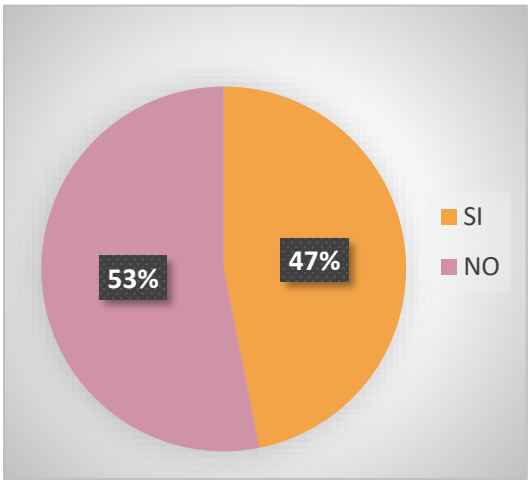
Día	**Hora**	**Personal**	**Tipo de instrumento**
02/01/2024	09:00	Profesores de la Unidad Educativa Excelso Espíritu Santo	Encuesta
03/01/2023	10:00	Docentes de la Unidad Educativa Excelso Espíritu Santo	Encuesta
08/01/2023	2:30	Vicerrector de la Unidad Educativa Excelso Espíritu Santo	Entrevista

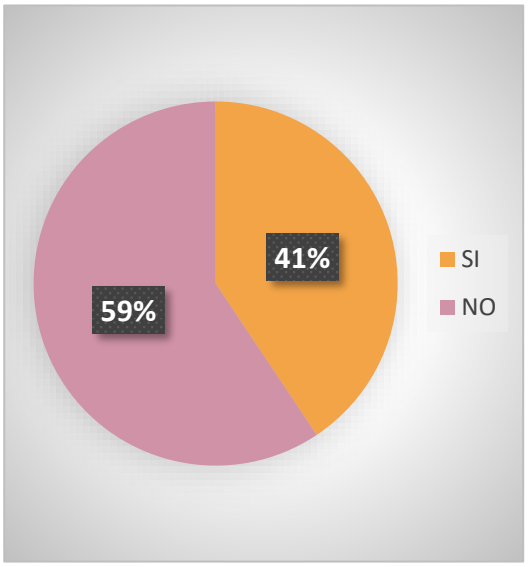
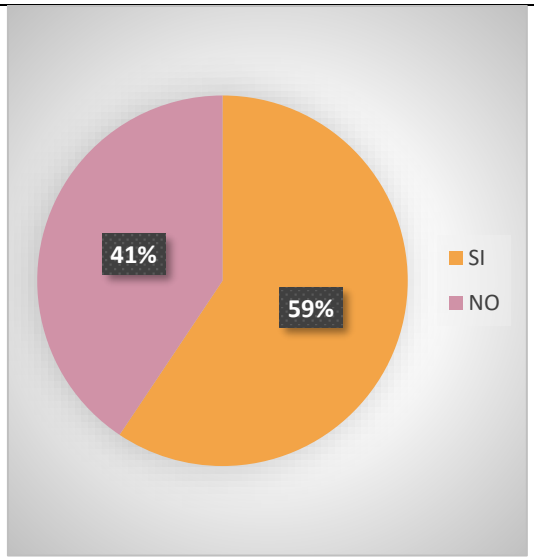
Tabla 1 Plan de recolección de datos

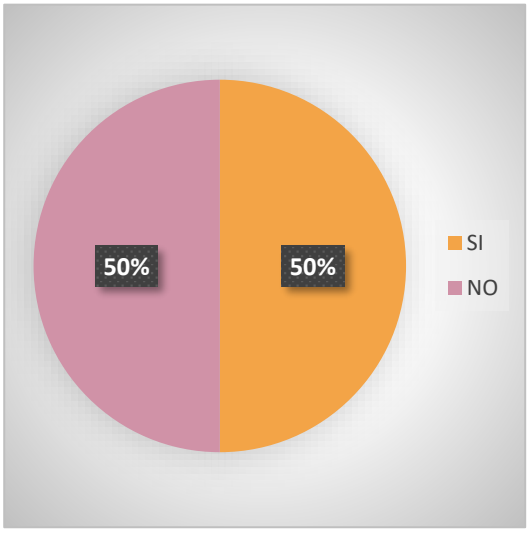
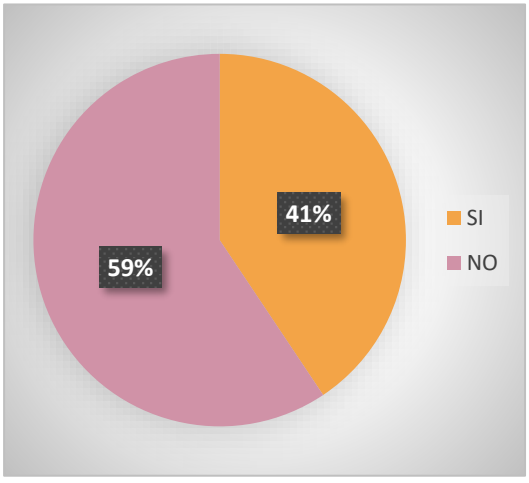
3.6 Análisis y presentación de resultados

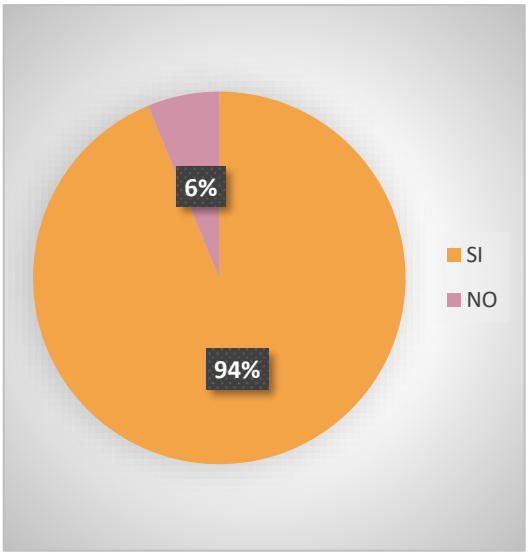
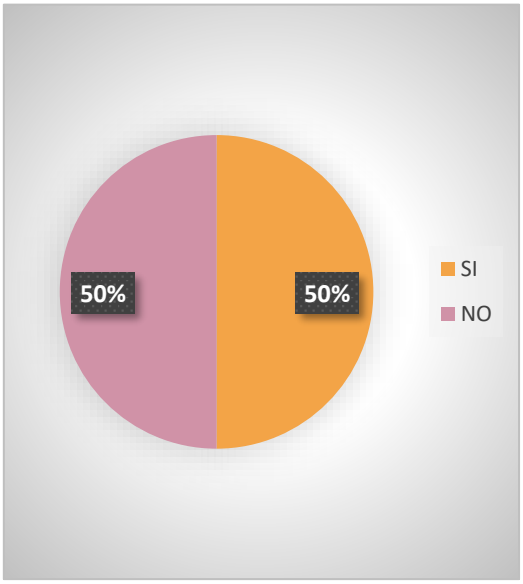
3.6.1 Tabulación y análisis de los datos

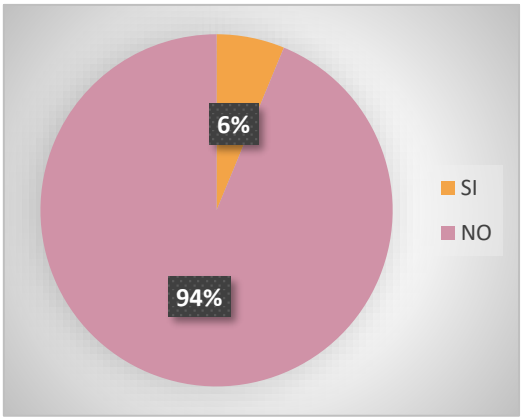
3.6.1.1 Encuesta aplicada a los docentes de la institución Excelso Espíritu Santo

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
1. ¿Conoce usted en que consiste la seguridad de la información?		De la muestra encuestada la gran mayoría conoce sobre la seguridad de la información
2. ¿Conoce usted sobre las políticas de seguridad de la información?		Más de la mitad de los encuestados desconoce sobre las políticas de seguridad de la información
3. **¿Conoce usted si la institución cuenta con políticas de seguridad de la información?**		Un poco más de la mitad de los docentes afirma que la institución no cuenta con políticas de seguridad de la información.

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
4. ¿La institución ha socializado con usted las políticas de seguridad de la información?		Más de la mitad de los docentes confirma que no les han socializado las políticas de seguridad de la información
5. ¿En el aula de clase existe restricciones para el uso de los equipos?		Más de la mitad de los docentes confirma que si existe restricciones para el uso de los equipos

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
6. ¿Ha recibido alguna capacitación sobre las mejores prácticas para el uso seguro de los equipos en el entorno educativo?		La mitad de los docentes han recibido capacitación sobre las mejores prácticas para el uso seguro de los equipos en el entorno educativo mientras la otra mitad no
7. ¿Está al tanto de los controles de confidencialidad implementados en los equipos informáticos que utiliza en clase?		Más de la mitad de los encuestados no conoce de los controles de confidencialidad implementados en los equipos informáticos que utiliza en clase

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
8. ¿Se realiza mantenimiento en los equipos informáticos que utiliza en el aula de clase?		Casi la totalidad de los docentes confirma que cuentan con mantenimiento en los equipos informáticos que utiliza en el aula de clase
9. ¿Utiliza contraseñas para acceder a su equipo informático del aula de clase?		La mitad de los docentes utilizan contraseñas para acceder al equipo informático del aula de clase mientras la otra mitad no lo hace

PREGUNTAS	RESPUESTAS	INTERPRETACIÓN
10. ¿Existen en el aula de clase un lugar visible de las instrucciones de cómo utilizar los equipos informáticos si sucede algún tipo de problema?		Más de la mitad de los docentes confirman que en las aulas de clase no tienen instrucciones de cómo utilizar los equipos informáticos si sucede algún tipo de problema

3.6.1.2 Entrevista aplicada al Vicerrector de la Unidad Educativa Excelso Espíritu Santo

PREGUNTAS	RESPUESTAS	CONCLUSIÓN
1. La institución cuenta con políticas de seguridad de la información	No	La institución no cuenta con políticas de seguridad de la información
2. La institución ha socializado con sus docentes las políticas de seguridad de la información	No	La Unidad Educativa no ha socializado con sus docentes porque no hay políticas de seguridad de la información
3. ¿Por qué medios ha realizado la socialización?	No ha realizado	Por ningún medio han realizado la socialización

	PREGUNTAS	RESPUESTAS	CONCLUSIÓN
4.	**¿Cuál es su opinión sobre si la implementación de políticas de seguridad de la información sería beneficioso para el entorno educativo?**	Es necesario para poder llevar una educación con estándar nacional e internacional (ISO)	El Vicerrector de la institución su opinión sobre la implementación de políticas
5.	**¿Podría compartir si existen restricciones específicas para el uso de los equipos informáticos en las aulas de clase de la institución?**	Si hay proceso de restricciones.	La institución cuenta con restricciones para el uso de los equipos informáticos
6.	**¿Qué capacitaciones se han desarrollado sobre los controles de confidencialidad de los equipos informáticos del aula de clase?**	Ninguna	La institución no ha realizado capacitaciones sobre los controles de confidencialidad de los equipos informáticos del aula de clase
7.	**La institución cuenta con un Sistema de Gestión de Seguridad de la información (SGSI)**	Sí, Plataforma de sistemas como Google classroom	La institución cuenta con un sistema de gestión de seguridad de la información

PREGUNTAS	RESPUESTAS	CONCLUSIÓN
8. ¿En relación con los equipos informáticos en las aulas, ¿se realiza algún tipo de mantenimiento regular para garantizar su funcionamiento y seguridad?	Sí, el proveedor de los equipos informáticos ofrece el servicio de mantenimiento preventivo	La institución cuenta con un proveedor que les ofrece a los equipos informáticos el servicio de mantenimiento preventivo
9. ¿Se proporciona información regular a los profesores sobre la importancia de utilizar contraseñas seguras en los equipos informáticos del aula de clase?	No	La institución no proporciona información regular a los profesores sobre la importancia de utilizar contraseñas seguras en los equipos informáticos del aula de clase
10. ¿Los docentes han reportado algún incidente de seguridad con los equipos informáticos?	Ninguno	Los docentes de la institución no han reportado incidentes de seguridad con los equipos informáticos

3.6.2 Presentación y descripción de los resultados obtenidos

El análisis de los resultados de la encuesta aplicada a los profesores de la institución reveló que no existen políticas de seguridad de la información, según lo indicado en la pregunta 3. Más de la mitad de los docentes afirmaron que la institución carece de dichas

políticas. De manera similar, en la pregunta 1 de la entrevista realizada al vicerrector, responsable de las aulas donde se encuentran los equipos informáticos, se confirmó la ausencia de políticas de seguridad.

En la pregunta 4 de la encuesta, más de la mitad de los maestros indicó que no se les ha informado sobre las políticas de seguridad. Las preguntas 2 y 3 de la entrevista reflejaron que la institución no se ha socializado estas políticas con sus docentes, ya que no existen, y no se ha llevado a cabo ninguna socialización por otros medios.

En la pregunta 5 de la encuesta, más de la mitad de los docentes confirmó que existen restricciones para el uso de los equipos. Esto coincide con la respuesta a la pregunta 5 de la entrevista, donde se aseguró que sí se aplican procesos específicos de restricción para el uso de los equipos informáticos en las aulas.

En la pregunta 7 de la encuesta, más de la mitad de los encuestados manifestó desconocer los controles de confidencialidad implementados en los equipos informáticos que utilizan en clase. Esto se refuerza con la respuesta a la pregunta 6 de la entrevista, que indicó que no se han realizado capacitaciones sobre los controles de confidencialidad en el uso de los equipos.

En la pregunta 9 de la encuesta, la mitad de los docentes señaló que utilizan contraseñas para acceder a los equipos en el aula, mientras que la otra mitad no lo hace. En la pregunta 9 de la entrevista, se evidenció que la institución no ha proporcionado información regular a los maestros sobre la importancia de utilizar contraseñas seguras.

Finalmente, en la pregunta 10 de la encuesta, más de la mitad de los profesores confirmaron que no cuentan con instrucciones sobre cómo utilizar los equipos informáticos en caso de algún problema. En la pregunta 10 de la entrevista, se corroboró que los docentes de la institución no han reportado incidentes de seguridad relacionados con los equipos.

3.6.3 Informe final del análisis de los datos

Con base en los resultados obtenidos en la pregunta 3 de la encuesta realizada a los maestros, se concluye que la UEEES no cuenta con políticas de seguridad de la información. Esta conclusión se ve reforzada por la entrevista realizada al responsable de la institución, quien también confirmó la ausencia de dichas políticas.

La implementación de políticas de SI es esencial en los centros educativos, ya que estas normativas son cruciales para proteger los datos sensibles. Contar con políticas de seguridad en la unidad para salvaguardar la integridad, confidencialidad y disponibilidad procesada en las CPU utilizados en los salones.

Además, establecer políticas de SI no solo cumple con los requisitos, sino que también contribuye a la creación de un entorno de aprendizaje más seguro.

CAPÍTULO IV

4. MARCO PROPOSITIVO

4.1 Introducción

Este capítulo presenta el desarrollo de la auditoría de seguridad informática realizada en los equipos de cada aula de la unidad educativa. La auditoría se enfocó en evaluar las vulnerabilidades, aplicando la norma ISO 27001. Se detalla la identificación de los recursos humanos, tecnológicos y económicos empleados en el trabajo de titulación, y se expone el desarrollo de lo planteado según la metodología establecida.

4.2 Descripción de la propuesta

El presente trabajo corresponde a una auditoría de seguridad informática realizado a los equipos de cómputo utilizado para el desarrollo de actividades académicas en la Unidad Educativa Excelso Espíritu Santo utilizando la ISO 27001 y su metodología PHVA, la norma ISO 27001 es una de la norma elaborada por ISO (Organización Internacional de Normalización) que ayudó administrar la seguridad de la información en la institución y llevar a cabo el análisis de forma individual a los equipos informáticos en cada aula, para obtener un ambiente informático más protegido, cumpliendo con los parámetros definidos por la norma.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recursos	Función	Actividad
1	Ing. Roberto Campos	Director de la institución	Participó en la autorización donde se pudo realizar el trabajo de titulación
1	Lcdo. Enver Faican	Responsable de los equipos de las aulas	Participó de la entrevista como líder del área informática
1	Katty Fuertes	Investigadora	Como investigadora se consultó las bases teóricas que sustentan el proyecto de titulación.

32	Docentes de la institución	Maestros del establecimiento auditada	Fueron población participe de la encuesta para la obtención de datos.

Tabla 2 Recursos Humanos

4.3.2 Tecnológicos

Cantidad	Recurso	Actividad
1	Portátil lenovo core i7 12 GB de RAM	Equipo informático utilizado para el desarrollo de la investigación.
1	Teléfono móvil Redmi Note 12 pro 5g con cámara fotográfica	Móvil usado para la toma de evidencias durante la realizar la investigación.
8 meses	Conexión de internet	Usado para investigar sobre el tema del proyecto de titulación
1	Impresora HP	Equipo para las hojas de la encuesta, entrevista y tesis.
1	Programa Microsoft Excel	Usado para la tabulación de datos de las encuestas y entrevista.

Tabla 3Recursos Tecnológicos

4.3.3 Económicos

Cantidad	Descripción	Precio	Subtotal
1	Portátil lenovo core i7 12 GB de RAM	$800	$800
1	Teléfono móvil Redmi Note 12 pro 5g	$350	$350
400	Impresiones	$0.15	$60
8 meses	Conexión a internet	$25	$200
60	Transporte	$0.40	$24
		Total	1.434

Tabla 4 Recursos Económicos

4.4 Desarrollo (Según metodología seleccionada)

Según Atehortúa (2008) La Norma ISO 27001 se centra en la identificación de riesgos, la implementación de controles de seguridad, la gestión de incidentes y la mejora continua, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. Al adoptar la norma ISO 27001, las instituciones pueden demostrar su compromiso con la seguridad de la información y aumentar la confianza en sus procesos.

Las fases de la Norma ISO 27001 son:

Planificar: En esta fase se implementa el Sistema de Gestión de Seguridad de la Información (SGSI). Se definen los objetivos, normativas y políticas relacionadas con la seguridad de la información.

Hacer: En esta fase se ejecutan las normativas establecidas en la fase de planificación. Se incorporan los controles y procedimientos necesarios para gestionar la información de manera segura y eficiente.

Verificar: Esta fase consiste en evaluar y verificar la eficacia del SGSI implementado. Se revisa si se cumple con la política de seguridad y se realizan auditorías para asegurar que el sistema funciona adecuadamente.

Actuar: En la fase final, se llevan a cabo actividades y planes correctivos y preventivos para mejorar el sistema, basándose en los resultados obtenidos en la fase de verificación.

