UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

PROYECTO INTEGRADOR

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

AUDITORÍA A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA ESCUELA BÁSICA HERIBERTO RODRÍGUEZ ANGULO

DEMERA MOREIRA MARÍA MICAELA

AUTORA

POZO HERNANDEZ CLARA GUADALPE

TUTOR

EL CARMEN, AGOSTO 2024

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 "Auditoría a la gestión de seguridad de la información en la Escuela Básica Heriberto Rodríguez Angulo 2023-2024", cuya autora es María Micaela Demera Moreira 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. Mora Marcillo Alex Bladimir Mg.
Presidente del tribunal de titulación

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

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

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

EXTENSIÓN EN EL CARMEN

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 **DEMERA MOREIRA MARÍA MICAELA**, 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 **"AUDITORÍA A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD EDUCATIVA HERIBERTO RODRÍGUEZ ANGULO"**

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, 23 de julio del 2024

Lo certifico,

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

DECLARACIÓN DE AUTORÍA

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: "Auditoría a la gestión de seguridad de la información en la Escuela Básica Heriberto Rodríguez Angulo", corresponde exclusivamente a: Demera Moreira María Micaela CI.1315417665 y los derechos patrimoniales de la misma corresponden a la Universidad Laica "Eloy Alfaro" de Manabí.

Autor

Demera Moreira María Micaela

CI.1315417665

DEDICATORIA

Dedico este trabajo de titulación principalmente a Dios, ya que gracias a el he podido llegar a este momento muy importante de mi vida, pudiendo así logra una meta más en mi vida profesional. Quiero tomar un momento para reconocer el esfuerzo, la dedicación y la pasión que he invertido en este proyecto de titulación, y así mismo dedicación y esfuerzo a lo largo de esta etapa universitaria. Cada página escrita, cada noche develada, cada lágrima y cada desafío superado son testigos de mi compromiso y mi determinación por alcanzar mis metas. Gracias a mí mismo por no rendirme, por mantener la fé en mis capacidades y por seguir adelante incluso cuando el camino parecía difícil.

A mi madre, María Beatriz Moreira Espinoza, por ser esa madre amiga que ha estado siempre a mi lado en lo momento más difíciles, apoyo condicional en cada fase de mi vida universitaria y ayudándome con la crianza de mi hijo. Así mismo, se la dedico de mi abuela Freya Esperanza Espinoza, por estar siempre presente y pendiente en mi vida y en la vida de mi hijo. Ella son las mujeres más importantes que tengo en mi vida, no sé qué haría sin ella. A mi hijo Angel David Velásquez Demera por haber llegado a mi vida en los momentos cuando más necesitábamos un ángel, por haberme enseñado lo hermoso que es ser madre, siendo mi fuerza siempre para no rendirme ya que él es quien me motiva día a día. A mi padre Pedro Antonio Demera Vera, por ser aquella persona que me financio económicamente mis estudios y por ser como un padre para mi hijo, y mi hermano Daniel David Demera Moreira por ser ese gran tío que adora a mi hijo.

Demera Moreira María Micaela

AGRADECIMIENTO

En primer lugar, quisiera agradecerla a mi padre Dios por haberme dado la vida y a sí mismo por haberme dado la fortaleza de permitirme haber estudiado la carrera de ingeniería en tecnología de la información y haberla culminando exitosamente. A si mismo deseo agradecerles a mis padres por haberme apoyado emocional y económicamente y así mismo por ser un pilar para mí y mi hijo durante este proceso académico, sin su apoyo este trabajo nunca se habría escrito, por lo cual este trabajo es también el suyo. También quisiera agradecerle a mi grupo de amigas que estuvieron desde el inicio hasta el final durante este proceso dándome un apoyo condicional.

También quisiera dar mi agradecimiento a mi tutora de tesis, que me acompañó durante este proceso de titulación a la Ing. Clara Pozo, sin ella no hubiera culminado estes proceso gracias por haberme dado esa oportunidad de aprender de usted y así mismo agradecerle por haberme tenido mucha paciencia durante este proceso. Gracias por la confianza depositada en mí.

Demera Moreira María Micaela

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

Como parte de este proyecto, se realizó una auditoría de gestión de seguridad en la Escuela Básica Heriberto Rodríguez Angulo, ubicada en el cantón El Carmen. El objetivo fue evaluar los problemas de seguridad existentes en la institución. Para sustentar el trabajo, se fundamentaron bibliográficamente los temas tratados. Se realizó una encuesta a los docentes y una entrevista al director Marco Antonio Caja, quien también es responsable del área informática de la escuela.

El propósito fue identificar si la institución cuenta con un reglamento para el uso del laboratorio, evaluar el estado de los equipos y verificar el cumplimiento de ciertos requisitos de seguridad. Se concluyó que los docentes están poco familiarizados con los requerimientos y controles de seguridad existentes en la institución. La propuesta incluyó la realización de una auditoría de seguridad en el área informática utilizando la metodología ISO 27001. Se aplicaron tres instrumentos: una evaluación de requisitos, un control de cumplimiento y un cuestionario de análisis de riesgos. Estos instrumentos permitieron identificar los riesgos y las carencias de políticas en la institución. Los resultados mostraron un bajo nivel de cumplimiento de los requisitos (17%) y de los controles (26%), lo que destaca la necesidad de mejoras significativas. Finalmente, se propuso la creación de un manual de gestión de seguridad informática. Este manual incluirá directrices para prevenir situaciones adversas, como posibles daños a los equipos de cómputo y condiciones ambientales que puedan afectar las instalaciones de la escuela.

ABSTRACT

As part of this project, a security management audit was conducted at Heriberto Rodríguez Angulo Elementary School, located in the canton of El Carmen. The objective was to evaluate the existing security issues within the institution. To support the work, the topics addressed were bibliographically founded. A survey was conducted among the teachers and an interview was held with Director Marco Antonio Caja, who is also responsible for the school's IT area.

The purpose was to identify whether the institution has a regulation for the use of the laboratory, to assess the condition of the equipment, and to verify compliance with certain security requirements. It was concluded that the teachers are not very familiar with the existing security requirements and controls within the institution. The proposal included conducting a security audit in the IT area using the ISO 27001 methodology. Three instruments were applied: a requirements evaluation, a control compliance assessment, and a risk analysis questionnaire. These instruments helped identify risks and policy deficiencies within the institution. The results showed a low level of compliance with the requirements (17%) and controls (26%), highlighting the need for significant improvements. Finally, the creation of an information security management manual was proposed. This manual will include guidelines to prevent adverse situations, such as potential damage to computer equipment and environmental conditions that may affect the school's facilities.

CAPÍTULO I

INTRODUCCIÓN

1.1 Introducción

La auditoría informática es un proceso que permite realizar evaluaciones y revisiones en el área de tecnología. En este caso, mediante esta auditoría el objetivo fue evaluar los equipos de cómputo y las instalaciones con las que cuenta la escuela básica Heriberto Rodríguez Angulo. A través de la auditoría, se evaluaron los procesos y políticas de seguridad de la institución educativa con el fin de identificar debilidades, riesgos, amenazas y áreas de mejora. El objetivo principal de este proyecto fue asegurar que las medidas de seguridad implementadas sean efectivas y adecuadas para la institución. En la auditoría de la gestión de seguridad implementada, se analizaron diversos temas como vulnerabilidades, amenazas, estrategias de seguridad, análisis y revisión posterior al incidente y plan de contingencia, entre otros temas.

Hasta el presente, se ha logrado encontrar libros de manera más eficiente sobre lo que es una auditoría informática y las ventajas que se obtienen al aplicarla. Para sustentar el trabajo realizado, fue necesario obtener fundamentos científicos y bibliográficos para tratar temas de suma importancia para este proyecto. Se aplicaron herramientas de recolección de datos, como encuestas y entrevistas, para recopilar información sobre el estado actual de la institución educativa. Se encuestó a los nueve docentes con los que cuenta actualmente la escuela básica Heriberto Rodríguez Angulo para determinar si conocen la existencia de los requisitos, controles y políticas de seguridad que debería tener el plantel educativo y para evaluar el estado actual de los equipos de cómputo. Luego, se entrevistó al director Marco Antonio Caja, quien también es el encargado del laboratorio, para verificar si se cumplen ciertos controles y políticas de seguridad en la institución y corroborar las respuestas de los docentes encuestados.

Como parte de la metodología, se realizó encuestas a los docentes y entrevistar al director, se pudo visualizar que los docentes de la institución están poco familiarizados con los requisitos y controles con los que cuenta el plantel educativo. Sabiendo el estado actual de la institución educativa, se propuso utilizar para este proyecto la metodología ISO 27001, ya que esta se centra en implementar controles y políticas de seguridad y permite evaluar e identificar los riesgos en la institución.

De acuerdo con la propuesta, se realizaron tres tipos de instrumentos para obtener datos más precisos y relevantes: el cuestionario de análisis de requisitos, el cuestionario de controles según las normas ISO 27001, y un cuestionario para el análisis de riesgos. Estos instrumentos se aplicaron al director Marco Antonio Caja.

Como resultado del cuestionario de cumplimiento de requisitos de control según las normas ISO 27001, se obtuvo que la institución educativa cumple con un nivel bajo de requisitos, con un 17% de cumplimiento, lo que deja una brecha del 83%. Uno de los requisitos con un 100% de brecha es el de mejora, ya que no existe ningún proceso o práctica que aborde este requisito. En el cuestionario de control, se obtuvo un 26% de cumplimiento, indicando un nivel bajo de controles de seguridad. Cuatro controles presentan un alto porcentaje de incumplimiento: relación con proveedores, adquisición, desarrollo y mantenimiento, criptografía y seguridad de recursos humanos, algunos de los cuales son responsabilidad del distrito de educación y no de la institución educativa. El control con mayor cumplimiento es el de organización de seguridad de la información, con un 71% de cumplimiento. En el instrumento de riesgo, se obtuvo un 45% de seguridad, lo que indica un nivel de riesgo significativo. El mayor riesgo identificado fue el de malware, con un 80% de riesgo, mientras que el área con menor riesgo fue la de incendio, con un 65% de seguridad.

Se llegó a la conclusión de que, para mejorar ciertas áreas, se debería implementar un manual de seguridad que contenga directrices claras para garantizar la protección y seguridad de los equipos de cómputo y su infraestructura. Este manual es esencial para implementar estrategias que eviten incidentes a corto o largo plazo y mitiguen ciertas amenazas o vulnerabilidades.

1.2 Presentación del tema

En Manabí- El Carmen se realizó una Auditoría a la gestión de seguridad de la información en la Unidad Educativa Heriberto Rodríguez Angulo.

1.3 Ubicación y contextualización de la problemática

En la Escuela Básica Heriberto Rodríguez Angulo, anteriormente conocida como la Escuela Fiscal Mixta U.N.E, ubicada en El Carmen, Manabí, en el km 36 de la vía Chone, en el barrio Santa Martha, hay 158 estudiantes y 9 docentes que trabajan en la jornada matutina. Hace

algunos años, se adquirieron equipos de computación y se agregó un laboratorio, ubicado junto a la oficina de dirección, con 20 máquinas destinadas al aprendizaje de los estudiantes. Sin embargo, debido a la falta de administración de los equipos, recursos económicos y mantenimiento, estos se han ido deteriorando con el tiempo, y actualmente solo funcionan 10 máquinas. En los últimos años, se ha observado un aumento de amenazas y riesgos para el laboratorio, lo que ha afectado significativamente las prácticas y el aprendizaje de los estudiantes dentro del laboratorio de computación.

1.4 Planteamiento del problema

1.4.1 Problematización

En la actualidad alrededor de mundo, la utilización de recurso tecnológicos en las instituciones educativas ha ido aumentando rápidamente, ya que ahora la tecnología es algo fundamental en nivel mundial y no tanto para la educación sino para diferentes ramas profesionales por ejemplos como para la administración de empresa, en el área de medicina y en el área de diferente tipo de industria, ya que este ayuda a optimizar las actividades de cada proceso, convirtiéndose en una herramienta valiosa.

Así mismo, la tecnología va evolucionando, trayendo consigo beneficios y contras, además de posibles riesgos que pueden provocar graves afectaciones. Es en este contexto donde entra en juego la auditoría de gestión de seguridad para evaluar los posibles riesgos a medio plazo. Para protegerse de estos riesgos y amenazas, es necesario que las instituciones implementen controles de seguridad. La auditoría de gestión de seguridad permite evaluar los niveles de seguridad.

1.4.2 Génesis del problema

Ecuador se caracteriza por ser un país rico en naturaleza y cultura, lo que lo convierte en un competidor comercial en varios ámbitos. Por esta razón, la tecnología es fundamental en el país, ya que ayuda a optimizar las actividades de cada proceso, facilitando y aumentando la eficiencia. La importancia de la tecnología se hizo especialmente evidente durante la pandemia de COVID-19, cuando surgieron numerosos problemas tanto en el ámbito educativo como en el laboral, afectando a diferentes áreas de trabajo a nivel mundial.

De igual manera, uno de los posibles riesgos es la pérdida de dispositivos o daños en los equipos debido al acceso no autorizado por parte de personas externas o incluso internas, como estudiantes o personal no autorizado. Otro riesgo es el uso indebido de los recursos, como el acceso a sitios web no autorizados o la descarga de contenidos ilegales, entre otros tipos de riesgos existentes.

1.4.3 Estado actual del problema

En la actualidad, la escuela básica Heriberto Rodríguez Angulo enfrenta diversos desafíos, como el deterioro de los equipos de cómputo, lo que disminuye su vida útil. Al mismo tiempo, es fundamental garantizar la implementación de medidas de seguridad. Existe una falta de auditoría de gestión de seguridad en la institución, lo que dificulta la identificación de los posibles peligros y amenazas. Además, la ausencia de auditorías de gestión de la seguridad puede complicar la identificación de áreas de mejora e impedir la implementación de acciones preventivas y correctivas adecuadas. Esto puede provocar una falta de preparación para emergencias y una respuesta inadecuada a los incidentes.

1.5 Diagrama causa – efecto del problema

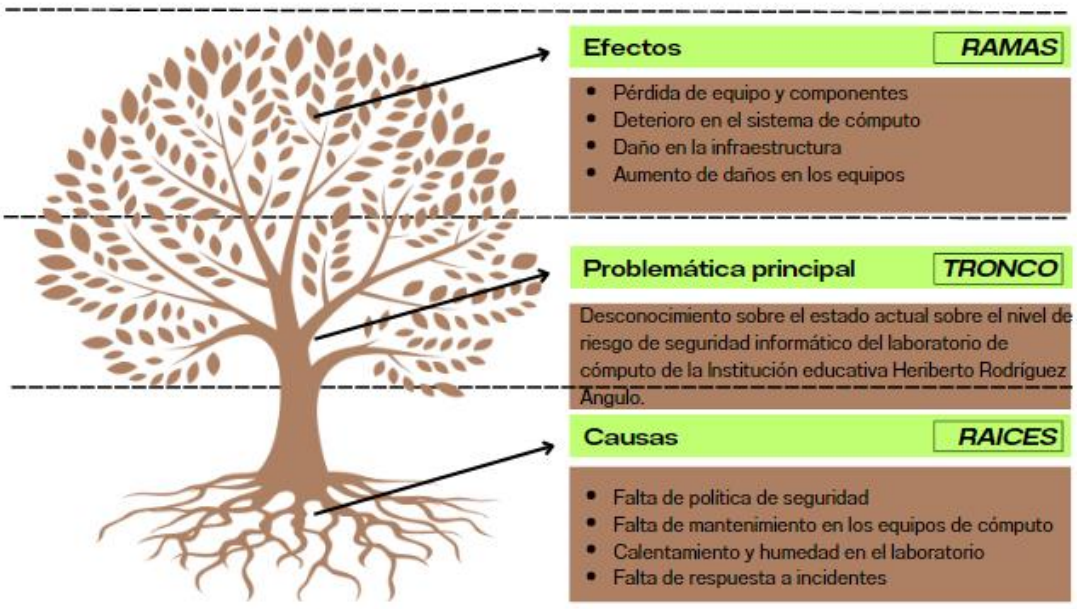


Ilustración 1: Diagrama causa efecto del problema

1.6 Objetivos

1.6.1 Objetivo general

- Elaborar una auditoría para la administración de seguridad de la información en la escuela básica Heriberto Rodríguez Angulo.

1.6.2 Objetivos específicos

- Identificar los posibles problemas que hay en el área informática de la unidad educativa Heriberto Rodríguez Angulo para definir el tema de titulación.
- Buscar diferente bibliografía o libros de las variables, para que sea justificado científicamente los temas de titulación**.**
- Diagnosticar la existencia del problema de seguridad en el área informática aplicando método y técnicas de investigación que justifique la existencia del problema.
- Evaluar los riesgos de seguridad del laboratorio de cómputo en la institución Heriberto Rodríguez Angulo aplicando las Normas ISO 27001.
- Elaborar un informe de auditoría con los resultados obtenidos de la investigación realizada, para identificar medida de seguridad y eficiencia en el área informática.

1.7 Justificación

La seguridad es importante en diferentes áreas, no solo en la educativa, sino también en la empresarial y otras áreas. La gestión de seguridad informática busca proteger la integridad de muchas industrias o empresas y, por tal razón, está sujeta a regulaciones normativas de seguridad. Además, la gestión de seguridad se enfoca en la planificación para situaciones de crisis, como desastres naturales, daños y pérdidas de equipos, entre otras situaciones.

Las razones, que justifica la presente investigación son las siguientes: Al hacerse énfasis en, la institución nunca antes se elaboró una auditoría de seguridad la cual la institución tiene la disposición y necesidad de conocer sobre la gestión de seguridad, para saber los problemas de seguridad y amenaza que se encuentra dentro de la institución Heriberto Rodríguez Angulo en el área informática, para que de esta manera pueda aportar con un diagnóstico eficiente, basándose en la realidad de la situación actual de la institución para que así vaya mejorando la

seguridad y poder prevenir posibles incidentes entre otros. La auditoría en gestión de seguridad ayudará a identificar los posibles riesgos y amenaza permitiendo implementar medidas preventivas para evitar incidentes, para así garantizar un entorno seguro para la institución.

1.8 Impactos esperados

1.8.1 Impacto tecnológico

La unidad educativa tiene que ir actualizándose con las tecnologías y avece es necesario implantarla en cuestiones de seguridad por ejemplo se podría implementar un sistema de seguridad digitalizado y automatizados como cámaras de vigilancia, sistemas de control de acceso y alarmas. Este sistema le permite monitorear eventos relacionados con la seguridad de la institución, como posibles robos o incidentes de seguridad. El impacto de esta tecnología sería significativo, ya que mejoraría la seguridad en la institución al proporcionar una vigilancia constante y una respuesta más rápida ante cualquier incidente.

1.8.2 Impacto social

Con la auditoría de gestión de seguridad, se pueden identificar y corregir posibles riesgos y vulnerabilidades. Al sugerir recomendaciones y medidas de seguridad evaluada, se mejoraría la seguridad en el área de informática protegiendo así los equipos de cómputo de la unidad educativa la cual logra un impacto positivo en la comunidad educativa al proporcional un ambiente más seguro al momento de que los estudiantes adquiera conocimientos informáticos y así promueve un mejor rendimiento académico mejorando la calidad de enseñanza y la eficiencia en la gestión de la unidad educativa.

1.8.3 Impacto ecológico

Al realizar una auditoría de gestión, se proponen medidas de mejora porque, al llevar a cabo la auditoría de gestión de seguridad, se evalúan los posibles inconvenientes que hay en la institución. Por ejemplo, se pueden identificar los posibles daños en los equipos de cómputo causados por un consumo muy alto de energía. Al corregir este problema, se puede reducir el consumo de energía y contribuir al medio ambiente. Otra manera de contribuir al medio ambiente es mediante la adecuada eliminación de equipos de cómputo obsoletos o innecesarios. Al establecer un plan de gestión de residuos electrónicos, se puede garantizar que estos

materiales sean reciclados o eliminados de manera segura, evitando la contaminación del suelo y del agua, y contribuyendo a la conservación del medio ambiente. Al realizar la auditoría y proponer medidas de mejora, se genera conciencia sobre la importancia de la gestión de seguridad y el impacto ambiental.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Antecedentes históricos

2.1.1 Antecedentes históricos de Auditoría Informática

A comienzos del siglo XX, la profesión de auditoría experimentó un crecimiento significativo y su demanda se expandió por toda Inglaterra, extendiéndose posteriormente a Estados Unidos durante este proceso, se sentaron las bases de las auditorías modernas, aunque se puso menos énfasis en la detección y prevención del fraude, relegándolas a un segundo plano y restándoles cierta importancia. En el año 1940, las auditorías tenían como objetivo principal examinar las posiciones financieras de las empresas, así como de sus socios y clientes, con el fin de establecer metas económicas basadas en estos análisis (LaEdu, 2021).

La auditoría se originó en el siglo XVII y consistía en escuchar fue reconocida como una profesión por primera vez en la Ley de Sociedades Británicas en 1862, y su reconocimiento general ocurrió durante el período de 1862 a 1905, cuando la profesión de auditoría en Inglaterra creció y prosperó. Alrededor de 1900, la auditoría se introdujo en los Estados Unidos con el objetivo principal de auditar los estados financieros y los resultados operativos. La auditoría informática surgió en 1960, cuando las primeras organizaciones comenzaron a utilizar sistemas informáticos. A medida que la tecnología de la información se volvió más importante y compleja, se hizo evidente la necesidad de tener un enfoque estructurado para evaluar y controlar los sistemas informáticos (Davila, 2018).

2.1.2 Antecedentes históricos de Gestión de Seguridad

En estos tiempos modernos, la información se ha convertido en el activo más preciado para las empresas. El avance de la informática y las redes de comunicación muestra una realidad diferente, donde los objetos físicos ahora existen como datos digitales, ocupando un espacio en otra dimensión y adquiriendo formas distintas a las originales. Sin embargo, su valor no se ha perdido, e incluso en ocasiones puede llegar a ser aún mayor. La importancia de la seguridad informática radica en su influencia directa sobre gobiernos, instituciones, compañías y personas individuales (Granados, 2012).

La base de la seguridad informática se creó en 1980. El Monitoreo y vigilancia de amenazas a la seguridad informática define los principales factores de las amenazas informáticas como "ataque" o "vulnerabilidad". El 30 de noviembre está declarado Día Internacional de la Seguridad de la Información desde 1988, y su propósito es dar a conocer sobre su significado de la seguridad de la información, su entorno y lo más importante su sistema(Delgado, 2017).

2.2 Revisión de investigaciones previas sobre el tema abordado

- En la investigación posteriores de los autores Rosales Montalbán, Martelo Gómez y Franco Borréet (2020) **" Diseño de una solución de gestión de seguridad informativa para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit".** Se diseñó un Sistema de Gestión de Seguridad de la Información (SGSI) para una institución educativa en Cartagena, Colombia, aplicado al proceso administrativo de gestión de infraestructura tecnológica. Este proyecto permitió identificar los activos que la organización debe considerar para implementar un sistema de gestión que cumpla con sus políticas, utilizando la norma ISO 27001 y la metodología MAGERIT. Se llevaron a cabo evaluaciones de riesgos, las cuales incluyeron la caracterización y valoración de los activos, así como la identificación de amenazas y las salvaguardas necesarias para la gestión de la infraestructura de la institución. Además, se presentaron mecanismos de protección específicos.
- **“Auditoría de sistemas informáticos en la Unidad Educativa 'Isabel de Godín' de la ciudad de Riobamba, provincia de Chimborazo, durante el período 2018”,** Fue un estudio práctico, de campo y documental. Además, se realizó una encuesta a docentes, técnicos y estudiantes de igual forma entrevistar al director de la institución para obtener información importante sobre el uso, seguridad y estado de los recursos informáticos. En conclusión, se evidenció a través de las técnicas de auditoría que no se evidenció que no siguieron las normas de la Contraloría General Estatal, especialmente en el área de tecnologías de la información y las comunicaciones, porque el nivel de riesgo era alto (González, 2019).
- **“Auditoría Informática a la Unidad Educativa General Antonio Elizalde Bucay, del cantón Bucay”,** provincia del Guayas, período 2019 y publicado en el año 2020 en su tema de investigación se establece que no existe una planificación documentada de cómputo, que permita controlar las actividades y proyectos desarrollados durante un período de tiempo determinado, de tal manera que se pueda evaluar su conformidad

y gestión. Su principal objetivo es dar la recomendaciones o medidas preventivas y correctivas a dichos problemas. (Castillo, 2020)

- **“Estado actual de la auditoria de seguridad en los sistemas de información de educación superior”** la metodología que se implantó en esta investigación la norma ISO 27001 e ISO 270002, las cuales tienen como objetivo garantizar la seguridad de los sistemas y optimizar los controles con el propósito de salvaguardar sus datos teniendo siempre presente la integridad, disponibilidad y confiabilidad la que se busca minimizar los riesgos mediante el uso de técnicas y acciones existentes. Mena et al, (2020)
- **"Diseño se desarrolló una directriz de seguridad de la información para el área de TICS de la Instituto Tecnológico Superior Central Técnico, basado en la norma de seguridad ISO/IEC 27002:2013"**, presentado en la Universidad Internacional Sek, Facultad de Arquitectura e Ingenierías, para optar al grado de Máster en Tecnologías de la Información con Mención en Seguridad en Redes y Comunicación. Este proyecto propone la implementación de medidas para mejorar el control de las amenazas que puedan comprometer las dimensiones de la seguridad de la información. Para identificar y evaluar las vulnerabilidades y amenazas a las que está expuesta la institución, se utilizó la metodología MAGERIT para generar una matriz de riesgos. Se analizó la norma internacional ISO/IEC 27002:2013, que permite gestionar la TI en cualquier tipo de organización. (Cevallos, 2019)

2.3 Definiciones conceptuales

Los subtemas de la variable Auditoria de la informática y la variable de la Gestión de seguridad, permite analizar y comprender de un modo más amplio de que se quiere llegar a tratar con la investigación de la auditoría, desglosando y así mismo examinando cada una de las variable de modo individual, para así luego sacar cada subtema teniendo en cuenta la definición de las variables para así poder relacionarla con el tema de nuestra investigación, ya que proporcionará una base sólida para establecer la relevancia y la originalidad del trabajo proveyendo una base teórica.

2.3.1 Auditoría Informática

2.3.1.1 Auditoría

La auditoría desempeña un papel crucial en la toma de decisiones empresariales al revelar deficiencias, prevenir errores y facilitar ajustes que impulsan la mejora continua y la competitividad de la organización en el mercado (Montesdeoca, 2020).

La auditoría implica una revisión detallada de las actividades, registros y operaciones de una persona u organización. Su objetivo principal es verificar el correcto funcionamiento de los procedimientos y controles internos, así como garantizar el cumplimiento de todas las normativas y regulaciones aplicables. Además, la auditoría puede identificar áreas de mejora y proporcionar recomendaciones para mejorar el rendimiento y la eficiencia de la entidad auditada (Alvarez, 2023).

2.3.1.2 Beneficio de la Auditoría

Según el autor Velastegui (2019) opina que control de los hechos pasados ayuda a las empresas a identificar oportunidades de mejora e implementar cambios necesarios en su estrategia y operaciones. Al ejercer un control sobre los hechos pasados es esencial para el éxito a largo plazo de cualquier empresa, se necesita una gestión efectiva para tomar decisiones y por ende, lograr rentabilidad. Los beneficios de la auditoria son reconocer los posibles riesgos de la entidad, detectar sus puntos débiles, generar confianza en los miembros de la empresa, prevenir desvíos y errores y desarrollar una mejora continua en una institución. Por lo tanto, realizar una auditoría es de gran beneficio para todas las comunidades, entre los más importantes para su desarrollo y crecimiento.

2.3.1.3 Clasificación de la Auditoría

Según los autores Chávez Tisalema, Steven Alexander (2022) la auditoría puede desarrollarse en un enfoque determinado, el auditor cuenta con un amplio campo de posibilidades para alcanzar su objetivo, dicho autor cree que se clasifica la auditoria por Auditoría Interna, Auditoría Externa, Auditoría Financiera, Auditoría Administrativa, Auditoría Gestión, Auditoría Integral, Auditoría Cumplimiento, Auditoría Informática o de Sistema.

