CONSTRUCCIÓN DE UN SISTEMA DE GESTÍON DE SEGURIDAD DE LA INFORMACION ALINEADO A LA NORMA ISO 27001 PARA EL CENTRO EDUCATIVO NOREAN DE AGUACHICA CESAR.

PAULA ANDREA GARNICA MOLINARES
DORIS NATALIA BAUTISTA ROMERO

UNIVERSIDAD POPULAR DEL CESAR
FACULTAD DE INGENIERÍAS Y TECNOLÓGICAS
PROGRAMA INGENIERÍA DE SISTEMAS
LÍNEA DE INVESTIGACIÓN, INGENIERÍA DEL SOFTWARE
SECCIONAL AGUACHICA, CESAR

2025

CONSTRUCCIÓN DE UN SISTEMA DE GESTÍON DE SEGURIDAD DE LA INFORMACION ALINEADO A LA NORMA ISO 27001 PARA EL CENTRO EDUCATIVO NOREAN DE AGUACHICA CESAR.

PAULA ANDREA GARNICA MOLINARES
DORIS NATALIA BAUTISTA ROMERO

Propuesta de proyecto de grado para optar el título de ingeniero de sistemas, modalidad presencial.

Director.
ERNEY ALBERTO RAMIREZ CAMARGO

Codirector
WILFER ESCALANTE

UNIVERSIDAD POPULAR DEL CESAR
FACULTAD DE INGENIERÍAS Y TECNOLÓGICAS
PROGRAMA INGENIERÍA DE SISTEMAS
LÍNEA DE INVESTIGACIÓN, INGENIERÍA DEL SOFTWARE
SECCIONAL AGUACHICA, CESAR

2025

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

_____

Firma del director: Erney Ramírez Camargo

_____

Firma del Co-director: Wilfer Escalante

_____

Firma del jurado 1: Danny Jhoan Ríos Barona

_____

Firma del jurado 2: Lina Arévalo Vergel

DEDICATORIA

Dedicatoria – Doris Natalia Bautista Romero.

A mi familia, por ser la base que sostuvo cada paso de este proceso. Gracias por su apoyo constante, por creer en mí incluso en los momentos de duda y por acompañarme con amor y paciencia. Cada logro obtenido refleja el esfuerzo compartido y la fuerza que siempre me han brindado para avanzar con determinación.

Dedicatoria – Paula Andrea Garnica Molinares.

A mi familia, cuya compañía ha sido un motor invaluable durante este camino académico. Su confianza, sus palabras de aliento y su presencia incondicional hicieron posible que este proyecto se culminara con dedicación y esperanza. Este trabajo es también un homenaje a su amor, que ha sido guía, impulso y refugio en todo momento.

AGRADECIMIENTOS

La presente tesis se realizó gracias al apoyo y acompañamiento de diversas personas e instituciones que contribuyeron de manera significativa a su desarrollo.

En primer lugar, se expresa un profundo agradecimiento a Dios, por brindar fortaleza, salud y sabiduría durante cada etapa de este proceso académico.

De igual manera, se agradece a la familia, cuyo respaldo incondicional, motivación y paciencia fueron fundamentales para culminar esta meta. Su confianza y apoyo constante permitieron avanzar incluso en los momentos más desafiantes.

Así mismo, se extiende un sincero agradecimiento al director de tesis, por su guía, orientación académica y aportes que enriquecieron el contenido y rigor del trabajo realizado. Su dedicación y compromiso fueron esenciales para alcanzar los objetivos planteados.

De manera especial, se reconoce a los docentes de la institución, quienes con sus enseñanzas y experiencia contribuyeron al crecimiento profesional y personal durante la formación universitaria. Finalmente, se agradece a todas las personas, compañeros y entidades que, de una u otra forma, aportaron al desarrollo de esta investigación. Cada apoyo recibido hizo posible la culminación satisfactoria de este proyecto.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las organizaciones dependen de sus sistemas de información, infraestructuras tecnológicas y procesos automatizados debido al aumento del uso de tecnologías de la información, lo que facilita una adecuada gestión de datos y permite competir en un mercado tecnológico en constante evolución (Pérez, 2017). Sin embargo, esta dependencia las expone a ciberataques y vulnerabilidades que comprometen la seguridad de los datos (Pando, 2024). Las tecnologías avanzan rápidamente y cada vez hay más ciberataques en la red, a medida que las empresas dependen cada vez más de su infraestructura, su exposición a las amenazas cibernéticas se expande (Check Point, 2023). Entre las consecuencias de un sistema de seguridad vulnerable se destacan la interrupción o retraso de procesos y operaciones, las pérdidas económicas y la disminución de clientes y proveedores (Bleeping Computer, 2023).”

Por otra parte, la revista (Forbes Staff, 2024) publicó un artículo acerca de los riesgos de ciberseguridad en Latinoamérica según el IBM en el 2024, en este mismo el país colombiano ocupo el segundo lugar entre los países con más vulnerabilidad a ataques. De tal manera, diferentes portales de noticias mencionan hechos de incidentes por errores del sistema de seguridad, tal es el caso del periódico “El Tiempo” (2022) que expresa el fallo de seguridad en un sistema de salud que puso en riesgo los datos de los pacientes, incluyendo información sensible como historias clínicas y datos personales, asimismo lo hizo “El espectador” (2023) con la noticia de la universidad que fue expuesta ante una vulnerabilidad en la seguridad de los datos de estudiantes y profesores.

Según la Organización de los Estados Americanos [OEA], el Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC] y el Banco Interamericano de Desarrollo [BID] (2017) el 51% de las medianas empresas y el 63% de las grandes empresas en Colombia sufrieron incidentes digitales en 2016. Con respecto a las entidades estatales, el 59% de las entidades de orden nacional identificaron incidentes digitales, mientras que un 56% de las entidades de orden territorial departamental respondieron de la misma forma. Por otro lado, el 42% de las entidades de orden territorial municipal también han

identificado incidentes digitales. Además, sólo el 37% de las organizaciones que participaron del estudio se creen preparadas para manejar un incidente digital.

En la actualidad existen distintos tipos de ataques que pueden llegar a perjudicar gravemente los activos informáticos de una organización. Dentro de los peligros más conocidos, podemos encontrar algunos como ingeniería social, keylogger, ransomware y softwares maliciosos (Quintero Asociados & Cía. Ltda., 2019). Un ejemplo significativo es el ataque de WannaCry, que tuvo lugar en mayo de 2017 el cual retenía la información de los usuarios y empresas, solicitando un rescate en Bitcoins para su devolución. Ese mismo año, este software malicioso paralizó los sistemas informáticos de 150 países y provocó pérdidas por valor de 400 millones de dólares en todo el mundo (Kaspersky Lab, 2020).

La pandemia del Covid-19, como indican Gaviria et al., 2023) , generó un escenario sin precedentes de aislamiento social que afectó distintos aspectos en el ámbito institucional, de tal manera que se vieron obligados a adaptarse a una operación remota improvisada, utilizando medios de comunicación, videoconferencias y plataformas basándose en tecnologías de la información (TIC), este cambio rápido y forzado también expuso nuevas vulnerabilidades en el ciberespacio. Según Franco (2024), ciberdelincuentes aprovecharon estas brechas, explotando vectores de ataque que ya no se limitan a la infraestructura física, sino que también incluye a los usuarios finales y sus dispositivos personales, lo que requiere protección extendida a la nube y entornos híbridos. A su vez, Vargas (2020), agrega que la creciente implementación de sistemas de información en entidades públicas deja en segundo plano las configuraciones de seguridad, aumentando el riesgo de ciberataques al no contar con una infraestructura adecuadamente protegida.