4.4.1 Fase 1 Planificar

4.4.1.1 Programa de Auditoría

Programa de auditoría informática de seguridad de la información de la Unidad Educativa Excelso Espíritu Santo		
Objetivo • Evaluar el nivel de madurez de gestión de seguridad de la información de la Unidad Educativa Excelso Espíritu Santo según ISO 27001. • Identificar los riesgos de seguridad de la información de la Unidad Educativa Excelso Espíritu Santo y determinar la gravedad de los mismos.		
Técnicas y Procedimientos	**Ref. a Papel**	**Fecha**
1.1 Revisar la norma ISO 27001	4.4.1.2	07/01/2024
1.2 Realizar una auditoría inicial (fase 1 ISO 27001)	4.4.1.3	08/01/2024
1.3 Análisis del Contexto (fase 2 ISO 27001)	4.4.2	09/02/2024
2.1 Elaborar cuestionarios para analizar riesgos	4.4.3	02/05/2024
2.2 Aplicación de análisis de riesgos	4.4.3.2	07/05/2024
2.3 Tabulación de análisis de riesgos	4.4.3.3	13/05/2024
2.4 Impacto de análisis de riesgos	4.4.3.4	16/05/2024
2.5 Valoración de riesgos	4.4.3.5	20/05/2024
2.6 Elaborar Informe	5.1	03/06/2024

Tabla 5 Programa de auditoría

4.4.1.2 Revisión de IS0 27001

La norma ISO 27001 establece un entorno integral para la gestión de la seguridad de la información en las organizaciones. Su estructura abarca 10 fases clave, que incluyen desde el contexto organizacional y el liderazgo hasta la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Estas fases incluyen la evaluación de riesgos, el control de seguridad, la gestión de activos de información, el control de acceso, la gestión de

incidentes y la auditoría interna, entre otros. La norma ISO 27001 garantiza la confidencialidad, integridad y disponibilidad de la información dentro de las organizaciones. (globalsuite, 2006)

Un SGSI, según la norma ISO 27001, se compone de procesos diseñados para implementar, mantener y mejorar continuamente la seguridad de la información. (pirani, 2014)

4.4.1.3 Auditoría Inicial

El análisis de brechas (GAP) es un método utilizado para evaluar el desempeño de los sistemas de información o programas de software, con el objetivo de determinar si cumplen con los requisitos de la institución. En caso de que no se cumplan estos requisitos, el análisis ayuda a identificar los pasos necesarios para lograr una implementación exitosa. La brecha se refiere a la diferencia entre "donde estamos" y "donde queremos estar" (el objetivo deseado). Mediante el análisis de brechas, se pueden identificar las necesidades y los recursos necesarios para alcanzar los objetivos establecidos.

Nivel de Madurez	
No existencia Nivel 0	No hay necesidad del requisito
Ad- hoc Nivel 1	Existe cierta valoración de la necesidad del requisito. Se aplica para algún inconveniente
Ejecutado (Nivel 2)	Los controles existen, pero no están documentados
Definido (Nivel 3)	Los controles se encuentran en su lugar y están documentados
Manipulable y mediable (Nivel 4)	Existe un control interno sobre la aplicación de controles y cumplimiento de requisito
Optimizado (Nivel 5)	Existe un control interno constante sobre la aplicación de controles y cumplimiento de requisitos. Se mide la capacidad de los requisitos determinados objetivos de progreso

Tabla 6 Nivel de madurez

Nivel Medio Cumplimiento = Puntuación total de cada Control /Número de controles	
Puntaje de madurez por debajo de 1.65	Esto indica que el control no cumple con los requisitos
Puntaje de madurez entre 1.66 y 3.25	Señala que el control cumple parcialmente con los requisitos
Puntaje de madurez por encima de 3.26	Indica el control cumple con los requisitos de la norma

Tabla 7 Nivel de cumplimiento

Cumplimiento de requisitos de seguridad de la Norma ISO 27001

Este instrumento permite evaluar el cumplimiento de los requisitos relacionados con la protección de los datos almacenados en los establecimientos de la institución. Está diseñado para identificar y asegurar el cumplimiento de los requisitos de protección de la información. A continuación, se detallan los requisitos de cumplimiento según la norma ISO 27001.

Requisitos	**Descripción**	**Ítems**
4 La Organización y su Contexto	Es el principio donde se comienza a desarrollar el SGSI y se basa en identificar los problemas internos y externos.	4
5 Liderazgo	Este requisito demuestra el compromiso relacionado con la seguridad de la información	3
6 Planificación	Este requisito reconoce los riesgos de seguridad de la información y establece los controles para disminuir los riesgos que se pueden presentar	2

7 Soporte	Se refiere a la necesidad de brindar recursos, sensibilización sobre seguridad	5
8 Operación	Implica la implementación de los controles y fases para garantizar la protección de datos	3
9 Evaluación del desempeño	Se refiere a las necesidades de monitorear, medir, analizar y evaluar el cargo sobre SGSI	4
10 Mejora	Son las necesidades que se identifica en la mejora continua del SGSI	2

Tabla 8 Descripción de requisitos según la Norma ISO

Diseño del Instrumento del cumplimiento de requisitos de la Norma ISO 27001

REQUISITOS		PREGUNTA	CUMPLIMIENTO
4 La Organización y su Contexto	4.1 Entendiendo la Organización y su contexto	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	
	4.2 Expectativas de las partes interesadas	1.- ¿Se han identificado las partes interesadas?	
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	
	4.4 SGS Sistema de Gestión de la Seguridad de la información	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	

5 Liderazgo	5.1 Liderazgo y compromiso	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	
	5.2 Política de la Seguridad de la Información	1.- ¿Se ha definido una Política de la Seguridad de la Información?	
		2.- ¿Se ha establecido un marco que permita el establecimiento de objetivos?	
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	
	5.3 Roles y Responsabilidades	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	

Tabla 9 Diseño de instrumento de requisitos

4.4.1.4 Ejecución

Se realizó una entrevista al vicerrector con el propósito de obtener información sobre la situación actual en relación con la seguridad, las políticas vigentes, los documentos pertinentes y el cumplimiento de los requisitos de seguridad según la norma ISO 27001.

Ilustración 5 Fotografía de entrevista

Tabulación de datos del cumplimiento de requisitos de la Norma ISO 27001

Se realizó la tabulación de datos en Microsoft Excel para evaluar el cumplimiento de los requisitos. Se aplicó un análisis de brechas utilizando el modelo de niveles de madurez, que se califica de nivel 0 a nivel 5.

Primero, se calculó el promedio de cada requisito. Luego, se determinó el estado de brecha (GAP) dividiendo el promedio obtenido entre 5. La brecha se calculó mediante una resta para obtener el valor porcentual. Con estos datos, se evaluó el estado de madurez de la Unidad Educativa Excelso Espíritu Santo, evidenciando que la institución cumple con la mayoría de los requisitos establecidos por la norma ISO 27001, alcanzando un estado de madurez que indica cumplimiento.

Requisitos		Pregunta	Cumplimiento	observación	Promedio	Estado GAP	Brecha	Estado de Madurez
4 La Organización y su Contexto	4.1 Entendiendo la Organización y su contexto	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	2	Existen pero no estan documentado	2,50	50%	50%	CUMPLE PARCIALMENTE
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	2	Existen pero no estan documentado				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	3	Existe documentacion adecuadamente				
	4.2 Expectativas de las partes interesadas	1.- ¿Se han identificado las partes interesadas?	3	Existe documentacion adecuadamente				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	2	Existen pero no estan documentado				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	2	Existen pero no estan documentado				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	3	Existe documentacion adecuadamente				
	4.4 SGS Sistema de Gestión de la Seguridad de la información	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	3	Existe documentacion adecuadamente				

Tabla 10 Tabulación de los requisitos de la norma ISO 27001

Test de Cumplimiento ISO 27001

Cumplimiento de controles

Este instrumento, proporcionado por la norma ISO, establece controles y buenas prácticas para la gestión de la seguridad informática en la institución. Está compuesto por varias cláusulas que abarcan diversos aspectos de la seguridad de la información. A continuación, se presentan las cláusulas de cumplimiento de controles según la norma ISO 27002:

CLÁUSULAS	Descripción	Ítems evaluados
A5 Políticas de Información	Determina la gestión de la seguridad de la información, contiene responsabilidades, objetivos y seguridad	1
A6 organización de Seguridad de la Información	Establece la gestión para iniciar y controlar la implementación de la seguridad	2

A7 seguridad de los recursos humanos	Establece controles en relación con la formación y responsabilidades de los empleados vinculado con la seguridad de la información	3
A8 gestión de activos	Describe los controles para clasificar y salvaguardar de los activos de información en las organizaciones	3
A9 Control de acceso	Define los controles para el acceso a los sistemas, incluyendo la autenticación, autorización y gestiones de contraseñas	4
A10 Criptografía	Describe los controles para el funcionamiento correcto de la criptografía para salvaguardar la información confidencial	1
A11 Seguridad Física y del entono	Establece los controles para resguardar los recursos de información contra amenazas, robos y daños	2
A12 seguridad en las operaciones	Asegurar la operación segura de las instalaciones de procesamiento de datos	7
A13 Seguridad en las comunicaciones	Establece salvaguardar los datos de redes y proteger la infraestructura	2
A14 Adquisición, desarrollo y mantenimiento de sistemas de información	Garantiza que la seguridad de la información es importante de los sistemas de información en su secuencia de vida	3
A15 Relación con proveedores	Establece la seguridad de los activos de la organización que sean autorizados por los proveedores	2
A16 Gestión de incidentes de seguridad de la información	Garantiza una perspectiva consistente para la seguridad de la información	1

A17 Gestión de la Continuidad del Negocio	Define los controles para asegurar la disponibilidad continua de los sistemas informáticos	2
A18 Cumplimiento	Establece los controles para salvaguardar que la organización cumple todas las normas	2

Tabla 11 Descripción de Cláusulas según la norma ISO

Diseño del instrumento de cumplimiento de controles de la Norma ISO 27001

Numeral	**Clausula**		**Requisito**	**CUMPLE**
A5	Políticas de Seguridad de la Información	A5.1 Dirección de gestión para la seguridad de la información	1.- ¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?	
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	
A6	Organización de la Seguridad de la Información	A6.1	1.- ¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	
			4.- ¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	
			5.- ¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?	
		A6.2. Dispositivos y teletrabajo	1.- ¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	
			2.- ¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?	

Tabla 12 Diseño de instrumentos de controles

4.4.1.5 Ejecución

Se realizó una entrevista al vicerrector encargado de los equipos informáticos para obtener información detallada sobre la seguridad y el cumplimiento de los controles de seguridad establecidos por la norma ISO 27001.

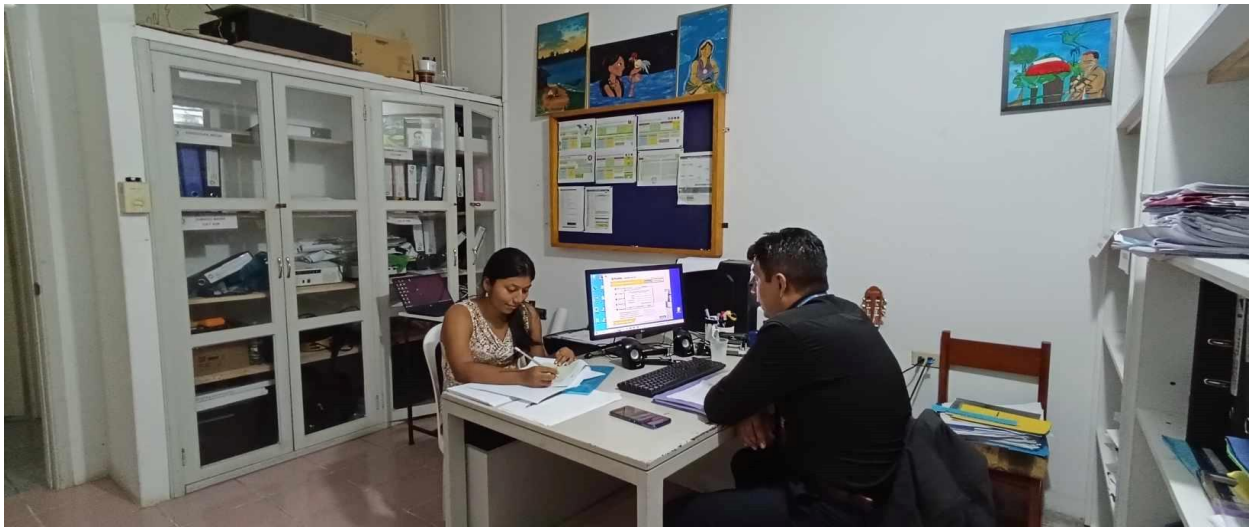


Ilustración 6 Fotografía de entrevista

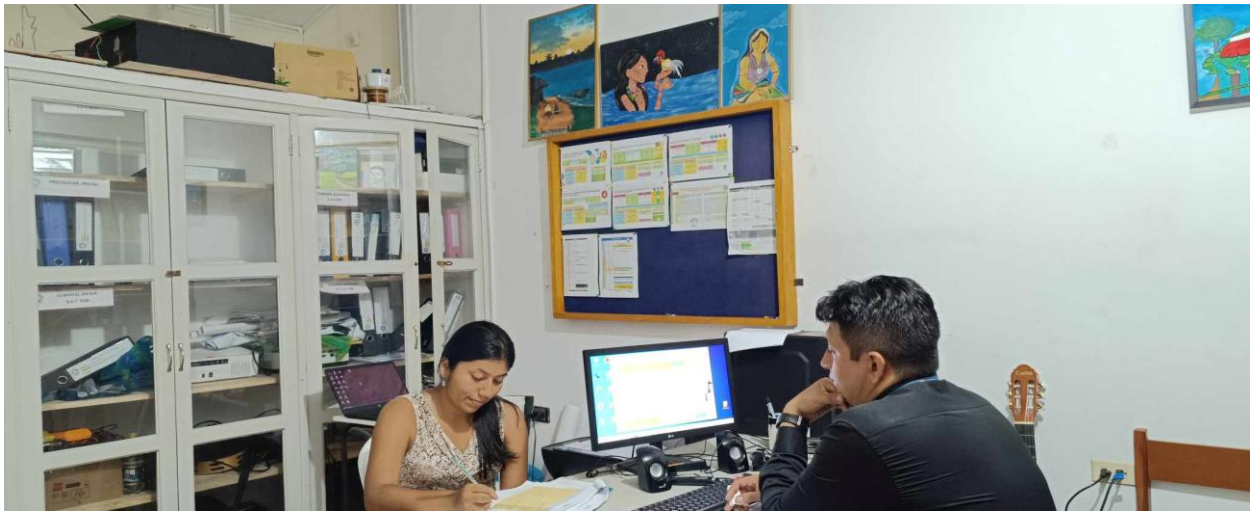


Ilustración 7 Fotografía de entrevista

Tabulación de datos del cumplimiento de controles de la Norma ISO 27001

La tabulación de datos se realizó en Microsoft Excel para evaluar el cumplimiento de los controles establecidos por la norma ISO 27001 en la Unidad Educativa Excelso Espíritu Santo. Se utilizó un sistema de codificación con los valores Sí (1), No (0) y No Aplica (2) para cada control.

Primero, se contabilizó el total de controles evaluados y los controles excluidos. A continuación, se calculó el número de controles que cumplen con los requisitos, restando el total de controles del número de controles excluidos. Finalmente, se determinó el valor porcentual de los controles que cumplen frente a los que no cumplen.

Numeral	Cláusula		Requisito	CUMPLE
A5	Políticas de Seguridad de la Información	A5.1 Dirección de gestión para la seguridad de la información	1.- ¿La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio?	0
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	0
A6	Organización de la Seguridad de la Información	A6.1	1.- ¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	0
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	0
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	1
			4.- ¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	1
			5.- ¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización?	1
		A6.2. Dispositivos y teletrabajo	1.- ¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	0

			2.- ¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?	1

Tabla 13 Datos de la institución

Nivel de Madurez

Después de calcular el cumplimiento de los controles, se determinó el porcentaje de requisitos que se cumplen y aquellos que no se cumplen. Asimismo, el análisis del cumplimiento de requisitos permitió observar el valor porcentual de si cada requisito cumple con la norma, así como identificar la brecha, representada por el porcentaje obtenido.

Cláusulas	**%Cumplimiento**	**% no Cumple**
A5 Políticas de Información	0%	100%
A6 organización de Seguridad de la Información	57%	43%
A7 seguridad de los recursos humanos	43%	57%
A8 gestión de activos	30%	70%
A9 Control de acceso	43%	57%
A10 Criptografía	0%	100%
A11 Seguridad Física y del entono	50%	50%
A12 seguridad	56%	44%

en las operaciones		
A13 Seguridad en las comunicaciones	57%	43%
A14 Adquisición, desarrollo y mantenimiento de sistemas de información	36%	64%
A15 Relación con proveedores	0%	100%
A16 Gestión de incidentes de seguridad de la información	43%	57%
A17 Gestión de la Continuidad del Negocio	0%	100%
A18 Cumplimiento	25%	75%
PROMEDIO	31%	69%

Tabla 14 Nivel de madurez de controles

REQUISITO DE ISO 27001	CUMPLE LA NORMA	BRECHA
4. La Organización y su Contexto	50%	50%
5. Liderazgo	53%	47%
6. Planificación	55%	45%
7. Soporte	74%	26%
8. Operación	62%	38%
9. Evaluación y desempeño	80%	20%
10. Mejora	93%	7%
Promedio Requisitos	**67%**	**33%**

Tabla 15 Nivel de madurez de requisitos

Conclusión

En esta primera fase se llevó a cabo la auditoría inicial conforme a la norma ISO 27001. Este proceso es crucial ya que permitió evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) en la Unidad Educativa Excelso Espíritu Santo, verificando el cumplimiento de los controles y requisitos de seguridad de la información. Como resultado de la auditoría, se concluyó que la institución posee un nivel medio de madurez en su gestión de seguridad de la información.

4.4.2 Análisis del Contexto

Se evaluó el análisis de contexto según la norma ISO 27001, considerando tanto factores externos como internos. Este análisis permitió identificar los riesgos y oportunidades relacionados con la seguridad de la información en la Unidad Educativa Excelso Espíritu Santo.

Contexto externo	Detalle
Partes interesadas	**Proveedores:** No aplica. **Clientes:** Comunidad de Santo Domingo y El Carmen que adquieren el servicio educativo. **Competidores:** Unidades Educativas cercanas Liceo Américas. **Reguladores:** ministerio de educación, ministerio relaciones laborales, SRI
Entorno político, legal y contractual	**Político:** • Espíritu de competencia • Ambientes de aprendizaje coloridos, ecológicos y digitales. • Seguimiento y control de estándares de calidad. • Educación integral en valores cristianos. • Capacitación e incentivo permanente al personal. • Educación basada en arte y deporte. • Aprendizajes basados en proyectos para el desarrollo del pensamiento crítico y reflexivo. • Autonomía institucional. • Desarrollo de competencias innovadoras. • Enseñanza basada en dos leguas. • Enseñanza basada en la cultura de nuestro país. • Orientación principal en lengua, matemáticas y ciencias. **Legal:** Políticas instituciones aprobadas por el ministerio de educación.
Entorno Competitivo	**Competencia:** Unidades Educativas cercanas Liceo de las Américas.
Entorno Económico	Está enfocado a personas con niveles económico, medio y alto.
Entorno Tecnológico	Sistemas de Tics. Cámaras de seguridad para los espacios educativos. Aire acondicionado para garantizar el nivel óptimo de

	temperatura en los niveles educativos.
Entorno Social y Ambiental	**Entorno Social:** los padres de familia son los principales financiadores y usuarios del servicio educativo. **Entorno Ambiental:** desarrollar acciones participativas que promuevan la cultura del manejo y cuidado del medio ambiente de parte de todos los miembros de la comunidad educativa.