2.3.1.4 Auditoría informática

Una auditoría informática es un proceso que permite evaluar y medir si un sistema de seguridad de la información implementado si está realizando sus tareas correctamente, permitiéndole resaltar y corregir posibles incidencias. Esto permite tomar las medidas adecuadas para minimizar el riesgo de materializar de una vulnerabilidad tomando medidas para eliminar o minimizar esos riesgos, a veces incluso aceptando el riesgo. También permite garantizar el cumplimiento de las leyes, regulaciones y procedimientos obligatorios para proteger los activos. (Menéndez, 2022)

2.3.1.5 Importancia de la Auditoria informática

Las auditorías informáticas son cruciales porque permiten identificar las fortalezas y debilidades de los sistemas de información de las organizaciones. Además, aseguran que se cumplan las normativas y regulaciones aplicables, protegiendo a la organización de posibles sanciones. También ofrecen recomendaciones valiosas para mejorar la seguridad y eficiencia operativa, contribuyendo así a la continuidad y sostenibilidad del negocio o institución. (Arcentales et al, 2017)

La importancia de realizar auditorías de manera periódica radica en su enfoque preventivo y proactivo, ya que se lleva a cabo un análisis exhaustivo de la seguridad de la empresa y se toman acciones en función de los resultados obtenidos (Alvarez, 2023). La tecnología de la información y el desarrollo de la tecnología de la información mejoran día a día, lo que a su vez causa problemas en el desarrollo de oportunidades y conduce a errores. Para que esto no suceda, es necesario revisar y revisar los proyectos, que es tarea del control, para garantizar un mejor trabajo de control para la sociedad. (González K. , 2018)

2.3.1.6 Objetivo de la Auditoría informática

- El tema de la definición de los objetivos de la auditoría informática es difícil y complejo. No hay un consenso total sobre cómo definir estos objetivos y, por lo tanto, sobre las funciones que debe desempeñar un auditor informático. (Agilar, s.f.)
- El objetivo es asegurar la eficiencia de los sistemas informáticos mediante la verificación del cumplimiento de las normas internas de la organización. También se

busca revisar la gestión efectiva de los recursos humanos y tecnológicos que tiene la organización. (Denny María Cobeña Bravo, 2021)

- Evaluar el desempeño de los activos de computó, se utilizan índices de desempeño para medir su rendimiento, utilizando herramienta permita identificar posibles problemas y proponer soluciones viables. Al finalizar el proceso, se elabora un informe técnico que incluye conclusiones y recomendaciones. (Izquierdo, 2020)

2.3.1.7 Control Interno

La entidad lleva a cabo un proceso interno con el fin de proporcionar normas y políticas establecidas y previene riesgos y amenazas que puedan afectar la consecución de los objetivos. También supervisa el cumplimiento de las normas y políticas establecidas y previene cualquier riesgo o amenaza que pueda perjudicar el logro de los objetivos., supervisando el cumplimiento de los estándares y normas establecidas. Para lograr esto, el control interno informático se encarga de establecer políticas y procedimientos, así como de realizar pruebas y evaluaciones para identificar posibles riesgos y debilidades en la organización. Además, se encarga de monitorear y supervisar el cumplimiento de los controles establecidos, y de implementar medidas correctivas en caso de detectar alguna falla o vulnerabilidad. En resumen, el control interno informático es fundamental para garantizar la confiabilidad y seguridad de la informática. Las informaciones obtenidas de los mecanismos implantados por cada responsable deben ser correctas y válidas (Erazo et al, 2020).

2.3.1.8 Objetivo del Control Interno

Los objetivos del control interno para el autor Erazo (2020) fueron los siguientes:

- Verificar que todas las actividades se lleven a cabo de acuerdo con los procedimientos y normas establecidas.
- Colaborar y apoyar en el trabajo de auditoría informática, así como en las auditorías externas al grupo.
- Definir, implementar y ejecutar mecanismos y controles para asegurar que se alcancen los niveles adecuados de servicio informático.
- Asegurar la seguridad y confidencialidad en el área informática.

2.3.1.9 Fase de la auditoría informática

Los autores Chávez Tisalema, Steven Alexander (2022) creen que la auditoría informática, al igual que cualquier otra auditoría, debe llevarse a cabo en 4 fases principales, las mismas incluyen todas las etapas requeridas para alcanzar el informe de auditoría con precisión. Es fundamental contar con información precisa y confiable para lograr resultados duraderos, adecuados y efectivos. Las fases de la Auditoría son: Planificación, preliminar y específica, Evaluación de control interno, Evaluación de área críticas, Comunicación de recurso.

2.3.2 Gestión de Seguridad

2.3.2.1 Concepto básico de Gestión de Seguridad

Se basa en un enfoque de riesgo empresarial para crear, implementar, operar, monitorear, auditar, mantener y mejorar la seguridad empresarial. Según la definición publicada en la norma NTC ISO 27000, consta de las políticas, procedimientos, lineamientos y recursos y actividades relacionados que una organización gestiona de manera colectiva para proteger sus activos de información; También puede entenderse como un enfoque sistemático para crear, implementar, utilizar, monitorear, controlar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales; basado en el análisis de riesgos de la organización y los niveles de aceptación de riesgos diseñados para abordar y gestionar eficazmente los riesgos. (Hurtado et al, 2022)

2.3.2.2 Análisis de riesgos e impactos

Según el autor (Palacios, 2020) menciona que, para empezar, es importante identificar los posibles daños o peligros para luego poder definir las medidas que debemos tomar. Es importante tener en cuenta varios factores al evaluar la seguridad de los activos: el valor de los activos, la frecuencia de amenazas y su desconocimiento, la secuencia de daño, la eficiencia de las medidas de seguridad y su costo.

El **análisis de riesgo** puede ser realizado por personal interno o externo, utilizando una metodología previamente diseñada para este propósito. Entre las conocidas se encuentran

Magerit (Metodología de Análisis de Riesgo de los Sistema de Información de las Administraciones Pública), Marion, Mehari, modelo de McCumber, y muchas más.

El **impacto** es una consecuencia desfavorable que una organización sufre cuando una función se detiene, lo que requiere tiempo para recuperarse y evitar la paralización completa. El impacto puede causar daños que varían en su grado de gravedad. En el análisis del impacto, el objetivo es identificar todas las funciones críticas y dar prioridad a las estrategias de recuperación para reducir al mínimo el tiempo de recuperación.

2.3.2.3 Análisis y Evaluación del Riesgo

Según el autor (Sánchez , 2019) considera a las fases metodológicas que deben desarrollarse para la implementación de un proyecto. la gestión de activos es fundamental para garantizar el éxito y la eficiencia de una organización desde la recopilación de datos hasta la evaluación de la magnitud de las amenazas, son las siguientes:

- Identificación de activos de información
- Tasación de activos de información
- Identificación de amenazas y posibilidades de ocurrencia
- Identificación de vulnerabilidades y posibilidades de ser explotada por las amenazas
- Estimación de la explotación al riego de los activos de la información
- Priorización de las amenazas por su exposición al riesgo

2.3.2.4 Vulnerabilidades

Según el autor Tigse (2020) las vulnerabilidades son debilidades en un sistema informático y en el entorno laboral. Por sí solas, la presencia de una o varias vulnerabilidades no causan daño, ya que es necesario que exista una amenaza para ocasionar problemas en una empresa. Por lo tanto, si una vulnerabilidad no tiene ninguna amenaza asociada, no será necesario implementar un control.

Las áreas susceptibles de presentar vulnerabilidades son:

- **Organización:** Se ve afectado porque es un lugar físico donde trabajan un conjunto de personas, ya sean internas o externas.

- **Ambiente:** El entorno se verá impactado negativamente si no se respetan a los alineamientos para asegurar un espacio estable y protegido contra amenazas.

- **Hardware y Software:** Al escoger el tipo de tecnología utilizar en las operaciones de la empresa, es importante considerar tanto la seguridad que proporciona como los beneficios que se obtienen al emplearla.

2.3.2.5 Amenaza

Cuando los activos como la información, la TI u otros son amenazados, no sufren el mismo nivel de impacto en todas sus dimensiones. Así que, una vez que se ha establecido que una amenaza tiene el potencial de causar daño a un activo, es necesario evaluar la vulnerabilidad de dicho activo en dos aspectos: 1) la degradación, que determina qué tan perjudicado resultaría el activo, ya que toda reparación o sustitución de un activo dañado conlleva un costo y 2) la frecuencia, que indica con qué frecuencia se materializa la amenaza. Después, se deberá identificar cuáles son las potenciales amenazas que podrían comprometer la integridad de los activos de la empresa y ocasionar un impacto significativo. (Jacinto, 2017)

2.3.2.6 La Norma ISO 27001

La familia ISO/IEC 27000 fue creada en conjunto por la ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional). Estas directrices y normas están vinculadas a la seguridad en el ámbito de las Tecnologías de la Información en el campo de la seguridad. Se trata de un patrón internacional que se centra en la gestión integral de la seguridad de la información en organizaciones de cualquier sector. La finalidad de ISO 27001 es proteger la privacidad, integridad y disponibilidad de la información en una organización, asegurando la seguridad de su activo más importante. (Mamani, 2020)

2.3.2.7 Seguridad de Hardware

La protección y seguridad de los componentes físicos de un sistema informático. Esto incluye el mantenimiento de la integridad de los dispositivos y la prevención de cualquier acceso no autorizado o daño físico a los mismos. La seguridad de hardware es esencial para garantizar el correcto funcionamiento y protección de la información almacenada y procesada en un sistema. Algunos ejemplos de medidas de seguridad de hardware incluyen el uso de sistemas de bloqueo físico, la protección contra sobrecargas eléctricas y la implementación de controles de acceso físico a los dispositivos. todos los equipos y dispositivos físicos sean seguros y confiables.

Se garantiza que un sistema informático esté protegido contra posibles amenazas. Esto implica evaluar regularmente los sistemas para garantizar que estén actualizados y protegidos contra amenazas externas. También se diría que este tipo de seguridad abarca una amplia gama de medidas y estrategias para proteger los activos digitales y mantener la integridad de los sistemas. (Londoño, 2020)

2.3.2.8 Plan de Gestión de Seguridad Informática

El plan de gestión de seguridad es una estrategia detallada para garantizar la protección de la información y los activos de una organización. Este plan abarca todos los aspectos relacionados con la seguridad, incluyendo la identificación de los riesgos potenciales, la implementación de medidas de protección, la respuesta a incidentes de seguridad y la Promover del negocio. Un plan de gestión de seguridad informática incluye diferentes componentes, como la identificación y evaluación de los activos de información, la identificación y evaluación de los riesgos, la implementación de controles de seguridad, la gestión de incidentes de seguridad y la formación y concienciación del personal, además también debe incluir la elaboración de políticas y procedimientos de seguridad, así como la asignación de responsabilidades en materia de seguridad. (Bautista, 2021)

Para desarrollar un plan de gestión de seguridad informática efectivo, es necesario realizar un análisis exhaustivo de lo que se desea proteger, esto implica identificar los posibles riesgos y amenazas que pueden afectar a los activos, evaluar su impacto potencial y definir las medidas de seguridad adecuadas para mitigarlos, una vez implementado el plan de gestión de seguridad informática, es importante llevar a cabo auditorías periódicas para garantizar su eficacia y

realizar las actualizaciones necesarias en función de los cambios del entorno tecnológico y de las nuevas amenazas que puedan surgir. (Huamani, 2021)

Es fundamental establecer un plan de acción y protocolos de seguridad bien definidos, lo cual implica identificar y evaluar los riesgos y amenazas potenciales que enfrenta la organización, así como implementar medidas preventivas y correctivas adecuadas. El plan de gestión de seguridad debe incluir un plan de respuesta a incidentes, que detalle los pasos a seguir en caso de una violación de seguridad. También se deben establecer acciones para garantizar la continuidad del negocio en caso de un desastre o emergencia. Para asegurar la seguridad informática de una organización, es vital establecer una estructura organizativa sólida, implementar políticas y protocolos de seguridad efectivos, comunicar y hacer cumplir estas políticas, y contar con sistemas de monitoreo y detección de incidentes. Además, es importante promover la conciencia sobre el uso responsable de los recursos informáticos y la importancia de mantener los sistemas actualizados y protegidos. (Bautista, 2021)

Con referencia, a llevar a cabo evaluaciones periódicas de seguridad informática, implica realizar pruebas de vulnerabilidad y auditorías para identificar posibles brechas de seguridad. En caso de que ocurra un problema o incidente informático, es esencial contar con procedimientos establecidos para manejar la situación de manera efectiva. Esto incluye la creación de un plan de respuesta a incidentes y la designación de un equipo responsable de gestionar y resolver los problemas. (Moposita, 2020)

2.3.3 ISO 27001

La metodología de las normas ISO 27001 tiene como objetivo detectar vulnerabilidades y aplicar un plan de seguridad. Se basa en identificar activos de información, evaluar riesgos, implementar controles de seguridad y monitorear continuamente para proteger la organización. (Geovanny, 2021)

La norma ISO 27001 es aplicable a cualquier tipo de organización, independientemente de su objetivo económico, tamaño o carácter público o privado. Es elaborada por expertos en la materia y proporciona una metodología para llevar a cabo la administración de la seguridad de la información en una organización. Además, permite que cualquier tipo de organización obtenga la certificación correspondiente, lo que significa que una entidad independiente ha

confirmado que se ha implementado la seguridad de la información en cumplimiento con las normas ISO 27001. Esta norma se ha convertido en la principal a nivel mundial para la seguridad de la información, y muchas empresas han obtenido su certificación. (Cuervo Alvarez, 2017)

Según el autor Alejandro Rivero (2019) estable que la norma ISO 27001 cumple con 4 fase que se base en ciclo de mejorar continua que son las siguientes:

- Planificación
- Ejecutar y gestionar los procesos establecidos en la fase de planificación.
- Fase de control de verificación
- Actuación, mantenimiento y mejora

2.4 Conclusiones del marco teórico

La auditoría informática es vital para garantizar la seguridad y gestión efectiva de la información en un entorno empresarial en constante evolución. La implementación de estándares y la adopción de enfoques estructurados para evaluar y controlar los sistemas informáticos son pasos esenciales para garantizar la seguridad de la información en las organizaciones. La realización de auditorías informáticas periódicas es fundamental para evaluar la efectividad de los sistemas de seguridad de la información y para identificar posibles vulnerabilidades. Estas auditorías no solo permiten detectar y corregir incidentes, sino que también brindan una visión clara de las fortalezas y debilidades del sistema de información de una organización. Además, la importancia de proteger los activos de información y garantizar la confidencialidad, disponibilidad e integridad de la información se destaca como un objetivo fundamental.

CAPÍTULO III

3 MARCO INVESTIGATIVO

3.1 Introducción

La seguridad es importante en cualquier establecimiento, y las instituciones educativas tanto públicas como privada, no son las expresiones. En este sentido, la evaluación es una herramienta súper que importante en este proyecto ya que por medio de ella permitirá ver resultado de problemas reales que se encuentra dentro de las instituciones educativas que en este caso es la institución educativa Heriberto Rodríguez Angulo.

Dentro de ese marco, el presente trabajo se presenta resultado obtenidos a partir de investigación cuantitativa, cualitativa, descriptiva y bibliográfica sobre existencia de reglamentos y controles de seguridad al momento que se refiere a los equipos de cómputo que se encuentra dentro de la institución educativa, también se obtendrá resultado sobre las causas de infecciones de virus dentro de los equipos y así mismo la falta de mantenimiento que hay dentro de la misma.

En cuanto, a los métodos que se utilizaron dentro de esta investigación fueron dos que son el método de investigación de campo y el método de análisis de brecha. En el método de investigación de campo, permitió visualizar las vulnerabilidades que cuenta la institución educativa Heriberto Rodríguez Angulo analizando así la falta de seguridad referente en el área informática, en cambio el otro método que es el de análisis de brecha la cual este método permitió ver es estado actual de seguridad que cuenta en el área informática y el estado deseado que debería tener.

Para lograr la recolección de la información las herramientas que se utilizaron fueron la encuesta y entrevista la cual las encuesta fueron dirigidas a los 8 docente de la institución educativa Heriberto Rodríguez Angulo y la entrevista fue exclusivamente para el director ya que en este caso no hay laboratorista ya que el mismo director se encarga de esa área. Lo temas que se analizaron en la encuesta y entrevista fue sobre la existencia de los reglamentos y controles que de seguridad informática incluyendo la medida suficiente para la protección de daños ambientales en los equipos de cómputo que se cuenta en la institución educativa entre otros temas que se incluyó en los materiales de recolección de la información.

3.2 Tipos de investigación

3.2.1 Investigación cuantitativa

La base del enfoque cuantitativo radica especialmente en utilizar técnicas matemáticas y recursos estadísticos para recolectar, analizar e interpretar datos con el objetivo principal de satisfacer preguntas investigativas específicas e indagar sobre hipótesis planteadas. Se pone el foco en la observación, medición, muestreo y tratamiento estadístico de las unidades de análisis. Tienes confianza en la precisión de las mediciones realizadas con diferentes variables e instrumentos (Palacios et al, 2023).

En el contexto de la auditoría en el manejo de la seguridad de la información en la escuela básica Heriberto Rodríguez Angulo, requiere obtener datos numéricos, así como realizar análisis estadísticos adecuados.

3.2.2 Investigación cualitativa

La investigación cualitativa se centra en reconstruir la realidad según la percepción de los participantes en un sistema social específico. Este enfoque es flexible y se adapta a los eventos para interpretar los datos de manera adecuada y desarrollar teorías pertinentes. Su metodología se basa en la recopilación de información no numérica, utilizando principalmente descripciones y observaciones (Escudero , 2017).

La investigación cualitativa se pudo implicar la realización de entrevistas en profundidad con el personal docente para comprender sus percepciones, actitudes y experiencias en relación con la seguridad de la información en la Unidad Educativa. La investigación cualitativa también se pudo implicar en el análisis de documentos, como políticas internas, planes de seguridad, y otros materiales para comprender el contexto y los procesos relacionados con la gestión de seguridad de la información en la institución.

3.2.3 Investigación descriptiva

La labor principal en la investigación descriptiva consiste en describir y analizar minuciosamente el estado actual del problema investigado. El fundamental radica en brindar una perspectiva clara y exhaustiva sobre los individuos involucrados o el tema objeto del

estudio para así lograr una mejor comprensión tanto del comportamiento como las características específicas relacionadas al mismo. Para realizar esta La investigación se utiliza diversos métodos de recolección de datos, entre ellos las encuestas, la observación directa y las entrevistas. Esto permite recabar información detallada acerca del tema investigado. (Nieto, 2022)

La finalidad principal de este estudio se llevó a cabo una investigación descriptiva detallada acerca del control y protección de activos en la Unidad Educativa, con el fin de comprender a fondo el manejo que se hace respecto a la seguridad informática, esta investigación descriptiva busca proporcionar una descripción minuciosa y exacta sobre cómo se lleva cabo este proceso dentro del contexto específico de la Unidad Educativa Heriberto Rodríguez Angulo, lo cual permitió detectar áreas potenciales para mejorar.

3.2.4 Investigación bibliográfica

La investigación bibliográfica o documental es fundamental en cualquier estudio, ya que implica la revisión exhaustiva de la literatura existente sobre el tema en cuestión. Al examinar el material bibliográfico disponible, se pueden identificar las fuentes de información más relevantes y confiables para respaldar la investigación. Este proceso de selección de fuentes es esencial para garantizar la calidad y la validez del estudio (Ávala, 2022).

La investigación bibliográfica consiste en examinar y evaluar la literatura disponible sobre un tema particular. En este caso Auditoría a la Gestión de Seguridad de la Información en la Unidad Educativa Heriberto Rodríguez Angulo, la investigación bibliográfica se aplicó para examinar y recopilar información relevante sobre la seguridad de la información, la auditoría en el ámbito educativo, y cualquier otro tema relacionado con la gestión de la seguridad de la información en instituciones educativas. Esto pudo incluir la revisión de libros, artículos académicos, normativas y estándares de seguridad de la información, así como cualquier otra fuente de información que pueda proporcionar antecedentes y contexto para el estudio de auditoría de seguridad en la Unidad Educativa Heriberto Rodríguez Angulo.

3.3 Métodos de investigación

Hoy en día es importante los métodos de investigación, ya que permite enfocar metodología cuidadosamente para lograr abordar cierto objetivo principales que puede tener una investigación. Uno de los objetivos que tiene el método de investigación es que ofrece soluciones prácticas a los problemas que se tiene en la investigación. La metodología de investigación no se limita solamente a la recuperación de datos sino un proceso estructurado, al llegar al investigador para de la investigación que queramos (Maya, 2014).

3.3.1 Método inductivo

El método inductivo, o inductivismo, es un enfoque científico que permite derivar conclusiones generales a partir de observaciones específicas. Este método, ampliamente utilizado en la investigación científica, se caracteriza por cuatro etapas fundamentales: la observación y registro de los hechos, la clasificación y análisis de los mismos, la generalización a través de la derivación inductiva basada en los hechos observados, y la posterior verificación de las conclusiones obtenidas. (Osman Arauz, 2020)

En la escuela básica Heriberto Rodríguez Angulo, el método inductivo ayuda a entender mejor cómo funcionan las cosas al observar casos específicos. Esto nos da una base sólida para sacar conclusiones que realmente reflejan lo que pasa en la escuela. Este enfoque es muy útil cuando queremos crear nuevas ideas o ajustar las que ya tenemos a situaciones particulares y complicadas.

3.3.2 Método deductivo

El método deductivo es un enfoque lógico de investigación que parte de premisas generales para llegar a conclusiones específicas. Este método se basa en la aplicación de reglas lógicas para deducir lo particular a partir de lo general, asegurando que, si las premisas iniciales son verdaderas, las conclusiones derivadas de ellas también lo serán. Es un proceso que, en su forma directa, permite obtener conclusiones sin intermediarios, mientras que, en su forma indirecta, utiliza el silogismo lógico para relacionar las premisas con una tercera proposición y así arribar a una conclusión particular. (ALissa Grijalva, 2017)

En la escuela básica Heriberto rodríguez Angulo, este método se emplea para verificar si las políticas y procedimientos de seguridad se ajustan a los estándares establecidos. Utilizando este enfoque, es posible aplicar teorías y principios generales de seguridad a las situaciones concretas de la escuela, asegurando que las medidas implementadas sean adecuadas y efectivas en el contexto específico de institución.

3.4 Fuentes de información de datos

3.4.1 Fuentes primarias – Fuente secundarias

3.4.1.1 Fuente secundaria - Encuestas

La encuesta se ha convertido en una herramienta fundamental en el ámbito de la investigación, gracias a su capacidad para recopilar y analizar datos de manera rápida y eficiente. Esta técnica implica la aplicación de una serie de procedimientos estandarizados que se utilizan para obtener información de una muestra representativa de una población más amplia. A través de la encuesta, se busca explorar, describir, predecir y explicar diversas características, lo que la convierte en una herramienta versátil y valiosa en el proceso de investigación social y científica (Zambrana et al, 2019).

Se realizó una encuesta a los 9 docente de la Unidad Educativa Heriberto Rodríguez Angulo para recolectar información para ver la percepción y conocimiento que tiene cada docente en el tema del cumplimiento de las políticas y también así mismo de lo que es seguridad informática. Mediante la auditoría que se le realizará en la institución se podrá identificar las posibles brechas en el tema de política de seguridad, ya que mediante la encuesta podría proporcionar información valiosa sobre el nivel de cumplimiento de las políticas.

3.4.1.2 Fuentes primaria -Entrevista

Por lo general, se destaca que las similitudes en una entrevista están relacionadas con la forma espontánea de plantear preguntas y argumentaciones, permitiendo una interacción libre y poco dirigida entre el entrevistador y el entrevistado. Además, se subraya la importancia de la cercanía emocional y la conexión entre ambas partes como elementos facilitadores de una comunicación efectiva. La empatía y la sintonía entre el entrevistador y el entrevistado

contribuyen a generar un ambiente propicio para la expresión abierta y sincera, lo que a su vez puede enriquecer la calidad de la información recopilada durante la entrevista (Lucía, 2019).

La entrevista se le realizó director de la institución que en este caso es del Ing Caja Marco Anthonio, ya que como encargado de la institución y así mismo encargado del área informática puede proporcionar información importante sobre la posible falencia que tiene la institución. Mediante la entrevista se va a elaborar unas series de preguntas referente a la relación de la seguridad informática como la compresión de la importancia de seguridad informática, política y procedimiento de seguridad e Incidentes de seguridad pasados.

3.5 Estrategia operacional para la recolección de datos

3.5.1 Población

Se trata de un fenómeno de estudio que abarca en su totalidad unidades de análisis o entidades de población que forman parte de dicho fenómeno, y que requiere ser cuantificado para llevar a cabo un estudio integral. Este enfoque implica considerar todas las partes constituyentes del fenómeno en cuestión, con el fin de obtener una comprensión completa y detallada de su naturaleza y características. La cuantificación de estas unidades de análisis es esencial para poder realizar un análisis exhaustivo y riguroso del fenómeno en estudio (Ordoñes, 2019).

La población que se escogerá son los 9 docente de la institución incluyendo al director de la Unidad Educativa Heriberto Rodríguez Angulo ya que ellos son los principales personajes que se ven afectados por la falta de seguridad y mantenimiento de los equipos del laboratorio de cómputo de la institución.

3.5.2 Muestra

Una muestra estadística es un subconjunto de unidades representativas de un conjunto más grande denominado población o universo. Esta muestra se selecciona de manera aleatoria y se somete a observación científica con el objetivo de obtener resultados válidos para la totalidad del universo investigado, dentro de ciertos límites de error y probabilidad que se pueden determinar en cada caso (López et al, 2017).

Para sacar una muestra necesitamos lograr tener una población grande, pero en este caso no se aplicará muestra por tal razón, que los estudiantes que se encuentra en la institución son menores de 18 años la cual solo se evaluaría a los 9 docente dando, así como resultado una población pequeña, la que no permitirá escoger una muestra.

3.5.3 Análisis de las herramientas de recolección de datos a utilizar

3.5.3.1 Encuesta

Se realizó un cuestionario de 11 pregunta cerrada con dos opciones (Si, No) dirigida a 8 docente de la institución educativa Heriberto Rodríguez Angulo para recolectar información sobre las faltas de reglamento, políticas, controles y falta de mantenimiento de los equipos de cómputo de la institución educativa. Antes de realizar las encuestas se les dio unas breve indicaciones a los docentes de cómo se realizaría y sobre los temas a tratar en la encuesta.

3.5.3.2 Entrevista

Se realizó una entrevista que fue dirigida al director Marco Anthonio Caja de la institución Educadita Heriberto Rodríguez Angulo. Se aplicó en la entrevista un cuestionario de 11 preguntas la cual está relacionada con la encuesta que se realizó a los docentes de la institución. Alguno tema que se trató en la entrevista fue sobre si la institución cuenta con algún reglamento o controles para el uso del laboratorio entre otras preguntas.