Debido al aumento exponencial de amenazas cibernéticas, Suárez (2024) indica que el 92 % de las organizaciones aumentará su inversión en protección de datos para lograr resiliencia cibernética ante el incremento de ciberataques, como ransomware y spear phishing, al igual que el estudio "Threat Mindset 2023" revela que más del 55 % de las empresas están más preocupadas por estas amenazas. Del mismo modo, Obando

(2024) señala que globalmente se bloquean 24,000 aplicaciones maliciosas al día, y en Colombia los delitos más reportados son hurto informático, violación de datos y acceso abusivo a sistemas. Por otro lado, Según Zevallos (líder de software de seguridad de IBM para la región), entrevistado por Forbes Colombia (2024), advierte que los cibercriminales han reevaluado el uso de credenciales como vector de ataque por su fácil obtención, y que, de mano de la inteligencia artificial, las empresas enfrentan nuevos desafíos que exigen defensas más avanzadas.

Al interior del centro educativo Norean, del Municipio de Aguachica, Cesar, se observa la inexistencia de un sistema de gestión de seguridad de la información o política de seguridad de la información (MPSI) bajo los lineamientos del Plan de Desarrollo Nacional "Colombia Potencia de la Vida 2022-2026", para las entidades públicas, bajo la supervisión del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Gobierno Digital, dando cumplimiento a sus funciones; establece que las entidades del orden público deben contar con un Modelo de Seguridad y Privacidad de la Información (MSPI), el cual debe estar alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas del Gobierno Nacional, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital (Ministerio de Tecnologías de la Información y las Comunicaciones, 2019).

1.1 FORMULACIÓN DEL PROBLEMA

¿De qué manera la construcción de un Sistema de Gestión de Seguridad de la Información (SGSI), alineado a la norma ISO 27001, contribuirá a mitigar los riesgos y fortalecer la confidencialidad, integridad y disponibilidad de la información en el Centro Educativo Norean, del municipio de Aguachica, Cesar?

1.2 JUSTIFICACIÓN

La seguridad informática se ha convertido en un aspecto crucial para toda entidad que desee no solo reducir los riesgos de amenazas internas y externas, Moya (2023) menciona que esto aumenta la confianza de los involucrados ante un compromiso claro con la seguridad de la información. De esta manera Muñoz y Palmera (2019) expresan que la construcción de un Sistema de Gestión de Seguridad de la información apoyado de prácticas efectivas brindará las condiciones adecuadas y necesarias para que se apoye la información extendida de los objetivos misionales y estratégicos de una empresa, del mismo modo señalan Guerrero et... al (2019) que la seguridad en las instituciones y diferentes organizaciones no se limita solamente a proteger activos económicos o bienes personales, sino también la información, que contribuye directamente en los objetivos que proponen las metas empresariales.

Al presente, Barcia (2023) recalca que es crucial considerar tanto a actores internos como externos que puedan afectar la capacidad de una organización para implementar de manera eficaz un Sistema de Gestión de la Seguridad de la Información (SGSI) y por esto el estándar ISO/IEC 27001 ha sido una respuesta a este desafío, proporcionando un marco para abordar los problemas de seguridad de la información. Dentro de este orden de ideas, Guevara et al., (2022) se refieren a la ITIL y la ISO 27001 como herramientas esenciales para fortalecer la seguridad de la información, ayudando a las organizaciones a mejorar la gestión de sus procesos y adaptarse a las necesidades actuales, con un enfoque específico en la protección de datos. Sin embargo, muchas instituciones educativas no gestionan correctamente la información, dejando vulnerabilidades por falta de políticas de seguridad claras expone datos críticos, afectando los procesos internos. Ruiz et al., (2020).

Poner en práctica un sistema de gestión de seguridad de la información (SGSI) es esencial para asegurar la protección y la integridad de los datos en cualquier organización, tal como lo citan Cajamarca et al., (2023), la norma internacional ISO/IEC 27001 es una de las herramientas más aceptadas para establecer políticas y controles que garanticen la confidencialidad y disponibilidad de la información. Dentro de este

contexto, muchas empresas a menudo descuidan el soporte y la actualización necesaria para mantener su efectividad; Castillo (2023) expresa que la ISO 27001 proporciona un marco adaptable a organizaciones de todo tipo y tamaño para proteger la información, facilitando la creación de instrumentos para la recolección y evaluación de datos. De tal forma, Minaya et al., (2023) manifiestan que el desarrollo de auditorías informáticas ha sido clave para vincular la estrategia tecnológica con los objetivos empresariales, permitiendo a las organizaciones identificar y minimizar riesgos, garantizando la eficiencia y seguridad de sus procesos tecnológicos.

1.2.1 Justificación Teórica.

La construcción de un Sistema de Gestión de Seguridad de la Información (SGSI) fundamentado en la norma ISO/IEC 27001 en la Institución Educativa Noreán se justifica en la necesidad de proteger los activos de información, considerados esenciales para el funcionamiento académico y administrativo. Esta norma internacional proporciona un marco estructurado para identificar, evaluar y tratar riesgos, garantizando la confidencialidad, integridad y disponibilidad de los datos. Asimismo, promueve un enfoque de mejora continua que permite a las instituciones adaptarse a cambios tecnológicos y responder de manera eficaz a amenazas emergentes.

Más allá del cumplimiento normativo, el SGSI se apoya en teorías de gestión de riesgos y buenas prácticas de ciberseguridad, que conciben la seguridad de la información como un proceso integral donde intervienen personas, procesos y tecnologías. En el ámbito educativo, esta perspectiva resulta esencial, pues protege datos personales, registros académicos y documentos institucionales, fortaleciendo la confianza de la comunidad educativa y garantizando la sostenibilidad y reputación de la institución.

1.2.2 Justificación Practica.

La construcción de un SGSI alineado a la norma ISO/IEC 27001 para la Institución Educativa Noreán tiene un impacto directo y tangible en la protección de la información crítica de la institución. Este sistema permitirá implementar políticas, procedimientos y

controles que fortalezcan la confidencialidad, integridad y disponibilidad de los datos, lo cual resulta fundamental en un contexto caracterizado por el creciente uso de las tecnologías de la información y el manejo de volúmenes cada vez mayores de información.

En el caso específico del Centro Educativo Noreán, la aplicación del SGSI contribuirá a organizar y resguardar la información académica, administrativa y personal de manera más segura. Esto se reflejará en beneficios concretos para la comunidad educativa: la administración contará con mayor control sobre los procesos, los docentes dispondrán de prácticas seguras en el uso de los recursos tecnológicos y los estudiantes tendrán garantizada la protección de sus datos personales. Además, se reducirá la vulnerabilidad frente a incidentes de seguridad y se mejorará la capacidad institucional de respuesta ante posibles amenazas.

1.2.3 Justificación metodológica.

En el contexto de este proyecto se basará en un enfoque cualitativo y descriptivo. A través de auditorías de seguridad informática y entrevistas con los responsables de la gestión de datos, se realizará un diagnóstico detallado de las vulnerabilidades actuales de centro educativo Norean. El uso de la norma ISO 27001 como guía permite establecer un conjunto claro de procedimientos y controles de seguridad, ajustados a las necesidades específicas de la institución.

La metodología contempla fases de evaluación, diseño y construcción del SGSI, acompañadas de un análisis de riesgos exhaustivo que permita priorizar las áreas críticas. Asimismo, el uso de encuestas y listas de chequeo facilitará medir el nivel de cumplimiento y el impacto de las medidas implementadas, asegurando que las políticas de seguridad sean efectivas y contribuyan al fortalecimiento de la gestión de la información en la institución. En conjunto, este método garantiza resultados medibles, que permiten valorar objetivamente las mejoras alcanzadas en la seguridad de la información.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Construir un sistema de gestión de seguridad de la información alineado a la norma ISO 27001 para el centro educativo Norean, del Municipio de Aguachica, Cesar.

1.3.1.1 OBJETIVOS ESPECÍFICOS

1.3.2 Analizar los riesgos asociados al uso de las tecnologías de la información mediante metodologías que permitan identificar, evaluar y priorizar amenazas, vulnerabilidades e impactos, como base para establecer un diagnóstico del estado actual de la seguridad de la información del centro educativo.

1.3.3 Diseñar un sistema de gestión de seguridad de la información (SGSI) para la Institución educativa alineados a la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y Comunicación MinTIC.