Tabla 16 Contexto externo de la institución

Contexto interno	**Descripción**
Partes I nteresadas	**Dirección** **Director:** responsable de la gestión y dirección de la Unidad Educativa. **Vicerrector:** apoya en la administración general y puede asumir responsabilidades específicas según sea necesario. **Gestor de Operaciones** Personal de mantenimiento: responsable del cuidado y mantenimiento de las instalaciones físicas de la institución. Personal de seguridad: encargado de garantizar la seguridad de los estudiantes, el personal y las instalaciones escolares. Personal de limpieza: responsable de mantener limpias y ordenadas las aulas de clase. Personal de transporte: conductores encargados del transporte escolar. **Personal de TI** Técnicos de soporte: personal encargado de brindar soporte técnico a estudiantes y personal docente. **Coordinador del SGSI** Servicio de coordinación del SGSI: responsable de supervisar la implementación y mantenimiento del SGI en la institución educativa.
Misión y Objetivos	**Misión:** Somos la Unidad Educativa, que ofrece educación de calidad desde el nivel Inicial a Bachillerato, con Valores

	Cristianos, cumpliendo las normativas y estándares de Calidad del Ministerio de Educación, con una metodología socio constructiva, con ambientes seguros y armónicos. **Visión:** Ser la Institución de Santo Domingo de los Tsáchilas Líder en Calidad Educativa y en la formación integral de nuestros estudiantes.
Organización Procesos y Funciones	**Organización:** Equipo directivo, departamentos académicos y del DECE, personal docente, personal administrativo, servicios estudiantiles, equipo de mantenimiento y servicios generales, consejo escolar, asociación de padres de familia, comités y grupos de trabajo. **Procesos estratégicos:** Se realiza una evaluación de las prácticas pedagógicas, el desempeño del personal docente y administrativo, así como una comprensión profunda de las necesidades y expectativas de los estudiantes y padres de familia. **Procesos operacionales:** Los procesos establecidos son la matrícula del estudiante, la programación de clases, la asignación de recursos educativos y la evaluación del desempeño del personal. **Procesos de apoyo:** El sistema de identificación temprana donde se supervisa el progreso académico y del bienestar emocional de los estudiantes, colaboración de maestros y psicología.
Recursos Disponibles	**Personal:** Cuentan con un equipo de profesionales motivados y capacitados que se esfuerzan por brindar la mejor enseñanza a los estudiantes. **Sede:** Aulas de clase, departamentos de administración, sala de profesores, comedor escolar, bar, sala de usos múltiples, instalaciones sanitarias, talleres de arte y oficios, centro de recursos y tecnología, infraestructura de acceso (parqueadero), canchas deportivas, espacios abiertos de áreas naturales, jardines educativos, seguridad, área de piscina, área de juegos

	infantiles, espacio de crianza de animales, invernadero para proyectos relacionados con la agricultura, infraestructura de agua potable y gestión de residuos.
Tecnología Vigente	**Equipos:** • Computadoras 26 Lg o Samsung • Proyectores 26 Epson **Servicios:** • Conexión a internet • Proyectores en las aulas de clase • Plataforma de aprendizaje en línea • Herramientas de comunicación • Sistema de gestión académica • Recursos educativos digitales • Dispositivos tecnológicos • Aplicaciones educativas **Software: P**lataforma educativa, páginas en redes sociales https://www.ueees.edu.ec/ **Sistemas:** Alarma, sensores antirrobo, video vigilancia, aire acondicionado y extintores.

Tabla 17 Contexto interno de la institución

4.4.3 Elaboración de cuestionarios para analizar riesgos

Se elaboraron cinco cuestionarios para analizar los riesgos, cada uno con un enfoque específico: 25 preguntas sobre daño a los equipos, 25 preguntas sobre incendios, 15 preguntas sobre inundaciones, 25 preguntas sobre robos y 25 preguntas sobre malware.

Para la elaboración de estos cuestionarios, se desarrollaron dos matrices: Una matriz general para evaluar los riesgos de forma global y otra matriz para evaluar los riesgos de manera individual en cada aula de la institución donde se encuentran los equipos informáticos.

Cuestionario para analizar riesgos			**C1**
Robo	**Respuestas**		**Observaciones**
	Si	**No**	
1. ¿Los docentes están autorizados para mover los dispositivos de un aula a otra?			
2. ¿El conserje se encarga de asegurar las aulas de clase al finalizar?			
3. ¿Se realizan inventarios periódicos para verificar la presencia de todos los equipos?			
4. ¿Los dispositivos portátiles se guardan en lugares seguros cuando no se usan?			
5. ¿Se utiliza cada aula de clase por un solo curso?			
6. ¿Se han registrado incidentes previos relacionados con el robo los equipos?			
7. ¿Existe un protocolo claro para reportar la pérdida o robo de un dispositivo?			
8. ¿Se controla el acceso a las aulas de clase para permitir solo la entrada de personas autorizadas?			
9. ¿Se utilizan las aulas de clase para otras actividades?			
10. ¿Cualquier persona puede utilizar los equipos informáticos?			
11. ¿La institución cuenta con un guardia de seguridad?			
12. ¿Existe un responsable de los equipos informáticos en las aulas de clase?			
Realizado por: **Fecha:**			**Revisado por:** **Fecha:**

Tabla 18 Cuestionario de análisis de riesgo

4.4.3.1 Ejecución de los cuestionarios para analizar riesgos

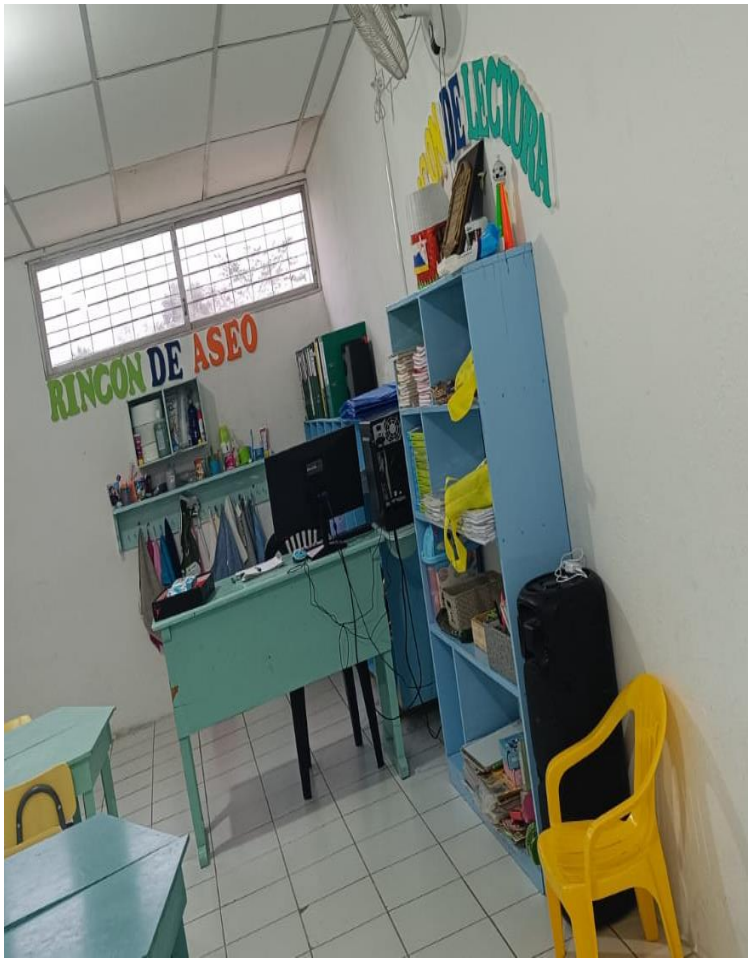
Se llevó a cabo una evaluación de los equipos informáticos en las 26 aulas, analizando riesgos relacionados con robo, daño a los equipos, incendio, inundaciones y malware. El objetivo fue determinar el valor total de seguridad y riesgo para cada aula.

Ilustración 8 Aplicación de cuestionarios de riesgos

4.4.3.2 Aplicación de análisis de riesgo

Se realizó una visita a la Unidad Educativa Excelso Espíritu Santo, durante la cual se entrevistó al encargado de los equipos informáticos de cada aula para evaluar los controles implementados.

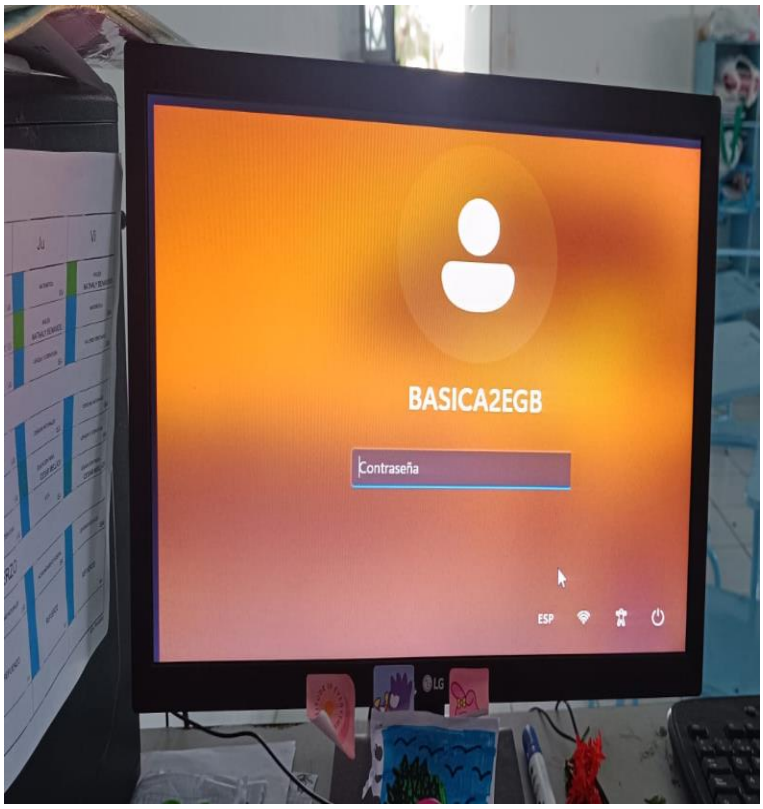
	Conexión de los equipos

	Ubicación de equipos en el escritor del docente
	Los productos de limpieza no están cerca de los equipos

	Las luces aulas
	Tienen proyectores y estructura metálica su estructura del techo de las aulas

	Protectores de las ventanas de las aulas
	Las aulas tienen aire acondicionado

	Cámaras para monitorear las aulas
	Pantallas en los grados superiores para visualizar lo que refleje el proyector

	Contraseñas para poder acceder a los equipos

4.4.3.3 Tabulación de análisis de riesgos

Se utilizó Microsoft Excel para tabular la información recopilada de los instrumentos aplicados en las 26 aulas de la Unidad Educativa Excelso Espíritu Santo. Además, se categorizó cada respuesta de los cuestionarios con los valores 0 (peligro), 1 (seguridad) y 2 (no aplica).

Cuestionario para analizar riesgos **Daños de Equipos**	**Inicial A**	**Inicial B**	**Inicial C**	**Primero A**
1.¿El personal ha recibido orientación sobre cómo evitar dañar los equipos durante su uso diario?	2	2	2	2
2. ¿Existe un registro actualizado de todos los equipos y dispositivos de las aulas?	1	1	1	1
3. ¿Se realizan inspecciones periódicas de los equipos para identificar daños visibles?	1	1	1	1
4.¿Se permite el consumo de bebidas, alimentos cerca de los equipos?	0	0	0	0

Tabla 19 Tabulación de análisis de riesgo

Escala de valor de aparición

Se utilizó una tabla de 5 niveles para evaluar la probabilidad de aparición en función del porcentaje de riesgos obtenidos en el análisis. Como se muestra a continuación la tabla:

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%**

Tabla 20 Escala de valor de aparición

Gravedad (Impacto)

Se utilizó una tabla de 5 niveles para evaluar la gravedad. A continuación, se muestra la tabla:

GRAVEDAD (IMPACTO)		**CONSIDERACIONES**
1	**MAS BAJO**	Las instalaciones quedan temporalmente cerradas o no puede operar, pero puede continuar su actividad. La interrupción es menor a 8 horas. Existe un daño limitado de activos. La mayoría de las instalaciones no se verán afectadas
2	**BAJO**	Las interrupciones y daños que pueden requerir atención pero que no comprometen las operaciones.
3	**MEDIO**	Las interrupciones y daños que podrían requerir una intervención considerable para continuar con normalidad.
4	**ALTO**	Daños con interrupciones y daños severos que requieren una respuesta urgente y podrían afectar la continuidad.
5	**MÁS ALTO**	Daños irreparables en instalaciones / afectada más allá del uso habitable. La mayoría de los datos y activos se pierden, destruyen o dañan sin posibilidad de reparación o restauración.

Tabla 21 Escala de Impacto

Nivel de Riesgo

El nivel de riesgo se clasifica en diferentes categorías de acuerdo con su gravedad:

Riesgo Muy Grave (Color Rojo): Debe ser abordado de inmediato antes de proceder con cualquier actividad relacionada con el proyecto.

Riesgo Importante (Color Naranja): Requiere la implementación de medidas preventivas y un control continuo durante el proyecto.

Riesgo Apreciable (Color Amarillo): Puede gestionarse con medidas preventivas si son económicamente viables.

Riesgo Marginal (Color Azul): Requiere medidas preventivas específicas, aunque es importante mantener una vigilancia constante.

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 las 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

Tabla 22 Nivel de riesgo

4.4.3.4 Impacto de análisis de riesgos

Se utilizó Microsoft Excel para calcular el impacto de cada nivel de riesgo relacionado con daño a los equipos, incendio, inundaciones, robo y malware. Se evaluaron aspectos como la confidencialidad, integridad y disponibilidad de la información en función del análisis de los datos recolectados en las 26 aulas de clase. Finalmente, se determinó el valor del impacto de cada riesgo.

RIESGO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	IMPACTO	
DAÑO DE EQUIPOS	2	3	4	3	
INCENDIO	3	3	3	3	
INUNDACIONES	4	4	4	4	
ROBO	3	3	3	3	
MALWARE	4	4	4	4	

Tabla 23 Impacto de análisis de riesgo

4.4.3.5 Valoración de riesgos

Primero, se contabilizó el total de controles clasificados como "No Aplica" (2). Luego, se calculó el total de controles evaluados restando los controles que no aplican del total general. Se contabilizaron también el total de controles de seguridad y el total de riesgos.

A continuación, se determinó el porcentaje de seguridad dividiendo el número de controles de seguridad entre el total de controles evaluados. De manera similar, se calculó el porcentaje de riesgo dividiendo el número de controles de riesgo entre el total de controles evaluados.

Finalmente, se obtuvo el promedio general del total de seguridad, el total de riesgo, el porcentaje de seguridad y el porcentaje de riesgo.

12.¿Hay barreras para evitar que entre agua al aula de clase?		0	0	0	0	0	0
13.¿Las puertas permite el ingreso del agua por la parte inferior?		0	0	0	0	0	0
14.¿Se han instalado sistemas de alerta para detectar inundaciones?		2	2	2	2	2	2
15.¿Las ventanas permite la entrada de agua?		0	0	0	0	0	0
	total controles no aplica	2	2	2	2	2	2
	total controles evaluados	13	13	13	13	13	13
	total seguridad	4	4	4	4	4	4
	total riesgo	9	9	9	9	9	9
	porcentaje seguridad	31%	31%	31%	31%	31%	31%
	porcentaje de riesgo	**69%**	69%	69%	69%	69%	69%

Tabla 24 Valoración de riesgos

4.4.3.6 Matriz de Riesgo

En Microsoft Excel se calculó la matriz de riesgo para daño de equipos, incendio, inundaciones, robo y malware. Se evaluó la probabilidad de cada riesgo en función del porcentaje de incidencia y se determinó el impacto de cada riesgo considerando la confidencialidad, integridad y disponibilidad de la información.

Luego, se calculó el valor del riesgo multiplicando la probabilidad de ocurrencia por la gravedad del impacto. Finalmente, se definió el nivel de riesgo de cada situación, asignando el color correspondiente según el nivel de gravedad.

Riesgo	Aparición probabilidad	Gravedad (Impacto	Valor del Riesgo	Nivel de Riesgo
DAÑO DE EQUIPOS	3	3	9	Importante
INCENDIO	5	3	15	Muy grave
INUNDACIONES	4	4	16	Muy grave
ROBO	3	3	9	Importante
MALWARE	4	4	16	Muy grave

Tabla 25 Matriz de riesgos

CAPÍTULO V

5. EVALUACIÓN DE RESULTADOS

5.1 Informe de auditoría

Dirigido a: Ing. Roberto Campos, Rector de la Unidad Educativa Excelso Espíritu Santo

Tipo de auditoría: Auditoría de seguridad Informática física a los equipos de cómputo de las aulas de clase

Motivo: Cumplir con los requisitos para el trabajo de titulación aplicado el área de auditoría informática.

Objetivos:

- Evaluar el nivel de madurez de gestión de seguridad de la información de la Unidad Educativa Excelso Espíritu Santo según ISO 27001.
- Identificar los riesgos de seguridad de la información de la Unidad Educativa Excelso Espíritu Santo y determinar la gravedad de los mismos.