3.5.3.3 Estructura de los instrumentos de recolección de datos aplicados

3.5.3.3.1 Encuesta (Cuestionario)

ENCUESTA

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

CARRERA DE INGENIERÍA DE TECNOLOGÍA DE LA INFORMACIÓN

Nombre de la empresa o institución: Unidad Educativa Heriberto Rodríguez Angulo

Encuesta Dirigido a: Docentes de la institución

Objetivo: Determinar problemas en la gestión de seguridad informática del laboratorio de computó que cuenta la institución

1. **¿Conoces sobre la existencia de un reglamento para el uso del laboratorio de la institución educativa?**
   Si ◯ **No** ◯
2. **¿La institución le ha socializado dicho reglamentó?**
   Si ◯ **No** ◯
3. **¿Existes controles al momento de utilizar los equipos de cómputo?**
   Si ◯ **No** ◯
4. **¿Ha tenido algún problema con infección de virus en lo equipo de cómputo?**
   Si ◯ **No** ◯
5. **¿Ha perdido información en los equipos de la institución?**
   Si ◯ **No** ◯

6. **¿Ha recibido capacitaciones sobre las políticas de seguridad que debe tener en un laboratorio de computó?**

Si ◯ **No** ◯

7. **¿Ha visualizado problemas de calentamiento y humedad en el laboratorio?**

Si ◯ **No** ◯

8. **¿Ha recibido orientación de cómo se maneja las actualizaciones de software y sistemas de seguridad informática en la institución?**

Si ◯ **No** ◯

9. **¿Las medidas de seguridad del laboratorio son suficientes para prevenir el acceso no autorizado a los sistemas informáticos?**

Si ◯ **No** ◯

10. **¿Se realiza mantenimiento en los equipos de cómputo que cuenta la institución?**

Si ◯ **No** ◯

11. **¿Se han implementado medidas suficientes para proteger los equipos de cómputo de problemas ambientales?**

Si ◯ **No** ◯

3.5.3.3.2 Entrevista (Guía de entrevista)

ENTREVISTA

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

CARRERA DE INGENIERÍA DE TECNOLOGÍA DE LA INFORMACIÓN

Nombre de la empresa o institución: Unidad Educativa Heriberto Rodríguez Angulo

Encuesta Dirigido al: Director de la institución el ing. Marco Caja

Objetivo: Obtener información relevante y precisa sobre la gestión de seguridad informática que cuenta la institución.

1. **¿Existen un reglamento para el uso del laboratorio de la institución educativa?**

2. **¿Le ha socializado dicho reglamentó a los demás docente de la institución?**

3. **¿Se han implementado controles al momento de utilizar los equipos de cómputo?**

4. **¿La institución ha tenido algún tipo problema con infección de virus en lo equipo de cómputo?**

5. **¿Se ha perdido información en los equipos de la institución?**

6. **¿La institución ha realizado capacitaciones sobre las políticas de seguridad que debe tener en un laboratorio de computó?**

7. **¿Cuáles son los principales problemas ambientales que han afectado a los equipos de cómputo?**

8. **¿Cómo se manejan las actualizaciones de software y sistemas de seguridad informática en la institución?**

9. **¿Existen medidas de seguridad para prevenir el acceso no autorizado a los sistemas informáticos?**

10. **¿Se ha establecido un programa de mantenimiento preventivo para los equipos de cómputo?**

11. **¿Qué medidas se han implementado para proteger los equipos de cómputo de problemas ambientales?**

3.5.4 Plan de recolección de datos

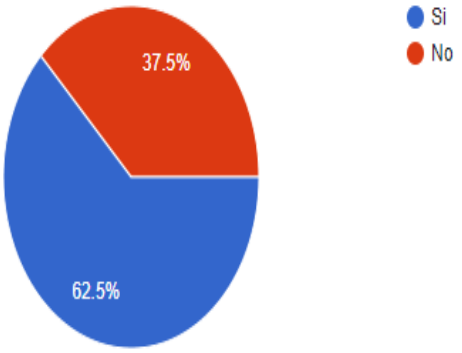
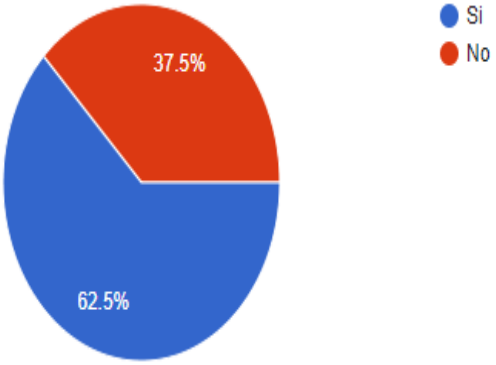
La recolección de datos se realizó mediante encuesta y entrevista de manera presencial, la que se elaboró un cuestionario de 11 preguntas tanto para la encuesta y así mismo para la entrevista.

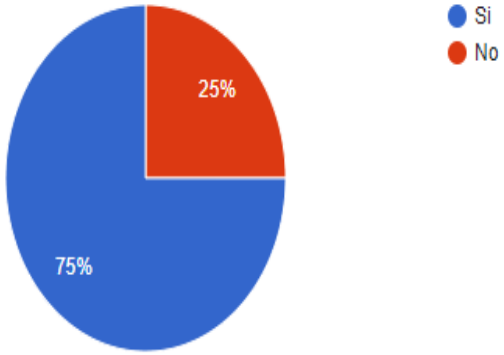
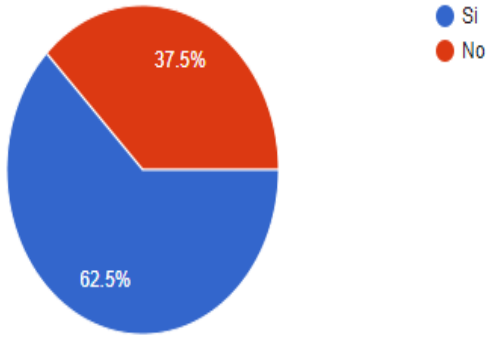
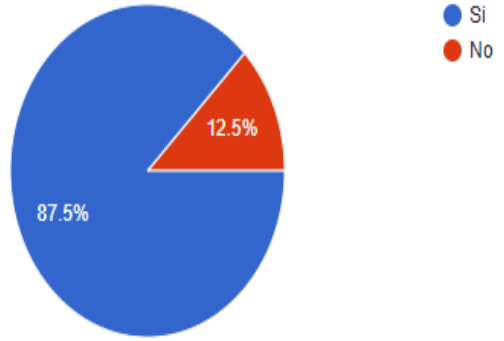
A los docentes de la institución se le aplicaron preguntas cerrada de (Si, No) en cambio la entrevista se la realizó al director ing. Marco Anthonio Caja, ya que como encargado de la institución y así mismo encargado del laboratorio, este pudo proporcionar información importante sobre la existencia de los reglamentos de la institución, controles y falta de mantenimiento que ha tenido últimamente la institución Educativa Heriberto Rodríguez Angulo.

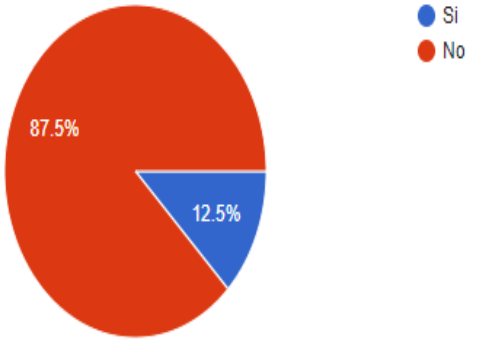
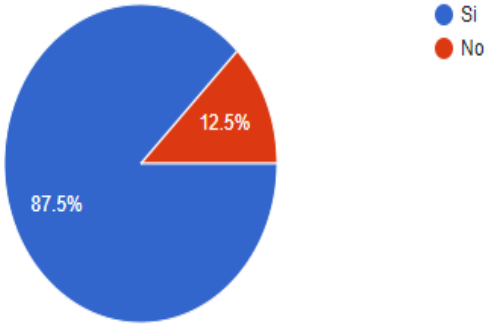
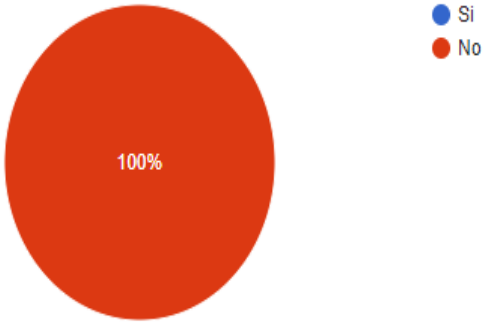
Actividad de recolección de datos	Fecha de inicio	Método	Dirigido a
Encuesta	23/01/2024	Presencial	A los 8 docente de la Institución educativa.
Entrevista	02/02/2024	Presencial	Director Marco Anthonio Caja

3.6 Análisis y presentación de resultados

3.6.1 Análisis de datos obtenidos a través de la encuesta

Preguntas	Respuestas	Interpretación
1. ¿Conoce sobre la existencia de un reglamento para el uso del laboratorio de la institución educativa?		En su mayoría los docentes conocen de la existencia de un reglamento para el uso del laboratorio de la institución también así mis hay una cantidad significativa de docente que no ésta familiarizado sobre la existencia del dicho reglamento.
2. ¿La institución le ha socializado dicho reglamento?		Podemos asumir que esta pregunta está familiarizada con la anterior, la cual nos da un resultado igual ya que si no conoce del reglamento del uso del laboratorio como se puede asumir que se ha socializado con todos los docentes.

Preguntas	Respuestas	Interpretación
3. ¿Existe controles al momento de utilizar los equipos de cómputo?		De la muestra encuestada, la gran mayoría de los docentes tiene conocimiento de los controles que existe al momento de utilizar los equipos de cómputo y hay un cierto porcentaje de los docentes que no tiene conocimiento de dichos
4. ¿Ha tenido algún problema con infección de virus en los equipos de cómputo?		La mayoría del docente encuestado han tenido problemas con virus en lo equipo que se encuentra en la institución la cuales una de las razones que están expuestos a virus informáticos.
5. ¿Ha perdido información en los equipos de la institución?		De los docentes encuestados en su gran cantidad si han perdió información de los equipos de la institución y hubo un pequeño porcentaje de que aún no han perdido información.

Preguntas	Respuestas	Interpretación
6. ¿Ha recibido capacitaciones sobre las políticas de seguridad que debe tener en un laboratorio de cómputo?		En el resultado de esta pregunta podemos observar que en su mayoría no ha recibido capacitaciones sobre la seguridad que se debería tener en el laboratorio de cómputo dentro de la
7. ¿Ha visualizado problemas de calentamiento y humedad en el laboratorio?		Por lo que podemos observar mediante la encuesta los docentes han visualizados problemas que hay de calentamiento y humedad dentro del laboratorio de computación.
8. ¿Ha recibido orientación de cómo se maneja las actualizaciones de software y sistemas de seguridad informática en la institución?		En la totalidad de los docentes que elabora en la institución ha manifestado mediante la encuesta que no se ha recibido orientaciones de actualizaciones de software y sistema de

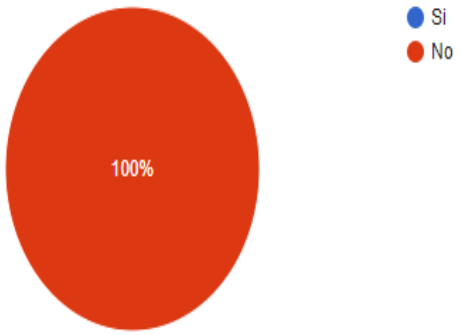
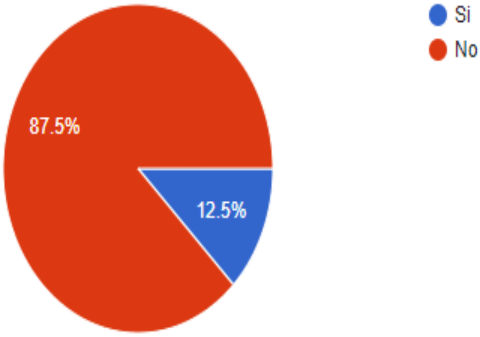
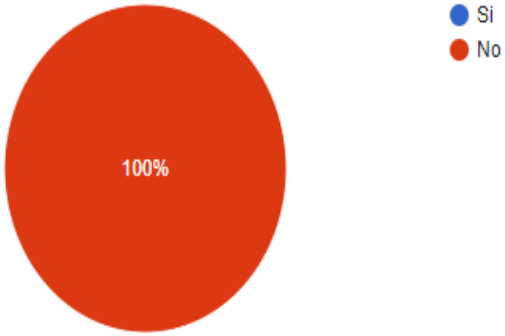
Preguntas	Respuestas	Interpretación
9. ¿Las medidas de seguridad del laboratorio son suficientes para prevenir el acceso no autorizado a los sistemas informáticos?		Por medio de la encuesta se puedo observar que los docentes consideran necesario implementar más medidas de seguridad para así prevenir el acceso no autorizado al sistema informático tanto físicamente como virtualmente.
10. ¿Se realiza mantenimiento en los equipos de cómputo que cuenta la institución?		En su mayoría de los docentes encuestado respondieron que no se realiza mantenimiento en los equipos que tiene la institución educativa.
11. ¿Se han implementado medidas suficientes para proteger los equipos de cómputo de problemas ambientales?		Mediante de la encuesta se pudo observar que todos los docentes en su totalidad creen que aún falta medidas para implementar con el objetivo de proteger los equipos de problemas ambientales.

Tabla 1 Análisis de datos obtenidos mediante la encuesta

3.6.2 Análisis de datos obtenidos a través de la entrevista

Pregunta	Respuesta	Interpretación
1. ¿Existen un reglamento para el uso del laboratorio de la institución educativa?	No existe debido a que las computadoras en la epidemia fueron apagadas por eso no hemos tratado hacer nuevamente el reglamento.	Anteriormente si había un reglamento para el uso del laboratorio y desde la epidemia no se ha establecido nuevamente el reglamento.
2. ¿Le ha socializado dicho reglamentó a demás docentes de la institución?	Obviamente se le ha enunciado, pero como no existe el reglamento no se le ha podido socializar ya desde la epidemia no se cuenta con un reglamento.	De socializar como quiere el reglamento con los docentes no solamente s ele a socializado ya que por el momento la institución desde la epidemia no cuenta con ningún reglamento ya que se tiene las computadoras mas no el reglamento.
3. ¿Se han implementado controles al momento de utilizar los equipos de cómputo?	Claro eso si se controlar, pero a través del tutor, por ejemplo, el encendido, la apertura de las páginas únicamente seleccionada por internet.	Los controles se realizan presencialmente mediate el tutor al momento que ingresa con estudiante al laboratorio.
4. ¿La institución ha tenido algún tipo problema con infección de virus en lo equipo de cómputo?	Todas las computadoras están afectadas por virus (Troyano) y no tiene los equipos de la institución antivirus, tanto las computadoras del laboratorio como la de secretaria.	En si las computadoras de la institución por falta de mantenimiento han sido invadidas por virus ya que no se realiza en el momento adecuado una planificación de mantenimiento.
5. ¿Se ha perdido información en los equipos de la institución?	Si se ha perdido información como archivos, actas, notas que se borra debido que avece hay virus sumamente fuerte como el Troyano que elimina o se perderá de eso y la única forma de eliminar es virus es formateándola.	Una de las causas que se ha perdió información dentro de la institución ha sido porque las computadoras han sido infectadas con virus informático, y por esa razón se ha necesitado formatear, perdiendo así toda la información que se encontrar dentro de los equipos.

Preguntas	Respuestas	Interpretación
6. ¿La institución ha realizado capacitaciones sobre las políticas de seguridad que debe tener en un laboratorio de computó?	En el mandato que tengo como director por el momento no, pero si se considera importante para el uso de seguridad de la información.	Se supo manifestar el director de la institución que si se considera importante aplicar una capacitación ya que su mandado nunca se han podido aun aplicarla.
7. ¿Cuáles son los principales problemas ambientales que han afectado a los equipos de cómputo?	Anteriormente era la humedad y actualmente por el calor ya que no hay enfriamiento dentro del laboratorio por el daño del aire acondicionado aparte el desuso y el polvo.	Con lo que comento el director en la entrevista y lo que anteriormente puede observar, el laboratorio no se encuentra en un estado favorable para los equipos.
8. ¿Cómo se manejan las actualizaciones de software y sistemas de seguridad informática en la institución?	Como aquí no hay seguridad de informática solamente nos mantenemos sin conexión a red abierta únicamente se mantiene las computadoras de secretaria con internet, pero se tiene cerrada con mi clave solamente para el uso adecuado de la institución.	En la actualidad solamente se le realiza actualizaciones de software a las computadoras de uso que son las de secretaria y como sistema de seguridad de dicha computadora es solamente una contraseña que al momento de iniciar sección con la clave del director.
9. ¿Existen medidas de seguridad para prevenir el acceso no autorizado a los sistemas informáticos?	De las computadoras del laboratorio no solamente de secretaria existente medida de ingreso, pero solamente para el personal autorizado que es mi persona y la secretaria.	Solamente al momento de iniciar sección en Windows tiene el acceso es el director y la secretaria de la institución, pero solamente en la secretaria. Luego las computadoras del laboratorio tienen acceso libre ya que no cuenta con ninguna clase de contraseña.

Preguntas	Respuestas	Interpretación
10. ¿Se ha establecido un programa de mantenimiento preventivo para los equipos de cómputo?	No se ha establecido lo único que podemos hacer como institución educativa es solicitar al distrito de educación al compañero encargado del TIC que nos ayude con la limpieza y mantenimiento y él lo hace debido a su tiempo.	Mediante de las respuestas del entrevistado se supo manifestar que ello no puede por su propia cuenta realizar mantenimiento ya que el encargado de realizar el debido mantenimiento es el encargado de la TIC del distrito de educación.
11. ¿Qué medidas se han implementado para proteger los equipos de cómputo de problemas ambientales?	Ahora ya se le puso cielo raso y se selló más la puerta para que no se pase los insectos o el polvo y también se construyó un muro al ingreso de la puerta para que no ingrese el agua dentro del laboratorio.	A simple vista se ve que hace falta implantar más medida de seguridad ya que con las que cuenta no son suficiente para proteger los quipos de cómputo.

Tabla 2 Análisis de datos obtenidos a través de la entrevista

3.6.3 Presentación y descripción de los resultados obtenidos

Más de la mitad manifestaron no conocer reglamento para el laboratorio, así lo mostraron en la pregunta número 1 los docentes, e igual se verifico en la pregunta 2 de los docentes, y un porcentaje igual se verifico en la pregunta 2 de los docentes. En la entrevista a su vez, se supo manifestar el director de la institución que no existe, ya que por la epidemia fueron apagado los equipos y aun no se ha tratado de crear nuevamente el reglamento, pero a los docentes sí se les ha anunciado la creación del reglamento, mas no socializado ya que aún no está existente.

En la pregunta 3, con los resultados que se obtuvo de los docentes, llegamos a la a conclusión que, si existen controles al momento de utilizar los equipos ya que al momento que se realizó la entrevista con director, se queda en claro que los controles que se implementa son al momento de utilizar el laboratorio con el tutor en su hora de clase dentro del laboratorio. En la pregunta 4 se habla sobre si los docentes de la institución han tenido problema de infecciones de virus en los equipos, la cual la respuesta que se obtuvo, por su mayoría fue un sí, ya que los

equipo no contiene un antivirus que permita proteger los equipos de una infección de virus informático.

La pregunta 5 se trató sobre si se ha perdido información en los equipos de la institución, ya que por medio de la encuesta se visualizó que la mayoría de los docentes si han perdió información por causa de infección de virus, ya que por tal razón se tiene que llegar formatear los equipo para le eliminación del virus, perdiendo así información como archivos, actas y notas que se encuentra en los equipos. En la pegunta 6 se habla sobre si la institución se ha realizado capacitaciones sobre las políticas de seguridad que debe tener en un laboratorio de cómputo, lo que se visualizó como resultado en la cuesta, que casi en su totalidad de docente no ha recibido ninguna capacitación.

La pregunta 7 se nombra si se ha visualizado problema de calentamiento y humedad en el laboratorio, que en lo obtenido en la encuesta se afirma casi en su totalidad de las respuestas de los docentes que el laboratorio cuenta con problema de calentamiento por falta de aire acondicionado y también hay humedad. En la pregunta 8 se refería si se ha recibido orientación de cómo se maneja las actualizaciones de software y sistemas de seguridad informática en la institución. La respuesta de esta pregunta por medio de los docentes en su totalidad fue no, ya que las actualizaciones se manejan directamente del distrito, mas no de la institución. En la pregunta 9 habla de las medidas suficiente de seguridad que debe tener la institución para prevenir el acceso no autorizado a los sistemas informáticos, ya que por medio de la encuesta se obtuvo un resultado negativo en su totalidad ya que solamente se protege los equipo por medio de contraseña al momento de ingresar a las computadoras, pero solamente en el área de secretaria.

La pregunta 10 trata sobre si la institución se realiza mantenimiento en lo equipo, la cual por medio de las respuestas de los docentes en un porcentaje considerado respondieron no, solamente fue una pequeña parde que respondieron un sí. La justificación de dichas respuestas de obtuvo de la entrevista que se obtuvo con el directo, ya que se manifestó que solamente se les hace mantenimiento a las computadoras de la secretaria, mas no del laboratorio. La última pregunta que se elaboró en la encuesta se trataba si la institución contaba con medidas suficientes para proteger los equipos de cómputo de problemas ambientales, las respuestas de los docentes fueron no, ya que se cree que hace falta implementar más medida de

seguridad en el sentido de problema ambientales, ya que con las medidas que se han implementado no son las suficiente para la protección de los equipos.

3.6.4 Informe final del análisis de los datos

El análisis de los datos recopilados a través de encuesta y entrevista en la escuela básica Heriberto Rodríguez Angulo ha revelado varias áreas críticas que requieren atención. Se observó que una gran mayoría de los docentes ni están al tanto de la existencia de un reglamento para el uso del laboratorio de cómputo, lo que refleja una falta de comunicación y actualización en las normativas de la institución. El director confirmo que, debido a la pandemia, no se ha trabajado en la reactivación de este reglamento.

Además, se identificó que, aunque existen ciertos controles para el uso de los equipos, estos no son suficientes para garantizar la seguridad informática, ya que los equipos, no son suficientes para garantizar la seguridad informática, ya que los equipos carecen de antivirus adecuado, lo que ha llevado a perdidas significativas de información. Los docentes también reportaron una falta casi total de capacitación en cuanto las políticas de seguridad informática, y problemas ambientales como el sobrecalentamiento y humedad en el laboratorio, que no se están abordando de manera efectiva.

Otro punto de preocupación es el mantenimiento de los equipos, que se limita a las computadoras del área de secretaría, dejando desprotegidos los recursos tecnológicos del laboratorio. También se detecto que no existen medidas suficientes para proteger los sistemas informáticos contra acceso no autorizados lo que podría comprometer la integridad de la información.

En conclusión, el análisis de los datos subraya la necesidad urgente de actualizar las políticas de seguridad para alinearlas con los estándares actuales, implementar un mantenimiento regular y preventivo que segure el correcto funcionamiento de los equipos, y proporcionar capacitación adecuada y continua a los docentes. Estas medidas no solo garantizarán la seguridad y eficiencia del entorno tecnológico en la institución, sino que también permitirá una mejor preparación frente a posibles riesgo y amenazas, creando un ambiente más seguro en la institución educativa Heriberto Rodríguez Angulo.

CAPÍTULO IV

4 MARCO PROPOSITIVO

4.1 Introducción

Mediante el trabajo de auditoría, realizado minuciosamente en la institución, se detectaron deficiencias en los requisitos, controles y política de seguridad. Durante esta investigación, se utilizó una variedad de recursos, incluyendo recursos humanos, tecnológicos y económicos.

Sin duda, el recurso humano fue fundamental, involucrando a los docentes de la institución Heriberto Rodríguez Angulo, así como al director encargado Marco Anthonio Caja y a la tutora de tesis Clara Guadalupe Pozo, quienes colaboraron proporcionando orientación a la auditora encargada de este trabajo. El recurso tecnológico también desempeñó un papel crucial, facilitando la documentación escrita y la captura de evidencia para respaldar el trabajo realizado. Por último, pero no menos importante, se empleó el recurso económico, que permitió llevar un registro detallado de los costos asociados durante la duración del trabajo de titulación, proporcionando una visión clara del gasto total incurrido en la elaboración de este proyecto.

De igual manera, para la obtención de los datos relevantes de los posibles riesgos que se encontraba en la institución educativa se tuvo que realizar tres tipos de instrumento de tipo cuestionario que fueron instrumentos de cuestionario para el análisis de riesgo, cuestionario de requiso de las normas ISO 27001 y como ultimo instrumento fue el cuestionario de control de las normas ISO 27001. Dicho instrumento fue realizo al docente Marco Anthonio Caja director del plantel educativa ya mencionada, para ser tabulado el Excel para permitir visualizar de mejor forma el impacto de riesgo que está expuesta la institución educativa Heriberto Rodríguez Angulo

4.2 Descripción de la propuesta

De acuerdo con el problema planteado en la investigación, se procedió a realizar una auditoría, con el propósito de poder identificar las faltas de políticas y faltas de controles que tiene la institución educativa Heriberto Rodríguez Angulo y así mismo poder identificar sus vulnerabilidades en el área informática. La auditoría aplicada en este caso fue una auditoría a la Gestión de Seguridad de la Información, la cual esta auditoria tuvo como objetivo principal identificar los problemas que existe en el área informática en dicha institución ya que mediante

de bibliografía y libros pudimos justificar científicamente los tema que se aplicaron en la auditoría.

Mientras tanto, los instrumentos de vital importancia que se utilizaron fueron encuesta y la entrevista, la cual por medio de ellos permitieron obtener información de importe relevancia obteniendo así resultados verdaderos de la problemática del área informática que está pasando dentro de la institución educativa Heriberto Rodríguez Angulo. Para el presente trabajo se utilizó la metodología de las Normas ISO 27001, la cual esta norma está enfocada en identificar y evaluar los riesgos informáticos la cual está pasando la institución educativa para poder así establecer controles y política de seguridad.

4.3 Determinación de recursos

4.3.1 Humanos

Cantidad	Recursos	Función	Actividad
1	Ing. Clara Pozo	Tutor del proyecto de titulación	Colaboradora de brindar orientación al estudiante en su proceso de proyecto de titulación.
1	Ing. Marco Caja	Director de la institución educativa y encargado de los equipos de computó	Colaborador del Permiso de la realización del trabajo de titulación y así mismo colaborador con la entrevista realizada en la institución.
8	Docentes de la institución educativa	Docentes de la institución educativa y participantes de la auditoría	Colaboradores de la realización del proceso de la encuesta.
1	Micela Demera	Auditora	Como Auditor pude identificó falta de política y controles de seguridad en la institución educativa.

Tabla 3 de Determinación de Recurso Humanos

4.3.2 Tecnológicos

Cantidad	Recurso	Actividad
1	Portátil Lenovo ADM Ryzen 3. Táctil con 10 puntos táctiles y 8 GB de memoria RAM	Equipo de tecnología utilizado para la elaboración investigación.
1	Celular marca Samsung A 31, almacenamiento de 128 GB y 4 de ram. Con cámara de 48Mp	Celular utilizado para recaudar fotografía de evidencia de la realización dentro de la institución educativa.
1	Paquete de Microsoft Office 365	Plataforma de uso para la elaboración de la titulación.
12 meses	Plan de internet	Plan de internet para poder ingresar a ciertas investigaciones ayudará con el tema de investigación, la que tendrá un costo de $25.

Tabla 4 Instrumento de Determinación de Recurso Tecnológico

4.3.3 Económicos

Cantidad	Descripción	Precio Unitario	Subtotal
1	Portátil Lenovo AMD Ryzen 3.	$985	$985
1	Celular marca Samsung A 31,	$300	$300
140	Impresiones	$0.15	$21
12 meses	Plan de internet	$25	$300
		Total	**$1606**

Tabla 5 Instrumento de Determinación de Recurso Económico

4.4 Desarrollo según metodología de las normas ISO 27001

A través del estudio que se llevó a cabo en la institución educativa Heriberto Rodríguez Angulo, se pudo observar la problemática que actualmente está pasando la institución educativa, la cual se pudo visualizar que la mejor metodología que se podría aplicar en este caso fuera la metodología de las normas ISO 27001, ya que esta norma proporciona a las organizaciones o en este caso a una institución educativa que puedan implementar controles y política de seguridad. Esta metodología permite evaluar y así mismo identificar los riegos que está expuesta el área informática de la institución educativa.