1.3.4 Establecer controles y políticas de seguridad de la información basados en la norma ISO 27001, que permitan mitigar riesgos y garantizar la confidencialidad, integridad y disponibilidad de los datos en los procesos del centro educativo.

2. MARCO REFERENCIAL

2.1 MARCO HISTORICO

Hoy por hoy la implementación de un sistema de gestión de seguridad de la información se ha convertido en un mecanismo fundamental en cualquier entidad que quiera garantizar la seguridad de sus datos e información, la falta de un sistema adecuado expone a estas entidades a riesgos significativos que pueden comprometer sus operaciones, datos sensibles y la confianza de sus clientes o usuarios. A continuación, se presenta una revisión de literatura (proyectos de grado, artículos científicos) donde se muestran proyectos enfocados la implementación de sistemas de gestión de seguridad para salvaguardar información en diferentes entidades, estos son planteados de manera internacional, nacional y local con la intención de tener una base sólida para lograr realizar la investigación planteada.

2.1.1 Nivel internacional.

A nivel internacional, en la ciudad de Callao, Perú, los autores Estalla y Morales (2024) realizaron una investigación titulada “Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la agencia de compras de las fuerzas armadas, 2023” con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de seguridad de la información de la Agencia de Compras de las fuerzas Armadas (ACFFAA), basado en la ISO/IEC 27001:2022.

En conformidad al desarrollo de la investigación se enfocaron en el método descriptivo con el enfoque aplicado, cito textualmente “Este estudio adopta una perspectiva de exploración alejándose del diseño descriptivo clásico para sumergirse en un análisis detallado de fenómenos en condiciones controladas”, asimismo utilizaron técnicas e instrumentos para recolectar la información necesaria e implementar el sistema de gestión de seguridad, tales como la técnica de exploración conceptual, auditorias y análisis de riesgos (Estalla y Morales, 2024).

Como resultado, crearon un diseño que incluía las políticas de los dominios basadas en la ISO 27001, así como la asignación de roles, detallando las funciones y las fases que se seguirían para el control del proceso. Además, se enfatizó la necesidad de contar con la aprobación de la alta gerencia para la correcta implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Finalmente, las conclusiones subrayaron la importancia de este respaldo gerencial como un factor crucial para el éxito del proyecto. (Estalla y Morales, 2024).

Siguiendo este punto, se encontró el proyecto titulado "Propuesta de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001 para la Oficina de Tecnologías de Información del Gobierno Regional Piura" (2020), realizado por el autor García, donde estableció como objetivos analizar la seguridad actual de la información en dicha oficina, evaluar los marcos de referencia que podrían mejorar esta seguridad, y proponer la aplicación de la Norma ISO/IEC 27001 para optimizar la protección de la información. Por lo tanto, permitió desarrollar un enfoque integral para fortalecer la seguridad en el Gobierno Regional Piura.

En este sentido, el tipo de investigación se determinó como cuantitativa, la cual utilizó principalmente información cuantificable. Es decir, este tipo de estudio abarca diseños experimentales, cuasiexperimentales y encuestas sociales, y se enfoca en la cantidad y el análisis de las proporciones de cada elemento evaluado. Por su parte, esta metodología se relacionó a través de su análisis, estableciendo las proporciones de cada elemento evaluado. El alcance abarcó un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información en la Oficina de Tecnologías de Información del Gobierno Regional Piura. (García, 2020)

En términos generales, el autor evaluó la situación actual de los procesos de seguridad en la oficina de tecnologías, teniendo en cuenta la norma ISO 27001, lo que permitió identificar problemas de seguridad. La evaluación de los marcos de referencia condujo a la propuesta de mejoras en la seguridad de la información, reforzada por los resultados de la dimensión de necesidad de un sistema basado en la norma ISO 27001, por

consiguiente, se determinó que la propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 mejoró los procesos de seguridad de la información y comunicación en la Oficina de Tecnologías de Información del Gobierno Regional Piura. (García, 2020).

En el año 2021, se realizó un proyecto de grado titulado “Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí (Ecuador)” en donde el principal objetivo era disminuir los riesgos en el almacenamiento de la información de la unidad informática de la entidad (Fernandez, 2021).

En relación con el desarrollo de la investigación, los autores optaron por emplear una metodología de riesgo, con el propósito de identificar y evaluar de manera estructurada los diferentes riesgos asociados. Para ello, realizaron un cuadro comparativo que abarcó las principales fases de varias metodologías, lo que les permitió analizar las opciones disponibles. Tras este análisis exhaustivo, consideraron que la Norma ISO/IEC 27005:2018 era la más adecuada para el proyecto, debido a su enfoque en el diseño e implementación de medidas de seguridad destinadas a garantizar la protección de la información. (Fernandez, 2021).

De este modo, concluyeron que desde el análisis inicial se identificó la vulnerabilidad del sistema y de esta manera se exponía a riesgos y amenazas que causarían daños a futuro, es por eso que la gestión implicaba un control para proteger la información y garantizar la continuidad del negocio. Con el avance tecnológico, fue esencial para ellos implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permite un análisis continuo y la detección temprana de incidentes. (Fernandez, 2021).

En este sentido, Torres y Serjino en el 2022, realizaron el proyecto "Propuesta de Mejora en el Diseño de Gestión de Seguridad de la Información bajo la Norma ISO 27001:2013 para la División de Apoyo Técnico Judicial de la Dirección Antidrogas de la Policía Nacional del Perú", en el que incluyeron varios objetivos clave, tal como llevar a cabo un análisis de brechas conforme a la norma ISO/IEC 27001:2013, en el que definieron una

metodología para identificar y clasificar activos de información vulnerables, así también, establecieron procesos para controlar documentos físicos y digitales.

Aparte de eso, aplicaron una metodología no experimental, ya que se observó como la información obtenida de la interceptación legal de las comunicaciones se convirtió en productos físicos, como actas, y en productos digitales, como archivos de audio. Asimismo, se aplicó un diseño transversal para observar a los analistas en todas las etapas del proceso. Por otra parte, este estudio se dirigió al personal del DIPATJ-DIRAND, compuesto por 203 funcionarios distribuidos en tres grupos: la Dirección y el área administrativa, con 3 funcionarios; los jefes de área, con 16 funcionarios; y el personal de analistas tácticos, con 184 funcionarios, quienes tenían acceso directo a la información sensible. (Torres y Serjino, 2022).

Por ende, los autores expresaron que para la ejecución de un sistema de gestión de seguridad basado en la norma ISO 27001 aplicado en los procesos administrativos es necesario evaluar cada área con la presencia física de los responsables para establecer correcciones y diseñar nuevos procesos que perfeccionaran las anomalías. Así también, a través de un método práctico, observaron el proceso hasta el cliente final, identificando el estado actual y los puntos que requerían atención para mejorar las políticas de seguridad, la gestión de activos, la seguridad física y del entorno, así como el control del diseño de gestión de seguridad de la información bajo la norma ISO 27001. (Torres y Serjino, 2022).

En la investigación titulada "Modelo de sistema de gestión de seguridad de la información para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del cantón naranja", realizado por Correa en 2023, en Ecuador, incluyendo como objetivos identificar los componentes para el modelo de gestión de seguridad de la información, para establecer una metodología de gestión y mejora continua que garantizara un adecuado tratamiento de la información.

El autor utilizó un estudio investigativo de carácter exploratorio, revisando primero trabajos publicados en bases de datos de SCOPUS y Web Of Science (WOS), e incluyendo una revisión bibliométrica con el término clave ISO/IEC 27001:2013, así como herramientas tecnológicas como Publish or Perish para acceder a Google Scholar, Open Alex y Semantic Scholar. En este contexto, se llevó a cabo la recolección de información de otros estudios relacionados con la implementación del SGSI bajo el estándar ISO/IEC 27001:2013 y su guía PDCA. Además, se elaboró una encuesta para conocer la opinión del personal del GAD Municipal de Naranjal, lo que permitió evaluar los resultados obtenidos. (Correa, 2023).