Alcance

- Revisar la norma ISO 27001
- Realizar una auditoría inicial (fase 1 ISO 27001)
- Análisis del contexto (fase 2 ISO 27001)
- Elaborar cuestionarios para analizar riesgos
- Aplicación de análisis de riesgos
- Tabulación de análisis de riesgos
- Impacto de análisis de riesgos
- Valoración de riesgos
- Elaborar Informe

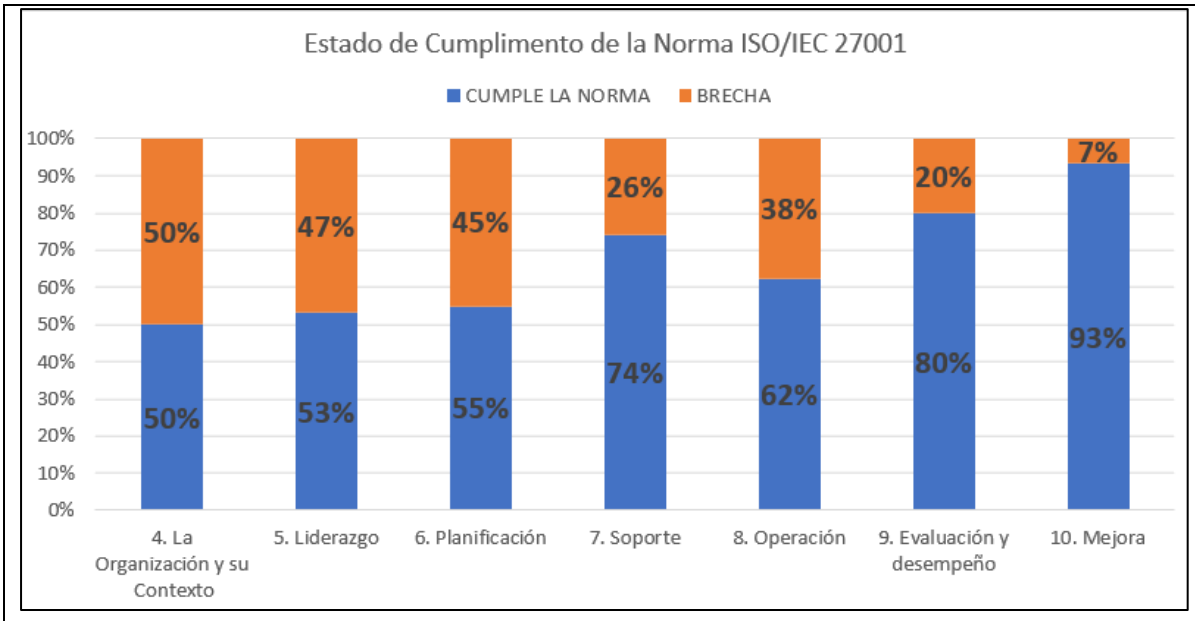
Personal relacionado

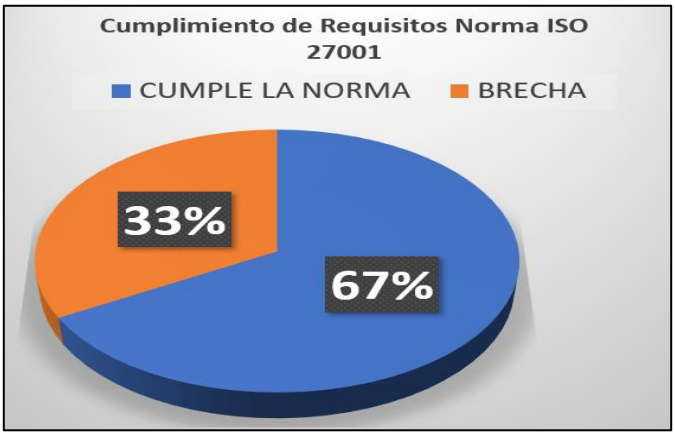
- Rector
- Vicerrector
- Encargado de las aulas de clase

Hallazgos:

Requisitos

Al aplicar el instrumento para verificar el cumplimiento de brecha se encontró lo siguiente con relación al cumplimiento de la norma ISO 27001.





Interpretación:

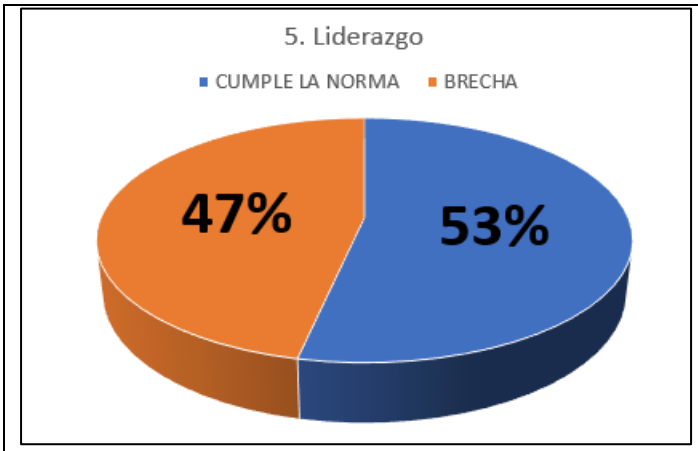
El estado de cumplimiento requisitos de la Norma ISO/IEC 27001 en la Unidad Educativa Excelso Espíritu Santo es medio, el que tiene mayor madurez los controles de mejora y el que tiene menos es el control de la organización y su contexto control la organización.

Interpretación:

La UEEES tiene implementada el requisito de la organización y su contexto la mitad y su nivel de madurez es **Medio.**

Causas:

- No se ha identificado las partes internas y externas puedan suponer amenazas o riesgos para la seguridad de la información.
- No se ha determinado el alcance del SGS y la conserva de la información documentada.
- El SGSI no está establecido, implementado y no se revisa de forma planificada considerando oportunidades de mejora.

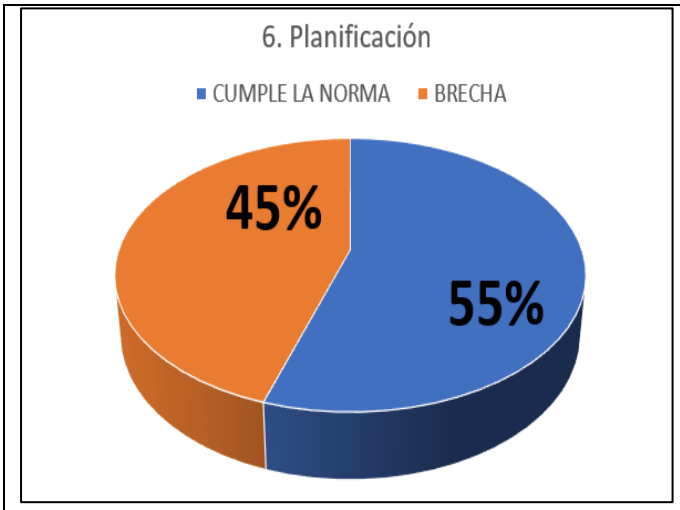


Interpretación:

Más de la mitad cumple con el requisito de liderazgo en la institución y su nivel de madurez es **Medio.**

Causas:

- No se ha establecido objetivos de la seguridad de la información acordes con los objetivos del negocio.
- No se ha avisado sobre la política a partes interesadas y a toda la empresa.
- No se ha asignado responsabilidades y autoridades sobre seguridad de la información.

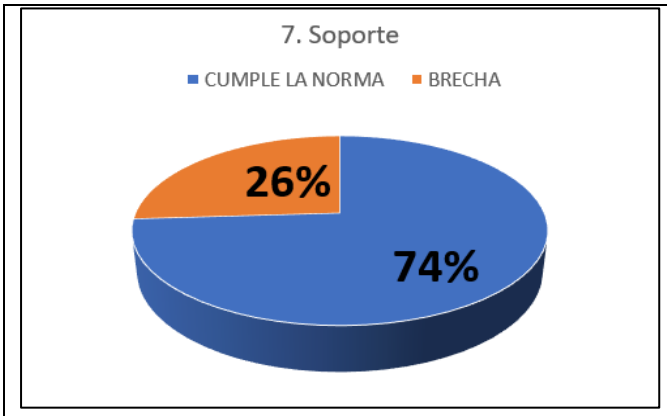


Interpretación:

En la institución tiene implementada más de la mitad el requisito de planificación y su nivel de madurez es **Medio.**

Causas:

- No se identifica ni se analiza los peligros por medio del método de evaluación y aceptación.
- No se ha determinado los criterios para crear una declaración de aplicabilidad.
- No se ha establecido objetivos de la seguridad de la información medibles acordes a los objetivos del establecimiento.

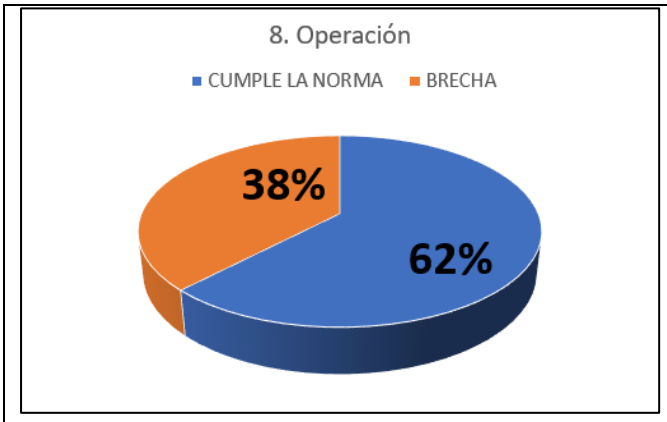


Interpretación:

Una segunda parte no tiene implementada el requisito de soporte en la institución y su nivel de madurez es **Bajo.**

Causas:

- No se identifica y asigna los recursos necesarios para el SGSI.
- No se mantiene información actualizada sobre la competencia del personal.
- No existe el conocimiento de los perjuicios que pueden generar al no seguir las pautas de la seguridad de la información.

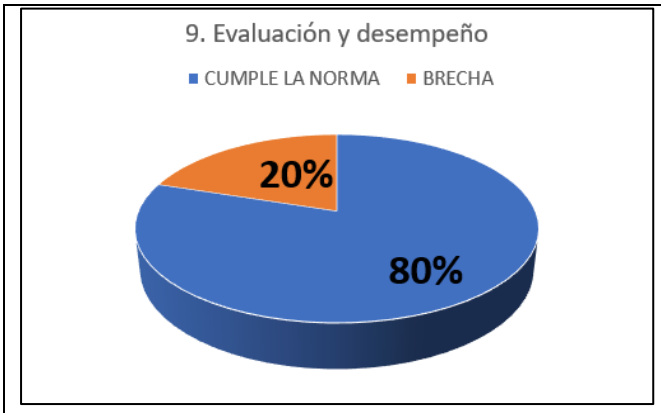


Interpretación:

Más de la mitad cumple con el requisito de operación en la institución y su nivel de madurez es **Medio.**

Causas:

- No tienen procesos de seguridad de la información que estén detallados para controlar lo que realizan según lo programado
- No se establece medidas para reducir los riesgos en la seguridad de la información ante cambios ejecutados.
- No se identifican y controlan los procesos externalizados en cuanto a los riesgos para la seguridad de la información.

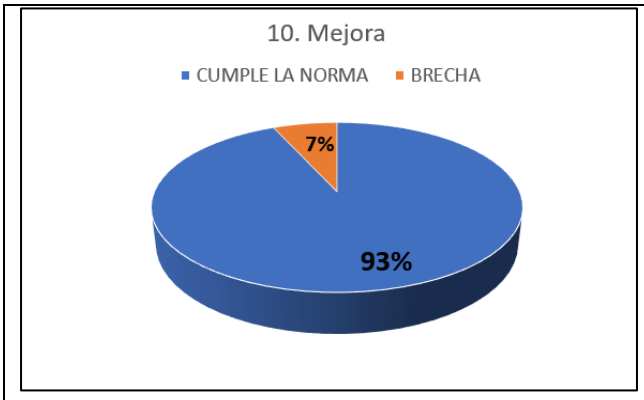


Interpretación:

Una segunda parte no tiene implementada el requisito de evaluación y desempeño en la institución y su nivel de madurez es **Bajo.**

Causas:

- No se ha designado una programación de auditoría interna y otorgado un encargado.
- No se ha determinado el alcance y los requisitos para el documento de auditoría.
- No se analiza las acciones correctivas y propuestas de cambio en la información de la auditoría.



Interpretación:

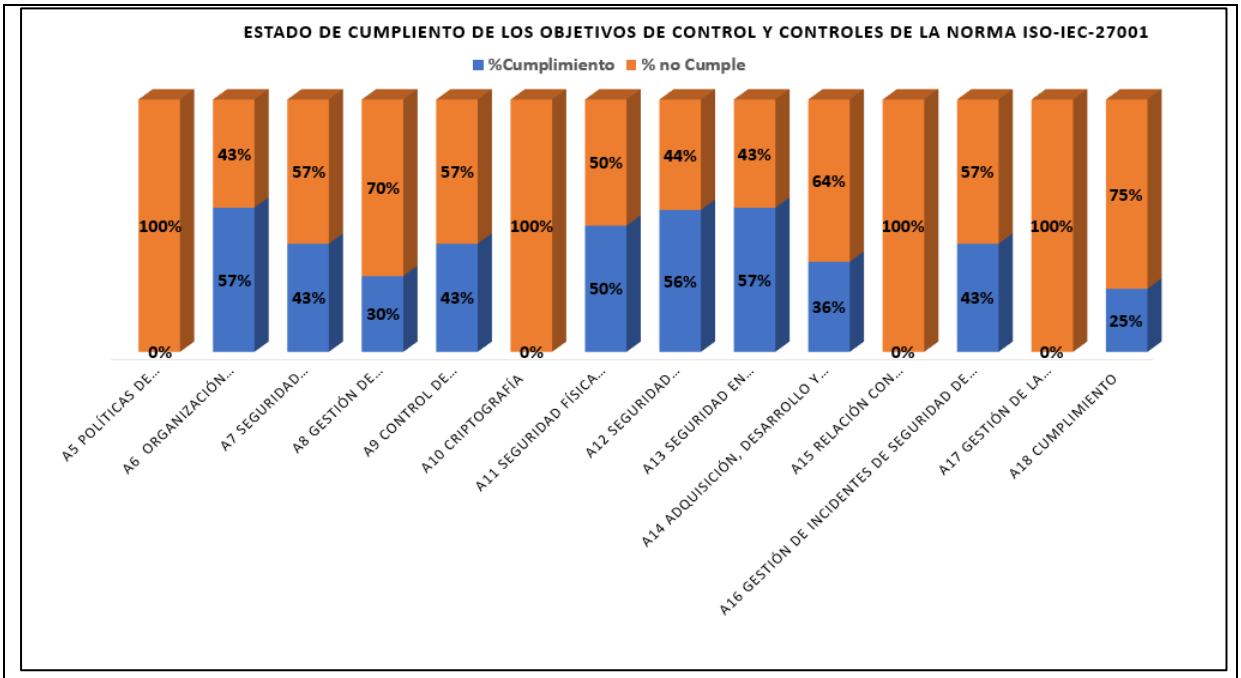
La institución cumple casi con su totalidad del requisito de mejora en la institución y su nivel de madurez es **Muy bajo.**

Causas:

- No existe un proceso detallado para identificar y registrar las aprobaciones.
- No existe un método para asegurar la mejora continua del SGSI reconociendo las posibilidades de mejora.
- No está en el ámbito de las correctivas no existe una variedad entre acciones correctivas sobre la no conformidad y sobre los motivos de la misma.

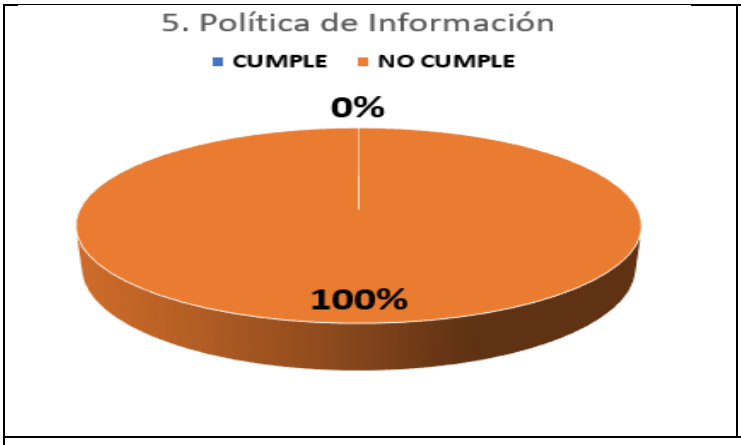
Controles

Una vez realizada la auditoría de seguridad a los equipos de las aulas de la Unidad Educativa Excelso Espíritu Santo se encontró lo siguiente con relación a la gestión de seguridad el cumplimiento de controles según la ISO 27001.



Interpretación:

El estado de cumplimiento de controles de la Norma ISO/IEC 27001 en la Unidad Educativa Excelso Espíritu Santo es medio, se puede evidenciar que en la institución no hay gestión de seguridad en lo que relaciona a políticas de seguridad de la información, criptografía, relación con proveedores y gestión de la continuidad del negocio y las que cumplen con la mitad del porcentaje de gestión de seguridad son organización de la seguridad de la información y seguridad en las comunicaciones.

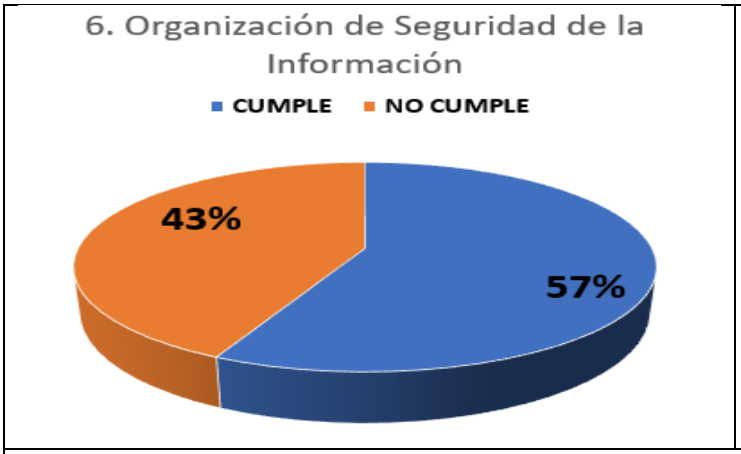


Interpretación:

La Unidad Educativa Excelso Espíritu Santo no cumple con política de Información.

Causas:

- No existe un proceso de planificación en la revisión de las políticas de seguridad de la información.
- No se ha publicado ni aprobado porque no existe en la institución políticas de seguridad de la información

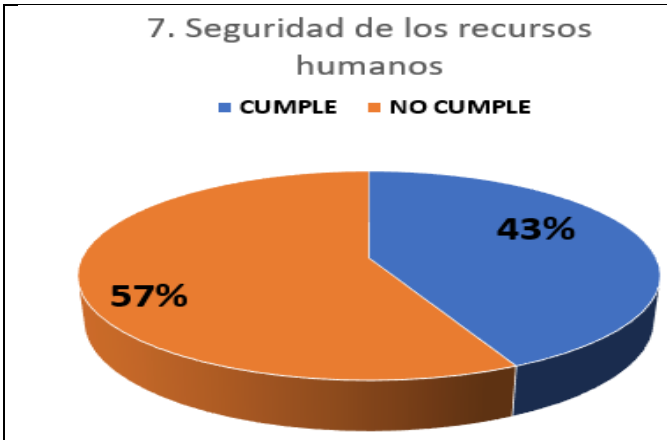


Interpretación:

La institución cumple un poco más de la mitad sobre la organización de seguridad de la información y su nivel es **Alto.**

Causas:

- No existen áreas sobre la seguridad de la información para acceso no autorizados o ingreso no autorizado.
- No se ha destinado y determinado las obligaciones sobre la seguridad de la información en las labores de la organización.
- No tienen requisitos para la seguridad de la información en el uso de dispositivos móviles.

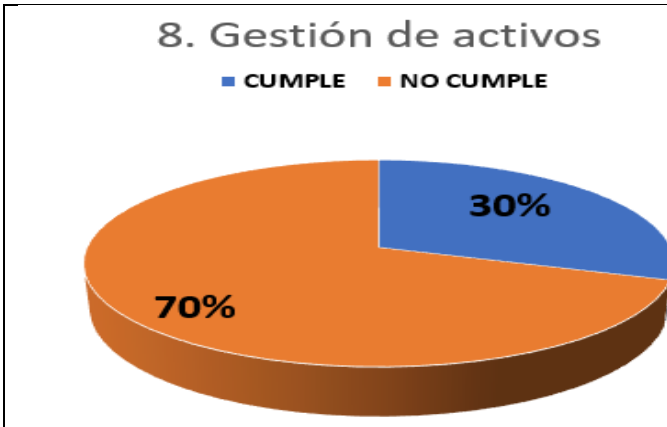


Interpretación:

La institución no cumple con más de la mitad de los controles de seguridad de los recursos humanos lo que indica que existen áreas de mejora en la implementación y gestión de estos controles, su nivel es **Medio.**

Causas:

- No existen procesos de información y desarrollo sobre las tareas de seguridad de la información.
- No existe un reglamento de disciplina donde se comunica a los miembros de la institución si no cumplen sobre las políticas de seguridad de la información.
- No existe un procedimiento que garantice la seguridad de la información en los cambios de empleado.