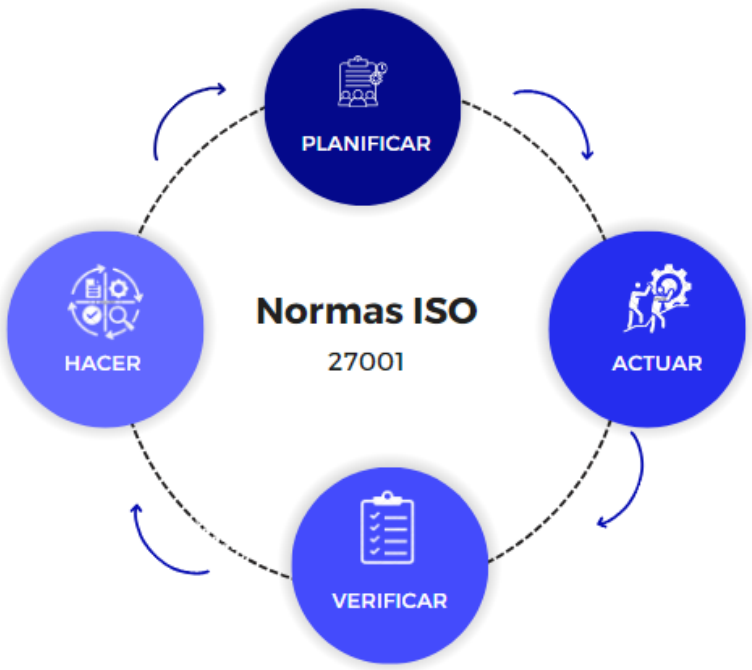


Ilustración 1 Gráfico de la fases de la Norma ISO 27001

4.4.1 Fase 1: Planificación

4.4.1.1 Programa de auditoría

Programa de auditoría informática para la gestión de seguridad de la información en la Unidad Educativa Heriberto Rodríguez Angulo		
Objetivo 1. Evaluar el nivel de cumplimiento de normas y política de seguridad en el laboratorio de cómputo de la Unidad Educativa Heriberto Rodríguez Angulo según la norma ISO 27001. 2. Identificar los posibles riegos de seguridad informática a los que está expuesto el laboratorio de la Unidad Educativa Heriberto Rodríguez Angulo		
Técnica y procedimiento		
	Referencia a papel de trabajo	**Fecha**
1. Revisar las normas ISO 27001	4.4.1.2	19/04/2024
2. Diseño de instrumento según ISO 27001 para evaluar cumplimento de controles y política de la institución en el área informática	4.4.1.3	20/04/2024
3. Elaborar instrumentos para evaluar riesgos	4.5.2.1.1	03/06/2024 10/06/2024
4. Entrevista a director de la institución educativa para llenar instrumento de la auditoría	4.5.3.1	10/06/2024
5. Entrevistar de los instrumentos al director encargado de la institución educativa	4.5.3.1	10/06/2024
6. Tabulación de datos	4.5.3.2	27/06/2024

7. Elaborar matriz de riesgos	4.5.3.5	29/06/2024
8. Análisis de resultados	5.3.3	03/07/2024
9. Elaboración de informe de la auditoría	5.1	09/07/2024
Realizado por: Demera Moreira María Micaela **Fecha:**	**Revisado por:** **Fecha**	

Tabla 6 Instrumento de programa de Auditoría

4.4.1.2 Revisión de ISO 27001

Las normas ISO 27001 son un estándar internacional que sigue una serie de etapas específicas y fundamentales para establecer, implementar y monitorear un sistema de gestión de seguridad de la información de manera estructurada. En el contexto de una organización o institución, como una institución educativa, la norma ISO 27001 permite identificar, gestionar y minimizar los riesgos que pueden causar daños o pérdidas en los equipos de cómputo, así como la pérdida de información crucial para los docentes que trabajan en el plantel educativo Heriberto Rodríguez Angulo.

A continuación, la descripción de la estructura de las normas ISO 27001:

# Ítems	Requisito	Descripción
4	La organización y su Contexto	Esta fase permitió recopilar suficiente información de la institución, identificando las necesidades específicas de la escuela educativa Heriberto Rodríguez Angulo y estableciendo expectativas de mejora para la institución.
5	- Liderazgo	Esta parte destaca las necesidades de los docentes y los estudiantes al aplicar normas y política de segura y controles en el área informática dentro de la institución educativa Heriberto Rodríguez Angulo. Para llegar a esto, la persona cargada de esta área que en este caso es director de la institución debe mostrar el liderazgo y compromiso en el sentido de seguridad, desarrollando política y controles que garantice un ambiente seguro y protegido para los activos de la institución.
6	Planificación	En esta parte se resaltaría la importancia de los riegos de la institución educativa para así lograr una planificación en el sistema de gestión de seguridad de la institución educativa Heriberto Rodríguez Angulo. Mediante la identificación de los riesgos, permitió plasmar nuestro objetivo específico relacionado con la seguridad de los activos que se encuentra en el plantel educativo. Es de suma importancia haber considerado los riesgos que pueda afectar los equipo, por eso es importante planificar medidas preventivas para la seguridad y protección de los equipos.
7	Soporte	En esta parte tiene que ver mucho con la información documentada que se realiza para el correcto funcionamiento y así mismo garantizar la seguridad de los equipos de cómputo de la institución Educativa Heriberto Rodríguez Angulo.
8	Operación	Esta parte se refiere a las necesidades de planificar e implementar política y controles de seguridad informática en la institución Educativa Heriberto Rodríguez Angulo, esto significa que se debe establecer y seguir un seguimiento detallado de la vulnerabilidades y riego que está expuesto los equipos de cómputo de la institución.

9	Evaluación del desempeño	Esta parte implica la necesidad, analizar, evaluar y revisar la gestión de seguridad con la que cuenta el laboratorio de la institución educativa Heriberto Rodríguez Angulo. Se llega hacer esta evaluación para ver que las medidas y controles de seguridad está cumpliendo acuerdo a lo planificado que es cumplir el objetivo de proteger los activos.
10	Mejora	En esta sección implica en detallar las responsabilidades que tiene en este caso la Institución Educativa Heriberto Rodríguez Angulo de abordar y corregir cualquier no conformidad que se detectaron en el área informática buscando constantemente mejoras, en la adecuación y eficiencia en el área informática.

Tabla 7 Descripción de la estructura de las normas ISO 27001

4.4.1.3 Diseño de Instrumentos

A continuación, veremos dos tipos de diseño de instrumento que se utilizaron.

El primer diseño de instrumento es el instrumento de cumplimiento de requisito, este permitió evaluar las deficiencias de madurez de una escala del 0 al 5, pudiendo así recolectar información de acuerdo con los estándares que corresponde a las normas ISO 27001

4.4.1.3.1 Cuestionario para el cumplimiento de requisito

Este instrumento permitirá recopilar datos importante y necesario, como recopilar información y evidencia sobre el cumplimiento de los requisitos de las normas ISO 27001 para poder evaluar si la institución educativa cuenta con los debidos requisitos, para poder así establecer e implementar y mejorar el sistema de gestión de seguridad de la institución educativa.

Cuestionario para el cumplimiento de requisito de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo				C1 Página 1 de 6
Requisitos		**Preguntas**	**Cumplimiento**	**Observación**
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?		
Realizado por: Demera Moreira María Micaela **Fecha:**			**Revisado por:** **Fecha:**	

Cuestionario para el cumplimiento de requisito de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo			C1 Página 2 de 6	
Requisitos		**Preguntas**	**Cumplimiento**	**Observación**
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?		
	5.3 Roles y Responsabilidades	1.- ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?		
		¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?		
6.- Planificación	**6.1 Tratamiento de Riesgos y Oportunidades**	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación con la Seguridad de la Información?		
Realizado por: Demera Moreira María Micaela **Fecha:**		**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de requisito de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo			C1 Página 3 de 6	
Requisitos		**Preguntas**	**Cumplimiento**	**Observación**
6.- Planificación	**6.1 Tratamiento de Riesgos y Oportunidades**	2.- ¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?		
		3.- ¿Se ha definido un proceso de tratamiento de riesgos?		
		4.- ¿Se han establecido criterios para elaborar una declaración de aplicabilidad?		
		5.- ¿Se mantiene información documentada de los puntos anteriores?		
	6.2 Planificación para consecución de objetivos	1.- ¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?		
		2.- ¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación		
		3.- ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?		
7.- Soporte	**7.1 Recursos**	1.- ¿Se identifican y asignan los recursos necesarios para el SGSI?		
	7.2 Competencia	1.- ¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?		
Realizado por: Demera Moreira María Micaela **Fecha:**			**Revisado por:** **Fecha**	

Cuestionario para el cumplimiento de requisito de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo				C1 Página 4 de
Requisitos		**Preguntas**	**Cumplimiento**	**Observación**
7.- Sopor	**7.2 Competencia**	2.- ¿Se mantiene información actualizada sobre la competencia del personal?		
	7.3 Concienciación	1.- ¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?		
		¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?		
	7.4 Comunicación	1.- ¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?		
		2.- ¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la		
	7.5 SGS Sistema de Gestión de la Seguridad de la información	1.- ¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de		
		2.- ¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de		
		3.- ¿Se controlan los documentos de origen externo?		
Realizado por: Demera Moreira María Micaela		**Revisado por:** **Fecha**		

Cuestionario para el cumplimiento de requisito de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo				C1 Página 5 de 6
Requisitos		**Preguntas**	**Cumplimiento**	**Observación**
8.-Operació	**8.1 Control Operacional**	1.- ¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?		
		2.- ¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?		
		3.- la Seguridad de la Información ante cambios realizados?		
		4.- ¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?		
	8.2 Análisis de riesgos de la Seguridad de la Información	1.- ¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia		
	8.3 Tratamiento de riesgos de la Seguridad de la Información	1.- ¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados		
		2.- ¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?		
		3.- ¿Se documenta el nivel de aplicación de todos los controles a aplicar?		
Realizado por: Demera Moreira María Micaela **Fecha:**			**Revisado por:** **Fecha:**	

Cuestionario para el cumplimiento de requisito de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo				C1 Página 6 de 6
Requisitos		**Preguntas**	**Cumplimiento**	**Observación**
9.- Evaluación del desempeño	**9.1 Seguimiento y medición**	1.- ¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?		
		2.- ¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?		
	9.2 Expectativas de las partes interesadas	1.- ¿Se ha establecido una programación de Auditorías Internas y asignado responsables?		
		2.- ¿Se ha definido el alcance y los requisitos para el informe de auditoría?		
		3.- ¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?		
	9.3 Informe de Revisión por la Dirección	1.- ¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?		
		2.- ¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la		
10.- Mejora	**10.1 No Conformidades y acciones correctivas**	1.- ¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?		
		2.- ¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y		
	10.2 Mejora continua	1. ¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?		
Realizado por: Demera Moreira María Micaela **Fecha:**			**Revisado por:** **Fecha:**	

Tabla 6 Cuestionario de cumplimientos de requisitos

4.4.1.3.2 Cuestionario para el cumplimiento de Controles

Este instrumento de cuestionario de controles permite evaluar si la institución educativa Heriberto Rodríguez Angulo está cumpliendo con los controles de seguridad que está establecido en las normas ISO 27001, ya esos controles son implementados para proteger los activos informático de la institución. El cuestionario es una herramienta útil para lograr tomar medidas correctivas para mejorar la protección de los activos que cuenta en la institución.

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						**C2** Página 1 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
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?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 2 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
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?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 3 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A6	**Organización de la Seguridad de la Información**	**A6.1**	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?			
A7	**Seguridad en Los Recursos Humano**	**A7.2. Durante el contrato**	1.- ¿Se investigan los antecedentes de los candidatos? - Formación - Experiencia -Verificar Titula			
			2.- ¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 4 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A7	**Seguridad en Los Recursos Humano**	**A7.2. Durante el contrato**	3.- ¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?			
			1.- ¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?			
		A7.3. Terminación del contrato	2.- ¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 5 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A8	**Gestión de Activos**	**A8.1 Responsabilidad sobre los Activos**	1.- ¿Se ha realizado un inventario de activos que dan soporte al negocio y de Información?			
			2.- ¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?			
			3.- ¿Se han establecido normas para el uso de activos en relación con su seguridad?			
			4.- ¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?			
		A8.2 Clasificación de la Información	1.- ¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?			
			2.- ¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 6 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A8	**Gestión de Activos**	**A8.2 Clasificación de la Información**	3.- ¿Existen procedimientos para el manipulado de la información de acuerdo con su clasificación?			
		A8.3 Manipulación de Soportes	1.- ¿Existen controles establecidos para aplicar a soportes extraíbles? - Uso -Cifrado -Borrado			
			2.- ¿Existen procedimientos establecidos para la eliminación de soportes?			
			3.- ¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad? - Control de salidas - Cifrado etc.			
A9	**Control de Acceso**	**A9.1 Requisitos generales para el control de acceso**	1.- ¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 7 de
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A9	**Control de Acceso**	**A9.1 Requisitos generales para el control de**	2.- ¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?			
		A9.2 Accesos de Usuario	1.- ¿Existen procesos formales de registros de usuarios?			
			2.- ¿Existen procesos formales para asignación de perfiles de acceso?			
			3.- ¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?			
			4.- ¿Se ha establecido una política específica para el manejo de información clasificada cono secreto? en cuanto a: -Autenticación - Compromisos			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 8 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A9	**Control de Acceso**	**A9.2 Accesos de Usuario**	5.- ¿Se establecen periodos concretos para renovación de permisos de acceso?			
			6.- ¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?			
		A9.3 Responsabilidades de los usuarios	1.- ¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?			
		A9.4 Control de acceso a sistemas y aplicaciones	1.- ¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?			
			2.- ¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 9 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A9	**Control de Acceso**	**A9.4 Control de acceso a sistemas y aplicaciones**	3.- ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?			
			4.- ¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?			
			5.- ¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?			
A 10	**Criptografía**	**A10.1 Control criptográfico**	1.- ¿Existe una política para el establecimiento u yo de controles criptográficos?			
			2.- ¿Existe un control del ciclo de vida de las claves criptográficas?			
A 11	**Seguridad Física y del entorno**	**A11.1 Áreas de Seguridad**	1.- ¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 10 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A11	**Seguridad Física y del entorno**	**A11.1 Áreas de Seguridad**	2.- ¿Existen controles de acceso a personas autorizadas en áreas restringidas?			
			3.- ¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?			
			4.- ¿Se controla o supervisa la actividad de personal que accede a áreas seguras?			
			5.- ¿Se controlan las áreas de Carga y descarga con procedimientos de control de mercancías entregadas etc.?			
A11	**Seguridad Física y del entorno**	**A11.2 Seguridad de los equipos**	1.- ¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?			
			2.- ¿Se protegen los equipos contra fallos de suministro de energía?			
			3.- ¿Existen protecciones para los cableados de energía y de datos?			
			4.- ¿Se planifican y realizan tareas de mantenimiento sobre los equipos?			
			3.- ¿Existen protecciones para los cableados de energía y de datos?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 11 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A11	**Seguridad Física y del entorno**	**A11.2 Seguridad de los equipos**	4.- ¿Se planifican y realizan tareas de mantenimiento sobre los equipos?			
			5.- ¿Se controlan y autorizan la salida de equipos, aplicaciones etc. Que puedan contener información?			
			6.- ¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?			
			7.- ¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?			
			8.- ¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?			
			9.- ¿Se establecen reglas de comportamiento para abandono momentáneos o temporales del puesto de trabajo?			
			1.- ¿Se documentan los procedimientos y se establecen responsabilidades?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 12 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A12	**Seguridad en las Operaciones**	**A12.1 Procedimientos y Responsabilidades**	2.- ¿Se controla que la información sobre procedimientos se mantenga actualizada?			
			3.- ¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?			
			4.- ¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?			
			5.- ¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?			
		A12.2 Protección contra software	1.- ¿Existen sistemas de detección para Software malicioso o malware?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 13 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
A12	**Seguridad en las Operaciones Seguridad en las Comunicaciones**	**A12.3 Copias de Seguridad**	1. - ¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?			
		A12.4 Registros y supervisión	1.- ¿Se realiza un registro de eventos? - Intentos de acceso fallidos/exitosos - Desconexiones del sistema -Alertas de fallos Etc.			
			2.- ¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?			
			3.- ¿Se protege convenientemente y de forma específica los accesos o los de los administradores?			
			4.- ¿Existe un control de sincronización de los distintos sistemas?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo						C2 Página 14 de 14
N°	**Clausula**		**Requisito**	**CUMPLE**		**Observación**
				Si	**No**	
14	**A12** **Seguridad en las Operaciones Seguridad en las Comunicaciones**	**A12.5 Control del Software**	1.- ¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en			
		A12.6 Vulnerabilidad Técnica	1.- ¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?			
			2.- ¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones			
			de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?			
Realizado por: Demera Moreira María Micaela **Fecha:**				**Revisado por:** **Fecha:**		

Tabla 8 Cuestionario de cumplimientos de control

4.4.1.3.3 Cuestionario para el análisis de riesgo

Mediante el cuestionario para el análisis de riesgo, se lo utilizó para evaluar y analizar ciertos riesgos que actualmente que cuenta la escuela básica Heriberto Rodríguez Angulo, la cual podríamos prevenir antes que se dé algún tipo de riesgo, este tipo de instrumento permite recoger datos detallado sobre vulnerabilidades, amenaza o cualquier tipo de consecuencia que puede ocurrir en las instalaciones del plantel educativo.

Cuestionario para el análisis de riesgos para la institución Educativa Heriberto Rodríguez Angulo			C 3 Página 1 de 5
Robo			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
1. ¿Tiene sistema de video vigilancia la institución?			
2. ¿La institución cuenta con personal de seguridad?			
3. ¿La institución ha sufrido robos?			
4. ¿La institución cuenta con un protocolo de respuesta en caso de Robo?			
5. ¿Se lleva un registro de los incidentes de los robos?			
6. ¿Se controla el acceso al ingreso al laboratorio?			
7. ¿Se utiliza sistema de cámara de seguridad?			
8. ¿Se utiliza alarma de seguridad?			
9. ¿Se realizan inspecciones regulares de alarma?			
10. ¿Las computadoras tienen un etiquetado para identificarlas?			
11. ¿Se utiliza cerradura de alta seguridad en las instalaciones?			
12. ¿Se realizan inspecciones regulares de las cerraduras?			
13. ¿Tienen personal encargado del laboratorio?			
14. ¿La institución cuenta con cerramiento físico en sus instalaciones?			
15. ¿Las computadoras se almacenan en gabinetes o cajas de seguridad?			
16. ¿El personal docente cuenta con tarjeta de identificación?			
17. ¿La institución cuenta con botón de pánico para cuando suceda un robo?			
18. ¿Se almacenan las computadoras de manera que sea difícil de mover?			
19. ¿El personal docente tiene acceso a todas las maquinas?			
20. ¿Tienen procedimientos ante la pérdida o robos de computadoras?			
21. ¿Se cuenta con un equipo de repuesto de emergencia en caso de robo?			
22. ¿Las computadoras están anclados con cable de seguridad?			
23. ¿Cuenta la institución con doctor de movimientos?			
24. ¿El personal esté entrenado de como reportar incidentes de seguridad?			
25. ¿La institución cuenta con un seguro de Robo?			
Realizado por: Demera Moreira María Micaela **Fecha:**	**Revisado por:** **Fecha:**		

Tabla 9 Análisis de riesgo de Robo

Cuestionario para el análisis de riesgos para la institución Educativa Heriberto Rodríguez Angulo			C 3 Página 2 de 5
Incendio			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
1. ¿Se realiza simulacro de incendio?			
2. ¿Se ha realizado un análisis de riesgo?			
3. ¿Se ha realizado una evaluación de riesgo de incendio en la institución?			
4. ¿Existe extintores de incendios accesibles en el laboratorio?			
5. ¿En el laboratorio cuenta con rutas de evacuación señalizadas?			
6. ¿Se ha recibido formación en prevención de incendios?			
7. ¿Se realiza inspección de los equipos de seguridad de incendio?			
8. ¿Hay un plan de emergencia establecido en caso de incendió?			
9. ¿Se instalados detectores de humo dentro del laboratorio?			
10. ¿Se establece medida para prevenir incendio en el laboratorio?			
11. ¿Los docentes están capacitados en el uso de los extintores?			
12. ¿Se ha visualizado alguna vez un destello inusual proveniente de			
13. ¿La institución cuenta con sistema de rociadores automáticos?			
14. ¿Se mantiene despejados los pasillos y salidas de emergencia?			
15. ¿Hay equipos eléctricos adecuadamente ventilados para prevenir sobrecalentamiento?			
16. ¿Se almacena productos inflamables de manera segura?			
17. ¿Los cables de los equipos de cómputo están en buen estado?			
18. ¿Se realiza inspecciones del laboratorio para prevenir un incendio?			
19. ¿Se ha realizado inspecciones regulares de los sistemas de seguridad			
20. ¿Hay un protocolo para desconectar fuentes de energía?			
21. ¿Se han instalado puertas y cortinas resistentes al fuego?			
22. ¿Existe un protocolo para notificar inmediatamente cualquier posible fuente de incendio?			
23. ¿La institución cuentas con alarmas de incendio?			
24. ¿Se lleva a cabo la limpieza y mantenimiento de extractores de humo?			
25. ¿El personal está informado sobre la ubicación de las salidas de			
26. ¿La instalación cuenta con botón para llamar bomberos?			
27. ¿Existe sistema de comunicación de emergencia en caso de incendio?			
Realizado por: Demera Moreira María Micaela **Fecha:**	**Revisado por:** **Fecha:**		

Tabla 10 Análisis de riesgo de Incendio

Cuestionario para el análisis de riesgos para la institución Educativa Heriberto Rodríguez Angulo			C 3 Página 3 de 5
Daño de equipo			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
1. ¿La electricidad es estable en la institución?			
2. ¿Tiene reguladores de voltaje cada computadora?			
3. ¿Las computadoras tienen nuevos componentes?			
4. ¿Poseen personal para el mantenimiento de las computadoras?			
5. ¿Mantienen las computadoras encendidas todo el tiempo?			
6. ¿Tiene protocolos de uso para las computadoras?			
7. ¿Las computadoras cuentan con enfriamiento para controlar un sobrecalentamiento?			
8. ¿Los cables de las computadoras cuentan con protecciones?			
9. ¿La institución cuenta con computadoras para remplazar las fallas de una computadora activa?			
10. ¿El personal docente cuenta con conocimientos para remplazar una computadora si hay fallos en una que se está utilizando?			
11. ¿Existe medidas para proteger los equipos del laboratorio de condiciones ambientales con la humedad?			
12. ¿Se lleva un registro de mantenimiento preventivo?			
13. ¿Se ha producido daños en equipos en el último año?			
14. ¿Se realizan inspecciones regulares de los equipos?			
15. ¿Se cuenta con un plan de contingencia en caso de fallos de equipos?			
16. ¿Existe un plan de respuesta ante cortes de energía prolongados?			
17. ¿Existen áreas con restricciones de acceso para proteger equipos críticos?			
18. ¿Se han experimentado cortes de energías en el último año?			
19. ¿Se protegen los equipos contra fluctuaciones de energía?			
20. ¿Se realiza simulacro en caso de daños de equipo?			
21. ¿Cuenta con una antivirus los equipos de la institución?			
22. ¿Los equipos de la institución está cerca de su vida útil?			
23. ¿Se encuentra los equipos de cómputo actualizados?			
24. ¿Existe políticas de uso de los equipos cómputo para evitar daño?			
25. ¿Los equipos dañados de cómputo ha sido reparado?			
Realizado por: Demera Moreira María Micaela **Fecha:**	**Revisado por:** **Fecha:**		

Tabla 11 Análisis de riesgo de Daños de equipos

Cuestionario para el análisis de riesgos para la institución Educativa Heriberto Rodríguez Angulo			C 6 Página 4 de 5
Inundación			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
1. ¿Has experimentado alguna vez una inundación dentro de las instalaciones de la institución?			
2. ¿Existen un sistema de detección de inundación instalada?			
3. ¿Se realiza regularmente un mantenimiento preventivo de inundaciones?			
4. ¿La institución cuenta con un plan de contingencia para enfrentar inundaciones?			
5. ¿Se llevan a cabo simulacros de inundación?			
6. ¿Cuenta con procedimiento de emergencia establecido en caso de inundación?			
7. ¿Los centros de datos están elevados para evitar daños por inundaciones?			
8. ¿La institución cuenta con sistemas de energía de respaldo para mantener operativos los sistemas durante una inundación?			
9. ¿Se realizan evaluaciones de registro periódico para identificar nuevas amenazas de inundaciones?			
10. ¿Hay procedimientos establecidos para desconectar rápidamente los sistemas electrónicos?			
11. ¿La institución tiene acuerdos de recuperación ante desastres con proveedores externos para garantizar la continuidad?			
12. 12. ¿Se realiza capacitación regular al personal sobre cómo responder ante situaciones de inundaciones?			
13. ¿Existe un protocolo para evaluar y documentar los daños causados por inundaciones?			
14. ¿La institución mantiene un inventario actualizado de los equipos de la tecnología para facilitar la recuperación?			
15. ¿Se lleva a cabo una revisión post inundación para analizar las elecciones aprendidas y mejorar la continuidad de las medidas de prevención?			
Realizado por: Demera Moreira María Micaela **Fecha:**	**Revisado por:** **Fecha:**		

Tabla 12 Análisis de riesgo de Inundación

Cuestionario para el análisis de riesgos para la institución Educativa Heriberto Rodríguez Angulo			C 3 Página 5 de 5
Malware			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
1. ¿La institución utiliza software antivirus actualizado en el sistema?			
2. ¿Se implementa regularmente un escaneo de malware en los equipos?			
3. ¿Todos los docentes reciben capacitación sobre prácticas seguras de navegación y correo electrónico?			
4. ¿La institución utiliza un firewall para proteger su red contra posibles amenazas?			
5. ¿Los docentes reciben capacitación sobre la prevención de malware?			
6. ¿Se realizan auditorías periódicas de seguridad en la infraestructura de la red en la institución?			
7. ¿La institución utiliza software de prevención de pérdida de datos para proteger cada uno de ellos?			
8. ¿Existe un proceso establecido para la actualización regular de sistemas operativos y aplicaciones?			
9. ¿Se monitorea y registran los eventos de seguridad en los sistemas de la institución?			
10. ¿La institución realiza pruebas de penetración para identificar posibles vulnerabilidades en sus sistemas?			
11. ¿Todos los docentes tienen permiso de acceso mínimos en los equipos?			
12. ¿Los equipos del laboratorio cuenta con contraseña sólida?			
13. ¿La institución utiliza Algún filtrado web para prevenir la visita del sitio?			
14. ¿Los correos electrónicos se someten a análisis antes de abrirse?			
15. ¿Se implementan medidas de control de acceso físico a los equipos de cómputo?			
16. ¿La institución utiliza algún tipo de cifrado para proteger la comunicación interna y externa?			
17. ¿Existe algún plan de respuesta a accidentes en caso de detectarse malware o ciberataques?			
18. ¿Se realiza copia de seguridad regular de los datos?			
19. ¿Los docentes están conscientes de la importancia de informar alguna actividad sospechosa?			
20. ¿Se utiliza medidas de control de dispositivos como USB?			
21. ¿Existen restricciones para la instalación de software no autorizados en los equipos?			
22. ¿Se lleva a cabo un seguimiento constante de los parches de seguridad y actualizaciones?			
23. ¿Existe un protocolo específico para maneja posibles infecciones de malware?			
24. ¿Se prohíbe descargar software no autorizado de los dispositivos?			
25. ¿Cuánta con un plan de respuesta rápida en caso de ataque de malware?			
Realizado por: Demera Moreira María Micaela **Fecha:**	**Revisado por:** **Fecha:**		

Tabla 13 Análisis de riesgo de Malware

4.4.2 Ejecución

4.4.2.1 Recolección de datos

Para lograr obtener datos de los riesgos que cuenta actualmente la institución, se necesitó realizar tres tipos de instrumento que fueron, el instrumento de cuestionario para el análisis de los riesgos y así mismo el instrumento de cuestionario de requisito de las normas ISO 27001 y como ultimo instrumento el cuestionario de controles de las normas ISO 27001.

La evaluación de los instrumentos ya mencionado se lo realizó al director Marco Anthonio Caja, ya que él también es el encargado del laboratorio y área informática de la unidad educativa Heriberto Rodríguez Angulo. En el instrumento de análisis de riesgo se tomaron en cuenta las siguientes amenaza y vulnerabilidades que fueron: robo, incendio, daños de equipos, inundaciones, malware. En cada uno de esa amenaza y vulnerabilidades se realizaron las preguntas necesarias que este caso fueron 25, pero excepto de inundaciones ya que en este apartado se realizó 15 preguntas, y en el apartado de incendio se realizó 27.