El estudio concluyó que la implementación de un modelo de gestión de seguridad, estandarizó la información y garantizó la seguridad, disponibilidad e integridad de los datos en el Departamento de Tecnologías de la Información del GAD Municipal de Naranjal. De esta forma, mediante encuestas a usuarios internos, se identificaron los componentes clave del modelo, lo que permitió evaluar y mejorar las estrategias de procesamiento de datos. Además, se sugirió gestionar la vinculación de nuevas estrategias para actualizar las acciones dirigidas al fortalecimiento de la calidad en la seguridad de la información. (Correa, 2023).

2.1.2 Nivel nacional.

Mientras tanto, a nivel nacional en la ciudad de Bogotá, Guzmán y García (2023), presentan la investigación de un “Diseño de un sistema de gestión de la seguridad de la información para los procesos críticos de la empresa ORANGE STAR S.A.S bajo la norma ISO 27001:2013” con el objeto de realizar un inventario de activos de información conforme a la norma ISO 27001:2013, priorizando la información según su importancia. Por consiguiente, efectuar un análisis de riesgos para identificar amenazas y vulnerabilidades, y se establecerán controles de seguridad apropiados para proteger la información y cumplir con la norma.

De acuerdo con esto, la metodología de la investigación fue dividida en tres fases, primeramente con una fase preliminar en la que seleccionaron un enfoque cualitativo para el levantamiento de las fuentes primarias acompañada de herramientas de recopilación de información, seguido de una fase de diagnóstico para la identificación del estado actual de los procesos y activos de la empresa, lo cual teniendo en cuenta el tipo de negocio se basaron en la metodología de análisis “MAEGERIT” debido a su flexibilidad y altos niveles de detallar las dimensiones seguridad, finalizando la tercera fase con la aplicación de las mencionadas anteriormente. (Guzmán y García 2023).

Para la conclusión del proyecto, Guzmán y García (2023), señalaron que la implementación del SGSI fue integral y abarco la recolección de información y análisis de riesgo, asegurando el enfoque robusto hacia la seguridad de la información en ORANGE STAR SAS, de esta manera dando como resultados el implemento de controles específicos de la norma ISO/IEC 27001:2013, asimismo, exaltando la importancia de revisar y actualizar periódicamente las políticas de seguridad y el plan de concientización para reducir la vulnerabilidad causada por el factor humano.

De igual forma, en Colombia, se implementó en Bogotá la propuesta hecha por (Rodríguez y Ruiz 2021) titulado “Diseño de un sistema de gestión de seguridad de la información para el área de talento humano de la secretaría de educación de Fusagasugá basado en la norma NTC-IEC ISO 27001:2013” donde tenían como propósitos identificar y clasificar la seguridad de los activos de información para realizar un análisis de riesgo e implementar los planes de tratamiento adecuados en el sistema de gestión de seguridad SGSI.

Además, la investigación fue realizada bajo una metodología mixta que integró tanto enfoques cualitativos como cuantitativos para el diseño del (SGSI) en el área de Talento Humano de la Secretaría de Educación. En la cualitativa incluyeron reuniones y entrevistas con diferentes actores clave, que fueron fundamental para comprender a profundidad el contexto, los procesos y las dinámicas internas de la gestión de la información en el área, por otro lado, la metodología cuantitativa, a través de las mismas

encuestas, les permitió medir objetivamente el estado actual de la seguridad y el nivel de cumplimiento con la norma ISO/IEC 27001:2013. (Rodríguez y Ruiz 2021)

Finalmente, esta combinación de enfoques les aseguró que el diseño del SGSI estuviera basado en un entendimiento profundo y en datos concretos, lo que aumenta su relevancia y efectividad, representando un avance significativo para la seguridad de la información en el área de Talento Humano de la Secretaría de Educación de Fusagasugá. Los autores demostraron que la implementación del SGSI propuesta permitió alcanzar un 95% de cumplimiento con la norma NTC-IEC ISO 27001:2013, superando ampliamente el actual 32%, este incremento no solo salvaguardó los activos de información, sino que también fomentará una cultura organizacional centrada en la seguridad. (Rodríguez y Ruiz 2021)

En el año (2021), Gallego y González, presentaron un proyecto de grado en la ciudad de Bogotá (Colombia), al que le otorgó el título de: “Diseño del sistema de gestión de seguridad de la información (SGSI) para una empresa del sector industrial basado en la norma ISO/IEC 27001:2013”, así mismo, tuvo como objetivo diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2013 que es proteger la información crítica de la empresa del sector industrial. A través de un análisis de brechas (GAP), se busca identificar las áreas de mejora en seguridad, valorar los activos tecnológicos y clasificar los riesgos.

La metodología utilizada en este proyecto se enfocó en un análisis estructurado, que combinaba la recolección de información cualitativa y cuantitativa a través de entrevistas, documentación y análisis de riesgos. Primeramente, las entrevistas proporcionaron una visión clara del estado actual de la seguridad de la información, permitiendo identificar las áreas de mejora y brechas en el cumplimiento de la norma ISO/IEC 27001:2013. De esta manera, facilitó una evaluación precisa del nivel de madurez de los procesos de seguridad de la empresa. Por otra parte, el análisis de riesgos permitió crear un mapa de riesgos detallado, priorizando las amenazas y evaluando sus posibles impactos, (Gallego y Gonzales 2021).

A corte de los resultados obtenidos, los autores documentaron los controles establecidos para mitigar los riesgos identificados y elaborar una política de seguridad de la información alineada con los objetivos del negocio, asimismo plantearon como conclusión que el análisis GAP reveló que la empresa se encuentra en una etapa inicial de madurez en cuanto a seguridad de la información. Por último, la evaluación mostró deficiencias en la identificación y clasificación de activos y riesgos al igual que la falta de políticas de seguridad integradas, demostrando así que estas brechas resaltaban la necesidad de implementar controles específicos para alinearse con la norma ISO/IEC 27001, (Gallego y Gonzales 2021).

En el proyecto liderado por Ospina (2023), titulado "Diseño de un sistema de seguridad de la información basado en la norma ISO 27001:2013 para el Fondo de Empleados Febimbo en el área de tecnología", se lograron varios objetivos. Primero, se caracterizó la situación actual del fondo, lo que permitió comprender detalladamente los procesos y procedimientos existentes. Luego, se identificaron los activos de información críticos para revisar los requisitos aplicables al diseño del sistema de seguridad. Además, se propusieron los controles principales según la norma ISO 27001:2013 para asegurar la disponibilidad e integridad de la información.

En cuanto al desarrollo de la investigación, se empleó una metodología que combinó teorías de investigación con métodos tanto cualitativos como cuantitativos. Esta combinación permitió una validación rigurosa en diversos aspectos de la norma ISO/IEC 27001:2013, así como en la metodología de riesgos, mediante análisis exhaustivos. A su vez, se integraron datos cuantificados provenientes de aportes y propuestas de mejora, lo cual permitió realizar una evaluación completa y fundamentada. Esta evaluación abarcó de manera integral las perspectivas cualitativas y cuantitativas, proporcionando un análisis más profundo y detallado del estudio.

Como resultado de la investigación, llegaron a la conclusión de que la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) había sido fundamental para administrar los recursos tecnológicos en Febimbo. De igual forma, la investigación evidenció que los controles y políticas del SGSI eran esenciales para garantizar la

seguridad de la información y la eficiencia operativa. Cada política fue adaptada a las necesidades de la empresa, lo cual resultó crucial para su operación efectiva. Finalmente, el desarrollo del sistema incluyó la colaboración de todos los niveles de la organización, mejorando el control interno y la confianza en el cumplimiento de normativas sobre almacenamiento de datos. (Ospina, 2023)

Los autores Gómez y Montaña (2020), en la ciudad de Bogotá, Colombia, realizaron un proyecto de investigación titulado: “Diseño del sistema de gestión de la seguridad de la información para el sistema de pedidos web de la empresa panamericana outsourcing s.a. basado en la norma ISO IEC 27001:2013”, donde su objetivo principal es poder establecer un sistema de seguridad de la información robusto y adaptado a las necesidades de Panamericana outsourcing s.a.