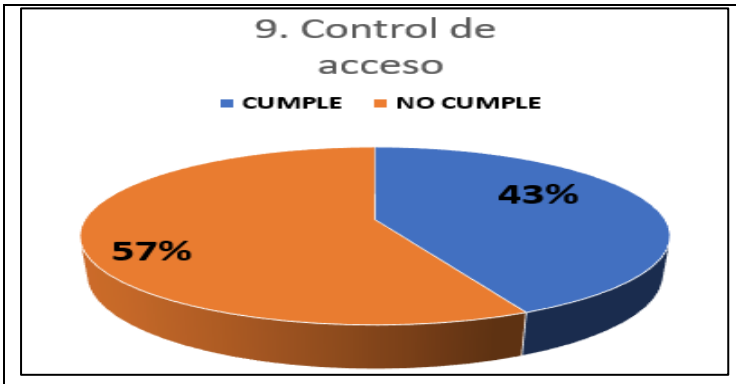


Interpretación:

En el control de gestión de activos a penas la tercera parte de los controle de la norma están implementados y su nivel es **Bajo.**

Causas:

- No se encuentran procedimientos para la recuperación de activos entregados a otras partes.
- No se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad.
- No tienen controles establecidos para aplicar a soportes extraíbles (Uso- Cifrado - Borrado).

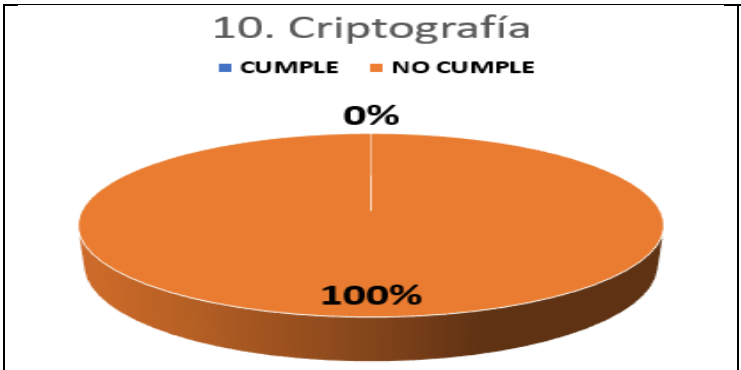


Interpretación:

La institución le falta más de la mitad implementar el control de acceso y su nivel es **Medio.**

Causas:

- No cuentan con una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según lo que requiera cada actividad.
- No existe una política específica para el manejo de información clasificada como confidencial en cuanto compromisos.
- No se definen fases para la renovación de autorización de acceso.

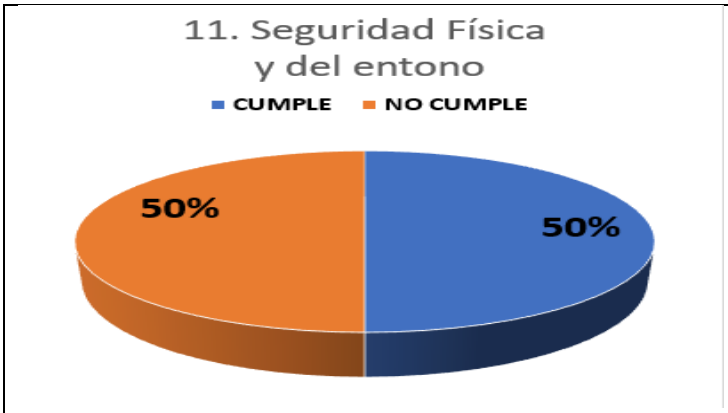


Interpretación:

La Unidad Educativa Excelso Espíritu Santo no cumple con el control criptografía.

Causas:

- No tienen una política para la institución de controles criptográficos.
- No existe un control del ciclo de vida de los códigos criptográficas.

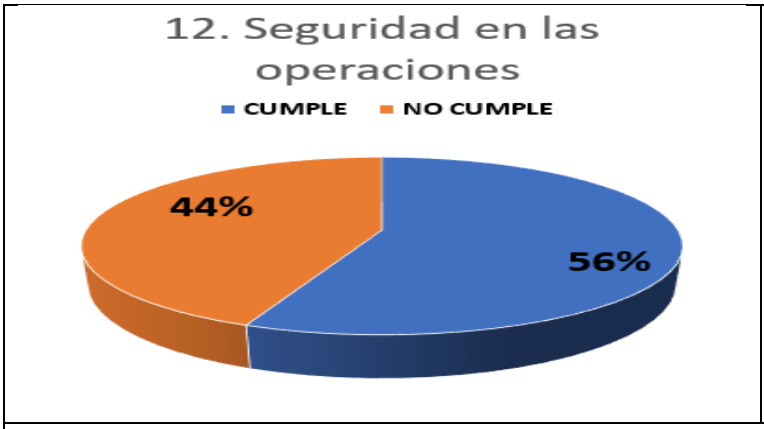


Interpretación:

La institución cumple con la mitad de los controles de seguridad física y del entorno, mientras que en la otra mitad no se cumple y su nivel es **Medio.**

Causas:

- No determinan perímetros de seguridad física donde sea necesario con barreras de acceso.
- No existen controles de acceso a personas no autorizadas en áreas restringidas.
- No se protege los equipos contra fallos de suministro de energía.



Interpretación:

La institución cumple más de la mitad del control de seguridad en las operaciones lo que indica un buen nivel de gestión en este aspecto y su nivel es **Alto.**

Causas:

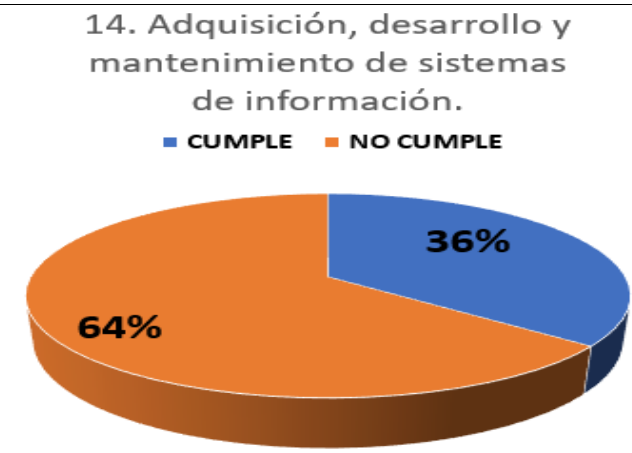
- No se documentan los procedimientos y se establecen responsabilidades.
- No se controla que la información sobre procedimientos se mantenga actualizada.
- No existe sistemas de detección para software malicioso o malware.

Interpretación:

La institución cumple con más de la mitad del control de seguridad en las comunicaciones y su nivel es **Alto.**

Causas:

- No se estipula condiciones de seguridad en los servicios de red tanto propios como subcontratados.
- No existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos.
- No se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades.



Interpretación:

La mayoría no cumple el control de adquisición, desarrollo y mantenimiento de sistemas de información que son estándares necesarios para áreas importantes para mejorar y su nivel es **Medio.**

Causas:

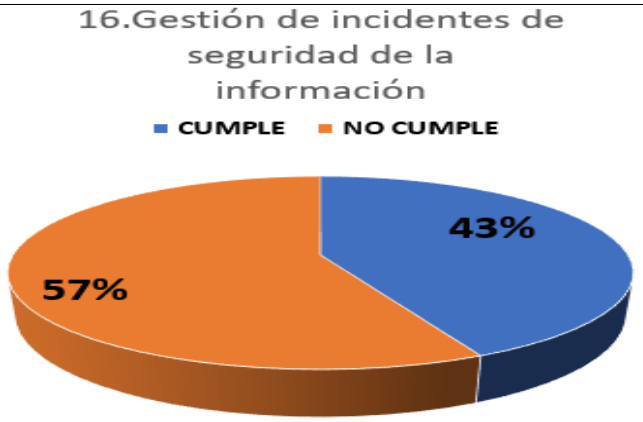
- No tienen documentos de los requisitos de seguridad de la información para los nuevos sistemas de información.
- No especifican los requisitos de seguridad de la información en el diseño de nuevos sistemas.
- No gestiona el control de cambios en relación con el impacto que puedan tener en los sistemas.

Interpretación:

La Unidad Educativa no cumple el control de relación con proveedores.

Causas:

- No existe una política de seguridad de la información para proveedores que acceden a los activos de la información del establecimiento educativo.
- No se controla el cumplimiento de los requisitos establecidos con proveedores externos.
- No han definido los requisitos de seguridad de la información en acuerdos con terceros.

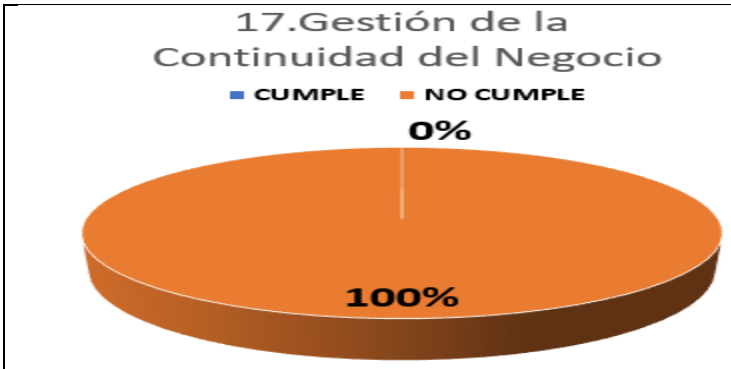


Interpretación:

Más de la mitad del control de gestión de incidentes de seguridad de la información no cumple con los estándares necesarios y su nivel es **Medio.**

Causas:

- No se definen responsabilidades para responder a las dificultades de la seguridad de la información.
- No se ha establecido un proceso para gestionar los incidentes en la seguridad de la información.
- No existe un procedimiento para dar respuesta a los sucesos de la seguridad de la información.

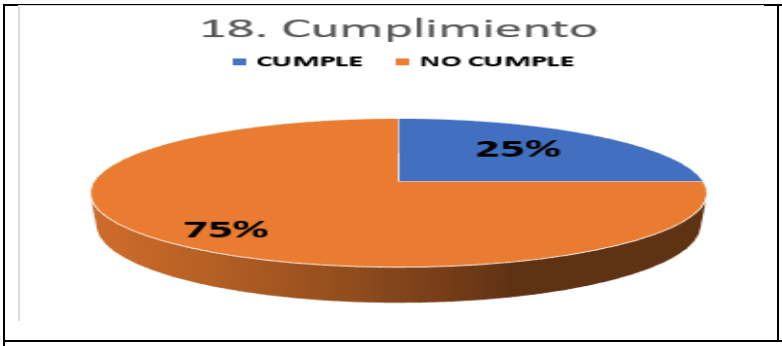


Interpretación:

La UEEES no cumple con el control de gestión de la continuidad del negocio

Causas:

- No se ha desarrollado un plan de continuidad ante incidentes de seguridad de la información.
- No se ha implementado las medidas de recuperación previstas en el plan de continuidad.
- No han evaluado la necesidad de concluir los activos críticos de la información.



Interpretación:

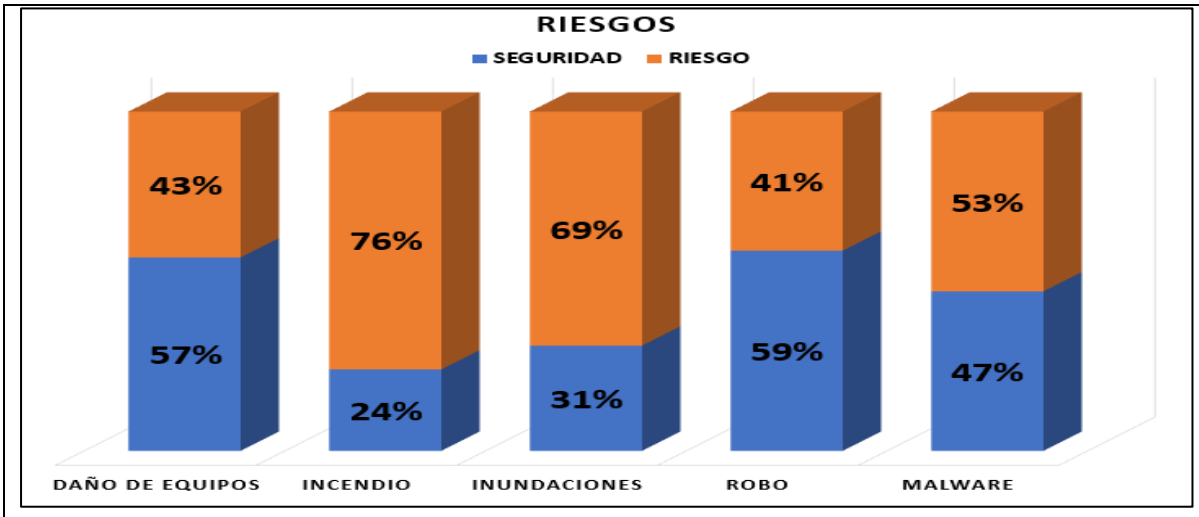
En el control de cumplimiento a penas la segunda parte de los controles están implementados en la institución y su nivel es **Bajo.**

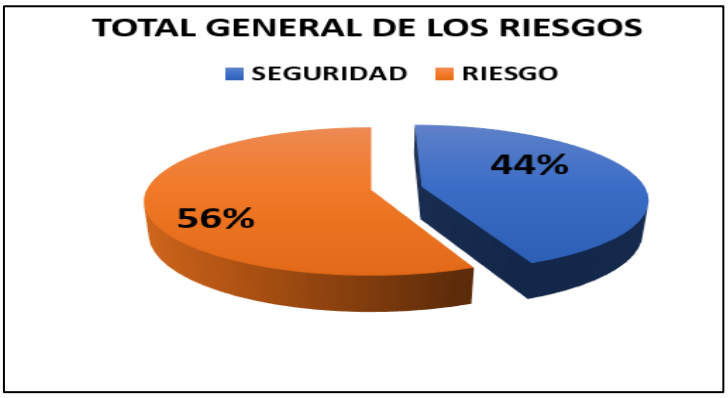
Causas:

- No existe métodos aplicados sobre la propiedad intelectual.
- No establecen medidas para la protección de datos personales de acuerdo con la legislación vigente.
- No realizan evaluaciones sobre el funcionamiento de las medidas técnicas de protección para la seguridad de la información.

Análisis de Riesgos

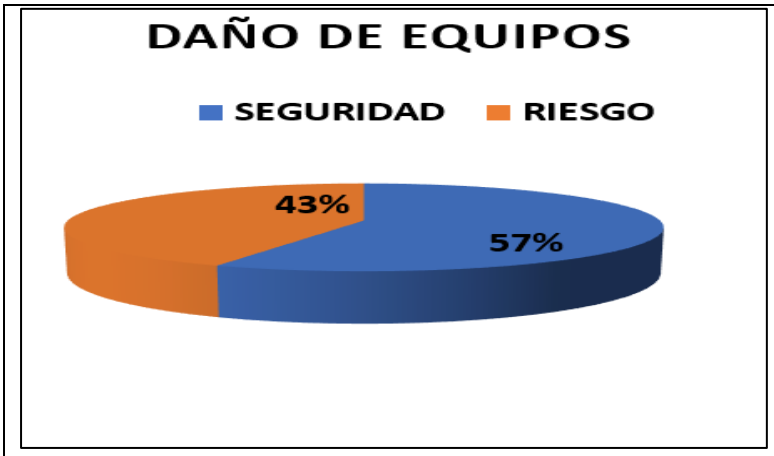
En cuanto a los riesgos de seguridad encontrados tenemos:





Interpretación:

El nivel general de riesgos es alto y el nivel de seguridad es medio, se muestra que incendio e inundaciones sus porcentajes son considerablemente altos lo cual indica una mayor posibilidad de ocurrencia. En cuanto los que tienen mayor seguridad son daños de equipos y robo.

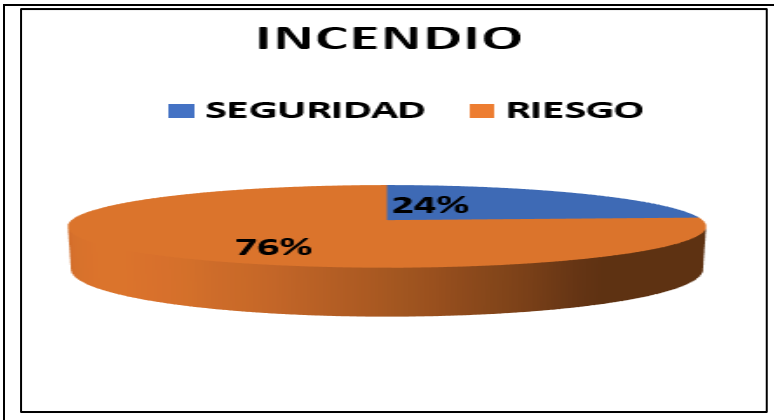


Interpretación:

El análisis de riesgo de daños de equipos en la Unidad Educativa Excelso Espíritu Santo más de la mitad tiene seguridad y su nivel de riesgo es **Importante**.

Causas:

- No se lleva un registro de las reparaciones y mantenimiento realizados a los equipos.
- Los equipos no están protegidos contra el polvo.
- Los cables de las computadoras de escritorio no están organizados y libres de enredos.

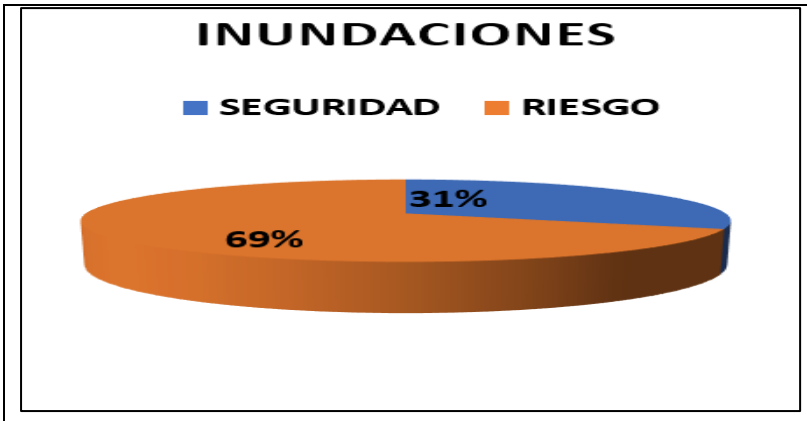


Interpretación:

El análisis de riesgo de incendio en la institución la segunda parte tiene seguridad y su nivel de riesgo es **Muy Grave**.

Causas:

- Las aulas no tienen sistemas de alarma contra incendios.
- No hay extintores de incendio visibles y accesibles en cada aula de clase
- Las puertas del aula no están hechas de materiales resistentes al fuego.
- Las aulas no tienen detectores de humo.