***Ilustración** 2 Plantel educativo*

***Ilustración** 3 Constancia de guardia de seguridad*

Ilustración ***4 Laboratorio de cómputo***

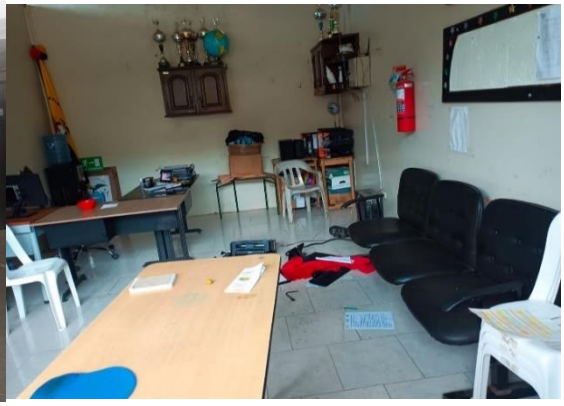


Ilustración ***5 Ultimo accidente de robo***

Ilustración ***6 Cerradura con la que cuenta la institución***

Ilustración ***7 Encuesta sobre los Instrumentos de Evaluación de Controles, Requisitos y Riesgos***

Ilustración ***8 Cortina del laboratorio***

Ilustración ***9 Extintor del laboratorio***

Ilustración ***10 Cableado de los equipos***

Ilustración ***11 Breaker de electricidad***

Ilustración ***12 Regulador de voltaje***

Ilustración ***13 Estado actual de la instalación***

Ilustración ***14 Muro para evitar el ingreso de agua***

Ilustración ***15 Instalaciones con humedad***

Ilustración 16 Señalización de salida de emergencia

4.4.2.2 Tabulación de datos

Los instrumentos la cuales se utilizaron para la recolección de dato fueron tabulados en Excel, que permitió analizar, de una forma más fácil mediante gráfico y porcentajes.

En el instrumento de cumplimiento de requisito se evaluó con una escala del 0 al 5, esta escala permitió evaluar el nivel de cumplimiento de los requiso que cuenta la institución educativa Heriberto Rodríguez Angulo, basándose en las normas ISO 27001. A continuación, veremos la tabla que se utilizó para evaluar:

(Nivel 0): No existencia	No hay reconocimiento de la necesidad del control o requisito
(Nivel 1): Ad-hoc	Existe cierto reconocimiento de la necesidad de control interno o requisito. Se aplica para algún problema o tarea específica, no generalizable
(Nivel 2): Ejecutado	Los controles existen, pero no están documentados.
(Nivel 3): Definido	Los controles están en su lugar y están documentados adecuadamente.
(Nivel 4): Manipulable y medible	Existe un control interno sobre la aplicación de controles y cumplimiento de requisito.
(Nivel 5): Optimizado	Existe un control interno y continúo sobre la aplicación de controles y cumplimiento de requisitos. Se mide la eficacia de los controles estableciendo objetivos de mejora.

Tabla 14Tipo de escala para cumplimiento de requisito

Por medio de la tabla ya mostrado, logramos evaluar los requisitos de las normas ISO 27001, para así calcular los porcentajes de cumplimiento de las normas y lograr calcular también el porcentaje de brecha. A continuación, los datos calculados de la evaluación ya realizada:

REQUISITOS		PREGUNTA	CUMPLIMIENTO	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	0,50	10%	90%	No cumple
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	1				
	4.2 Expectativas de las partes interesadas	1.- ¿Se han identificado las partes interesadas?	0				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	0				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	0				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información documentada?	0				
	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?	0				

Tabla 16 Forma en la que se evaluó el cumplimiento de requisito

	REQUISITO DE ISO 27001	Cumple la Norma	BRECHA
1	4. Organización y Contexto	10%	90%
2	5. Liderazgo	18%	82%
3	6. Planificación	15%	85%
4	7. Soporte	40%	60%
5	8. Operación	20%	80%
6	9. Evaluación y desempeño	17%	83%
7	10. Mejora	0%	100%
	Promedio Requisitos	**17%**	**83%**

Tabla 15 Resultados obtenido del porcentaje de cumplimiento de las normas ISO 27001 de Brecha

En el instrumento de cumplimiento de controles, mediante una tabla de evaluación del 0 al 2 se puedo evaluar los porcentajes de cumplimiento de controles basándose en las normas ISO 27001. Para evaluar el cumplimiento de controles se utilizó la siguiente tabla:

SI	*1*
NO	*0*
No Aplica	*2*

Tabla 17 Tipo de escala para evaluar el cumplimiento de control

Mediante la tabla ya menciona, se puedo calcular porcentaje de controles de cumplimiento y no cumplimiento arrogando así un promedio total de las cláusulas de las normas 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?	1	*1*
			2.- ¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	0	*2*
		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?	1	*3*
			2.- ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	1	*4*
			3.- ¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	1	*5*

Tabla 18Forma en la que se evaluó el cumplimiento de controles

logrando así visualizar en manera general los cumplimientos de controles que cumple la institución educativa Heriberto Rodríguez Angulo. A continuación, la tabla de porcentaje de cumplimiento de control de institución ya mencionada.

CLAUSULAS	%Cumplimiento	% no Cumple
A5 Políticas de Información	50%	50%
A6 organización de Seguridad de la Información	71%	29%
A7 seguridad de los recursos humanos	0%	100%
A8 gestión de activos	50%	50%
A9 Control de acceso	14%	86%
A10 Criptografía	0%	100%
A11 Seguridad Física y del entono	50%	50%
A12 seguridad en las operaciones	31%	69%
A13 Seguridad en las comunicaciones	29%	71%
A14 Adquisición, desarrollo y mantenimiento de sistemas de información	0%	100%
A15 Relación con proveedores	0%	100%
A16 Gestión de incidentes de seguridad de la información	43%	57%
A17 Gestión de la Continuidad del Negocio	25%	75%
A18 Cumplimiento	0%	100%
PROMEDIO	***26%***	***74%***

Tabla 19 Resultados obtenido del porcentaje de cumplimiento de control

En los instrumentos de cuestionario de análisis de riesgo fue tabulado con los siguientes en una valoración del 0 al 2. En la siguiente tabla veremos el impacto de riesgo que tiene cada escala.

Escala estimada	
0	Representa riesgo
1	Representa seguridad
2	No aplica

Tabla 20 Tipo de evaluación para calcular el análisis de riesgos.

Esta escala se utilizó para evaluar cada pregunta que habíamos realizado para el instrumento de cuestionario de análisis de riesgo. Dependiendo la respuesta de la entrevista que se elaboró dentro de la institución educativa Heriberto Rodríguez Angulo, se utilizó la escala que ya se habíamos mencionado para poder evaluar el impacto del riesgo que cuenta la institución.

14	¿La institución cuenta con cerramiento físico en sus instalaciones?	0
15	¿Las computadoras se almacenan en gabinetes o cajas de seguridad?	1
16	¿El personal docente cuenta con tarjeta de identificación?	0
17	¿La institución cuenta con botón de pánico para cuando suceda un robo?	0
18	¿Se almacenan las computadoras de manera que sea difícil de mover?	0
19	¿El personal docente tiene acceso a todas las maquinas?	0
20	¿Tienen procedimientos ante la pérdida o robos de computadoras?	1
21	¿Se cuenta con un equipo de repuesto de emergencia en caso de robo?	0
22	¿Las computadoras están anclados con cable de seguridad?	0
23	¿Cuenta la intitución con dector de movimientos?	0
24	¿El personal esté entrenado de como reportar incidentes de seguridad?	0
25	¿La institución cuenta con un seguro de Robo?	0
	TOTAL CONTROLES NO APLICADOS:	1
	TOTAL DE CONTROLES EVALUADOS	24
	TOTAL CONTROLES SEGURIDAD:	10
	TOTAL CONTROLES RIESGO:	14
	PORCENTAJE SEGURIDAD	42%
	PORCENTAJE RIESGO	58%
		100%

Tabla 21 Forma en la que se evaluó el análisis de riesgos.

4.4.2.3 Impacto

Cuando se menciona el impacto, se hace referencia a diversos tipos de consecuencias no anticipadas en un área específica. En contraste, según las normas ISO 27001, el impacto se refiere directamente a la magnitud de los posibles daños que cualquier riesgo pueda causar en una organización, pero en esta situación daños, que puede ocasionar en la institución educativa Heriberto Rodríguez Angulo, y se evalúa en una escala del 1 al 5, esta escala se refiere a que tan probable es que ocurra ese impacto. Los impactos de riesgo se evalúan con los factores de integridad, disponibilidad y confidencialidad, así como veremos a continuación:

Columna1	CONFIDENCIALIDAD	DISPONIBILDAD	INTEGRIDAD	PROMEDIO
ROBO	5	5	3	4
INCENDIO	3	5	4	4
DAÑO DE EQUIPOS	2	5	2	3
INUNDACIÓN	3	5	2	3
MALWARE	5	3	5	4

Tabla 22 Evaluación realizadas de impacto.

4.4.2.4 Probabilidad

Cuando se habla de probabilidad, se hace referencia a la posibilidad de que ocurra un evento o hecho. En el contexto de las normas ISO 27001, la probabilidad se refiere a qué tan factible es que un riesgo pueda ocasionar un impacto negativo dentro de la institución educativa Heriberto Rodríguez Angulo. A continuación, la tabla de escala para asignar valores de aparición de nivel de probabilidades de riesgo:

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

Tabla 23 Escala para asignación de valores de aparición de nivel de probabilidades de riesgo

La escala que se presenta surge de los instrumentos de análisis de riesgo la, que permitió evaluar los riesgos dependiendo del nivel de probabilidad, si la escuela de educación básica Heriberto Rodríguez Angulo, si tiene un mayor porcentaje de cumplimiento de controles disminuye la posibilidad de riesgo a daños y accidente.

4.4.2.5 Matriz de riesgos

Una matriz de riesgo es una herramienta la cual permite identificar y evaluar la probabilidad de gravedad de riesgo por falta de seguridad que cuenta la organización, que en este caso es la institución educativa Heriberto Rodríguez Angulo.

Mediante la matriz de riesgo permite clasificar los riesgos por categoría de una manera que sea fácil de entender e interpretar, para lograr una mejor compresión de los riesgos evaluados que se encuentra en la institución. A continuación, se presentará la matriz de riesgo que obtuvimos mediante del instrumento de cuestionario de análisis de riesgo aplicado en la institución educativa Heriberto Rodríguez Angulo.

MATRIZ DE RIESGOS				
RIESGO	Aparición probabilidad	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
ROBO	4	5	20	Muy grave
INCENDIO	2	3	6	Apreciable
DAÑO DE EQUIPOS	4	4	16	Muy grave
INUNDACIÓN	3	3	9	Importante
MALWARE	5	4	20	Muy grave

Tabla 24 Evaluación realizada para calcular el nivel de riesgo.

CAPÍTULO V

4.5 EVALUACIÓN DE RESULTADOS

5.1 Informe de Auditoría

Mediante el presente informe se presenta los resultados obtenidos mediante la tabulación que se realizó, para la auditoria de gestión de seguridad de la institución educativa Heriberto Rodríguez Angulo, para visualizar de una mejor forma la falta de cumplimiento de política y controles que cuenta la institución y los porcentajes de riesgo y vulnerabilidades que está expuesta actualmente el plantel educativo.

Dirigido a: Mgtr. Marco Anthonio caja, Ing. director de la Escuela Básica Heriberto Rodríguez Angulo

Motivo: permite a garantizar la seguridad de daños en los equipos como también en riesgo para los docentes y estudiantes de la institución, ya que permite establecer pautas claras, reduciendo los riesgos que puede estar presente en el plantel educativo, también logra fomenta buenas prácticas en el uso de los equipos de cómputo.

5.1.1 Objetivo

- Evaluar el nivel de cumplimiento de normas y política de seguridad en el laboratorio de cómputo de la Unidad Educativa Heriberto Rodríguez Angulo según la norma ISO 27001.
- Identificar los posibles riegos de seguridad informática a los que está expuesto el laboratorio de la Unidad Educativa Heriberto Rodríguez Angulo

5.1.2 Persona relacionada

En el presente trabajo que se realizó de auditoría se contó con la disponibilidad del director Marco Anthonio Caja y los demás docentes de la institución educativa Heriberto Rodríguez Angulo.

5.2 Alcance

Mediante el presente trabajo se aplicaron diferentes tipos técnicas, procedimiento e instrumentó, permitiendo lograr obtener información necesaria para respalda la auditoría realizada en la escuela Básica Heriberto Rodríguez Angulo, tales como:

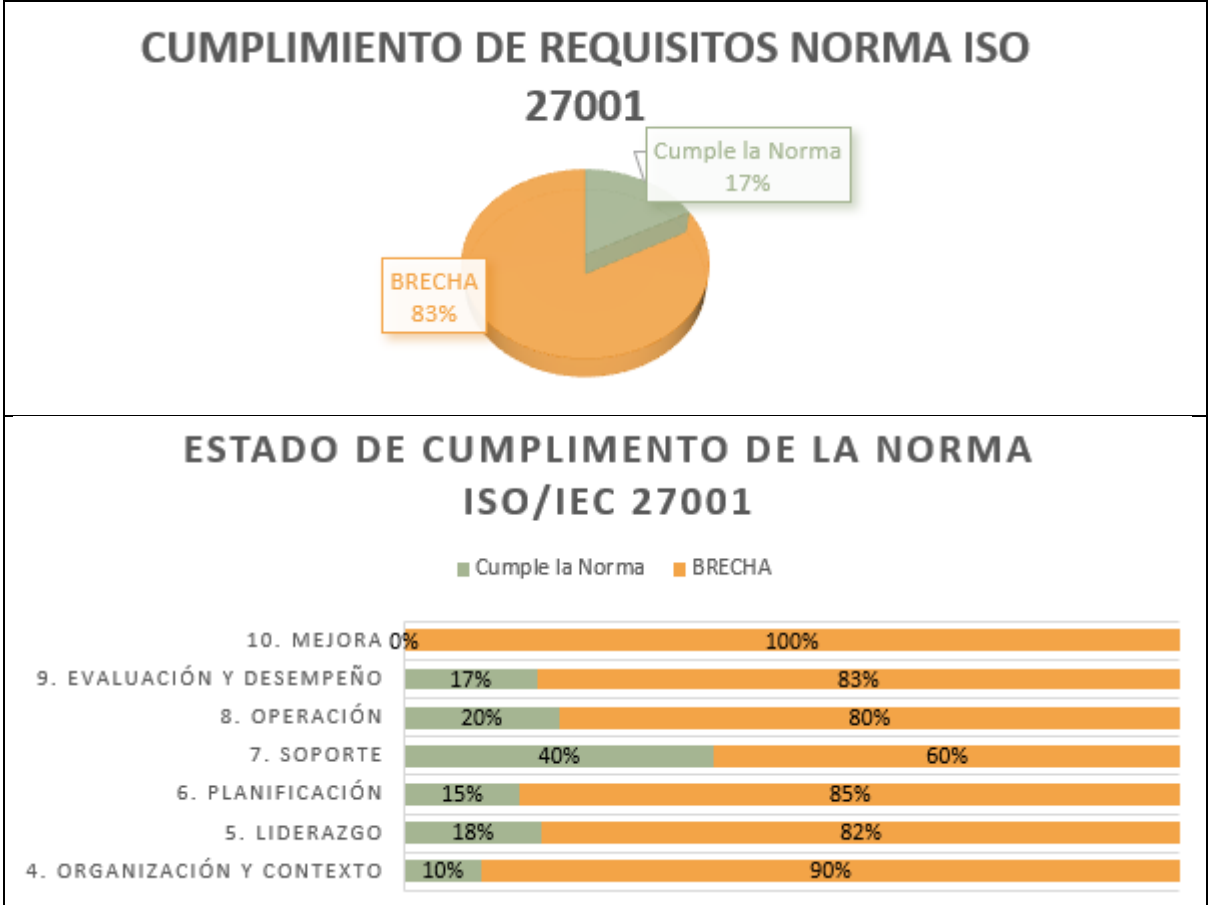
- Revisar las normas ISO 27001
- Diseño de instrumento según ISO 27001 para evaluar cumplimento de controles y política de la institución en el área informática

- Elaborar instrumentos para evaluar riesgos
- Entrevista a director de la institución educativa para llenar instrumento de la auditoría
- Entrevistar de los instrumentos al director encargado de la institución educativa
- Tabulación de datos
- Elaborar matriz de riesgos
- Análisis de resultados
- Elaboración de informe de la auditoría

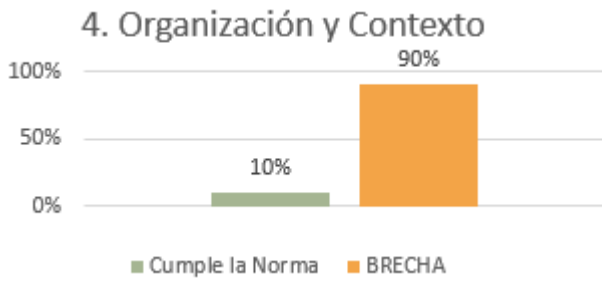
5.3 Hallazgo

Al realizar la auditoria se logra visualizar los riesgos, falta de controles y requisito que cuenta actualmente la institución educativa Heriberto Rodríguez Angulo.

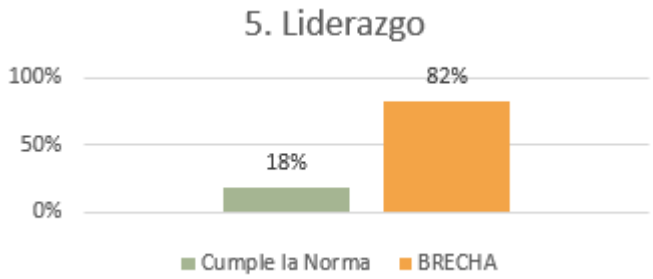
5.3.1 Cumplimiento general de requisitos



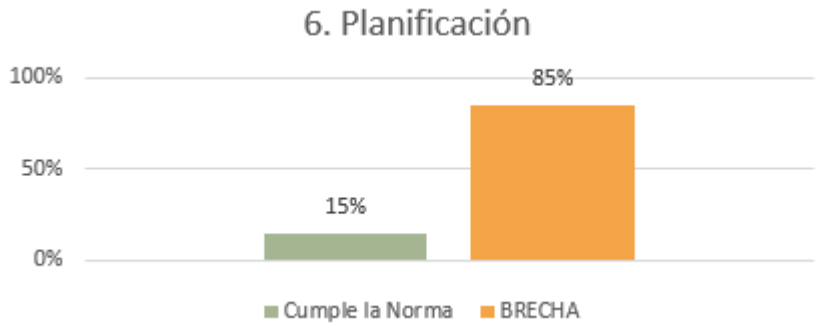
Intepretación: Tomando en consideración el análisis de requisito de estado de cumplimiento de las normas ISO 27001 evaluado, se llegó a cabo la conclusión que hay un nivel de cumplimiento del estándar, que falta de cumplir con las normas de requisito, la es un 83%, lo que significa que tiene un nivel de madurez muy alto, la cual existe ciertos conocimientos de las necesidades en la institución. Logrando notar que los requisitos que cumple el mayor porcentaje de estándar, es soporte ya que casi llega a la mitad que es 40% y el que meno cumple es el requisito de mejora, porque la institución no cuenta con ninguno de los requisitos que pide la norma.



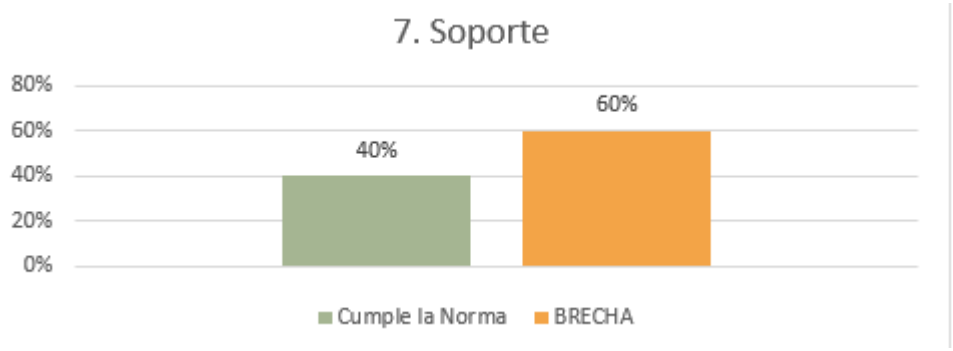
Interpretación: En institución educativa en organización y contexto existe un estado de madurez muy alto por lo tanto el cumplimiento de requisito de organización y su contexto sugiere la institución no están tomando adecuadamente en cuenta la importancia de proteger a información.
En lo requisito que tuviera menos valoración de cumplimiento son:
No se han identificado las partes interesadas.
No existe un listado de requisitos de seguridad de la información para las partes interesadas. Tampoco se dispone con un listado de requisitos relacionados con la seguridad de la información que correspondan a reglamentos, exigencias legales y requisitos contractuales.
No se ha definido el alcance del SGS ni se conserva la información documentada.



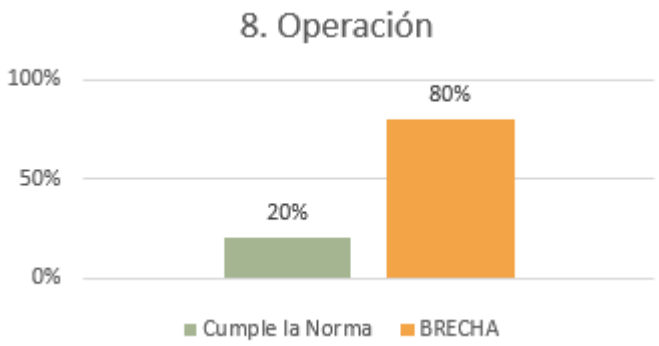
interpretación: En el cumplimiento de requisito de liderazgo se encuentra en un nivel muy alto ya que existe algunos controles que no esté completamente documentado o que se aplique consistentemente. Como los siguientes:
No se han definido los objetivos de la Seguridad de la Información.
No dispone de una dirección ni proporciona los recursos materiales y humanos necesarios.
No se ha creado un marco para el establecimiento de objetivos.
No se ha comunicado la política de Seguridad de la Información a las partes interesadas. No se mantiene documentación sobre la política del SGSI.



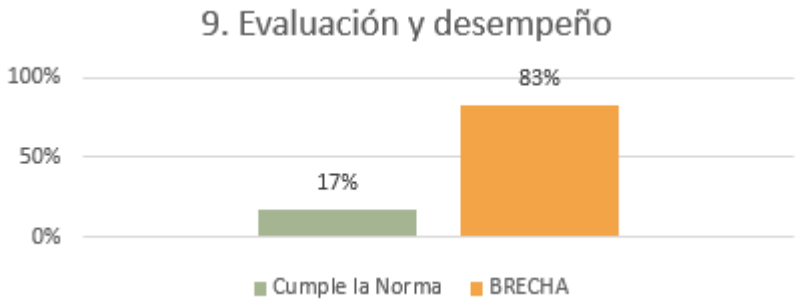
Interpretación: En la parte de requisito de planificación no cumple con las normas suficiente de cumplimiento, la cual cuenta con un nivel de madurez muy alto. La cual existe cierto reconocimiento de los requisitos de planificación, pero no obstante son limitados o inconsistentes y no está completamente documentado, para ello la institución educativa necesita trabaja en la documentación. El origen de un porcentaje alto de la brecha es producido por la siguiente causa:
No hay un plan para abordar riesgos de Seguridad de la Información
Actuado.
No ha identificado ni analizado riesgo mediante evaluación.
Se ha identificado proceso de tratamiento de riesgo, pero no se ha documentado.
No se han establecido criterios para elaborar una declaración de aplicabilidad
No cumplen con los objetivos de la seguridad de la información planificada mediante, Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación



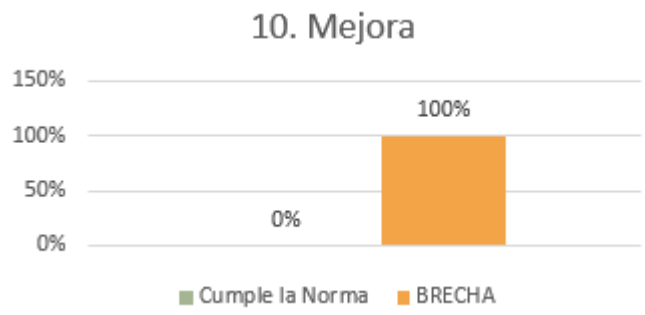
Interpretación: La institución cuenta con un requisito de soporte, la que tiene un nivel de madures medio. Esto significa que alguno requisito de seguridad existen, pero no están documentado de manera forma. La cual la institución debe enfocarse en definir los requisitos para mejorar su nivel de madurez. Una de las cusa de las brechas dentro de la institución son: No se evalúa la competencia en Seguridad de la Información de las personas que realizan tareas que pueden impactar en la seguridad. No se mantiene información actualizada sobre la competencia de las personas. No existe un proceso para comunicar deficiencias o malas prácticas en la Seguridad de la Información.
No se controlan los documentos de origen externo.



Interpretación: La institución educativa en la parte de operación cuenta con un estado de madurez muy alto, la que existe un cierto nivel de conocimiento de control interno, pero se aplica en forma aislada. La brecha tiene un porcentaje elevado por la siguiente causa:
No hay un método para evaluar los riesgos en la seguridad de la información previo a realizar modificaciones en sistema de gestión y procesos de seguridad.
No se define medidas ni planes en la seguridad de la información frente a la modificación de riesgos que controlan los procesos externalizados con respecto a los riesgos para la Seguridad de la Información.
No se ha implementado un plan de tratamiento de riesgos.