De acuerdo a lo expuesto anteriormente, el proyecto se basó en una investigación empleada en el análisis y revisión de la norma ISO 27001:2013, enfocándose en la gestión de la seguridad de la información. Así también para llevar a cabo este proceso, utilizaron una lista de verificación adaptada de una herramienta de autodiagnóstico creada para la alta consejería distrital TIC de Bogotá, la cual fue modificada para su aplicación en Panamericana Outsourcing. El enfoque se organizó en tres logros que corresponden al ciclo PHVA (Planificar, Hacer, Verificar y Actuar): Planear, Hacer y Verificar y Actuar. Cada uno de estos logros se evaluó con un porcentaje específico, con el objetivo de alcanzar una calificación total del 100%. (Gómez y Montaña 2020)

Como último término, una vez implementada la investigación, se definen los resultados, en los cuales, los autores expresan que el sistema de gestión permitió identificar los riesgos a los que está expuesta la organización, basándose en el plan de tratamiento de riesgos según la norma ISO IEC 27001:2013. De esta manera, evaluaron el estado actual de la seguridad de información en relación al sistema de pedidos, encontrando que la empresa aplica algunos aspectos. Una vez valorado los riesgos, determinaron que el nivel de riesgo es bajo o muy bajo, lo cual fue aceptado por la empresa, posibilitando así alcanzar la certificación ISO 27001:2013, requerida contractualmente para sus relaciones comerciales. (Gómez y Montaña 2020)

En 2022, Osorio llevó a cabo un proyecto de grado titulado "Diseño de un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013 para el área de tecnología en la Unidad Administrativa Especial Cuerpo Oficial de Bomberos de Bogotá" con el objetivo principal de evaluar y mejorar la seguridad informática en dicha área, mediante un diagnóstico del estado actual, el análisis de riesgos y su impacto, así también la implementación de medidas correctivas y preventivas junto a la evaluación de la pertinencia de la política de seguridad informática en función de los hallazgos obtenidos.

De esta manera, el autor se apoyó en la metodología del Modelo Integrado de Planeación y Gestión (MIPG), con el propósito de asegurar que las actividades de las entidades y organismos públicos se desarrollaran de manera eficiente y alineada con los planes de desarrollo establecidos y así también garantizar que dichas instituciones pudieran responder de manera efectiva y oportuna a las necesidades de los ciudadanos, asegurando tanto la calidad como la integridad en la prestación de sus servicios. Además, Osorio (2022) subrayó la importancia de este enfoque para mejorar la coordinación entre las diferentes áreas de la administración pública y optimizar el cumplimiento de los objetivos estratégicos de las entidades involucradas.

Por otro lado, en la conclusión, el autor sintetizó que de acuerdo al diagnóstico realizado un conforme a la norma ISO 27001:2013, se identificó 66 vulnerabilidades, siendo el 33.3% relacionadas con activos de software y el 16.6% con hardware. En consecuencia, se destaca lo esencial que es establecer un plan de comunicación y una matriz de políticas operativas que definan acciones y responsables, involucrando a todos los interesados. Además, la política actual debería alinearse con la norma ISO 27001:2013 y actualizarse según los hallazgos del diagnóstico, dado que la entidad maneja información sensible. (Osorio, 2022).

2.1.3 Nivel local o regional

A nivel regional, en la ciudad de Riohacha, Guajira, se realizó un proyecto de grado titulado: “Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en la empresa Magdaniel Ltda. en el Distrito Especial, Turístico y Cultural de Riohacha” por la autora de Suárez (2021).Este proyecto se enfatizó en la importancia de aplicar sistemas de gestión de seguridad conforme a la norma ISO/IEC 27001:2015, con el objetivo de manejar adecuadamente la información y proteger la confidencialidad tanto de la empresa como de sus clientes.

En otro aspecto, los autores desarrollaron el marco metodológico utilizando un enfoque cuantitativo para interpretar los resultados numéricos de manera precisa. Además, aplicaron el método explicativo como tipo de estudio, ya que se centraba en la observación y descripción detallada de las fuentes de conocimiento. Por último, la investigación recopiló toda la información a partir de datos obtenidos de la empresa Magdaniel Ltda., siguiendo las directrices de la norma ISO/IEC 27001:2015. Este enfoque permitió asegurar la validez y confiabilidad de los datos, garantizando un análisis riguroso y fundamentado. (Suárez 2021)

A modo de cierre, como conclusiones se mencionan que aún la empresa cumpliendo con la política de seguridad de la norma aplicada, existen deficiencias significativas en la seguridad física y del entorno, las cuales colocan en riesgo los activos de información y afectan los procesos, de igual forma, el abandono de controles generó altos niveles de vulnerabilidad, los que requirieron de esfuerzos adicionales para cumplir con los controles y mitigar las amenazas y riesgos. Para terminar, a través de estos lineamientos, se establecieron etapas para la mejora continua y la protección de la información, además de mecanismos para concientizar sobre la importancia del SGSI, fortaleciendo así la cultura de seguridad en la empresa. (Suarez, 2021).

En el ámbito local, particularmente en la ciudad de Aguachica (Cesar), se desarrolló el proyecto de grado titulado “Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 para los procesos soportados en la Dirección

Académica de la Universidad Popular del Cesar, seccional Aguachica, alineado a la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)" (Téllez, 2022). Este estudio resaltó la importancia de estructurar un SGSI conforme a los lineamientos de la norma ISO 27001, con el fin de fortalecer la protección de la información en los procesos académicos y asegurar su alineación con las directrices establecidas por el MinTIC.

Metodológicamente, aplicó un enfoque cualitativo, orientado a la recolección de información sin medición numérica, lo que permitió analizar las consecuencias y probabilidades de los riesgos presentes en la dependencia evaluada. De igual modo, adoptó el ciclo PHVA, establecido por la Organización Internacional de Normalización (ISO) en la versión 27001:2013, como estructura metodológica para el diseño e implementación del SGSI (Téllez, 2023).

Entre las principales conclusiones del estudio, se determinó que, aunque la institución contaba con diversas políticas de seguridad de la información, persistían deficiencias en controles técnicos y administrativos, lo que evidenciaba la existencia de vulnerabilidades que requerían acciones correctivas inmediatas. Asimismo, el proyecto planteó lineamientos y políticas orientadas al fortalecimiento y mejora continua del SGSI, promoviendo la concientización institucional sobre la relevancia de la seguridad de la información y contribuyendo al fortalecimiento de una cultura organizacional orientada a la protección de los activos informacionales (Téllez, 2023).

2.2 Marco Contextual

El Centro Educativo Norean se localiza a 10 km de la cabecera municipal de Aguachica, en el corregimiento que lleva su mismo nombre, con acceso por la vía al mar. La institución se encuentra en una zona turística reconocida por la quebrada del sector. Es una entidad educativa de carácter oficial y orientación académica, que opera bajo el calendario A y pertenece al estrato 1. Su sede está ubicada en una zona rural y ofrece

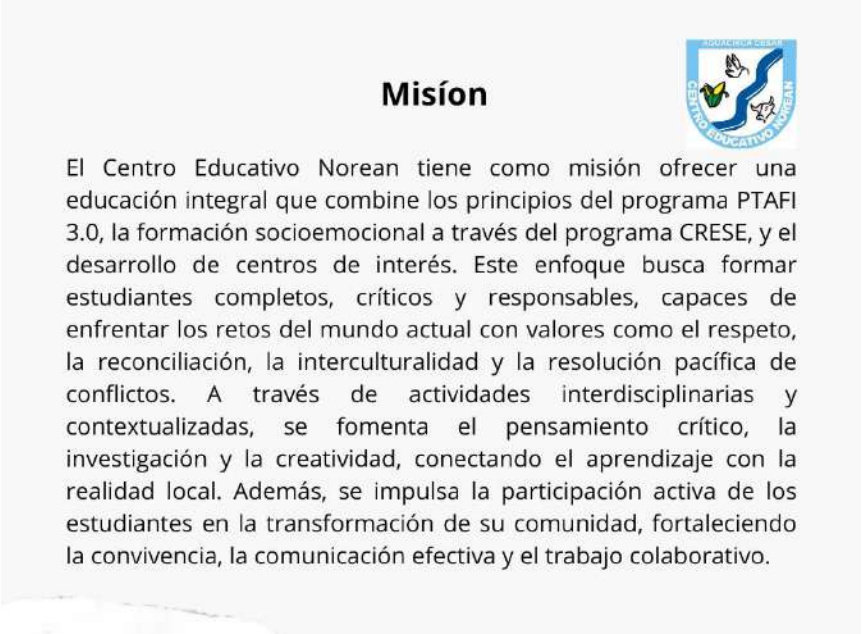
educación mixta en las jornadas mañana, tarde y fines de semana, lo que facilita el acceso a la formación para diversos grupos de estudiantes.