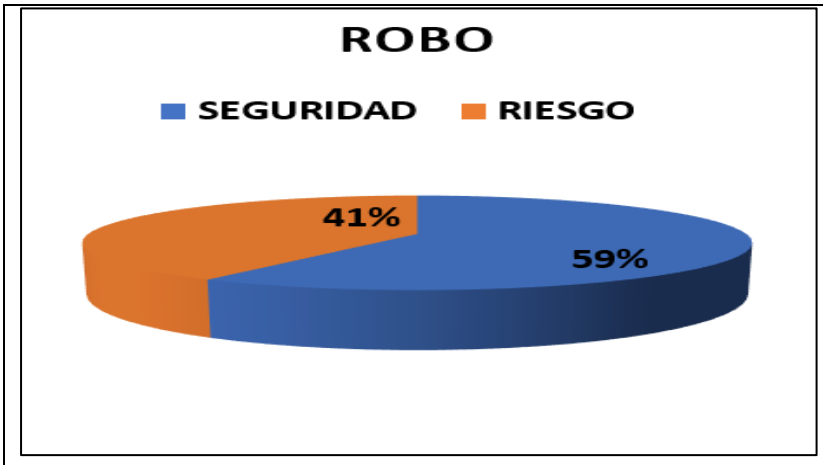


Interpretación:

El análisis de riesgo en la UEEES de inundaciones tiene una tercera parte de seguridad y su nivel de riesgo es **Muy grave.**

Causas:

- No se ha realizado simulaciones de inundaciones para resistir inundaciones.
- No hay canalones en las aulas de clase para evacuar las aguas lluvias.
- No hay barreras para evitar que entre agua al aula de clase.

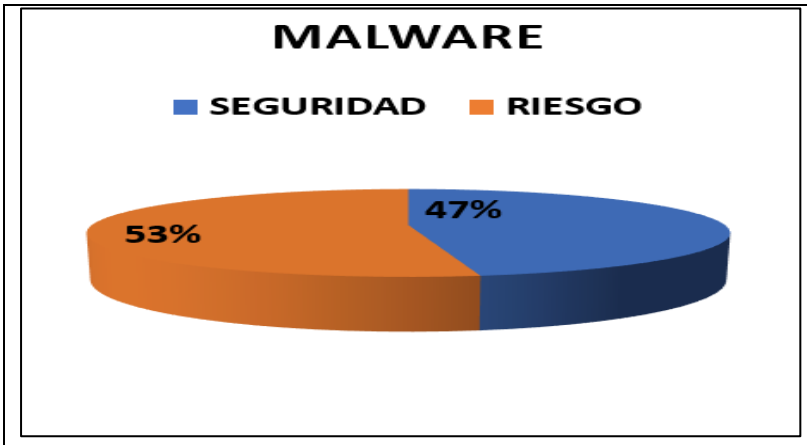


Interpretación:

El análisis de riesgo de robo de la Unidad Educativa Excelso Espíritu Santo más de la mitad tiene seguridad y su nivel de riesgo es **Importante.**

Causas:

- No hay alarmas en cada aula de clase.
- No tienen rejas las puertas de las aulas
- No están los cables y periféricos asegurados para evitar su desconexión.
- La institución no tiene guardia de seguridad.



Interpretación:

El análisis de riesgo de malware en la institución más de la mitad tiene riesgo y su nivel de riesgo es M**uy grave.**

Causas:

- No verifican la integridad de los archivos descargados por correo electrónico.
- No se revisa el historial de navegación en los equipos regularmente.
- No cuentan con antivirus los equipos.

Opinión:

Con respecto al nivel de madurez de seguridad se encontró lo siguiente:

REQUISITO DE ISO 27001	CUMPLE LA NORMA	NIVEL DE MADUREZ
4. La Organización y su Contexto	50%	MEDIO
5. Liderazgo	53%	MEDIO
6. Planificación	55%	MEDIO
7. Soporte	74%	ALTO
8. Operación	62%	MEDIO
9. Evaluación y desempeño	80%	ALTO
10. Mejora	93%	ALTO
Promedio Requisitos	**67%**	**MEDIO**

Tabla 26 Total del nivel de madurez

Con relación al objetivo 2 los riesgos identificados y su nivel de gravedad se detalla a continuación:

RIESGOS	SEGURIDAD	NIVEL DE GRAVEDAD
DAÑO DE EQUIPOS	57%	IMPORTANTE
INCENDIO	24%	MUY GRAVE
INUNDACIONES	31%	MUY GRAVE
ROBO	59%	IMPORTANTE
MALWARE	47%	MUY GRAVE
GENERAL	**44%**	**MUY GRAVE**

Tabla 27 Nivel de matriz de riesgo

5.2 Conclusiones y Recomendaciones

Considerando que el impacto es muy grave, se requiere que el proyecto no se inicie sin la aplicación urgente de medidas. Los riesgos de nivel importante deben ser controlados mediante la implementación de medidas preventivas que regulen las variables de riesgo durante el proyecto. En el caso de riesgos apreciables, es necesario evaluar la viabilidad de

implementar medidas adicionales para su reducción. Finalmente, los riesgos de nivel marginal deben ser evaluados, aunque no cuenten con medidas preventivas específicas.

Se recomienda tomar en consideración el manual de seguridad ver en anexo 1

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Con la colaboración de las autoridades de la Unidad Educativa Excelso Espíritu Santo, incluyendo al vicerrector encargado de los equipos informáticos y a los docentes que utilizan las computadoras a diario, se identificó la problemática de la ausencia de políticas de seguridad de la información.

- Se fundamentaron teóricamente las variables dependientes (SGSI) e independientes (área académica relacionada con los equipos informáticos) mediante la búsqueda de información relevante en libros recientes (últimos 5 años) y diversos autores. Este proceso permitió crear una estructura sólida, leer y parafrasear adecuadamente la información para completar el marco teórico, citando correctamente y sin faltas ortográficas.

- Se realizó una entrevista al encargado de los equipos informáticos de la Unidad Educativa Excelso Espíritu Santo y se aplicaron encuestas a los docentes que utilizan estos equipos en las aulas. Con la información recopilada, se diagnosticó el problema y se llevó a cabo la tabulación y análisis general de los datos obtenidos en el establecimiento educativo.

- Se evaluaron las vulnerabilidades de seguridad en las computadoras de las aulas para identificar los riesgos en el entorno informático, siguiendo las fases de la norma ISO 27001. Este enfoque sistemático permitió cumplir con los estándares de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información en el establecimiento educativo.

- Finalmente, se elaboró un informe de auditoría que reveló las áreas que requieren mejoras en seguridad y gestión. Se creó un manual para la Unidad Educativa

Excelso Espíritu Santo con recomendaciones útiles para mejorar la infraestructura y optimizar el área informática del establecimiento.

6.2 Recomendaciones

- Se recomienda que la Unidad Educativa Excelso Espíritu Santo implemente el manual de seguridad informática para asegurar el uso adecuado de los equipos. Esta medida ayudará a prevenir riesgos que puedan ocasionar daños a los dispositivos.
- Se sugiere que la carrera de Tecnología de la Información promueva la socialización de proyectos relacionados con la gestión de seguridad en instituciones educativas. Esto permitirá a los estudiantes adquirir conocimientos prácticos sobre cómo manejar y proteger la información en entornos educativos.
- Es aconsejable que la Unidad Educativa Excelso Espíritu Santo organice capacitaciones para sus docentes sobre la importancia de la seguridad informática. Esta formación contribuirá a que los docentes comprendan mejor cómo proteger la información y los recursos tecnológicos de la institución.

BIBLIOGRAFÍA

27001, I. (Julio de 2013). *normaiso27001*. Obtenido de normaiso27001: https://normaiso27001.es/

Abadías Selma, A., & Bustos Rubio, M. (2020). *Una Década de Reformas Penales Análisis de diez años de cambios en el código penal (2010-2020).* BoschEditor. https://doi.org/https://www.google.com.ec/books/edition/Una_d%C3%A9cada_de_reformas_penales/uLkTEAAAQBAJ?hl=es&gbpv=1&dq=UNE-EN+ISO+/IEC+27001&pg=PA91&printsec=frontcover

Acurio, J. (2019). *Propuesta de sistemas de gestión de seguridad de la información utilizando la norma ISO 27001 para la Unidad Educativa Nuestra Señora de Fátima.* Quito. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/1901

Adidas, W. (2019). *Lo esencial del hackeo.* Adidas Wilson. https://doi.org/https://www.google.com.ec/books/edition/Lo_esencial_del_hackeo/mBuyDwAAQBAJ?hl=es&gbpv=0

Alan Neill, D., & Cortez Suárez, L. (2018). *Procesos y Fundamentos de la Investigación Científica.* UTMACH. https://doi.org/http://repositorio.utmachala.edu.ec/bitstream/48000/14232/1/Cap.4-Investigaci%C3%B3n%20cuantitativa%20y%20cualitativa.pdf

Allueva , A., & Alejandre , J. (2020). *Practicas docentes en los nuevos escenarios tecnológicos de aprendizaje.* Prensas de la Universidad de Zaragoza. https://doi.org/https://elibro.net/es/lc/uleam/titulos/160371

Arroyo Guardeño, D. -G.-H. (2020). *Ciberseguridad.* Los libros de la Catarata. https://doi.org/https://elibro.net/es/ereader/uleam/233122

Atehortúa, F., Bustamante, R., & Valencia de los Ríos, J. (2008). *Sistema de gestión integral. Una sola gestión, un solo equipo.* Universidad de Antioquia.

https://doi.org/https://www.google.com.ec/books/edition/Sistema_de_gesti%C3%B3n_integral_Una_sola_ge/15nVyh1Fn6MC?hl=es&gbpv=0

Baena, G., Mendoza, R., & Coronado, E. (2019). IMPORTANCIA DE LA NORMA ISO/EIC 27000 EN LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN. *eumed*. https://doi.org/https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html

Barría , C. (2020). *Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio.* Editorial ebooks Patagonia - Ediciones UM. https://doi.org/https://elibro.net/es/ereader/uleam/195463

Batanero, J. (2019). *Formación del profesorado para la incorporación de las TIC en alumnado con diversidad funcional.* Octadero. https://doi.org/https://books.google.es/books?hl=es&lr=&id=VeuvDwAAQBAJ&oi=fnd&pg=PA1&dq=gesti%C3%B3n+del+aprendizaje+tic&ots=P4y8KY6_zF&sig=rn0VJ_5LK8UFqP0ueS-ntKzq9U0#v=onepage&q=gesti%C3%B3n%20del%20aprendizaje%20tic&f=false

Berrueta , E. (2022). *Transmisión de información por medios convencionales e informáticos.* Ediciones Paraninfo, S.A. https://doi.org/https://www.google.com.ec/books/edition/Transmisi%C3%B3n_de_informaci%C3%B3n_por_medios/T5Z3EAAAQBAJ?hl=es&gbpv=0

Bohórquez Gómez, M. R., & García González, A. J. (2022). *Educación, calidad de vida y redes sociales en las relaciones integeneracionales.* Aranzadi. https://doi.org/https://www.google.com.ec/books/edition/Educaci%C3%B3n_calidad_de_vida_y_redes_socia/ynx9EAAAQBAJ?hl=es&gbpv=1&dq=dispositivos+en+el+%C3%A1mbito+acad%C3%A9mico&pg=PT7&printsec=frontcover

Briceño , E. (2021). *Seguridad de la información.* 3ciencias. https://doi.org/https://doi.org/10.17993/tics.2021.4

Cabrerizo, D. (2019). *Cultura científica 4º ESO (2019).* Editex. https://doi.org/https://www.google.com.ec/books/edition/Cultura_cient%C3%ADfica_4%C2%BA_ESO_2019/_86UDwAAQBAJ?hl=es&gbpv=1

Castrillón, O., Willian, S., & Ruiz, S. (2020). Predicción del rendimiento académico por medio de técnicas de. *Scielo, XIII*(1), 93-102. https://doi.org/https://www.scielo.cl/scielo.php?pid=S0718-50062020000100093&script=sci_arttext

Catagua, J., & Cevallos, Á. (2019). El uso académico de las redes sociales: estrategias metodológicas de aplicación en el aula de clases. *utm, IV*(3), 29-38. https://doi.org/https://revistas.utm.edu.ec/index.php/Rehuso/article/view/2366

Catalá, J. (2018). *Elaboración SGSI seguridad 365.* UOC. https://doi.org/https://openaccess.uoc.edu/bitstream/10609/88306/10/jcatalahTFM1218memoria.pdf

Cavassa, C. R. (2005). *La gestión administrativa en las instituciones educativas.* Limusa. https://doi.org/https://books.google.es/books?hl=es&lr=&id=3peF_dZUveYC&oi=fnd&pg=PA9&dq=evolucion+de+gestion+academica&ots=AfLJDyV7Kp&sig=kk2LmRCQpV2KA_pYYJFGsYmg_i4#v=onepage&q=evolucion%20de%20gestion%20academica&f=false

Cazurro Brahona, V. (2022). *Seguridad del tratamiento: Aspectos técnicos (Parte I).* J.M. Bosch Editor. https://doi.org/https://www.google.com.ec/books/edition/Seguridad_del_tratamiento_Aspectos_t%C3%A9cn/8Uu3EAAAQBAJ?hl=es&gbpv=0

Chicano Tejada, E. (2023). *Auditoría de seguridad informática. IFCT0109 (2a. ed.).* IC Editorial. https://doi.org/https://elibro.net/es/ereader/uleam/232692

Cienfuegos Gayo, S. -G.-M. (2021). *Guía para la realización de las auditorías internas de los sistemas de gestión.* AENOR - Asociación Española de Normalización y Certificación. https://doi.org/https://elibro.net/es/ereader/uleam/177349

Cordero Viguri, J. A. (2021). Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos. *IDP. Revista de Internet, Derecho y Política*, 1-12. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8222608

Cuvi, G. P. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información mediante la apliación de la norma internacional ISO/IEC 27001:2013 en la Unidad Educativa Adventista Gedeón.* Quito. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/2159

Delerna Rios, G. E., & Rodriguez, D. L. (2021). Importancia de las tecnologías de información en el fortalecimiento de competencias pedagógicas en tiempos de pandemia. *Revista Científica De Sistemas E Informática*, *I*(1), 69-78. https://doi.org/https://doi.org/10.51252/rcsi.v1i1.104

Fabre, J., Barrios, J., & Rojas, R. (2021). *Conocimiento y frecuencia de uso de las TIC en docentes de la Educación Superior.* Tecnocientífica Americana. https://doi.org/https://elibro.net/es/lc/uleam/titulos/190039

Fernández, A. C. (2019). *Nuevos paradigmas en los procesos de enseñanza-aprendizaje.* Adaya Press. https://doi.org/https://books.google.es/books?hl=es&lr=&id=vTf-DwAAQBAJ&oi=fnd&pg=PA1&dq=RECURSOS+TECNOLOGICOS+PARA+EL+APRENDIZAJE&ots=qqYTpHk4XC&sig=6q60EWrLgxuxYwL9aY_NNQwv-Ek#v=onepage&q=RECURSOS%20TECNOLOGICOS%20PARA%20EL%20APRENDIZAJE&f=false

García Alías, A., & Cebrián Robles, D. (2019). *Tecnologías para la información de profesionales en educación.* Dykinson. https://doi.org/https://elibro.net/es/ereader/bibliotecautpl/128512

Gayoso Martínez, V. -H.-A. (2020). *Ciberseguridad.* Editorial CSIC Consejo Superior de Investigaciones Científicas. https://doi.org/https://elibro.net/es/ereader/uleam/172144

globalsuite. (2006). *globalsuite*. Obtenido de globalsuite: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Gómez Fernández, L. -F. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* AENOR - Asociación Española de Normalización y Certificación. https://doi.org/https://elibro.net/es/ereader/bibliotecautpl/53624

Gómez, Á. (2015). *Auditoría de seguridad informática.* RA-MA Editorial. https://doi.org/https://elibro.net/es/ereader/bibliotecautpl/62464

González, H. T. (2019). Recursos tecnológicos para la integración de la gamificación en el aula. *Tecnología, Ciencia y Educación*(13), 75-117. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=6936268

Grados, Á., & Sánchez, E. (2017). *La entrevista en las organizaciones.* El manual moderno S.A de C.V. https://doi.org/https://books.google.com.ec/books?id=Xb5ZDwAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false

Guachamin, L. J. (2023). *Implementación de un SGSI basado en la norma ISO 27001 para la Unidad Educativa "El libertador".* Cedia. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/67415/1/B-CINT-PTG-N.%20969%20Lara%20Guachamin%20%20Teddy%20%20Joel.pdf

Guarín, P., Guillermo, R.-G., Liliana, R.-R., & Yuber. (2020). *Investigación en Sistemas de Gestión.: Avances y retos de la gestión integral.* usantotomas. https://doi.org/https://books.google.es/books?hl=es&lr=&id=jgv5DwAAQBAJ&oi=fnd&pg=PT4&dq=ELEMENTOS++de+sistema+de+gestion+de+seguridad+de+la+informacion&ots=3qZLvsEPdz&sig=ygHZ70CEHoD3fkaEg52LcwyWbOE#v=onepage&q=ELEMENTOS%20%20de%20sistema%20de%20gestion%20de%20seguridad

Guevara Alban, G., Verdesoto Arguello, A., & Castro Molina, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO, 4*(3), 163-173. https://doi.org/https://www.recimundo.com/index.php/es/article/view/860

Heredero, C., López , J., Romo, S., & Salgado, S. (2019). *Organización y transformación de los sistemas de información en la empresa.* ESIC. https://doi.org/https://www.google.com.ec/books/edition/Organizaci%C3%B3n_y_transformaci%C3%B3n_de_los_s/9uiFDwAAQBAJ?hl=es&gbpv=1&dq=implementacion+del+SGSI+evidencias&printsec=frontcover

Heredia Sánchez, B. D., Pérez Cruz, D., Cocón Juárez, J. F., & Zavaleta Carrillo, P. (2020). La Gamificación como Herramienta Tecnológica para el Aprendizaje en la Educación Superior. *Revista Docentes 2.0, IX*(2), 49–58. https://doi.org/https://ojs.docentes20.com/index.php/revista-docentes20/article/view/144

Hernández, B. (2020). *Ciclo de vida de desarrollo ágil de software seguro.* Fundación Universitaria Los Libertadores. https://doi.org/https://elibro.net/es/ereader/bibliotecautpl/197008

Herrero , L. (2022). *Hacking ético.* RA-MA Editorial. https://doi.org/https://elibro.net/es/ereader/uleam/222693

Hervás Gómez, N. D. (2021). *Normativa de Ciberseguridad.* Ra-Ma. https://doi.org/https://www.google.com.ec/books/edition/Normativa_de_Ciberseguridad/Jc24EAAAQBAJ?hl=es&gbpv=1&dq=El+proceso+de+certificaci%C3%B3n+de+la+Norma+UNE-EN+ISO+/IEC+27001&pg=PT107&printsec=frontcover

Hinojo Lucena, F. J.-A. (2019). *Avances en recursos TIC en innovación educativa.* Dykinson. https://doi.org/https://elibro.net/es/ereader/uleam/128531

LISOT. (14 de mayo de 2018). *¿Qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)?* Obtenido de ¿Qué es un Sistema de Gestión de la Seguridad de

la Información (SGSI)?: https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/#

López , E. (2020). *Las tecnologías de la información y la comunicación en la praxis.* Octadero. https://doi.org/https://books.google.es/books?hl=es&lr=&id=Ui3pDwAAQBAJ&oi=fnd&pg=PA1&dq=recursos+tecnol%C3%B3gicos&ots=LnPoX9hGFu&sig=Yhg#v=onepage&q&f=false

López, A. (Octubre de 2005). *iso27000*. Obtenido de iso27000: https://www.iso27000.es/Acerca.html#Acercade