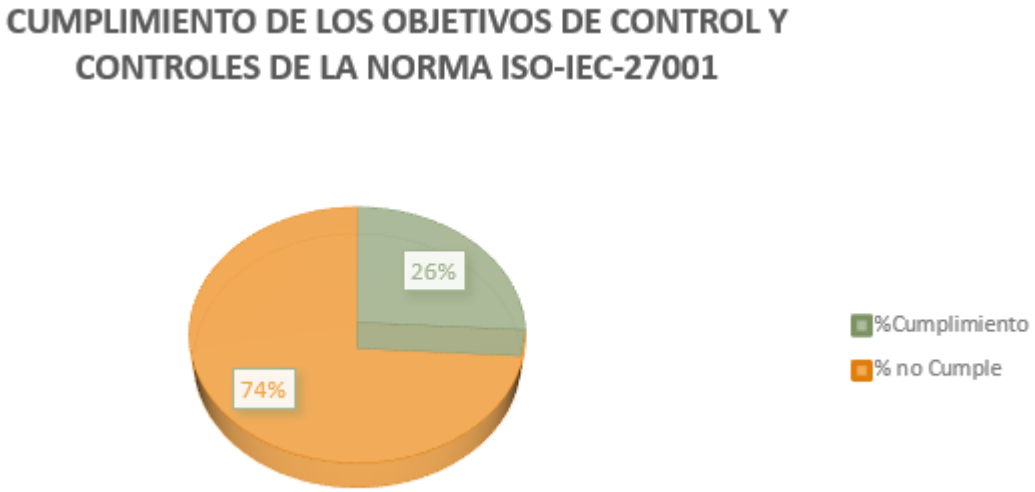


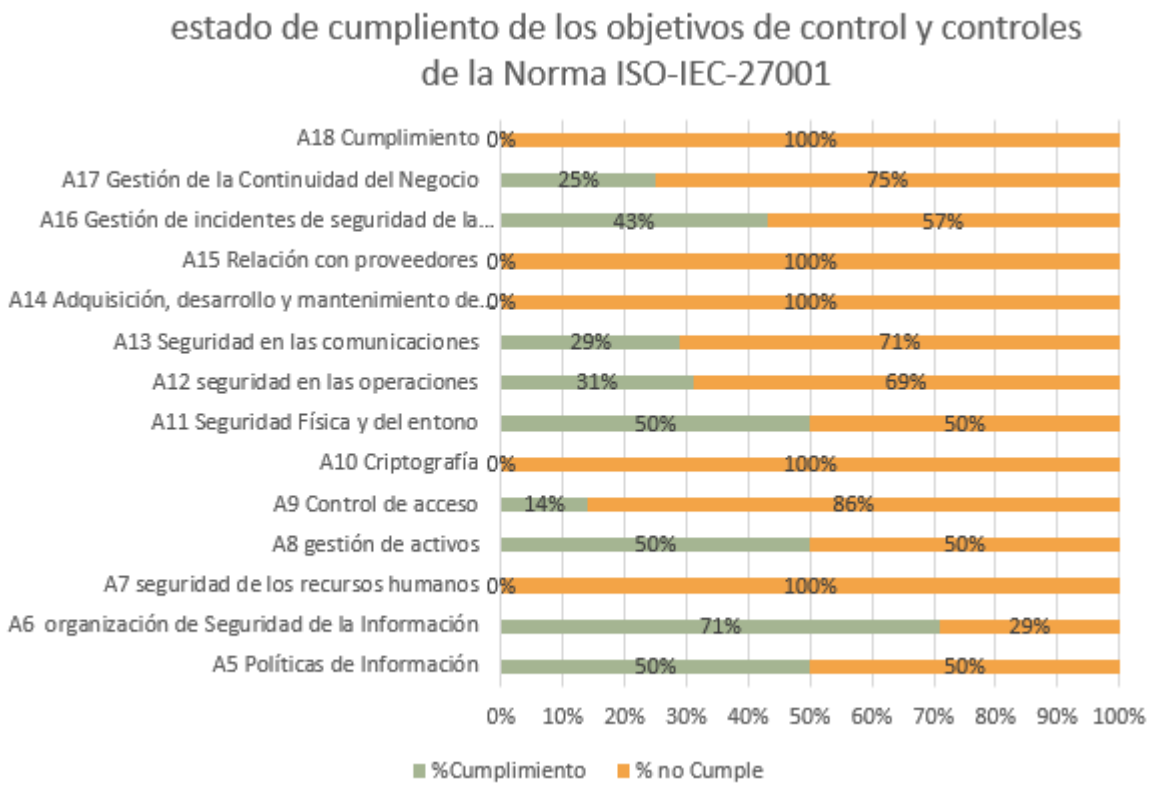
Interpretación: La institución educativa en el requisito de evaluación y desempeño cuenta con estado de nivel de madurez muy alto, la cual indica que la institución cuenta con un conocimiento mínimo de evaluación de desempeño, pero con un enfoque limitado y poco estructurado. Causada por las siguientes causas:
No se ha creado un procedimiento documentado para evaluar los resultados de las mediciones como de la Seguridad de la Información.
No se ha establecido una programación de Auditorías Internas y no se ha asignado responsables.
No hay una programación para los informes de la dirección y no hay evidencia de su realización periódica.



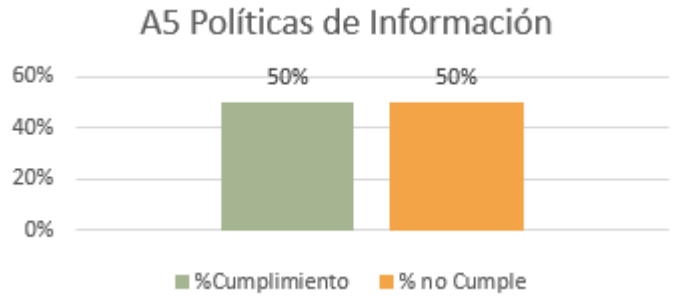
Interpretación: La institución no cuenta con un nivel de cumplimiento total, ya que la institución no tiene ningún proceso o práctica para aborta el requisito de mejora en el término de seguridad de la información, por tal razón cuenta con un nivel de madurez muy alto. Es fundamental que la institución educativa comience a establecer y a desarrollar una mejora continua.
por la siguiente causa tiene en su totalidad una brecha elevada:
No hay un protocolo documentado para detectar y registrar las no conformidades **y** su tratamiento. En cuanto a las acciones correctivas, no se distingue entre las acciones correctivas dirigidas a la no conformidad y las enfocadas en sus causas.
No existe un proceso para asegurar la mejora continua del SGSI mediante la identificación de oportunidades de mejora.

Cumplimiento general de controles

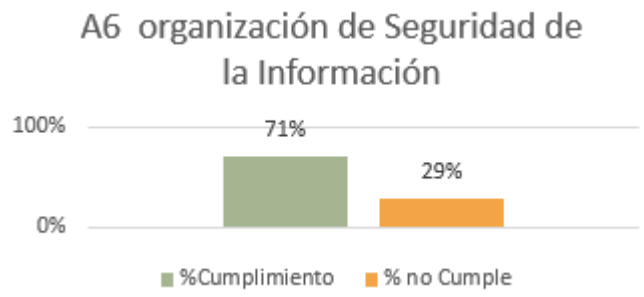




Intepretación: Tomando en consideración el análisis de control evaluado, en el grafico se muestra que la institución educativa no está cumpliendo con los controles de las normas ISO 27001 adecuado la que cuenta con un nivel bajo de controles cumplido. En particular hay área critica con un porcentaje total que no cumple ningún control como Criptografía, Adquisición, desarrollo y mantenimiento de sistemas de información, Relación con proveedores, Cumplimiento, ya que alguno de esos controles no está encargado la institución educativa sino el distrito de educación.



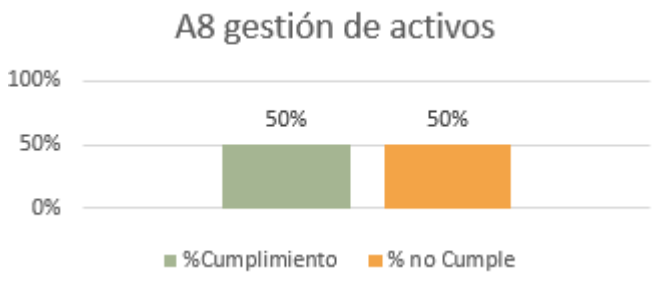
Interpretación: La institución educativa hay un equilibrio exacto entre las políticas de información eso quiere decir que debe trabajar en las áreas faltante para logra alcanzar un nivel de cumplimiento completo y fortalecer su postura de seguridad de la información.
Entre la cusa porque no cumple en su totalidad es la siguiente:
No existe un procedimiento estructurado y comprobable para revisar de las políticas de seguridad de la información.



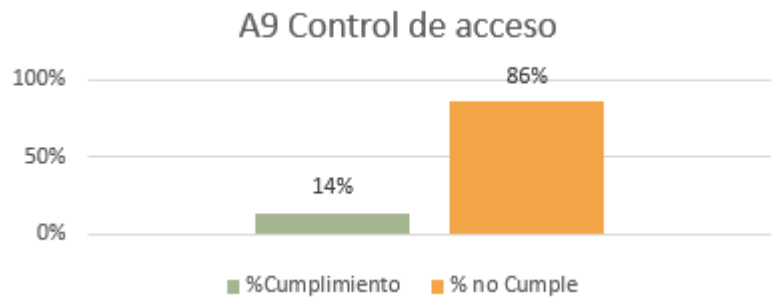
Interpretación: Mediante la evaluación realizada indica que las políticas de organización de seguridad tienen una buena base en término de protección de la información, mostrando un esfuerzo considerable en mantener la seguridad de la información y logra mejor en ciertas áreas para alcanzar un nivel óptimo de seguridad.

No cuenta con todos los controles, por las siguientes causas:
No hay medios ni se han creado vínculos con grupos de interés y asociaciones relacionadas con la seguridad de la información para estar actualizados sobre noticias e información en el área de seguridad. No hay requisitos para tratar temas de seguridad de la información en la gestión de proyectos de la organización.

Interpretación: La institución no cuenta con controles de seguridad del recurso humano ya que ese procedimiento se encarga el distrito de educación y mas no el plantel educativo. Ya que la institución educativa no implementa el área de recurso humano.

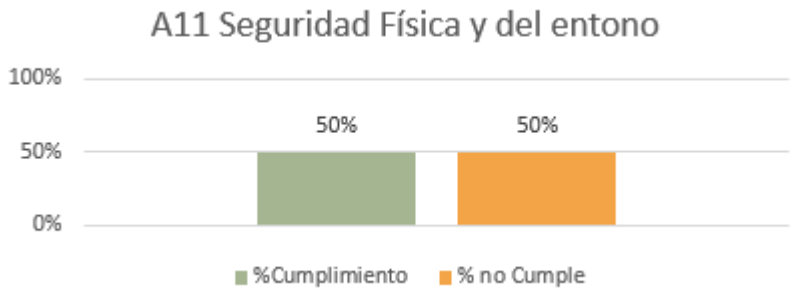


Interpretación: Con los porcentajes se indica la gráfica se refleja, que la mitad de los controles están siento seguido adecuadamente no obstante la otra mitad puede señalar debilidades en ciertas áreas, pero se tiene una base establecida, mas no significa que no necesite mejorar. Algunos controles no cumplidos son:
No se ha hecho un registro de los activos que respaldan en la institución y la información.
No existen controles establecidos para aplicar a soportes extraíbles:
No hay controles definidos para gestionar soportes extraíbles.
Falta de medidas de control establecidas para los dispositivos de almacenamiento extraíbles.
No se han implementado mecanismos de control para el manejo de soportes de datos extraíbles.

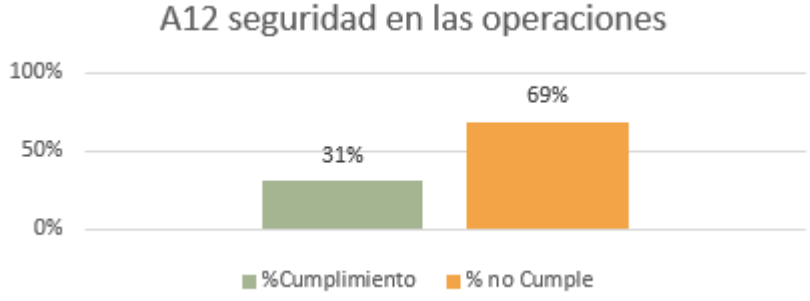


Interpretación: En la institución educativa cuenta solamente con ciertos controles ya que en su totalidad no cumple con los controles, representando así un riesgo significativo y alarmante de seguridad, ya que sin un control de acceso adecuado se expone a cierto riesgo.
Algunas de las cusa son:
No hay una política que establezca controles de acceso a la información con criterios selectivos.
No se han establecido procedimientos formales para registrar a los usuarios.
Falta una política concreta para el manejo de datos considerados secretos.
No se establecen niveles y perfiles específicos de acceso para los sistemas de información que restrinjan la información a la actividad específica a desarrollar.
Falta la implementación de niveles y perfiles de acceso que restrinjan la información a las actividades concretas en los sistemas de información.
No se establecen medidas para asegurar la creación de contraseñas seguras.
No se controla la capacitación y perfil de las personas con permisos de administración en perfiles bajos de seguridad.
No se restringe el acceso a los códigos fuente de los programas ni se controla cualquier tipo de cambio a realizar en ellos.

Interpretación: Se indica mediante el gráfico que no cumple con la política necesaria, ya que no está relaciona la institución educativa con el uso de técnica de criptografía, esta situación presenta un riesgo extremadamente alto, y expone los datos de la institución a acceso no autorizado y posible manipulaciones. Una de las causas de la criptografía que está expuesta la institución es:
No existe una política para el establecimiento de controles criptográficos.



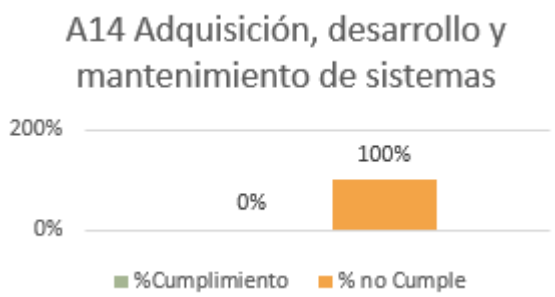
Interpretación: La institución educativa indica que la mitad de los controles de seguridad física está siendo seguido adecuadamente, la cual esta obstante de ciertas debilidades en el área de seguridad física, ya que indica que la otra mitad de ciertos controles no se implementa, la que indica que hay que seguir mejorando.
Algunas causan la cual no cumple en su totalidad con el control es:
No se establecen perímetros de seguridad física.
No hay protecciones para los cables de energía y de datos.
No se planifican ni ejecutan tareas de mantenimiento en los equipos.
No se controla ni autoriza la salida de equipos, aplicaciones, etc.
No se implementan medidas de protección específicas para los equipos utilizados fuera de las instalaciones.



Interpretación: La institución educativa indica que cumple con un tercio de los controles en la seguridad en las operaciones, señalando debilidades en ciertas áreas, teniendo así área significativa que se necesita mejorar. Alguna causa por que no cumples sus controles en totalidad son las siguientes:

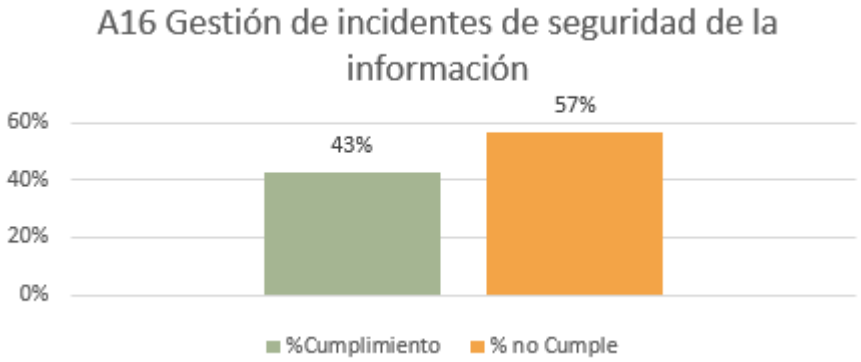
No hay un método establecido para valorar el impacto en la seguridad de la información.
No existen sistemas de detección para Software malicioso y malware.
No se realiza un registro de eventos como intentos de acceso fallidos, desconexiones del sistema, Alertas de fallos Etc.
Claro, aquí tienes la versión parafraseada:
No existe un sistema que garantice la protección de los registros a través de la división de tareas y la realización de respaldos.
No se protegen adecuadamente los accesos ni los de los administradores.
No existe un control para la sincronización de los distintos sistemas.
Las instalaciones de nuevas aplicaciones de software o modificaciones no son verificadas en entornos de prueba y no hay protocolos de seguridad establecidos para su instalación.
Falta la implementación de métodos de control para identificar vulnerabilidades técnicas, como el uso del hacking ético.
Falta de medidas restrictivas que regulen la instalación de software de acuerdo con el personal autorizado.
Falta un sistema de auditoría para examinar la efectividad de las medidas de seguridad en los sistemas.
No se establecen protocolos específicos para la realización de auditorías de software que consideren su impacto en los sistemas.

Interpretación: En la institución educativa cuenta con un tercio de los controles relacionado con la seguridad de las comunicaciones, ya que cuenta con algunos controles implementado, pero aún tiene significativas necesidades de mejoras.
Unas de las cusas por la que no cumple en su totalidad con los controles son:
En el entorno de red no se administra la protección de los sistemas.
No se definen condiciones de seguridad para los servicios de red.
No hay separación ni segregación de redes.
No se establecen límites ni acuerdos de responsabilidad en el intercambio de información.
No se establecen normas o criterios de seguridad para la mensajería electrónica.

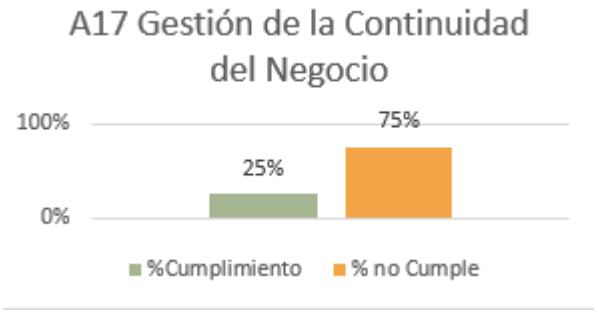


Interpretación: En la institución no se realiza manteamiento de sistema, ya que eso se encarga el distrito de educación, por razones que no tiene autoridad el director para realizar esas actividades de manera independiente, tal razón no cumple en su totalidad ningún control de adquisición, desarrollo y mantenimiento de sistema.

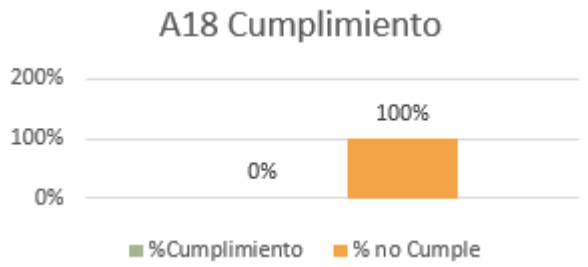
Interpretación: La institución no cuenta con relaciones de proveedores ya que no cuenta con un marco formal para interactuar con proveedores ya que esa función la realiza el distrito de educación, la cual la institución no tiene autoridad para establecer relaciones con proveedores directamente ya que ellos son los encargados de esa área, por tales razones no cumple con ningún control para cumplir el plantel educativo.



Intepretación: La institución educativa tiene una base la cual construir ya que se ha cumplido con cierta controles efectivo, para gestionar incidente de seguridad de la información, obstante a eso no significa que no se necesario aplicar mejora en ciertas áreas.
Cierta causa de no completa algunos controles son:
No se han definido responsabilidades y procedimientos para la respuesta a los incidentes de Seguridad de la Información.
No se han establecido canales apropiados para la comunicación de incidentes relacionados con la Seguridad de la Información.
No se han habilitado mecanismos adecuados para la respuesta a los eventos de Seguridad de la Información.

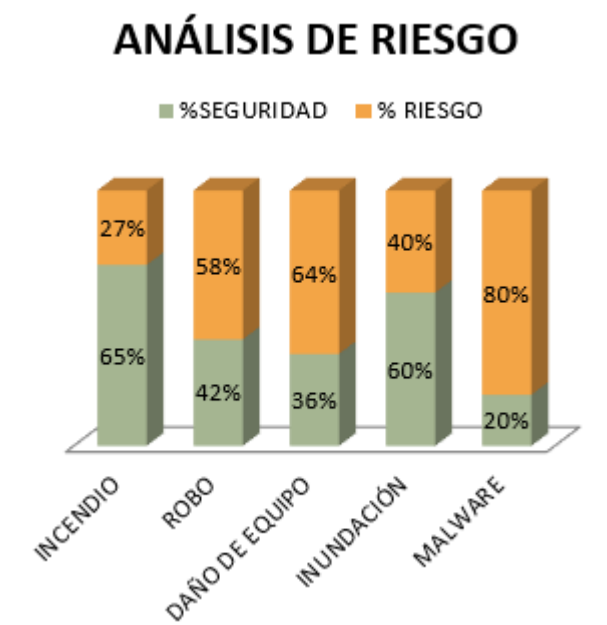


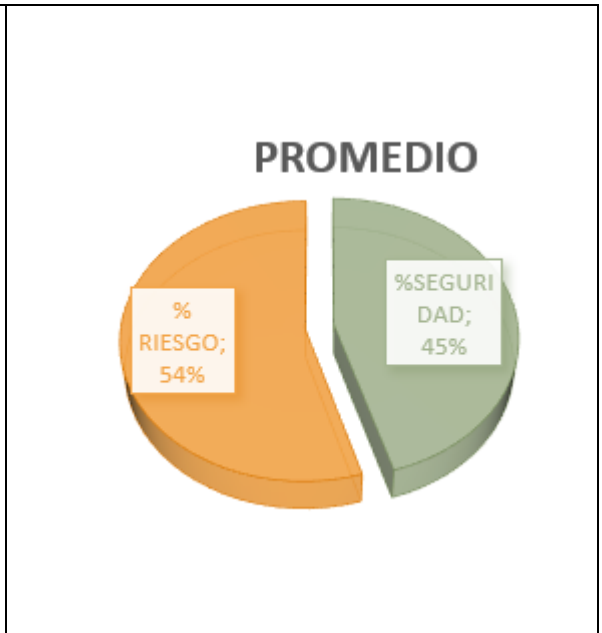
Intepretacción: La institución educativa cuenta con una base muy limitada sobre la cual construir o cumplir los controles de gestión de continuidad, la que se debería desarrollar un plan formal para gestionar ciertos controles.
No se ha elaborado un plan de continuidad en la institución ante incidentes de Seguridad de la Información.
No se han llevado a cabo las medidas de recuperación contempladas en el plan de Continuidad de la institución.
No se han comprobado ni probado las acciones establecidas en el plan de Continuidad de la institución.



Interpretación: La institución educativa se encuentra en una situación crítica, ya que no cumple con ninguno de los controles de cumplimiento. Es necesario abortar esa falta de control ya que sin eso controles la institución está expuesta a riesgo o consideraciones legales. Alguna de esas causas es:
No se han determinado las leyes aplicables a la protección de datos personales ni su cumplimiento.
No se han implementado procedimientos relacionados con la propiedad intelectual. No se han definido criterios para la clasificación de registros y las medidas de protección según los niveles.
No se han establecido medidas para la protección de datos personales conforme a la legislación vigente. No se emplea el cifrado.
No se revisan los controles de Seguridad de la Información.
Falta una revisión periódica para verificar si se están cumpliendo las políticas y controles de seguridad de la información.
Falta una evaluación para verificar la efectividad de las medidas técnicas de protección de la seguridad de la información.

Nivel de Riesgo General



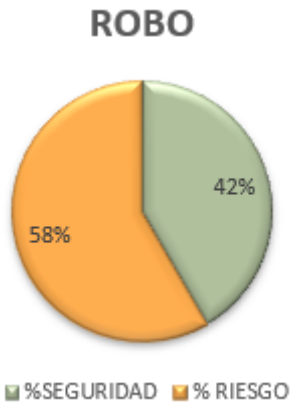


Interpretación: El nivel de seguridad del laboratorio es del 45% que corresponde a un nivel medio.
En el gráfico general, el nivel de riesgo más alto es el de malware, con un 80% de exposición al peligro. También se observa un alto porcentaje de riesgo en el equipo, con un 64%. El control de robo presenta un riesgo del 58%. Entre los controles más seguros, el riesgo de incendio está controlado con un 65% de seguridad y el riesgo de inundación con un 60% de seguridad.

Nivel de Riesgo de Incendio

	**Causas:** La institución no cuenta con detectores de humo No cuenta con sistema de rociadores automáticos Los equipos de cómputo no están adecuadamente ventilados No cuenta con cortinas y puerta resistentes al fuego No cuentan con alarma de incendio
Interpretación: El nivel de riesgo contra incendio es apreciable, en comparación con otro riesgo, de igual manera se merece la debía atención para asegurar la protección adecuada.	

Nivel de Riesgo de Robo

	**Causas:** No cuenta con un sistema de video vigilancia No cuenta con un personal de seguridad En ocasiones ha sufrido accidente de robos No cuenta con protocolo de respuesta en caso de robo No se hace un seguimiento de recuperación de los equipos de cómputo No se utiliza alarma de seguridad No cuenta con un cerramiento adecuado en la institución Los equipos no se almacenan de gabinete de seguridad Los docentes no cuentan con tarjeta de identificación No cuenta con un botón de pánico para cuando suceda un robo El personal docente tiene acceso a todas las computadoras No cuenta con equipo de repuesto de emergencia Los equipos de cómputo no están anclados con cables de seguridad Los equipos no cuentan con dispositivo o cerradora de seguridad No cuenta con seguro de robo
Interpretación: El nivel de riesgo de robo en la institución es muy grave, este corresponde a un nivel de riesgo muy alto, lo que requiere tomar en consideración medidas de seguridad urgente.	

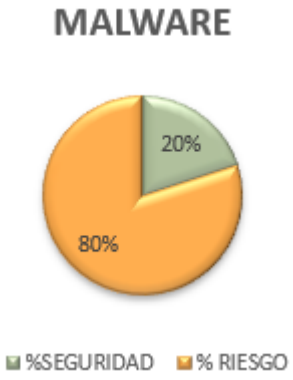
Nivel de Riesgo de Daños de equipos

	**Causas:** Las computadoras no cuentan con nuevos componentes No cuenta con personal para el mantenimiento de las computadoras No cuenta con enfriamiento los equipos Los cables de las computadoras no cuentan con su debida protección No cuenta con computadoras para reemplazar las fallas de una computadora activa Los docentes no cuentan con conocimiento para remplazar una computadora en caso de que tenga fallas No cuenta con un seguro de computadoras No realiza un registro de mantenimiento preventivos de los equipos Se ha producido daños últimamente en los equipos No se realiza impresiones regulares de los equipos No cuenta con un plan de contingencia en caso de fallo de equipos críticos No existe un plan de respuesta antes cortes de energía prolongados No existe área de restricción de acceso para proteger los equipos críticos No se protege los equipos contra fluctuaciones de energía No se realiza simulacro contra incendio En los equipos no cuenta con un antivirus Los equipos ya cumplieron su vida útil No se encuentra los equipos actualizados Los equipos dañados no han sido reparados
Interpretación: El nivel de riesgo en daños de equipo en la institución es muy grave, la cual subraya la necesidad urgente de implementar medidas preventivas y correctiva, para la prevención de los equipos de cómputo del plantel educativo.	

Nivel de Riesgo de Inundación

	**Causas:** No existen un sistema de detección de inundación instalada No se realiza regularmente un mantenimiento preventivo de inundaciones No cuenta con sistemas de energía de respaldo para mantener operativos los sistemas durante una inundación No acuerdos de recuperación ante desastres con proveedores externos para garantizar la continuidad
Interpretación: El nivel de riesgo contra inundaciones está en un nivel de riesgo importante, ya que cuenta con un nivel de seguridad considerado, la que se indica la necesidad de mantener y mejorar las medidas de protección existente y así mismo implementar ciertas medidas que aún está ausente.	

Nivel de Riesgo de Malware

<table>
<tr>
<td> 
</td>
<td>Causas:
No utiliza software antivirus actualizado en el sistema
No implementa regularmente un escaneo de malware en los equipos
Los docentes no reciben capacitación sobre prácticas seguras de navegación y correo electrónico
La institución no utiliza un firewall para proteger su red contra posibles amenazas
Los docentes no reciben capacitación sobre la prevención de malware
No se realiza auditorias de seguridad en la red
No utiliza software de prevención para pérdida de datos
No existen un proceso establecido para la actualización regular de sistemas operativos
No se monitorea los eventos de seguridad en los sistemas No realiza pruebas de penetración para identificar posibles vulnerabilidades en sus sistemas
Los equipos del laboratorio no cuentan con contraseña sólida
No cuenta con filtrado web para prevenir la visita del sitio
Los correos electrónicos no se someten a análisis antes de abrirse
No Se implementan medidas de control de acceso físico a los equipos de cómputo
No utiliza algún tipo de cifrado para proteger la comunicación interna y externa
No existe plan de respuesta a accidentes en caso de detectarse malware o ciberataques
No realiza copia de seguridad regular de los datos
No existe protocolo específico para maneja posibles infecciones de malware
No Cuánta con un plan de respuesta rápida en caso de ataque de malware</td>
</tr>
<tr>
<td colspan="2">Interpretación: En el nivel de riesgo de Malware en la institución educativa es de un nivel muy grave, ya que tiene un porcentaje alto de riesgo, la cual se indica una necesidad urgente de implementar meditas preventiva para reducir esta vulnerabilidad, poniendo así en riesgo los equipos e información del plantel educativo.</td>
</tr>
</table>

5.4 Opinión

A finalizar la auditoría se puedo obtener el nivel de cumplimiento de los requisito y controles de seguridad de las normas ISO 27001, la cual es el siguiente:

Institución Educativa	% de cumplimiento de Requisito de seguridad	% de cumplimiento de controles de seguridad
Escuela Básica Heriberto Rodríguez Angulo	17% (Baja)	26% (Baja)

Tabla 25 Porcentaje de cumplimiento de los requisito y controles del plantel educativo

La escuela básica Heriberto Rodríguez Angulo se ubica en un nivel de cumplimiento de madurez parciamente según las normas ISO 27001, las que se indica que algunos controles existen, pero no están documentado de una forma adecuada, ya que abarca solamente ciertos aspectos de las norma.