Ilustración 1 Fachada principal del Centro Educativo Norean.

Fuente: los autores.

El plan de estudios de la Institución estructura las áreas obligatorias y optativas, con sus respectivas asignaturas, identificando contenidos, temas y actividades pedagógicas. De esta forma, establece una metodología que incluye el uso de materiales didácticos, laboratorios, textos escolares, herramientas audiovisuales e informática educativa. Por otro lado, en el área de tecnología informática, el enfoque pedagógico promueve el desarrollo integral de los estudiantes, preparándolos para el entorno laboral mediante el uso adecuado de nuevas tecnologías. En relación a esto, la informática se emplea como herramienta para proyectos que involucran la búsqueda, selección, organización y visualización de información, así como para la simulación, el diseño asistido y el trabajo colaborativo, dentro del marco más amplio de las TIC.

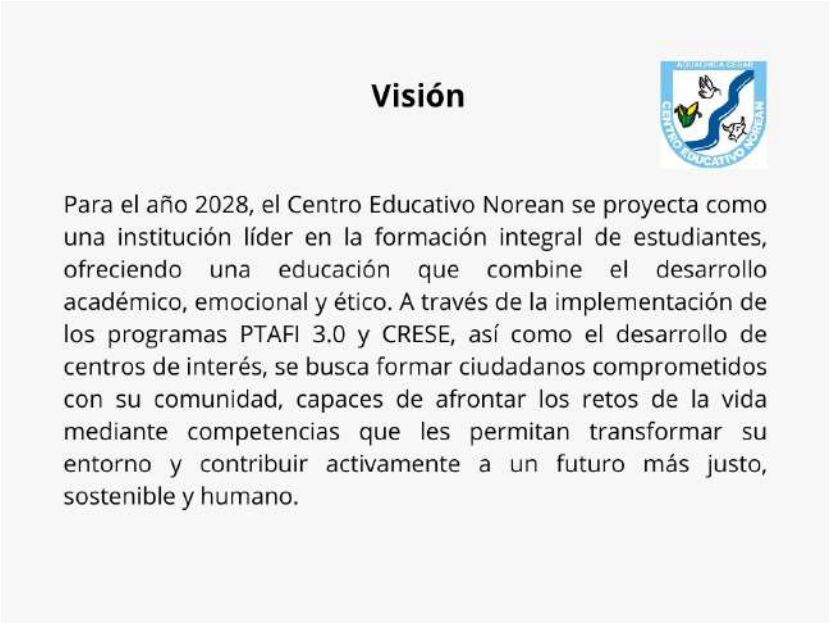
Ilustración 2 Misión del Centro Educativo Norean



Misíon

El Centro Educativo Norean tiene como misión ofrecer una educación integral que combine los principios del programa PTAFI 3.0, la formación socioemocional a través del programa CRESE, y el desarrollo de centros de interés. Este enfoque busca formar estudiantes completos, críticos y responsables, capaces de enfrentar los retos del mundo actual con valores como el respeto, la reconciliación, la interculturalidad y la resolución pacífica de conflictos. A través de actividades interdisciplinarias y contextualizadas, se fomenta el pensamiento crítico, la investigación y la creatividad, conectando el aprendizaje con la realidad local. Además, se impulsa la participación activa de los estudiantes en la transformación de su comunidad, fortaleciendo la convivencia, la comunicación efectiva y el trabajo colaborativo.

Ilustración 3 Visión del Centro Educativo Norean



Visión

Para el año 2028, el Centro Educativo Norean se proyecta como una institución líder en la formación integral de estudiantes, ofreciendo una educación que combine el desarrollo académico, emocional y ético. A través de la implementación de los programas PTAFI 3.0 y CRESE, así como el desarrollo de centros de interés, se busca formar ciudadanos comprometidos con su comunidad, capaces de afrontar los retos de la vida mediante competencias que les permitan transformar su entorno y contribuir activamente a un futuro más justo, sostenible y humano.

Fuente: *Centro Educativo Norean. (2025). Organigrama Institucional. Documento interno de Proyecto Educativo Institucional (PEI), Aguachica, Cesar.*

2.2.1 Filosofía Institucional

La filosofía del Centro Educativo Norean y sus Escuelas Anexas en el municipio de Aguachica se basa en una educación integral que atiende las necesidades sociales, económicas, físicas, éticas, morales, estéticas, espirituales, emocionales y culturales de cada estudiante, promoviendo su desarrollo completo. Se busca formar líderes con una visión futurista orientada al progreso, impulsando valores de equidad, justicia, participación, pluralismo y solidaridad. A través de la aplicación del conocimiento, los estudiantes serán capaces de identificar y resolver problemas de la comunidad, fundamentados en principios de paz, convivencia, protección y cuidado del medio ambiente.

La institución tiene como objetivo cumplir su misión y visión mediante un esfuerzo constante por construir una comunidad educativa comprometida con la participación y la responsabilidad social, fomentando valores como el respeto, la tolerancia, la perseverancia, la libertad, la honestidad, la responsabilidad y la confianza en uno mismo. Estos principios guiarán la formación de hombres y mujeres capaces de desempeñarse productivamente en su entorno.

El Proyecto Educativo Institucional (P.E.I.) de la Institución Educativa Norean es el resultado de una construcción colectiva que refleja la reflexión y participación activa de toda la comunidad educativa. Su propósito es crear una institución inclusiva, en la que todas las personas puedan acceder al sistema educativo, garantizando una educación de calidad, humana y orientada a la formación integral, que esté alineada con los principios del programa PTAFI 3.0, la formación socioemocional a través de CRESE, y los centros de interés diseñados para 2025. Por lo tanto, estos elementos, junto con la orientación en valores y el trabajo por el bienestar de la comunidad, buscan asegurar que cada estudiante sea parte activa de su propio proceso de aprendizaje y del desarrollo de su entorno.

2.2.2 Valores Institucionales.

En el Centro Educativo Norean, Se defienden valores fundamentales que fortalecen los pilares del conocimiento y forman individuos comprometidos con su entorno. Entre ellos se destacan la solidaridad, la justicia y el respeto a la diversidad, los cuales promueven la equidad y un ambiente inclusivo. Asimismo, se impulsa la responsabilidad personal y social, junto con la valoración del trabajo como motor del desarrollo individual y colectivo.

De igual manera, se reafirma la defensa de los derechos humanos y el compromiso con la paz, favoreciendo la resolución pacífica de los conflictos y una convivencia armónica. Finalmente, se promueve la conservación del entorno y la dignidad cultural, estimulando el cuidado de los recursos y la valoración de la riqueza cultural local y global.

Por otro lado, se promueve una visión holística del mundo que facilite la comprensión integral de los fenómenos sociales, económicos y ambientales. En este marco, el rol del docente requiere una formación continua que incluya la actualización disciplinar, el dominio de tecnologías digitales y la adopción de una pedagogía interdisciplinaria. Asimismo, debe orientar a los estudiantes en el análisis crítico de la información, mantener conocimiento de la realidad social y prepararlos para los retos del ámbito laboral y ciudadano. Con este enfoque, el programa CRESE fortalece competencias intelectuales, sociales y profesionales.