Lopez, P. L. (2004). POBLACIÓN MUESTRA Y MUESTREO. *scielo, 09*(08), 69-74. https://doi.org/http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012#:~:text=Es%20un%20subconjunto%20o%20parte,parte%20representativa%20de%20la%20poblaci%C3%B3n

López, R. A. (2017). *Sistema de Gestión de la seguridad informática.* Bogotá : Areandino. https://doi.org/https://core.ac.uk/download/pdf/326424017.pdf

Martín, I. D., & Fernández, I. A. (2020). *Ciencia de datos para la ciberseguridad.* RA-MA Editorial. https://doi.org/https://elibro.net/es/ereader/uleam/222714

Menéndez , S. (2022). *Auditoría de seguridad informática: curso práctico.* RA-MA Editorial. https://doi.org/https://elibro.net/es/ereader/uleam/222672

Minaya Macias, M. M., Minaya Macias, R. W., & Intriago, M. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. *pentaciencias, 5*(4), 584–599. https://doi.org/https://doi.org/10.59169/pentaciencias.v5i4.700

Morales, V. D. (2023). *SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD ESTATAL AMAZÓNICA.* REPORSITORIO UTA. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/37329

Móran, F., Móran, L., Móran , F., & Sánchez, J. (2021). Tecnologías digitales en las clases sincrónicas de la modalidad en línea en la Educación Superior. *Revista de Ciencias Sociales, XXVII*(3), 317-333. https://doi.org/https://dialnet.unirioja.es/servlet/articulo?codigo=8090623

Morán, G. L., Morán, J. P., Morán, J. N., Plúa, C. R., & Irene, M. (2017). *Modelo de Plan estratégico de sistemas para la gestión y organización a tráves de una plataforma informática.* 3ciencias. https://doi.org/https://books.google.es/books?hl=es&lr=&id=c-mQDgAAQBAJ&oi=fnd&pg=PA3&dq=evolucion+de+gestion+academica&ots=7uGxA6i5Vb&sig=U55p5SI1SCflhbXV1vzlibBUkY4#v=onepage&q&f=false

Murcia, M. (2020). *Diseño instruccional para profes: guía para la innovación educativa con TIC.* Ediciones USTA. https://doi.org/https://elibro.net/es/ereader/uleam/140725

Ortega, J. (2019). *El concepto escolar de tecnología: una mirada alternativa.* Editorial Unimagdalena. https://doi.org/https://www.google.com.ec/books/edition/El_concepto_escolar_de_tecnolog%C3%ADa_una_m/YW_KDwAAQBAJ?hl=es&gbpv=0

Palacio, E. B. (2021). *Sistema de gestión de riesgos en seguridad y salud en el trabajo.* Ediciones de la U. https://doi.org/https://books.google.es/books?hl=es&lr=&id=PiwaEAAAQBAJ&oi=fnd&pg=PP1&dq=libro+de+SEGURIDAD+DE+LA+INFORMACION&ots=nWT0ANxMl3&sig=vSepiGii_tVCaxe-J9St2pswRJU#v=onepage&q=libro%20de%20SEGURIDAD%20DE%20LA%20INFORMACION&f=false

Paniagua, M. (2021). *Lenguajes de marcas y sistemas de gestión de información.* Paraninfo. https://doi.org/https://books.google.es/books?hl=es&lr=&id=zHA-EAAAQBAJ&oi=fnd&pg=PR5&dq=caracteristicas+de+Sistema+gestion+de+seguridad+de+la+informacion&ots=lijkz_atoG&sig=OaMDwrBwhNbyJ9kzXh-oPCgeOLM#v=onepage&q=caracteristicas%20de%20Sistema%20gestion%20de%20seguridad

Pereyra, L. E. (2020). *Tecnologías de la información y comunicación II (Módulo II).* Klik. https://doi.org/https://www.google.com.ec/books/edition/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_comuni/O3c_EAAAQBAJ?hl=es&gbpv=1

Pérez, A. (2020). IMPORTANCIA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DE TECNOLOGÍA. *unipiloto*, 1-11. https://doi.org/http://repository.unipiloto.edu.co/handle/20.500.12277/6841

Piña, A., & Novoa, J. (2014). *Preparación Física.* Pila Teleña. https://doi.org/https://www.google.com.ec/books/edition/Preparaci%C3%B3n_F%C3%ADsica/lY2nDwAAQBAJ?hl=es&gbpv=0

pirani. (2014). *piranirisk.* Obtenido de piranirisk: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

Pobea, M. (2015). *La encuesta.* https://web.archive.org/web/20180424060624id_/http://files.sld.cu/bmn/files/2015/01/la-encuesta.pdf.

Postigo, A. (2020). *Seguridad informática.* Paraninfo. https://doi.org/https://books.google.es/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=SEGURIDAD+DE+LA+INFORMACION+&ots=-H1Wjl8Tj4&sig=ZtOr2spARHirJvFzTtA75IVw6dE#v=onepage&q&f=false

Quintas, A. (2020). *Teoría educativa sobre tecnología, juego y recursos en didáctica de la educación infantil.* UNE. https://doi.org/https://books.google.es/books?hl=es&lr=&id=LBnLDwAAQBAJ&oi=fnd&pg=PA156&dq=recursos+tecnol%C3%B3gicos&ots=Ob44gjY8bZ&sig=COKZYqpN897RxtC_Yib56xHlUSE#v=onepage&q&f=false

Quitian, J. (2019). Las aplicaciones tecnológicas al servicio de la educación superior. *Revista electrónica En educación Y pedagogía, III*(5), 95-109.

https://doi.org/https://revedupe.unicesmag.edu.co/index.php/EDUPE/article/view/82/362

Reynoso Holguín, J. D., Mejía María, o. J., & Cruz, M. (2020). La Tecnología del Aprendizaje y el Conocimiento (TAC): un enfoque hacia las matemáticas. *Amelica, XIX*(29). https://doi.org/http://portal.amelica.org/ameli/jatsRepo/499/4992369006/html/

Romero Rodríguez, J. M., Cruz Campos, J. C., & Martínez Domínguez, J. A. (2022). *Investigación educativa sobre recursos tecnológicos y métodos activos.* Octaedro. https://doi.org/https://www.google.com.ec/books/edition/Investigaci%C3%B3n_educativa_sobre_recursos/e2GjEAAAQBAJ?hl=es&gbpv=1&dq=recursos+tecnol%C3%B3gicos&pg=PA45&printsec=frontcover

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD.* 3ciencias. https://doi.org/https://www.3ciencias.com/libros/libro/introduccion-a-la-seguridad-informatica-y-el-analisis-de-vulnerabilidades/

Ruiz Enríquez, H., Sanipatín Ponce, L., & Quinde Sari, F. (2018). *Redec hacia la integración académica.* Universidad Polítecnica Estatal del Carchi. https://doi.org/https://books.google.es/books?hl=es&lr=&id=7aOLEAAAQBAJ&oi=fnd&pg=PA74&dq=la+norma+iso+27001+historia&ots=aZ4FD7X2vn&sig=vXn4YrNmSj8ktdooKDNAtmFGbUA#v=onepage&q&f=false

Ruiz, R. (2006). *HISTORIA Y EVOLUCIÓN DEL PENSAMIENTO CIENTÍFICO.* https://doi.org/https://www.eumed.net/libros-gratis/2007a/257/7.1.htm#:~:text=El%20M%C3%A9todo%20anal%C3%ADtico%20es%20aquel,de%20un%20hecho%20en%20particular

Salazar Ayala, E. -R.-G. (2019). *Educación, innovación tecnológica y auto-aprendizaje.* Brujas. https://doi.org/https://elibro.net/es/lc/uleam/titulos/130170

Santander Becas. (10 de Diciembre de 2021). *Satander Becas*. Obtenido de Satander Becas: https://www.becas-santander.com/es/blog/cualitativa-y-cuantitativa.html

Segundo, J. (22 de Noviembre de 2018). *Enciclopedia Humanidades*. Obtenido de Enciclopedia Humanidades: https://humanidades.com/metodo-deductivo/

Serrano Carrillo, M. (2019). *Mantenimiento de equipos informáticos.* Ministerio de Educación y Formación Profesional. https://doi.org/https://www.google.com.ec/books/edition/Mantenimiento_de_equipos_inform%C3%A1ticos/9O6kDwAAQBAJ?hl=es&gbpv=1&dq=La+seguridad+y+mantenimiento+del+hardware+educativo&printsec=frontcover

Serrano Junco, C. L. (2022). *Metodologías ágiles en las pymes: un modelo integral de auditoría en la gestión interna.* Corporación Universitaria Minuto de Dios. https://doi.org/https://elibro.net/es/ereader/uleam/231777

Silva, H. T. (2021). *Integración de las TIC en la formación inicial de profesores.* Universidad de la Serena. https://doi.org/https://books.google.es/books?hl=es&lr=&id=w30wEAAAQBAJ&oi=fnd&pg=PA7&dq=gesti%C3%B3n+del+aprendizaje+tic&ots=xtmV0eEjjv&sig=xJqokPcSI3X2Au5Lpz_mfEJuzgA#v=onepage&q&f=false

Tablado Rodríguez, M. S. (2019). *Calidad de la Educación: Debates, investigaciones y prácticas.* Editorial Dykinson, S.L. https://doi.org/https://www.google.com.ec/books/edition/Calidad_de_la_Educaci%C3%B3n_Debates_investi/xdOfDwAAQBAJ?hl=es&gbpv=0

Tejerina, O., & Beltrán, M. (2020). *Aspectos jurídicos de la ciberseguridad.* RA-MA Editorial. https://doi.org/https://elibro.net/es/ereader/uleam/222712

Toledo, M. A. (2022). *Elaboración de una guía de implementación de un SGSI para la corporación ecuatoriana para el desarrollo de la investigación y la academia-cedia.* dspace. Obtenido de https://dspace.ups.edu.ec/handle/123456789/22091

Tonysé de la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad, XIII*(5), 495-506. https://doi.org/http://scielo.sld.cu/scielo.php?pid=S2218-36202021000500495&script=sci_arttext

Unesco. (2019). *Marco de competencias de los docentes en materia de TIC UNESCO.* Organizaciones de las Naciones Unidas para la educación la Ciencia y la Cultura. https://doi.org/https://www.google.com.ec/books/edition/Marco_de_competencias_de_los_docentes_en/XGq1DwAAQBAJ?hl=es&gbpv=1

Vasquez, J. (2023). ISO/IEC 27000. *UCT, III*(2), 80-84. https://doi.org/https://doi.org/10.46363/high-tech.v3i2.3

Vázquez, E. (2021). *Medios, recursos didácticos y tecnología educativa.* UNED - Universidad Nacional de Educación a Distancia. https://doi.org/https://elibro.net/es/lc/uleam/titulos/173778

Veiga Ferro, J. M. (2020). *Perito Judicial en Mantenimiento y Protección del Hardware.* https://doi.org/https://www.google.com.ec/books/edition/Perito_Judicial_en_Mantenimiento_y_Prote/TVnMDwAAQBAJ?hl=es&gbpv=0

Veiga Ferro, M. J. (2020). *Asesor/Gestor en seguridad privada integral Curso superior en dirección de seguridad privada.* https://doi.org/https://www.google.com.ec/books/edition/Asesor_Gestor_en_seguridad_privada_integ/suXJDwAAQBAJ?hl=es&gbpv=0

Ventura León, J. L. (2017). ¿Población o muestra?: Una diferencia necesaria. *scielo*, *43*(4), 648-649. https://doi.org/http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662017000400014&lng=es&tlng=en

7. ANEXOS

Anexo 1 Manual de seguridad de los equipos informáticos de la institución

MANUAL DE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS DE LA UNIDAD EDUCATIVA EXCELSO ESPÍRITU SANTO

Contenido

Introducción

El manual es importante para proteger y utilizar correctamente las computadoras que se encuentran en las aulas de clase de la Unidad Educativa Excelso Espíritu Santo para ofrecer un entorno de aprendizaje estable y eficiente. Este manual de política de seguridad está diseñado para la seguridad de los equipos informáticos en cómo utilizarlos correctamente, definiciones importantes, responsabilidades, responsables, recomendaciones para evitar riesgos de robo, malware, incendio, inundaciones, daños de equipos y restricciones.

Objetivo

Definir las directrices de políticas para garantizar un ambiente seguro y seguir con las actividades educativas minimizando cualquier riesgo que pueda afectar.

Alcance

La implementación del manual de seguridad informática incluye el control de acceso físico a los equipos informáticos, los riesgos de seguridad y el reglamento del uso correcto de las computadoras de las aulas de clase de la institución Unidad Educativa Excelso Espíritu Santo estas políticas deben conocer los docentes y estudiantes ya que son quienes utilizan los equipos.

Responsables

Vicerrector: Es responsable de supervisar y garantizar el desarrollo de las políticas de seguridad informática en la Unidad Educativa Excelso Espíritu Santo.

Docentes: Son responsables de aplicar las políticas de seguridad informática durante las clases y vigilar el uso correcto de las computadoras por parte de los estudiantes.

Estudiantes: Tienen que cumplir con las políticas de seguridad establecidas, incluyendo el uso correcto de las computadoras en las horas de clase cuando el docente autorice utilizar.

Responsabilidades

- El vicerrector es encargado de los equipos informáticos de autorizar el ingreso a un tercero, el control de algún cambio de los dispositivos de los equipos a otra aula y de solucionar los problemas reportados por los docentes de los equipos.
- Los docentes deben participar en cursos de capacitación en relación con la seguridad informática, utilizar las computadoras correctamente encenderlas siguiendo los pasos en el manual y al finalizar sus clases apagar correctamente desconectando los cables del equipo, autorizan el uso de los equipos informáticos a los estudiantes en las aulas en hora de clases y los controles del aire acondicionado, del proyector deben guardar en el armario de las aulas.
- Docentes y estudiantes de la Unidad Educativa Excelso Espíritu Santo deben cumplir con el reglamento y procesos de la política de seguridad informática. Cualquier incumplimiento será tratado según el reglamento.
- Los empleados de limpieza son encargados de cerrar las ventanas y puertas de las aulas de clase.

Definiciones importantes

Acceso lógico: Ingresar la contraseña para poder ingresar a las aplicaciones de las computadoras a través de internet.

Acceso físico: La entrada física a los equipos informáticos de las aulas y utilizarlos para lo académico.

Cerraduras de seguridad: Son dispositivos físicos instalados en puertas para prevenir robos o accesos no autorizado.

Actualizaciones de licencia: Son actualizaciones regulares que se realizan asegurando los programas estén legalmente y actualizados con las últimas funciones.

Contraseña: Son cadenas de caracteres secretas utilizadas para proteger el acceso a sistemas informáticos.

Software antivirus: Es una aplicación que permite detectar, prevenir y eliminar software malicioso de las computadoras.

Equipos informáticos: Son de utilidad para la enseñanza donde se puede realizar tareas educativas en las aulas de clase.

Dispositivo: Son periféricos extra conectados a los equipos informáticos, como impresoras y proyectores

Cámaras de seguridad: Son dispositivos de vigilancia instalados alrededor de las aulas de clase de la institución educativa para monitorear y proteger los equipos informáticos contra robos.

Pasos a seguir sobre encender y apagar los equipos correctamente:

Pasos para encender la computadora:

1. Primero verificar los cables si están conectados del computador
2. Encender el regulador de voltaje
3. Encender el monitor
4. Encender el CPU

Pasos para apagar la computadora:

1. Cerrar todos los programas
2. Dar clic en el botón de inicio
3. Luego elegir la opción apagar equipo
4. Dar clic en apagar
5. Desconectar los cables del computador

Políticas para evitar riesgos

Objetivo: Establecer las prevenciones de seguridad para evitar los riesgos en la Unidad Educativa Excelso Espíritu Santo

Los riesgos son posibles amenazas que puede afectar la seguridad, integridad de los equipos informáticos que se utilizan diariamente en las aulas de clase. A continuación, como prevenir:

Definición de riesgo de Robo:
Posibilidad de personas no autorizadas ingresen a tomar algún dispositivo o información de los equipos.

Para prevenir:

- No se debe mover los dispositivos de un aula a otra porque se puede perder
- No se puede utilizar las aulas de clase para otras actividades
- No pueden utilizar otras personas las computadoras sin autorización del vicerrector de la institución.
- Tener un guardia de seguridad dentro de la institución
- Los equipos deben contar con etiquetas de identificación
- Deben tener iluminación adecuada las aulas donde están los equipos informáticos
- Deben contar con un sistema de alarma dentro de las aulas
- Las ventanas de las aulas deben tener rejas
- Las ventanas deben tener cerraduras
- Las puertas de las aulas deben tener cerraduras
- Las puertas deben tener rejas
- Afuera de las aulas de clase deben tener una iluminación adecuada
- La institución debe contar con cámaras de seguridad para monitorear todas las aulas

Definición de riesgo Daño de equipo: Las computadoras sufren por fallos técnicos o malas condiciones.

Para prevenir:

- Los equipos informáticos de las aulas deben reciben mantenimiento.
- Los equipos informáticos deben disponer de reguladores
- Deben tener un aire acondicionado todas las aulas
- Deben tener alfombrillas para los mouses de los equipos
- Los equipos no deben estar en áreas donde reciban luz solar durante largos períodos
- Los enchufes electrónicos que se conectan los equipos deben estar en buen estado
- Los proyectores deben estar ubicados en un lugar seguro
- Los escritores deben estar asegurados la estabilidad para prevenir el riesgo de los equipos al mover
- Los cables deben tener etiquetas para identificar su función o dispositivo correspondiente en caso de daño

Definición de riesgo de Incendio:
Desate de un fuego a causa de no tener en buen estados los equipos informáticos o las aulas de clase.

Para prevenir:

- No se debe permitir comer o beber cerca de los equipos informáticos
- Se debe realizar mantenimiento a los equipos
- Se debe capacitar a los docentes y estudiantes como actuar en caso de un incendio en las aulas
- Deben tener un sistema de alarma contra incendio todas las aulas
- Deben tener todas las aulas de clase extintores de incendio visibles y accesibles
- Las luces deben estar en buen estado y correctamente instaladas en las aulas
- Las aulas de clase deben tener detectores de humo
- Los cables se deben encontrar en buen estado sin estar (pelados o deteriorados)
- El aire acondicionado debe estar configurando para mantener una temperatura segura en las aulas
- Tener letreros que no se permite fumar dentro de las aulas de clase
- Al finalizar las clases las computadoras deben quedar apagadas y para más seguridad desconectadas
- Almacenar los materiales inflamables como cuadernos, papel lejos de equipo
- Los productos químicos de limpieza deben estar lejos de los equipos

Definición de riesgo de Inundaciones: Es un fenómeno natural que sucede cuando el área se llena de agua por las lluvias fuertes.