Institución Educativa	Nivel de Madurez
Escuela Básica Heriberto Rodríguez Angulo	Parcial (Medio)

Tabla 26 Nivel de madurez de seguridad

La escuela básica Heriberto Rodríguez Angulo se ubica en un nivel de madurez dos, que es un nivel ejecutable según las normas ISO 27001, indica que algunos controles existen, pero no están documentado de una forma adecuada. El plantel educativo cuenta con el conocimiento de la importancia de tener controles de seguridad.

Escuela Básica Heriberto Rodríguez Angulo			
Riegos	**Valor del porcentaje de seguridad**	**Valor del porcentaje de riesgo**	**Nivel de riesgo**
Incendio	65%	27%	Apreciable
Robo	42%	58%	Muy grave
Daño de equipos	36%	64%	Muy grave
Inundación	60%	40%	Importante
Malware	20%	80%	Muy grave

Tabla 27 Valoración de riesgo

La escuela básica Heriberto Rodríguez Angulo se enfrenta con un nivel grave de riesgo tales como robo, daños de equipos y malware, la cual es un alto impacto de amenaza la que es necesario prevenir y abortar periódicamente antes de que ocurra y afecte a la institución, en cambio en el riesgo de inundación también se logra considera un riesgo importante para tomar en cuenta y considera implementar mas medida de seguridad, también contamos con un nivel apreciables en incendio, aunque se un nivel de riesgo menor aun debe ser considerado en cuenta.

5.5 Conclusiones y Recomendaciones de la Auditoría

5.5.1 Conclusiones

Se concluyo que la escuela Básica Heriberto Rodríguez Angulo no toman en consideración la importancia de la seguridad ya que no cuenta con cierto requisito y controles de seguridad, logrando así cierta brecha de vulnerabilidades y amenaza en el plantel educativo, la que se debe tomar en cuenta y llegar a saber sobre las políticas de controles y requisito para tener cuidado de las posibles amenazas que se llegara a dar.

5.5.2 Recomendaciones de la Auditoría

Se recomienda un manual de seguridad ya que el Manuel proporciona directrices claras y normas que permite garantiza la protección y seguridad de los equipos y así mismo de las instalaciones del plantel educativo. Un manual puedes ser una herramienta muy valiosa para la importancia de prevenir riesgo y vulnerabilidades. A continuación, el manual:

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Fue importante analizar los problemas que se encontraba actualmente en la escuela básica Heriberto Rodríguez Angulo la mediante este proceso se reveló áreas de vulnerabilidad y deficiencia que proporcionó un marco claro para lograr a enfocar la investigación.
- En búsqueda de libros, artículos científico y cierto trabajo actualizados permitió un conocimiento entendible de las variables dependiente e independiente más allá de eso logramos mejora el intelecto de cómo funciona una auditoria de seguridad basándose en el área tecnológica, la que logramos tener un conocimiento solido para la realización este trabajo.
- Tras el diagnóstico que se realizó mediante las herramientas de encuesta y entrevista se puedo obtener cierta información de gran importancia para la realización de este trabajo, proporcionando una compresión clara de la situación actual, logrando así identificar ciertas vulnerabilidades, amenaza y falta de controles y requisito de seguridad.
- Mediante evaluación de cierto instrumento que se realizó tales como cuestionario de requisito, cuestionario de control según ISO27001y de evaluación de riesgo, dicho instrumento fue de gran importancia en este trabajo, ya que permitió ver resultados actuales de la falta de política y vulnerabilidades que está expuesta la escuela básica Heriberto Rodríguez Angulo.
- Se puedo concluir, que a través del informe de auditoría que se realizó se mostró cierta evidencia, contando así con falta de política y requisito, también con cierta riesgo y vulnerabilidades en el plantel, llegando así elaborar un Manuel de seguridad que pueda ayudar al plantel educativo en reducir cierto riesgo o aumentar más vulnerabilidad y amenaza del plantel.

6.2 RECOMENDACIONES

- Se recomienda a la escuela Básica Heriberto Rodríguez Angulo que se realice evaluación exhausta cada determinado tiempo para identificar si hay nuevas vulnerabilidades o amenaza para lograr así prevenirlas con un tiempo.

- Se recomienda que sea necesario que la persona que está al frente de la institución que es el directo que crea y aplique cierta prevenciones y así mismo que cumpla controles con lo que aún no cuenta.
- Utilizar el manual a la institución educativa Heriberto Rodríguez Angulo para lograr prevenir ciertos accidente o riesgo que se puede presentar en la institución, logrando así disminuir riesgos y vulnerabilidades por la cual está pasando el plantel educativo.

7. BIBLIOGRAFÍAAFÍA

Arcentales-Fernández, D. A., & Caycedo-Casas, X. (2017). Auditoría informática: un enfoque efectivo. http://file:///C:/Users/mz395/Downloads/Dialnet-AuditoriaInformatica-6102836%20(2).pdf

Arteaga, G. (2022, febrero 28). Qué es la investigación de campo: Definición, métodos, ejemplos y ventajas. TestSiteForMe. https://www.testsiteforme.com/investigacion-de-campo/

Avala, A. M. (s/f). Investigación Bibliográfica: Definición, Tipos, Técnicas. http://file:///C:/Users/mz395/Downloads/Investigaci%C3%B3n%20Bibliogr%C3%A1fica%20(3).pdf

Carlos Leonel Escudero Sánchez, L. A. C. S. (2017). Técnica y métodos cualitativi para la investigación científica. Edu.ec. http://repositorio.utmachala.edu.ec/bitstream/48000/14209/1/Cap.3-Dise%C3%B1o%20de%20investigaci%C3%B3n%20cualitativa.pdf

Chávez Tisalema, S. A. (2022). Auditoría informática en la empresa Distribuidora los Paisas [UNIVERSIDAD TÉCNICA DE AMBATO]. https://repositorio.uta.edu.ec/bitstream/123456789/34802/1/T5282i.pdf

Cisneros, O. A. M. (2021). Efectos de la implementación de una auditoría informática a las empresas de seguros a través de la ISO 27001:2013 ubicadas en el norte del DMQ [UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO]. https://dspace.ups.edu.ec/bitstream/123456789/19918/1/UPS-TTQ245.pdf

Fernanda, R. P. E. (2019). Auditoría de calidad a la gestión de seguridad escolar de la Unidad Educativa Particular Interamericano. Edu.ec. https://dspace.uazuay.edu.ec/bitstream/datos/9017/1/14662.pdf

Falcón, V. L., Pertile, V. C., & Ponce, B. E. (2018). La encuesta como instrumento de recolección de datos sociales: Resultados diagnóstico para la intervención en el Barrio Paloma

de la Paz (La Olla) - ciudad de Corrientes (2017-2018). Edu.ar. https://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.13544/ev.13544.pdf

Gerea, C. (2021). Entrevista en profundidad: del diseño al análisis. FREED TOOLS. https://freed.tools/blogs/ux-cx/entrevistas-profundidad

Gonzalez, K. (2019). Pasos e importancia de una auditoría informática. https://www.academia.edu/39375545/Pasos_e_importancia_de_una_auditor%C3%ADa_inform%C3%A1tica

Huamani, R. E. R. (2021). Implementación de un plan de seguridad informática basado en la norma ISO IEC/27002, para optimizar la gestión en la Corte Superior de Justicia de Lima [UNIVERSIDAD PRIVADA DEL NORTE]. https://repositorio.upn.edu.pe/bitstream/handle/11537/29848/Rumiche%20Huamani%20Ruben%20Eduardo_Total.pdf?sequence=2&isAllowed=y

Garrido Álvarez, J. M., & Flores Murillo, J. J. (2022). Análisis del sistema de información en el Catex según norma ISO 27001:2013 [Tesis de licenciatura, Universidad Tecnológica Centroamericana UNITEC]. https://repositorio.unitec.edu/bitstream/handle/123456789/12328/An%C3%A1lisis%20del%20sistema%20de%20informaci%C3%B3n%20en%20el%20Catex%20seg%C3%BAn%20norma%20ISO%2027001-2013.pdf?sequence=1&isAllowed=y

Lino, C. M. L. (2019). Diseño de un plan de seguridad informática para la cooperativa de ahorro y crédito 'Por el Pan y el Agua' de la ciudad de Jipijapa [UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ]. https://repositorio.unesum.edu.ec/bitstream/53000/1543/1/UNESUM-ECU-SIATEMAS-2019-09.pdf

López-Roldán, P., & Fachelli, S. (2017). Metodología de la investigación social cuantitativa. Uab.cat. https://ddd.uab.cat/pub/caplli/2017/185163/metinvsoccua_cap2-4a2017.pdf

Luis, T. M. J. (2020). Plan de gestión de seguridad informática basado en la norma ISO 27001 para el departamento de tecnología de la información en la empresa PlasticaUcho Industrial

S.A [UNIVERSIDAD TÉCNICA DE AMBATO]. https://repositorio.uta.edu.ec/bitstream/123456789/30696/1/Tesis_t1663si.PDF

Lucía, S. N. (2019). La entrevista y la historia de vida. Uoc.edu. https://openaccess.uoc.edu/bitstream/10609/147145/6/MetodosDeInvestigacionCualitativaEnElAmbitoLaboral_Modulo3_LaEntrevistaYLaHistoriaDeVida.pdf

Mamani, M. E. C. (2020). Diseño de un plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001: Caso Universidad Nacional de Moquegua [UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI VICERRECTORADO DE INVESTIGACIÓN ESCUELA DE POSGRADO]. https://repositorio.ujcm.edu.pe/bitstream/handle/20.500.12819/848/Maribel_tesis_grado-academico_2020.pdf?sequence=1&isAllowed=y

Mena, A. J., & Resumen, M. (2020). Estado actual de la auditoría de seguridad en los sistemas de información de educación superior. Edu.co. https://dspace.tdea.edu.co/bitstream/handle/tdea/1391/Informe%20Auditoria%20seguridad.pdf?sequence=1&isAllowed=y

Meneses, J. L. E. (2021). Desarrollo de un sistema web para fortalecer el proceso de auditoría y seguridad informática en instituciones de educación superior [UNIVERSIDAD TÉCNICA DEL NORTE]. http://repositorio.utn.edu.ec/bitstream/123456789/11368/2/04%20ISC%20591%20TRABAJO%20GRADO.pdf

Mera, W. J. N. (2017). Revisión documental: El estado actual de las investigaciones desarrolladas sobre empatía en niñas y niños en las edades comprendidas entre los 6 a 12 años de edad surgidas en países latinoamericanos de habla hispana. Uniminuto.edu. https://repository.uniminuto.edu/bitstream/10656/5218/1/TP_NunezMeraWendyJohanna_2017.pdf

Morante, N. R. N. (2018). Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque

[UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"]. https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

Nieto, N. T. E. (2022). Tipos de investigación. Edu.pe. http://repositorio.usdg.edu.pe/bitstream/USDG/34/1/Tipos-de-Investigacion.pdf

Ordoñes, J. M. (2019). Población y muestra. Slideshare.net. https://es.slideshare.net/juanmontenegro2000/jmo-2019-poblacin-y-muestra

Rey, J. (2019). Conoce el método de observación directa. okdiario.com. https://okdiario.com/curiosidades/conoce-metodo-observacion-directa-3628568

Rengifo, M. E. E. (2022). Propuesta de diseño de un sistema de gestión de seguridad de la información para las áreas de educación y protección social de la Fundación Tierra Nueva con base en la norma internacional ISO/IEC 27001:2013 [UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO]. https://dspace.ups.edu.ec/bitstream/123456789/22192/1/UPS%20-%20TTS676.pdf

Riveros, A. (2019). Fases para implementar la ISO 27001 en una organización. EALDE Business School. https://www.ealde.es/fases-implementar-iso-27001-seguridad-informacion/

Sarah, L. (2022). Cómo implementar el análisis de brechas para alcanzar los objetivos de negocios. Asana. https://asana.com/es/resources/gap-analysis

Tapia, N. (2015). Introducción a la auditoría informática. https://www.academia.edu/15617137/I_Introducci%C3%B3n_a_la_auditor%C3%ADa_inform%C3%A1tica

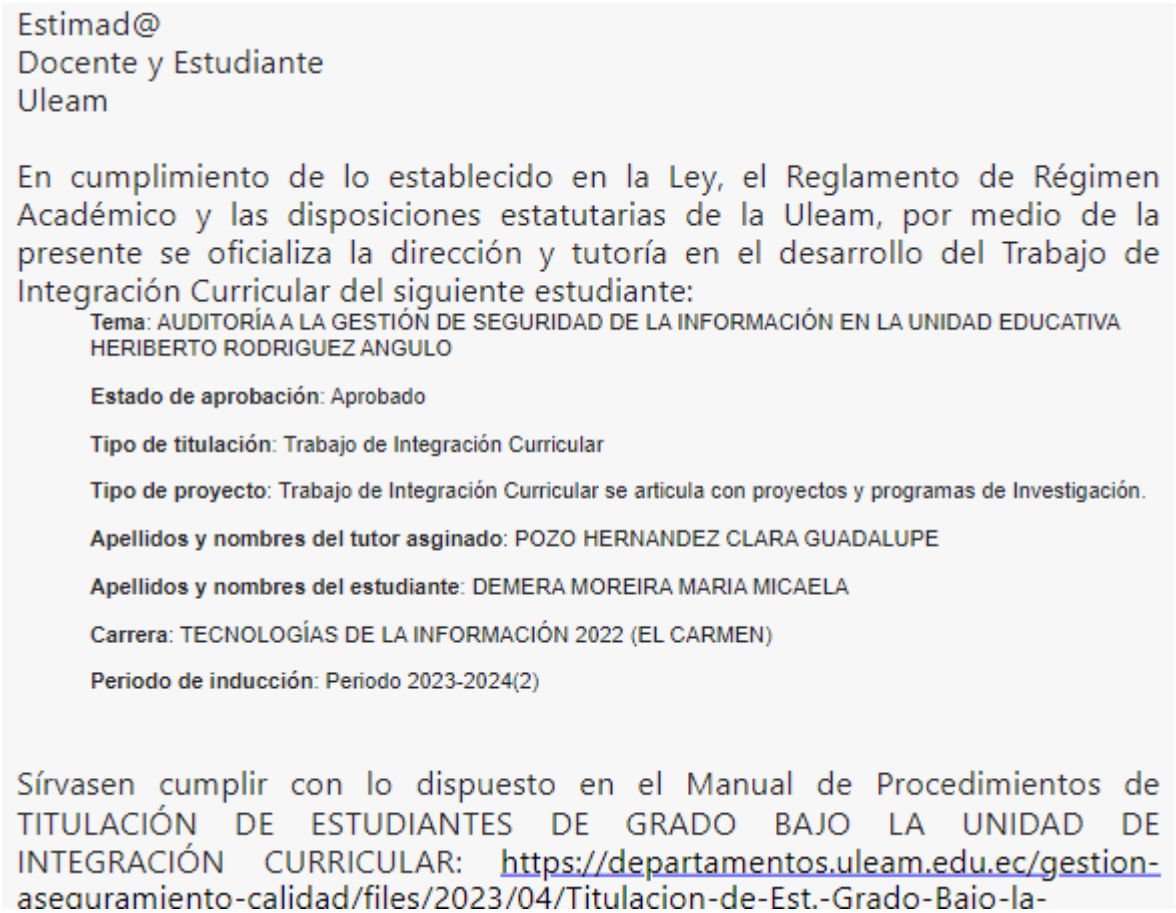
Velastegui, D. X. R. (2019a). Auditoría informática al departamento de tecnología de la información y comunicación del hospital provincial general docente Riobamba [ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO FACULTAD DE ADMINISTRACIÓN DE EMPRESAS]. http://dspace.espoch.edu.ec/bitstream/123456789/11605/1/82T00950.pdf

Velastegui, D. X. R. (2019b). Auditoría informática al departamento de tecnología de la información y comunicación del hospital provincial general docente Riobamba [ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO]. http://dspace.espoch.edu.ec/bitstream/123456789/11605/1/82T00950.pdf

Zambrana, C. M. (2019). Hablemos un poco de encuestas y muestreo. Escueladedatos.online. https://escueladedatos.online/tutorial/hablemos-un-poco-de-encuestas-y-muestreo/

ANEXOS

Anexo A: Asignación de tutor



Estimad@
Docente y Estudiante
Uleam

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

Tema: AUDITORÍA A LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD EDUCATIVA HERIBERTO RODRIGUEZ ANGULO

Estado de aprobación: Aprobado

Tipo de titulación: Trabajo de Integración Curricular

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

Apellidos y nombres del tutor asginado: POZO HERNANDEZ CLARA GUADALUPE

Apellidos y nombres del estudiante: DEMERA MOREIRA MARIA MICAELA

Carrera: TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

Periodo de inducción: Periodo 2023-2024(2)

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

Anexo A: Asignación de tutor

Anexo B: Certificado de la empresa

ESCUELA DE EDUCACIÓN GENERAL BÁSICA
"HERIBERTO RODRÍGUEZ ANGULO"
AMIE: 13H04641

DIREC-CERT-001- El Carmen 13 de agosto del 2024

CERTIFICADO

Por medio del presente, se certifica que la estudiante Demera Moreira María Micaela, portadora del número de cédula 131541766-5, ha realizado con éxito su trabajo de titulación en el laboratorio de computación de esta institución Educativa.

El trabajo titulado "MANUAL DE POLÍTICA DE SEGURIDAD PARA EL ÁREA DE TIC'S DE LA ESCUELA DE EDUCACIÓN BÁSICA HERIBERTO RODRIGUEZ ANGULO", desarrollado bajo la supervisión del Director Marco Cajas, ha sido ejecutado de acuerdo a los lineamientos académicos y con el objetivo de fortalecer la gestión de seguridad de la información dentro de nuestras instalaciones.

Por lo tanto, extendemos el presente certificado en reconocimiento a su esfuerzo y dedicación.

Atentamente,

Lcdo. Marco A Cajas
Director
0994292945
marco.cajas@educacion.gob.ec

Av. Chone Km 36
Barrio, Santa Martha
El Carmen Manabí

Anexo B: *Certificado de la empresa*

Anexo C: Certificado de entrega del manual a la institución

ESCUELA DE EDUCACIÓN GENERAL BÁSICA
"HERIBERTO RODRÍGUEZ ANGULO"
AMIE: 13H04641

CERTIFICADO

DIREC-CERT-002- El Carmen 13 de agosto del 2024

Por medio del presente, se certifica que el manual de políticas de seguridad para el laboratorio de computación ha sido entregado por la estudiante Demera Moreira María Micaela, portadora del número de cédula 131541766-5. Este manual ha sido desarrollado y entregado la institución educativa bajo la supervisión del Director Marco A Cajas y cumple con los lineamientos académicos establecidos por la Escuela de Educación Básica "Heriberto Rodríguez Angulo".

Atentamente,

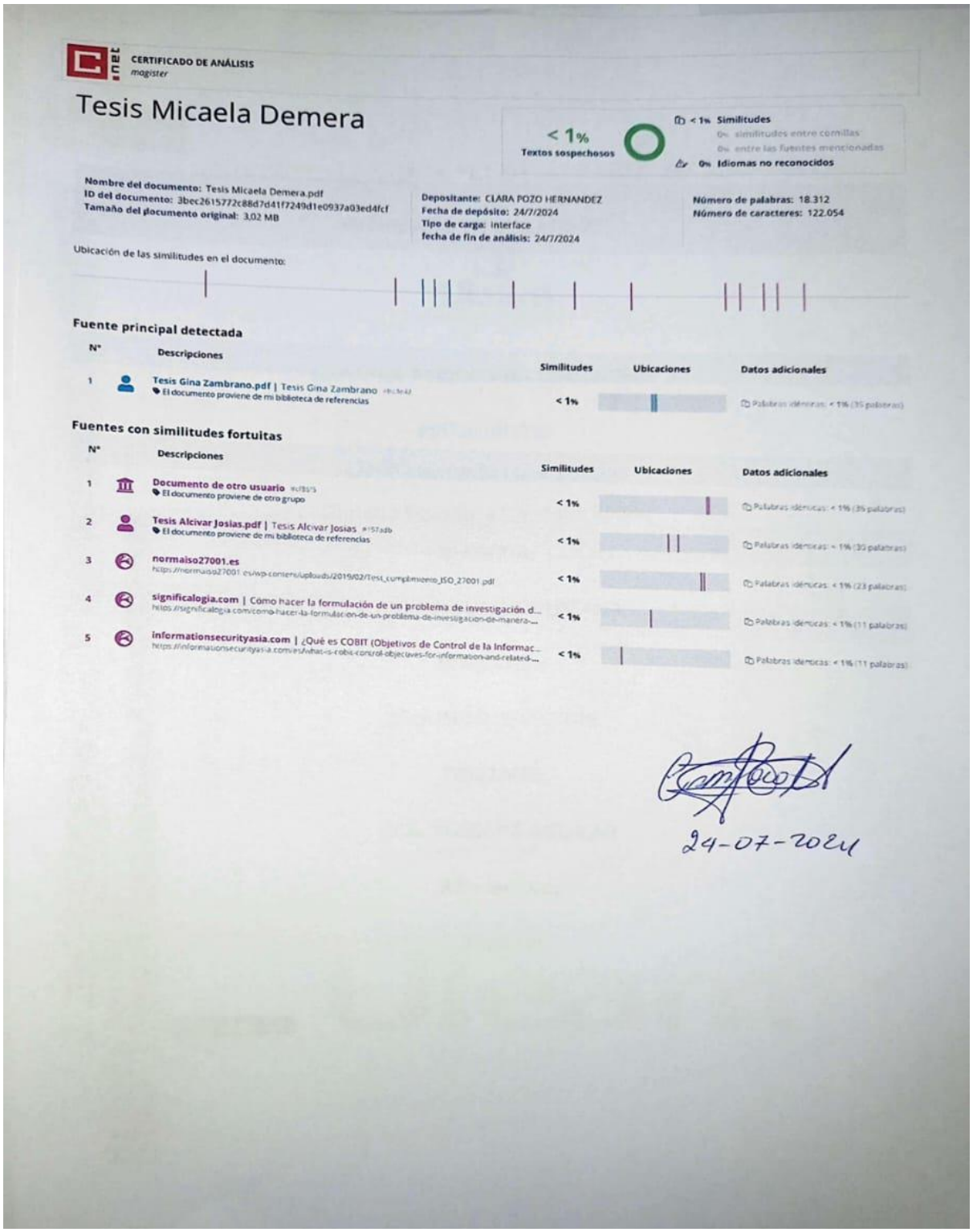
Lcdo. Marco A Cajas
0994292945
marco.cajas@educacion.gob.ec

Demera Moreira María Micaela
Cédula 131541766-5

Av. Chone Km 36

Anexo C: ***Certificado de entrega del manual a la institución***

Anexo D: Reporte del sistema antiplagio



CERTIFICADO DE ANÁLISIS
magister

Tesis Micaela Demera

< 1% Textos sospechosos

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

Nombre del documento: Tesis Micaela Demera.pdf
ID del documento: 3bec2615772c88d7d41f7249d1e0937a03ed4fcf
Tamaño del documento original: 3,02 MB

Depositante: CLARA POZO HERNANDEZ
Fecha de depósito: 24/7/2024
Tipo de carga: interface
fecha de fin de análisis: 24/7/2024

Número de palabras: 18.312
Número de caracteres: 122.054

Ubicación de las similitudes en el documento:

Fuente principal detectada

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Tesis Gina Zambrano.pdf | Tesis Gina Zambrano El documento proviene de mi biblioteca de referencias	< 1%		

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (35 palabras)
2	Tesis Alcivar Josias.pdf | Tesis Alcivar Josias El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (32 palabras)
3	normaiso27001.es https://normaiso27001.es/wp-content/uploads/2019/02/Test_Cumplimiento_ISO_27001.pdf	< 1%		Palabras idénticas: < 1% (23 palabras)
4	significalogia.com | Cómo hacer la formulación de un problema de investigación d... https://significalogia.com/como-hacer-la-formulacion-de-un-problema-de-investigacion-de-manera-...	< 1%		Palabras idénticas: < 1% (11 palabras)
5	informationsecurityasia.com | ¿Qué es COBIT (Objetivos de Control de la Informac... https://informationsecurityasia.com/es/what-is-cobit-control-objectives-for-information-and-related-...	< 1%		Palabras idénticas: < 1% (11 palabras)

24-07-2024

Anexo D: Reporte del sistema antiplagio

Anexo E: Fotografías

*Ilustración **17 Institución educativa***

*Ilustración **18 Guardia de seguridad***

*Ilustración **19 Laboratorio de cómputo***

*Ilustración **20 Último incidente de robo***

Ilustración ***21 Realización de los instrumento según ISO 27001***

Ilustración ***22 Puerta del laboratorio***

Ilustración ***23 Cerradura con la que cuenta el laboratorio***

Ilustración ***24 Interior de laboratorio***

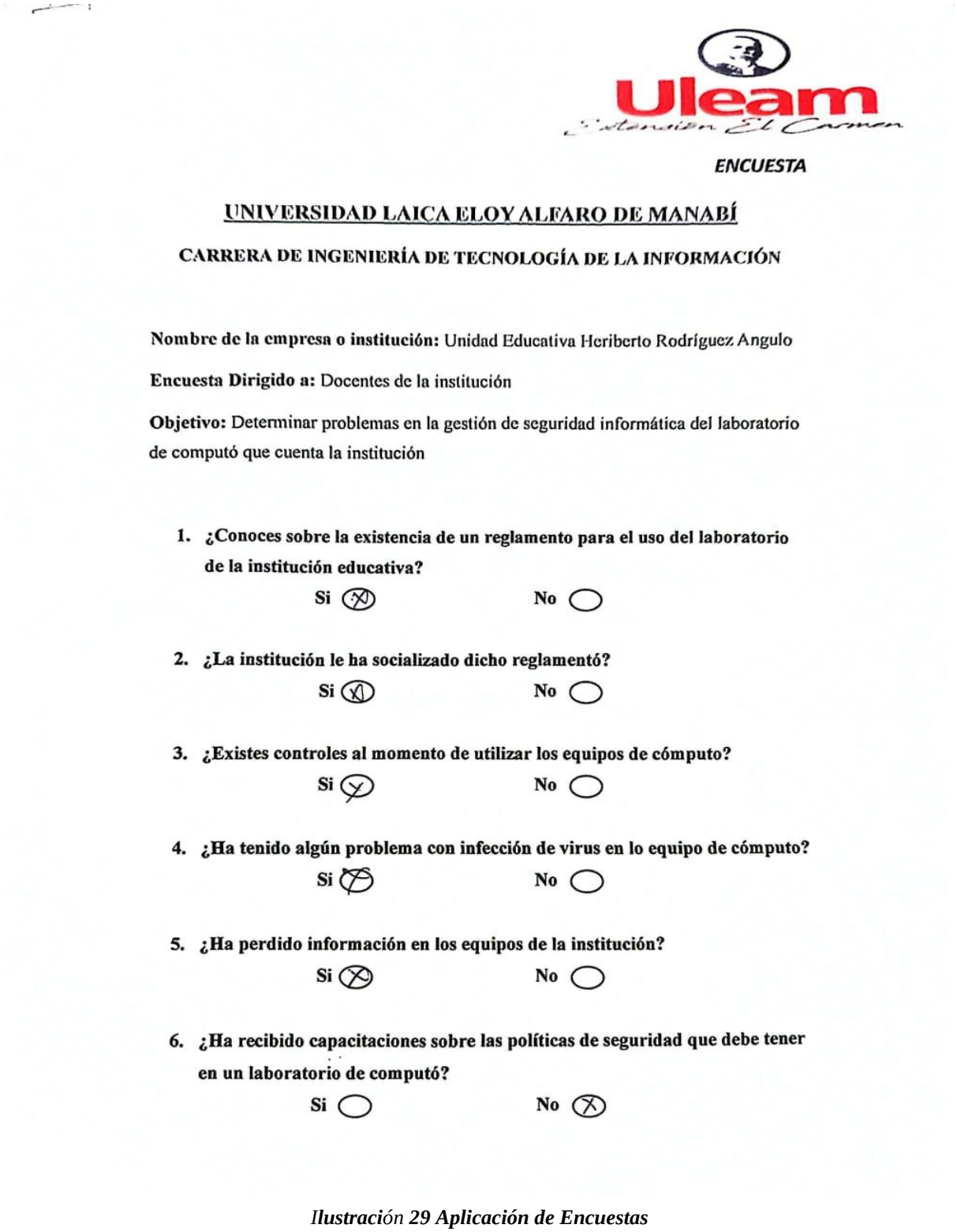
Ilustración ***25 Infraestructura del laboratorio de cómputo***

Ilustración ***26Extintor del laboratorio***

Ilustración ***27 Cortina con la que cuenta el laboratorio***

Ilustración ***28 Braeke de electricidad***

Anexo G: Evidencia de aplicación de encuestas, entrevistas e instrumento de las normas 27001



Uleam
Extensión El Carmen

ENCUESTA

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

CARRERA DE INGENIERÍA DE TECNOLOGÍA DE LA INFORMACIÓN

Nombre de la empresa o institución: Unidad Educativa Heriberto Rodríguez Angulo

Encuesta Dirigido a: Docentes de la institución

Objetivo: Determinar problemas en la gestión de seguridad informática del laboratorio de computó que cuenta la institución

1. **¿Conoces sobre la existencia de un reglamento para el uso del laboratorio de la institución educativa?**
   Si (X) **No** ( )
2. **¿La institución le ha socializado dicho reglamentó?**
   Si (X) **No** ( )
3. **¿Existes controles al momento de utilizar los equipos de cómputo?**
   Si (X) **No** ( )
4. **¿Ha tenido algún problema con infección de virus en lo equipo de cómputo?**
   Si (X) **No** ( )
5. **¿Ha perdido información en los equipos de la institución?**
   Si (X) **No** ( )
6. **¿Ha recibido capacitaciones sobre las políticas de seguridad que debe tener en un laboratorio de computó?**
   Si ( ) **No** (X)

*Ilustración **29 Aplicación de Encuestas***

Uleam
Extensión El Carmen

ENTREVISTA

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

CARRERA DE INGENIERÍA DE TECNOLOGÍA DE LA INFORMACIÓN

Nombre de la empresa o institución: Unidad Educativa Heriberto Rodríguez Angulo

Encuesta Dirigido al: Director de la institución el ing. Marco Caja

Objetivo: Obtener información relevante y precisa sobre la gestión de seguridad informática que cuenta la institución.