Este programa impulsa una formación integral que fortalece el desarrollo cognitivo, emocional y social de los estudiantes, promoviendo un aprendizaje significativo alineado con los centros de interés proyectados para 2025. En este contexto, iniciativas como PTAFI 3.0 favorecen la adquisición de habilidades técnicas y humanas vinculadas al proyecto de vida y al mundo laboral, integrando el emprendimiento y la creatividad como elementos que motivan la participación activa en la construcción de un futuro más equitativo.

Asimismo, el rol del docente se orienta hacia la actualización constante en disciplinas básicas, el dominio de herramientas digitales y la adopción de una pedagogía interdisciplinaria. De igual manera, debe mantenerse informado sobre las dinámicas

sociales contemporáneas, guiar el pensamiento crítico de los estudiantes y prepararlos para los retos del ámbito laboral y ciudadano.

2.2.3 Principios Institucionales

La Institución Educativa Norean orienta su labor formativa bajo principios que fortalecen el desarrollo integral del estudiante, en coherencia con el programa PTAFI 3.0. Se promueven valores como el respeto, la justicia, la solidaridad y la convivencia pacífica, garantizando una educación humanista que atiende las dimensiones física, intelectual, social y emocional.

Asimismo, la institución impulsa la construcción del proyecto de vida mediante el emprendimiento y la participación activa en los contextos económico, social y cultural. Este enfoque se complementa con una formación científica y técnica que proporciona conocimientos en áreas como tecnología, humanidades y ciencias, permitiendo a los estudiantes desarrollar habilidades críticas y creativas para enfrentar los retos de su entorno.

Finalmente, se destaca el compromiso con la diversidad cultural, la unidad nacional y la responsabilidad social. La institución fomenta la valoración de las distintas identidades culturales, la conciencia ambiental y el cuidado del patrimonio, alineándose con las metas del programa CRESE y con una educación orientada al progreso social y al desarrollo sostenible.

2.3 Marco Teórico.

Al abarcar la revisión de la literatura de la investigación es de gran importancia resaltar las teorías en las cuales se han enfocado, a través de los años, para realizar un sistema de gestión de seguridad de la información, que sea adecuado para alcanzar el éxito deseado y se adapte a las necesidades presentes en la organización que desee implantarlo. De igual modo, encontrarán las metodologías y sustentos teóricos que hoy

rigen a las organizaciones públicas en Colombia, según lo establecido dentro de la política de Gobierno Digital enmarcadas en los planes de desarrollo nacional, en donde es necesario para las entidades públicas empezar a implementar estándares que le permitan salvaguardar la información y sus activos.

Teoría de la Información.

La Teoría de la Información nos muestra, entre otras cosas, el camino a seguir para determinar la cantidad de información útil a partir de unos datos. Y para comprimir la información de manera que los datos se representen de una manera eficiente. Nace de la necesidad de optimizar los contenidos de las informaciones, en una época histórica en la que la comunicación alcanzaba un destacado papel (Shannon, 1948, citado en Meneses et al., 2016), esto después del nacimiento del código binario (Hartley, 1927, citado en Meneses et al., 2016) y los primeros pasos de encriptación (Turing, 1936). En consecuencia, se debía encontrar una forma en la cual determinar "la cantidad de información" que entregaba un mensaje.

El mayor investigador de este tema fue Claude Shannon quién aportó el concepto de que la información debe dejar de verse como inmaterial y subjetiva, sino que como perfectamente material y cuantificable. Así pasó a considerarse de una manera independiente un dispositivo de representación y se dio la posibilidad de hablar de procesos de representación y manipulación de la información sin hacer énfasis si era el cerebro o un ordenador quien realizaba dichos procesos. Esto permitió, dar el primer paso para la cibernética: el control de las máquinas para realizar tareas humanas, (Meneses et al., 2016).

La información es el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando técnicas criptográficas entre otras herramientas (Ramió Aguirre, 2006).Por tanto, la teoría de la información mide la cantidad de

información que tiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.

ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001, (Advisera, 2021)

La norma ISO 27001 proporciona un marco normativo que facilita a las organizaciones el desarrollo de un SGSI eficaz. Según lo expuesto por Parra, (2020), su adopción requiere una serie de pasos estructurados, entre los que se destacan la delimitación del alcance del SGSI, la evaluación de riesgos y la implementación de los controles de seguridad pertinentes para mitigar dichas amenazas. En este sentido, la seguridad de la información se presenta como una prioridad fundamental para las organizaciones, lo que convierte la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una necesidad imperante para la protección de los activos digitales.

Un SGSI basado en la norma ISO 27001 puede ser complementado mediante estándares adicionales, como ISO 27032, que refuerza los controles específicamente orientados a la ciberseguridad. Puesto que, este estándar amplía el enfoque al abordar amenazas propias del entorno digital, como el hacking, el ransomware y los ataques de ingeniería social. Además, las normas ISO 27017 e ISO 27018, orientadas a entornos de computación en la nube, pueden integrarse para proporcionar una mayor protección en

términos de seguridad y privacidad. De esta manera, las organizaciones pueden adaptar su SGSI para enfrentar tanto los riesgos tradicionales como las amenazas emergentes en el ámbito tecnológico, asegurando la confidencialidad, integridad y disponibilidad de la información crítica para su operatividad continua. Parra (2020).

La familia de normas ISO/IEC 27000 constituye un marco teórico fundamental para la gestión de la seguridad de la información. Según los autores Figueroa y Malagón (2016) cada norma dentro de esta serie aborda aspectos importantes para la protección de la información en organizaciones de cualquier tamaño, tanto públicas como privadas. La norma ISO/IEC 27001, es particularmente relevante en esta serie, establece los requisitos específicos del Sistema de Gestión de Seguridad de la Información (SGSI) y es el estándar utilizado para la certificación a través de auditorías externas. A su vez esta norma propone un enfoque integral que no solo abarca los sistemas informáticos, sino que también incluye toda la información de la empresa puesto que limitarse exclusivamente a los sistemas tecnológicos podría dejar vulnerable información clave afectando la continuidad operativa de la organización.

Por consiguiente, Figueroa y Malagón (2016) señalan que la implementación de la norma ISO 27001 se complementa eficazmente con el ciclo de Deming, una metodología de mejora continua aplicable a todos los procesos del SGSI. Este ciclo, originado por Walter Shewhart y popularizado por Edwards Deming, consta de cuatro fases: planificar, hacer, verificar y actuar. De la misma forma, a través de esta metodología, las organizaciones no solo logran implementar su SGSI, sino que también optimizan y ajustan sus procesos de manera constante, asegurando una protección eficaz contra accesos no autorizados y evitando la divulgación indebida de información, con el objetivo de destacar la importancia de la seguridad de la información para asegurar la integridad, disponibilidad y confidencialidad de los activos.

Seguridad de la información desde la Teoría de las Limitaciones

El eslabón más débil de la cadena

A cualquier profesional le suena: "La seguridad es como una cadena, es tan fuerte como el eslabón más débil" (Reid, 1786, citado en Ramos, 2007). Esto se dice por varios motivos: Para enfatizar la naturaleza de seguridad como proceso, como sistema, pero también para entender que se trata de una posición de defensa débil, es decir, el defensor tiene que defender todos los puntos, mientras que al atacante le basta con encontrar un punto vulnerable para tener éxito en su ataque.

Sin embargo, aunque se está convencido de que esto es así, muy pocos (por no decir, ninguno) realiza la gestión de este proceso conforme a esta máxima. Porque si se gestionará la seguridad teniendo este paradigma en mente, lo mejor sería emplear la misma estrategia que cualquier otro sistema cuya producción esté gobernada por su factor limitante. Me explico, después de identificarlo, habría que hacer que este factor limitante produjese al máximo nivel.