Para prevenir:

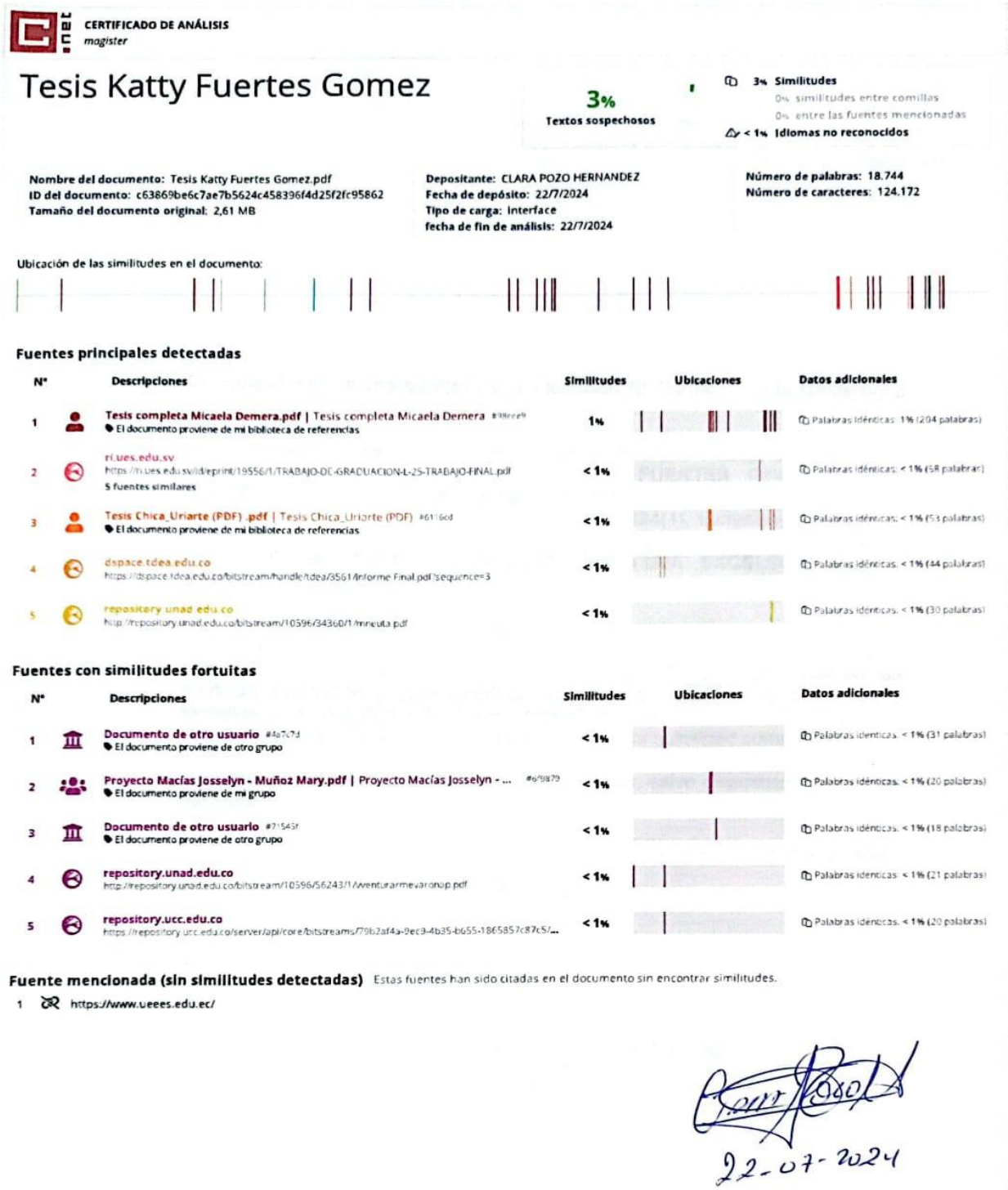
- Deben contar con un plan de contingencia en caso de inundaciones
- No debe estar cerca de las aulas tanques elevados
- Las alcantarillas deben estar limpias y despejadas para evitar problemas de inundación durante lluvias
- Los equipos de cómputo deben estar ubicados en un área elevada
- Las aulas de clase deben tener canalones para evacuar las aguas de las lluvias
- Los techos deben estar en buen estado
- Los techos de las aulas tienen que tener una estructura metálica para mayor resistencia del agua
- Las ventanas deben estar aseguradas para no permitir el ingreso del agua

Definición de riesgo de Malware:
Amenaza de un virus malicioso que puede afectar al equipo informático su funcionamiento y seguridad

Para prevenir:

- Realizar capacitación a los docentes sobre el uso seguro de los equipos
- No realizar descargas de archivos maliciosos
- Al usar dispositivos extraíbles USB, discos duros externo primero se debe examinar para evitar algún tipo de virus
- No conectar a los equipos teléfonos a cargar
- Realizar copias de seguridad regularmente
- Revisar el historial de navegación en los equipos
- Se debe utilizar una red Wifi segura
- Debe contar todos los equipos con un antivirus y actualizarlo regularmente
- Deben contar con un sistema de firewall
- Todos los programas en los equipos deben ser originales
- Las computadoras deben tener contraseñas
- Deben contar con licencia de Windows con las últimas actualizaciones
- Deben tener la licencia de Microsoft office con las últimas actualizaciones

Reporte del sistema antiplagio



CERTIFICADO DE ANÁLISIS
magister

Tesis Katty Fuertes Gomez

3%
Textos sospechosos

3% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
< 1% Idiomas no reconocidos

Nombre del documento: Tesis Katty Fuertes Gomez.pdf
ID del documento: c63869be6c7ae7b5624c458396f4d25f2fc95862
Tamaño del documento original: 2,61 MB

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

Número de palabras: 18.744
Número de caracteres: 124.172

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**Tesis completa Micaela Demera.pdf** | Tesis completa Micaela Demera El documento proviene de mi biblioteca de referencias	1%		Palabras idénticas: 1% (204 palabras)
2	ri.ues.edu.sv https://ri.ues.edu.sv/id/eprint/19556/1/TRABAJO-DE-GRADUACION-L-25-TRABAJO-FINAL.pdf 5 fuentes similares	< 1%		Palabras idénticas: < 1% (58 palabras)
3	**Tesis Chica_Uriarte (PDF) .pdf** | Tesis Chica_Uriarte (PDF) El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (53 palabras)
4	dspace.tdea.edu.co https://dspace.tdea.edu.co/bitstream/handle/tdea/3561/Informe Final.pdf?sequence=3	< 1%		Palabras idénticas: < 1% (44 palabras)
5	repository.unad.edu.co http://repository.unad.edu.co/bitstream/10596/34360/1/mneuta.pdf	< 1%		Palabras idénticas: < 1% (30 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	**Documento de otro usuario** El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (31 palabras)
2	**Proyecto Macías Josselyn - Muñoz Mary.pdf** | Proyecto Macías Josselyn - ... El documento proviene de mi grupo	< 1%		Palabras idénticas: < 1% (20 palabras)
3	**Documento de otro usuario** El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (18 palabras)
4	**repository.unad.edu.co** http://repository.unad.edu.co/bitstream/10596/56243/1/Aventurarmevaronap.pdf	< 1%		Palabras idénticas: < 1% (21 palabras)
5	**repository.ucc.edu.co** https://repository.ucc.edu.co/server/api/core/bitstreams/79b2af4a-9ec9-4b35-b655-1865857c87c5/...	< 1%		Palabras idénticas: < 1% (20 palabras)

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

1 https://www.ueees.edu.ec/

22-07-2024

Anexo 2 Reporte del sistema antiplagio

Entrevista al vicerrector de la Unidad Educativa Excelso Espíritu Santo

Anexo 3 Entrevista al vicerrector de la institución

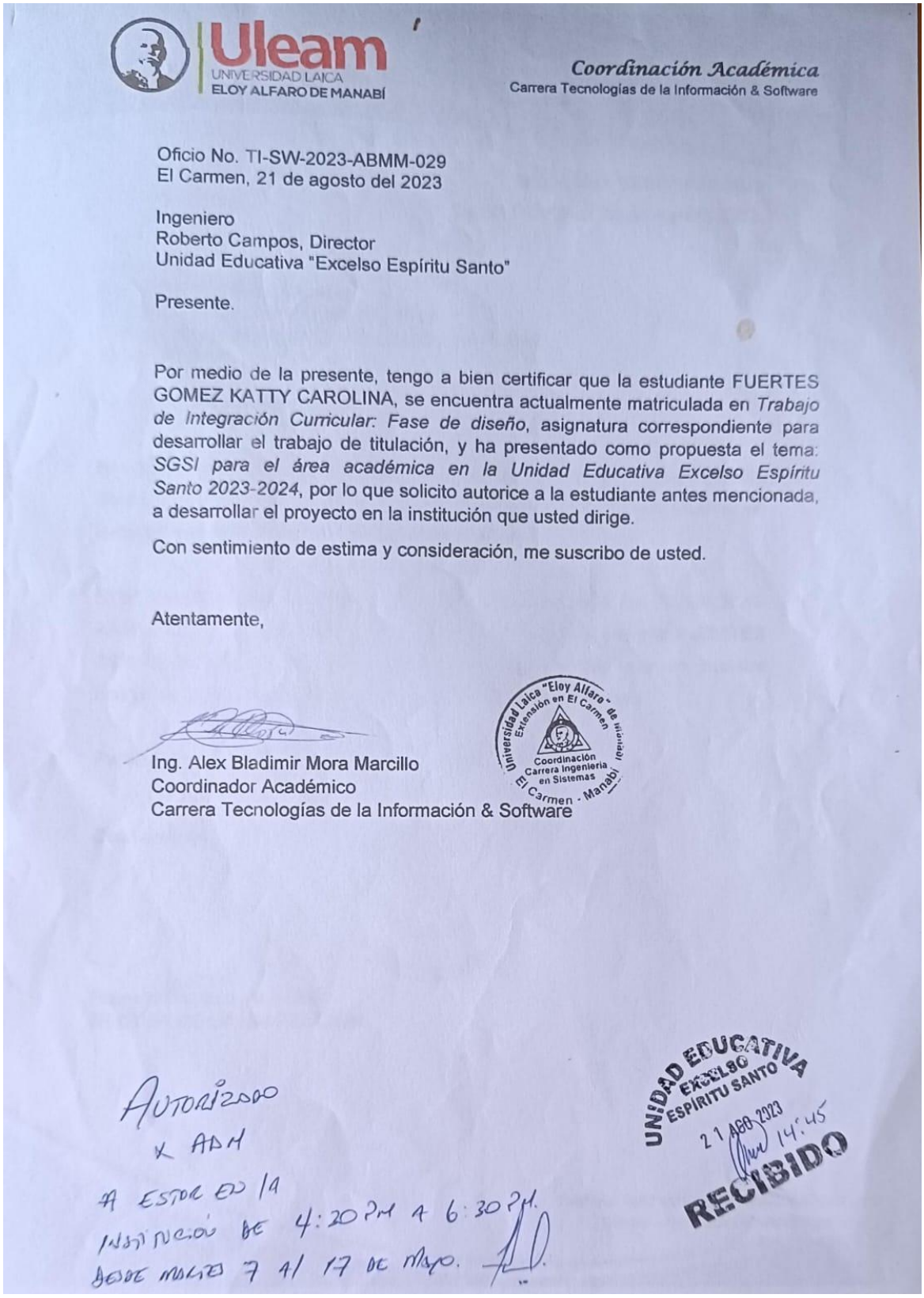
Encuestas a los docentes de la Unidad Educativa Excelso Espíritu Santo

Anexo 4 Encuesta a los docentes de básica de la institución

Anexo 5 Encuesta a los docentes de bachillerato de la institución

Anexo 6 Encuesta a los docentes de inicial de la institución

Oficio de ULEAM a la Unidad Educativa Excelso Espíritu Santo



Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Coordinación Académica
Carrera Tecnologías de la Información & Software

Oficio No. TI-SW-2023-ABMM-029
El Carmen, 21 de agosto del 2023

Ingeniero
Roberto Campos, Director
Unidad Educativa "Excelso Espíritu Santo"

Presente.

Por medio de la presente, tengo a bien certificar que la estudiante FUERTES GOMEZ KATTY CAROLINA, se encuentra actualmente matriculada en *Trabajo de Integración Curricular: Fase de diseño*, asignatura correspondiente para desarrollar el trabajo de titulación, y ha presentado como propuesta el tema: *SGSI para el área académica en la Unidad Educativa Excelso Espíritu Santo 2023-2024*, por lo que solicito autorice a la estudiante antes mencionada, a desarrollar el proyecto en la institución que usted dirige.

Con sentimiento de estima y consideración, me suscribo de usted.

Atentamente,

Universidad Laica "Eloy Alfaro" de Manabí
Extensión en El Carmen
Coordinación Carrera Ingeniería en Sistemas
El Carmen - Manabí

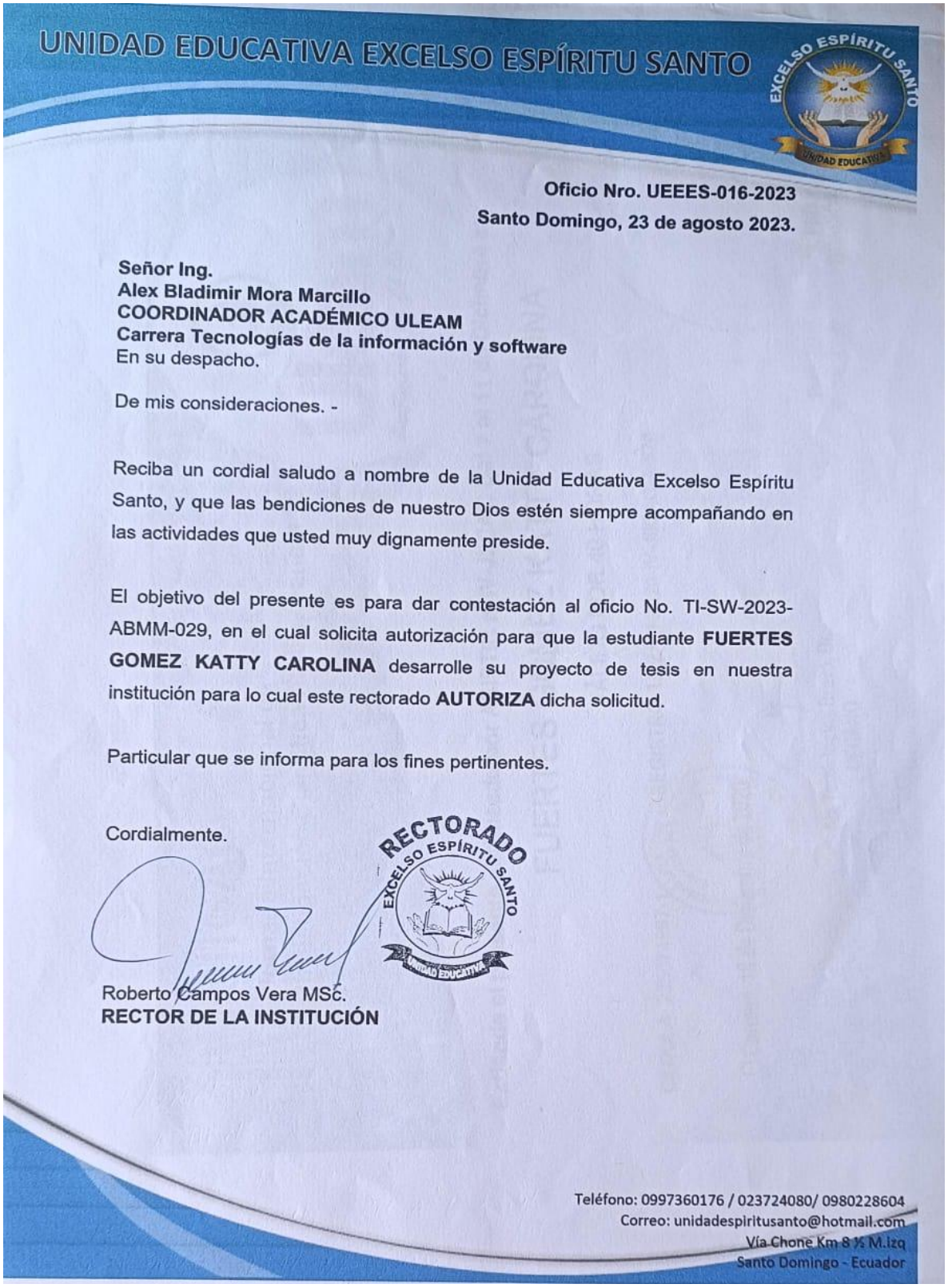
Ing. Alex Bladimir Mora Marcillo
Coordinador Académico
Carrera Tecnologías de la Información & Software

UNIDAD EDUCATIVA EXCELSO ESPÍRITU SANTO
21 AGO 2023
14:45
RECIBIDO

AUTORIZADO
X ADM
A ESTAR EN LA
INSTITUCIÓN DE 4:20 PM A 6:30 PM.
DESDE MAYO 7 AL 17 DE Mayo.

Anexo 7 Oficio de Uleam a la Unidad Educativa Excelso Espíritu Santo

Autorización de la Unidad Educativa Excelso Espíritu Santo



UNIDAD EDUCATIVA EXCELSO ESPÍRITU SANTO

Oficio Nro. UEEES-016-2023
Santo Domingo, 23 de agosto 2023.

Señor Ing.
Alex Bladimir Mora Marcillo
COORDINADOR ACADÉMICO ULEAM
Carrera Tecnologías de la información y software
En su despacho.

De mis consideraciones. -

Reciba un cordial saludo a nombre de la Unidad Educativa Excelso Espíritu Santo, y que las bendiciones de nuestro Dios estén siempre acompañando en las actividades que usted muy dignamente preside.

El objetivo del presente es para dar contestación al oficio No. TI-SW-2023-ABMM-029, en el cual solicita autorización para que la estudiante **FUERTES GOMEZ KATTY CAROLINA** desarrolle su proyecto de tesis en nuestra institución para lo cual este rectorado **AUTORIZA** dicha solicitud.

Particular que se informa para los fines pertinentes.

Cordialmente.

RECTORADO EXCELSO ESPÍRITU SANTO

Roberto Campos Vera MSc.
RECTOR DE LA INSTITUCIÓN

Teléfono: 0997360176 / 023724080/ 0980228604
Correo: unidadespiritusanto@hotmail.com
Vía Chone Km 8 ½ M.Izq
Santo Domingo - Ecuador

Anexo 8 Autorización de la Unidad Educativa Excelso Espíritu Santo

Glosario

A

Académica

Requisito de organizar y gestionar las acciones de los centros educativos, 9

Activos

Describe los controles para clasificar y salvaguardar de los activos de información, 48

Actuar

Los resultados de la comprobación se dirigue a buscar, corregir o prevenir algún inconveniente en la politíca, 13

Auditor

Tiene experiencia en realizar auditorías y la documentación, 16

Auditoría

Es un instrumento positivo que ayuda a identificar incapacidades enel sistema y detectar peligros, 16

B

Brechas

Es un método para evaluar el desempeño de los sistemas de información o programas de software para identificar si cumple las condiciones, 42

C

Comprobar

Es realizar un seguimiento y evaluación de los procesos propuestos en la seguridad, 13

Confidencialidad

Garantiza el ingreso solo a usuarios que sipongan el nivel de actualización, 14

Controles

Diferentes cláusulas que contiene diferentes aspectos de la seguridad de la información, 47

Criptografía

Describe los controles para el fucionamiento correcto, 48

Cumplimiento

Salvaguardar que la organización cumple todas las normas, 49

D

Disponibilidad

Coordina que el acceso a la información solo se puede ingresar y hacer el personal autorizado, 14

Documentación

Garantiza la realización positiva y mejorar las prácticas de seguridad de la información en una empresa, 14

E

Educación

Derecho a prepárarmps para un buen fufuro, 19