1. **¿Existen un reglamento para el uso del laboratorio de la institución educativa?**

- Podría mencionar algunas norma que se puede seguir al momento de utilizar el laboratorio
- Cual es el procedimiento para utilizar el uso del laboratorio

No existe
Debido que computadora a Sido capaga -

pero los docente estan atento de ese reglamento porque en la encuesta que se realizo tuvo un porcentaje de 4 docente que contes

2. **¿Le ha socializado dicho reglamentó a los demás docente de la institución?**

- Como sele fue presentado el reglamento a los docente
- fue a través de una reunión o a través de un documento impreso

pero son 4 docente que no esta enterado de dicho reglamento

3. **¿Se han implementado controles al momento de utilizar los equipos de cómputo?** 6 (Si) 2 (No)

Podia mencionar algunos controles que se aplican al utilizar los equipo de computo

- encendido
- condecion con:
- Pagina seby

4. **¿La institución ha tenido algún tipo problema con infección de virus en lo equipo de cómputo?** (6 (Si) 1 (NO)

A
cual fue la naturaleza de la infección de virus en los equipo
N
- considera importante tener medidas preventivas para evitar infección de virus

por que cree que an tenido problema de virus

5. **¿Se ha perdido información en los equipos de la institución?** 7 (Si) 1 (NO)

A
- que tipo de informacion han perdido y la causa de la perdida y como se maneja la situación

N
- considera importante tener medida de respaldo para la información y como cree que deberia implementarla

Archivo
Acta
Nota

Ilustración 30 Aplicación de Entrevista

Cuestionario para el análisis de riesgos para la institución Educativa Heriberto Rodríguez Angulo			C 3 Página 1 de 5
Robo			
Preguntas	**Respuestas**		**Observación**
	Si	**No**	
1. ¿Tiene sistema de video vigilancia la institución?		X	
2. ¿La institución cuenta con personal de seguridad?		X	Aveces
3. ¿La institución ha sufrido robos?	X		
4. ¿La institución cuenta con un protocolo de respuesta en caso de Robo?		X	
5. ¿Se lleva un registro de los incidentes de los robos?	X		1
6. ¿Se controla el acceso al ingreso al laboratorio?	X		1
7. ¿Se realiza un proceso de seguimiento de recuperación de los equipos de cómputo?		X	
8. ¿Se utiliza alarma de seguridad?		X	
9. ¿Se realizan inspecciones regulares de alarma?		X	
10. ¿Las computadoras tienen un etiquetado para identificarlas?	X		1
11. ¿Se utiliza cerradura de alta seguridad en las instalaciones?	X		1
12. ¿Se realizan inspecciones regulares de las cerraduras?	X		
13. ¿Tienen personal encargado del laboratorio?	X		1
14. ¿La institución cuenta con cerramiento físico en sus instalaciones?	X		Dio
15. ¿Las computadoras se almacenan en gabinetes o cajas de seguridad?		X	
16. ¿El personal docente cuenta con tarjeta de identificación?		X	
17. ¿La institución cuenta con botón de pánico para cuando suceda un robo?		X	
18. ¿Se almacenan las computadoras de manera que sea difícil de mover?		X	
19. ¿El personal docente tiene acceso a todas las maquinas?	X		
20. ¿Tienen procedimientos ante la pérdida o robos de computadoras?	X		1
21. ¿Se cuenta con un equipo de repuesto de emergencia en caso de robo?		X	
22. ¿Las computadoras están anclados con cable de seguridad?		X	
23. ¿Las computadoras portátiles cuentan con dispositivos o cerraduras de seguridad?		X	
24. ¿La institución cuenta con seguros de robos de computadoras?		X	
25. ¿La institución cuanta con un seguro de Robo?		X	
Realizado por: Demera Moreira María Micaela **Fecha:**		**Revisado por:** **Fecha:**	

*Ilustración **31 Instrumento de análisis de Riesgos***

	REQUISITOS	PREGUNTA	CUMPLIMIENT	Promedio	Estado GAP	Brecha	ESTADO MADURI
4 La Organización y su Contexto	4.1 Entendiendo la Organiza	1.- ¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?	3				
		2.- ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	1				
		3.- ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	3				
	4.2 Expectativas de las parte	1.- ¿Se han identificado las partes interesadas?	4				
		2.- ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?	1				
		3.- ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?	4				
	4.3 Alcance del SGSI	1.- ¿Se ha determinado el alcance del SGS y se conserva información	1				
	4.4 SGS Sistema de Gestión	1.- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerand	3				
5 Liderazgo	5.1 Liderazgo y compromiso	1.- ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	4				
		2.- ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	4				
		3.- ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	3				
	5.2 Política de la Seguridad d	1.- ¿Se ha definido una Política de la Seguridad de la Información?	4				
		2.- ¿Se ha establecido un marco que permita el establecimiento de	4				
		3.- ¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?	3				
		4.- ¿Se mantiene información documentada de la política del SGSI y de sus	4				
	5.3 Roles y Responsabilidad	1 - ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	4				
		2.- ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?	-				
6 Planificación	6.1 Tratamiento de Riesgos	1.- ¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la					
		2.- ¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	2				
		3.- ¿Se ha definido un proceso de tratamiento de riesgos?	3				
		4.- ¿Se han establecido criterios para elaborar una declaración de	1				
		5.- ¿Se mantiene información documentada de los puntos anteriores?	1				
	6 2 Planificación para conse	1.- ¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?	3				
		2.- ¿Los objetivos de la Seguridad de la Información estan planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación	2				
		3.- ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones	3				
7 Soporte	7.1 Recursos	1.- ¿Se identifican y asignan los recursos necesarios para el SGSI?	1				
	7.2 Competencia	1.- ¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	1				
		2.- ¿Se mantiene información actualizada sobre la competencia del	1				
	7.3 Concienciación	1.- ¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?	2				
		2.- ¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	4				
	7.4 Comunicación	1.- ¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	3				
		2.- ¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?	3				
	7.5 Información Documenta	1.- ¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones	1				
		2.- ¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección	1				
		3.- ¿Se controlan los documentos de origen externo?	1				

Ilustración 32 Instrumento de cumplimiento de requisito

Cuestionario para el cumplimiento de controles de las normas ISO 27001 para la institución Educativa Heriberto Rodríguez Angulo				C2 Página 2 de 10	
Numeral	**Clausula**		**Requisito**	**CUMPLE**	
				Si	**No**
A6	**Organización de la Seguridad de la Información**	**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?	X	
A7	**Seguridad en Los Recursos Humano**	**A7.1. Antes de contratar a un empleado**	1.- ¿Se investigan los antecedentes de los candidatos? -Formación -Experiencia -Verificar Titula		X
			2.- ¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?		X
		A7.2. Durante el contrato	1.- ¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?		X
			2.- ¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?		X
			3.- ¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?		X
		A7.3. Terminación del contrato	1.- ¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?		X
			2.- ¿Se definen responsabilidades sobre la Seguridad de la información que se extiendan más allá de la finalización de un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información?		X
A8	**Gestión de Activos**	**A8.1 Responsabilidad sobre los Activos**	1.- ¿Se ha realizado un inventario de activos que dan soporte al negocio y de Información?		X
			2.- ¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	X	
			3.- ¿Se han establecido normas para el uso de activos en relación con su seguridad?	X	
			4.- ¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?		X
Realizado por: Demera Moreira María Micaela **Fecha:**			**Revisado por:** **Fecha:**		

*Ilustración **33 Instrumento de cumplimiento de***

*Ilustración **34 Realizando la encuesta a los docentes de la institución***

*Ilustración **35 Realizando la debida entrevista a director de la institución.***

*Ilustración **36 Evaluando los instrumento de las normas ISO 27001***

MANUAL DE SEGURIDAD PARA EL LABOTARORIA DE LA ESCULA DE EDUCACIÓNBÁSICA "HERIBERTO RODRIGUEZ"

EL CARMEN, JULIO 2024

Manual de política de seguridad

Introducción

El bienestar y seguridad de los docente y estudiante del plantel educativo Heriberto Rodríguez Angulo es una prioridad fundamental para el plantel educativo. En ese sentido en el plantel educativo debe por lo tanto adoptarse con herramienta necesarias para actuar de una manera rápida y precisa y evitar o reducir caso de riesgo o daños en tales situaciones que se lleguen a dar o se produzca un siniestro, accidente, por tal razón es necesario, desarrollar e implementar un manual de seguridad, donde se logra contar con la guía necesaria para evitar o reducir riesgo o amenaza.

Un manual de seguridad es una herramienta de gestión que estable como actuar mediante un accidente y permite prevenir ciertas situaciones de emergencia que puede suceder en las instalaciones del plantel, con la finalidad de reducir una situación de emergencia, la que puede causar daños de los equipos de cómputo y así mismo causar peligro tanto en los docentes o los estudiantes del plantel educativo.

Objetivo y alcance

Objetivo:

El objetivo de este manual es proporcionar políticas y controles de seguridad para estables pausas clara, para así logra un entorno más seguro en la unidad educativa Heriberto Rodríguez Angulo. Este manual buscar asegurar todos los aspectos tenga relacionado con la protección de los equipos de cómputo.

Alcance:

Este manual está realizado pensado en la escuela de educación general básica ¨Heriberto Rodríguez Angulo¨ la cual permitirá ser una guía importante para los docentes de la institución, logrando ser una herramienta posible de percudir posibles riesgo o amenaza a corto o largo plazo, logrando así ser una guía esenciar para la institución educativa a lo que permite abraca una serie de procedimiento y recomendaciones de seguridad

informática, adaptándose con la necesidades que cuanta actualmente la escuela básica Heriberto Rodríguez Angulo .

Seguridad en las instalaciones

En primer lugar, se debe que tomar en cuenta la seguridad física de las instalaciones de la institución educativa Heriberto Rodríguez Angulo, la cual es el lugar donde se elabora y debe ser un lugar adecuado para los docentes la cual cumple sus funciones en ese plantel educativo. Los puntos para tomar en cuenta al poner a funcionar en el plantel educativo son:

1. Las paredes deben ser de concreto sólido.
2. Contar con salida de emergencia y extintores de fuego.
3. Las instalaciones de las áreas de trabajos deben contar con tomacorrientes regulados con conexión a tierra.
4. El lugar debe contar con aire acondicionado por ductos para evitar que los equipos se sobrecalienten.
5. Las instalaciones eléctricas deben encontrarse ocultas, así como el cableado de datos y de redes.
6. En e l caso de seguridad eléctrica debe existir un UPS en caso de variación de la energía eléctrica que evite daños a los equipos de cómputo, y la seguridad de la información.
7. Contar con los espacios físicos suficiente.
8.

Medidas de seguridad al realizar mantenimiento de equipos de cómputo

El mantenimiento de los es algo delicado, ya que, si no se tiene los conocimientos adecuados o la experiencia suficientes, es mejor buscar ayuda de un profesional que sepa lo suficiente, ya que puede provocar daños físicos en los equipos de cómputo irreparable.

Entre las medidas de seguridad al realizar un mantenimiento de los equipos de cómputo están:

1. Observar que el computador este en buen estado, debe revisar la CPU, monitor, teclado, mouse, parlantes; es decir las condiciones generales del equipo de cómputo.
2. Realizar un diagnóstico de funcionamiento al equipo de cómputo.
3. Probar los periféricos de entrada y salida.
4. Ser precavidos en el manejo de tornillos del sistema, pues ellos no están diseñados para todos los putos.
5. Para realizar el mantenimiento preventivo o correctivo del equipo de cómputo se debe tomar en cuenta lo siguiente:
    a. Todo mantenimiento debe ser realizado con el debido tiempo y sin prisas.
    b. Para realizar el manteamiento siempre se debe tomar en cuentas las normas de seguridad establecida en un manual.
    c. Cuando se vaya a abrir la CPU asegúrese de desconectar los cables de corriente, video, dispositivo USB, etc.
    d. Debe que tener claro cómo funcionan las herramientas que se utilizará en el mantenimiento, ya que puede ser las no adecuadas para tal proceso.
    e. Utiliza la matilla antiestática, esto para evitar que la energía estática dañe algún componente cuando manipule el equipo, en el caso de no poseer una manilla debe descarga la electricidad estática que todo poseen tocando previamente algo de metal antes de destapar el computador.
    f. Antes de desarmar, desconectar o quitar piezas es recomendable que preste suma atención de cómo y dónde van las piezas o cable que esta retirando, si bien la gran mayoría de los componentes encaja de una sola forma y en un solo lugar, a los principiantes puede causar inconvenientes.

Medida de seguridad al ingresar al laboratorio de Cómputo

Al ingresar al laboratorio de cómputo hay que considerar los aspectos a cumplirse y las normas de seguridad que se disponga:

1. Escuchar con atención las indicaciones del responsable del laboratorio de cómputo, ya que el indicará el correcto funcionamiento de los equipos y su seguridad.
2. Mirar atentamente las instalaciones del laboratorio y sugerir si le hace falta un cambio o modificación.

3. Prevenir accidentes laborables, siguiendo adecuadamente las normas de seguridad e indicaciones.
4. Observar objetos que pueda causar daños mientras usted se encuentra en la instalación del laboratorio de cómputo.
5. Evitar la autoconfianza ya que siempre de prever algún inconveniente dentro de un lugar donde se utiliza equipos con una conexión eléctrica.
6. El uso de hardware debe estar normalizado por los siguientes aspectos:
    a. Los usuarios deben de tener acceso a los equipos de cómputo que el docente le haya asignado.
    b. El docente debe que tener un control estricto de los usuarios que ingresan a las instalaciones del laboratorio de cómputo.
    c. La prueba, instalación y puesta en marcha de los equipos de cómputo debe estar a cargo del docente del laboratorio.
    d. La institución debe que contar con una póliza de seguros que ayude a enfrentar un posibles siniestro.
    e. Debe mantener una hoja de vida de cada equipo de cómputo, con la finalidad de comunicar sobre posibles mantenimiento o reparaciones que se puede ser afectado dentro de su vida útil.

Medidas de seguridad al utilizar los equipos de cómputo

Con el fin de garantizar un correcto funcionamiento de los equipos de computación (computadores, impresora y cualquier dispositivo anexo) se debe contar con un plan de mantenimiento tanto preventivo como correctivo, los mismos que garanticen la utilización de los equipos de una manera rápida y efectiva. Las medidas de seguridad al permanecer en el laboratorio son:

Para los usuarios:

1. No ingerir alimentos cercas de los computadores, porque podría llegar a dañar el equipo y las conexiones.
2. No insertar objetos extraños en las ranuras de los quipos de cómputo ni en los muebles, ya que podría ocasionar grandes daños.

Para lo responsable del laboratorio

1. Conservar los equipos en adecuadas condiciones ambientales.
2. Apagar los equipos cuando no estén en uso.
3. Observar la energía eléctrica sea regulada a 110 voltios y con polo a tierra, asesórese debidamente para garantizar una buena toma eléctrica.
4. Realizar un formato de entrega del equipo, lo dispositivos que tienen o le fata y mirar cuáles son sus óptimas condiciones y cuales están dañados.
5. Ubicar de manera adecuado los números de serie e identificativos adicionales a cada computador.

Medidas de seguridad en la información de los usuarios de los quipos de cómputo.

La información como recurso valioso de una institución y como historial está expuesta a actos tanto intencionales como accidentales de violación de su confidencialidad, alteración, borrados y copia, por lo que se hace necesario que el usuario, propietario de esa información, adopte medidas de protección contra accesos no autorizados.

Par proteger la información los usuarios deben tener en cuentas las siguientes medidas de seguridad:

1. Poseer una clave en el computador, ésta habilitará o bloqueará a los usuarios no autorizados.
2. Siempre el usuario deberá grabar su información en dispositivos externos, con la finalidad de que su información no sea copiada, borrada, adulterada, modificada y usada para fines distinto para lo que fue creada.
3. Realice una copia de la información suficiente y guárdala en un lugar seguro.
4. Realiza el manteamiento de software con la finalidad de que no exista redundancia e inconsideración en la información.
5. Clasificar la información de acuerdo con su importancia y guardarla en un sitio seguro.

6. Solicitar al docente de los equipos de cómputo la instalación de un antivirus actualizado, ya que la información está expuesta a unas seris de virus, los mismos que provocan que los programas no funciones bien, alteran su normal funcionamiento. Los virus pueden destruir la información contenida en los medios de almacenamiento llegando incluso a dañar partes físicas de la computadora.

7. Utilizar únicamente software original legalmente adquirido y autorizado e instalados por el docente del laboratorio de cómputo.
8. No debe instalar en las computadoras de software "pirata'' ni de ''juegos".
9. Estar atento a los mensajes de aleta emitidos por el computador.
10. El docente del laboratorio debe aplicar un antivirus periódicamente.

Medidas de seguridad al permanecer en el laboratorio de cómputo

Contar con buenos programas de mantenimiento preventivo de los equipos de computación, no garantiza totalmente su opresión satisfactoria, ni eliminan los riesgos de desperfecto que como cualquier elemento electrónico puede presentar. Pero si este equipo cuenta además con los cuidados de instalación, limpieza, temperatura, humedad, eléctricos, se estará brindando un estado óptimo de trabajo con un mínimo de revisiones y reparaciones.

Las siguientes recomendaciones, acogida en el manual prolongarán la vida de los equipos:

1. No traslade una computadora sin la autorización y asesoría del docente del laboratorio.
2. Cada usuario, al momento de terminar las labores, deberá apagar los quipos.
3. Evite colocar encima o cerca de las computadoras ganchos, clips, bebidas y comidas que se puede caer accidentalmente en los equipos de cómputo.
4. Por su seguridad los usuarios nunca deben destapar y tratar de arreglar los equipos por su cuenta.
5. Los usuarios del laboratorio de cómputo siempre deben que buscar ayuda en los casos que no entienda o no comprenda el funcionamiento de los equipos.
6. La pantalla y el teclado deben estar cubierto con funda plásticas cuando no haga uso de ellos por el tiempo considerable o si se planea el aseo o preparación del aleñadas al computador.

7. Los usuarios deben cuidar los equipos informáticos mientras estén haciendo uso de ellos.

Medidas de seguridad frente a catástrofes naturales

En materia de prevención de riesgo resulta fundamentales el establecimiento de las medidas de seguridad que se debe adoptar para prevenir o reducir los riesgos a los que se encuentran expuestos los bienes y las personas que usan el laboratorio de cómputo.

Los desastres naturales que pueden ocurrir en las instalaciones del laboratorio son:

1. **Incendios, los mismos que pueden ser provocados por cortocircuitos, este tipo de desastre puede prevenirse tomando las siguientes medidas:**

a. Gestionar una buena conexión eléctrica, tomando en cuenta todos los estándares de seguridad eléctrica.
b. Contar con la conexión de un UPS que proteja a los equipos de cómputo, en el caso de una posible falla eléctrica.
c. No conectar equipos que afecten a las instalaciones del laboratorio de cómputo.
d. Es conveniente hacer revisiones periódicas de las instalaciones eléctricas, por personal especializado, para comprobar que cumplen con la normativa.
e. Es recomendable contar con un plano en el que se indique la colocación del equipo contra incendio, los extintores y estaciones de vigilancia.
f. Establecer rutas de evacuación, las salidas de emergencia y los puntos de reunión
g. Evitar que las rutas de evacuación y salida de emergencia sean obstruidas
h. Verificar que los lugares en donde se encuentran los equipos contra incendio se encuentren libres de cualquier obstáculo
i. Llevar a cabo ejercicios y simulacros de evacuación en forma periódica involucrando al personal en los mismos
j. Realizar una socialización de la ubicación de los extintores y la manera de utilizarlos
k. Evitar la acumulación de basura en las instalaciones de los laboratorios de computo
l. Solicitar al personal que antes de salir de su lugar de trabajo se cerciore que los aparatos eléctricos que por su propia naturaleza no deban quedar conectados y encendidos, sean apagados y desconectados
m. Hay que recordar que todo contacto o interruptor debe tener su tapa debidamente aislada.
n. No sobrecargue los enchufes con demasiadas clavijas, se debe distribuir las cargas o solicitar circuitos adicionales
o. Antes de cualquier reparación de la instalación eléctrica, desconecte el interruptor general y compruebe la ausencia de energía.
p. No sustituya los fusibles por alambres o monedas.

q. No conecte aparatos que se haya humedecido y cuide que no se mojen las clavijas e instalaciones eléctricas
r. Procure no usar ni tocar aparatos eléctricos si este descalzo, aun cuando el piso está seco.

2. Inundaciones, este tipo de desastre puede ocurrir debido a que las aguas de lluvias fuertes no tienen un desahogo eficiente. Las medidas a tomar en cuenta en este tipo de desastre son las siguientes:

a. Realizar las gestiones necesarias para que las autoridades competentes implementen vías de acceso y desalojo de aguas lluvias en el caso de ocurrir tempestades
b. Procurar que las alcantarillas funcionen adecuadamente y pueda fluir el agua sin inconvenientes
c. Revisar periódicamente las instalaciones de agua potable con la finalidad de evitar derrames en las instalaciones cercanas al Laboratorio de cómputo
d. Cambiar si es posible las mangueras que suministran el agua potable
e. Contar con un manual de seguridad externa para toda la institución donde se de guías de evacuación.

3. Sismos, el Ecuador presenta una serie de ''vulnerabilidades'' al estar ubicado en una zona de alto riesgo sísmico, según advertencias de los técnicos del instituto geofísico de la Politécnica Nacional (IGPN). Situación por la cual los ecuatorianos deberían prepararse mejor para enfrentar cualquier catástrofe, como un terremoto. Por tal razón se pone en consideración las siguiente medidas o precauciones de seguridad.

a. Buscar una cultura de prevención, la misma que ayude a capacitarse sobre los posibles movimientos a los que se pueda enfrentar nuestra provincia
b. Solicitar al departamento de seguridad la elaboración de un plan de contingencia sobre posibles sismos
c. Socializar algunas normas de seguridad en caso de presentarse algún tipo de sismo
d. Elaboración de un sistema de alerta
e. Preparación de una vía de escape
f. Plan de evacuación en el caso de un sismo

g. Conocer e identificar su entorno
h. Informarse y prepararse para actuar de la mejor manera cuando se produzca el próximo sismo.
i. Practique simulacros de terremoto.
j. Conozca donde y como cerrar el paso de la electricidad los interruptores y tomar precauciones.
k. Conserve la calma y tranquilice a las personas de su alrededor
l. Si tiene la oportunidad de salir rápidamente del laboratorio hágalo inmediatamente, pero en orden, recuerde: no grite, No corra, no empuje y diríjase a una zona segura.
m. Aléjese de estanterías, muebles, ventanas, mesas que no sean seguras
n. En caso de encontrarse lejos de una salida, ubíquese debajo de una mesa o escritorio resistente, que no sea de vidrio, cúbrase con ambas manos la cabeza y colóquelas junto a las rodillas, en su caso diríjase a una esquina o columna
o. Una vez terminado el sismo desaloje el inmueble y recuerde: no grite, no corra, no empuje.
p. Tenga a mano los números telefónicos de emergencia.
q. Ubique y revise periódicamente las instalaciones eléctricas.

GLOSARIO

A

Auditoría

Es un examen sistemástico y meticuloso realizado de manera independiente y documentda sobre las cuentas, registro, actividades y procesos de una organización para verificar su conformidad con las normas, regulaciones y políticas establecidas.

C

componentes

Los componentes son las partes individuales o elementos que al unirse, forman un sistema o conjunto mas complejo.

continuidad

Se refiere a la capacidad de una organización para mantener susu operaciones y servicios criticos durantees y despues de un incidentes disruptivo como desaster naturarl, fallo tecnologicos o ataques ciberneticos .

Contraloría

Es una entidad o departamineto dentro de una organización encragado de supervisar y controlar la gestión administrativas para asegurar la correcta utilización de los recusros y el cumpliminetos de políticas, normas y regulación ·

E

exhaustivo

Se refiere a u enfoque que es completo y detallado, cubriendo tdo los apsecto relevante de un tema, proceso o actividad.o analisi Exhaustivo minuciosoo todo los elementos pertinentes, asegurando que no se omita ninguna información importante y por proporcionan una evaluación d presisa y confiable.

I

IEC

La comisión Electrotécnica es unaorganización global que prepara y publica normas internacionales para todas las tecnologías.

ISO

Organización internacional independientes es una unidad gubernamental internacional que se desarrolla y publicar normas internacionales consensuada por expertos de diferentes países para asegurar la calidad, seguridad, eficiencia, servisios y sistemas en una variedad de industria.

M

MAGERIT

Es una metodología desarrollada por el Consejo Superior de administración electr de Españas para la gestión integlal de riesgos en los sistemas de información , su objectivo principal es indentificar, analizar y evaluar los riesgos a los que están expuestos los ectivos de la información, estabblece medidas de protección adecuadas para mitigar riesgos

para asegurar su correo funcionamineto, detectar desviaciones, y tomas de medidas correctivas cuando sea necesario.

P

promover

Significa fometar, apoyar o impulsar activamente una idea, proyecto, producto o políticas. En ell

contexto organizacional, promover puede implicar actividades de comunicacione para aumentar la conciencia y aceptación .

Significa proteger y asegurar la integridad, confidencialida y disponibilidad de los activos de l información contra amenaza y risgo. · 10

S

salvaguardar

significa proy=tejer y asegurar la integridad, confidencialidad y diponibilidad de los acyivos de la información contra amenaza y riegos.

T

TICS

La técnologia de la información y comunicación se referie y comprende una amplia gama de herramintas, sistemas y recursos tecnológicos utilizados para procesar, almacenar, gestionar y trnasmitir información de manrera eficinete y efctiva.