Esta forma de gestionar la seguridad cambiaría sobremanera el enfoque actual del proceso de gestión. Si se sigue lo establecido en los estándares, por ejemplo, el estándar ISO/IEC 27001 que establece las pautas para montar un Sistema de Gestión de la Seguridad de la Información (SGSI) "certificable", tenemos que (como ya hemos comentado aquí anteriormente) llevar a cabo un análisis de riesgos que nos permita identificar el nivel de riesgo por cada área o dominio del alcance establecido y pasar a gestionar el riesgo en función de la estrategia definida.

Si se plantea la seguridad como un sistema en el que el output fuera el nivel de seguridad de la organización (parece obvio, ¿no?), el máximo nivel estaría marcado por el máximo caudal que pudiera gestionar el cuello de botella del sistema, es decir, el nivel de seguridad de la organización sería el del eslabón más débil de la cadena.

¿Cuál es la diferencia entre estas dos maneras de gestionar la seguridad? la diferencia es que no tendría tanto interés realizar un análisis de riesgos como el hecho de encontrar cuál es el factor limitante, cuál es el eslabón más débil, puesto que sería el que marcaría

el nivel de seguridad de nuestra organización. A partir de ahí, si se quiere elevar el nivel de seguridad de nuestra organización, se debería gestionar esa limitación y eso, ya se sabe, hay que preguntarle a Goldratt el cómo (Ramos, 2007).

Dentro del contexto de la construcción de un Sistema de Gestión de Seguridad de la Información, es importante considerar la segunda política nacional de seguridad cibernética adoptada por Colombia en 2016. Esta política, mencionada por el equipo técnico de Banco Interamericano de Desarrollo en el año 2020, tiene como objetivo fortalecer las capacidades del Estado para responder a amenazas cibernéticas, subrayando la importancia de que todas las partes interesadas, incluidas las instituciones educativas, gestionen, traten y mitiguen los riesgos de seguridad digital. De la misma forma, resaltan la creación de un Comité de Seguridad Digital, que refuerza la necesidad de una coordinación centralizada que garantiza la seguridad en la gestión de la información dentro de una institución educativa como la del proyecto.

De acuerdo a lo anterior, el modelo de seguridad y privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), también descrito por los autores, ofrece un marco de buenas prácticas y estándares aplicables en la protección de activos críticos de información. Este enfoque se alinea con la norma ISO 27001, ya que promueve la mejora continua en la gestión de riesgos y la seguridad de la información. Así también, la Ley N° 1.581 de 2012 sobre la protección de datos personales, también mencionada en el artículo, resalta la relevancia de implementar medidas de confidencialidad, integridad y disponibilidad de la información, pilares fundamentales de un SGSI, asegurando así el cumplimiento normativo en la gestión de datos en la institución educativa involucrada en el proyecto.

La privacidad y la seguridad en la era digital, especialmente en la “era de la información líquida”, plantean nuevos retos para la protección de los derechos de los usuarios. Mendivelso, (2024) señala que la información circula sin restricciones de tiempo o espacio, lo que ha hecho que la privacidad sea cada vez más vulnerable a la vigilancia panóptica y a los avances tecnológicos. Esta vigilancia, descrita por Bentham y

popularizada por Foucault, muestra que la recopilación masiva de datos personales convierte a las personas en víctimas y participantes de un sistema de control invisible. Por lo tanto, es necesario proteger los datos personales tanto a nivel legal como ético para asegurar la autonomía y dignidad de los usuarios.

Un progreso notable en las leyes de protección de datos ha sido impulsado por la necesidad de equilibrar los derechos de privacidad con la seguridad en línea. Normativas como el Habeas Data permiten a las personas controlar sus datos personales, dándoles la capacidad de conocer, actualizar y corregir la información recopilada y procesada por entidades públicas y privadas. Esta regulación se adapta al contexto global, donde la vigilancia digital es omnipresente y la protección de datos enfrenta el desafío de asegurar que los usuarios mantengan su privacidad frente a prácticas como la comercialización de datos por grandes empresas tecnológicas. Estos mecanismos de protección buscan reducir el impacto del cibercrimen y preservar la confidencialidad, integridad y disponibilidad de la información en una era de vigilancia masiva y datos fluidos.

El ciberespacio ha revolucionado las relaciones internacionales, emergiendo como un nuevo ámbito de interacción y conflicto entre países. Por el lado de América Latina se enfrenta grandes retos en el desarrollo de políticas nacionales de ciberseguridad y en la construcción de capacidades para defenderse de las amenazas cibernéticas, que impactan tanto la seguridad nacional como la política exterior. Según Aguilar (2021) existen estudios de la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), donde mencionan la existencia significativa de brechas en la implementación de marcos regulatorios efectivos, identificación de ciber amenazas y formulación de políticas y estrategias en países como Uruguay, Colombia y Chile.

Aparte de estos avances, varios países de la región han comenzado a desarrollar capacidades militares en el ámbito cibernético, reconociendo que el ciberespacio no solo es un nuevo escenario de confrontación y cooperación internacional, sino también un entorno de riesgo para la seguridad nacional. Los países que no han logrado establecer

políticas sólidas se ven afectados por la falta de cooperación regional y el compromiso limitado con la Agenda Global de Ciberseguridad (AGCS). Dentro de este contexto, el continente necesitaría mejorar su cooperación tanto interna como externa para crear marcos de seguridad cibernética más robustos que incluyan respuestas rápidas a las crisis cibernéticas y mecanismos que fortalezcan su participación en el ámbito global.

Gobierno Digital

La constante evolución del gobierno electrónico en Colombia, ha dejado clara la importancia de las TIC para mejorar la gestión en las entidades públicas, así como los servicios que el Estado presta al ciudadano, no obstante, ahora surge una nueva realidad en donde la política de Gobierno Digital no solamente mejora los procesos y los servicios existentes, sino que permite llevar a cabo procesos de transformación digital que modifican la forma en que tradicionalmente el Estado se ha venido relacionando con el ciudadano.

En este nuevo contexto, Gobierno Digital se constituye en el motor de la transformación digital del Estado, permitiendo que las entidades públicas sean más eficientes para atender las necesidades y problemáticas de los ciudadanos y que éstos sean los protagonistas en los procesos de cambio a través del uso y apropiación de las tecnologías digitales. En este sentido, la política de Gobierno Digital define los lineamientos, estándares y proyectos estratégicos, que permiten llevar a cabo la transformación digital del Estado, a fin de lograr una mejor interacción con ciudadanos, usuarios y grupos de interés; permitiendo resolver necesidades satisfactoriamente, resolver problemáticas públicas, posibilitar el desarrollo sostenible y en general, crear valor público (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021b).

Modelo de Seguridad y Privacidad de la Información – (MSPI).

El Modelo, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la

seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

¿Para qué y cómo lo hace?

Para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021a).

Modelo IT4+

El modelo de gestión sobre el que se construyó la Estrategia TI para Colombia es IT4+®. Éste es un modelo resultado de la experiencia, de las mejores prácticas y lecciones aprendidas durante la implementación de la estrategia de gestión TIC en los últimos 10 años. IT4+® es un modelo integral que está alineado con la estrategia empresarial u organizacional y permite desarrollar una gestión de TI que genere valor estratégico para la organización y sus clientes.

El modelo busca que la tecnología contribuya al mejoramiento de la gestión apoyando los procesos para alcanzar una mayor eficiencia y transparencia en su ejecución, para que facilite la administración y el control de los recursos y brinde información objetiva y

oportuna para la toma de decisiones en todos los niveles. Permite la alineación de la gestión de TI con los objetivos estratégicos de la entidad, el aumento la eficiencia de la organización y la mejora de la forma como se prestan los servicios misionales (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016a).

2.4 Marco Conceptual

Seguridad de información.

Solarte, Enríquez y Benavides (2015) describen la seguridad de la información como un conjunto de acciones preventivas que buscan proteger la confidencialidad, integridad y disponibilidad de la información. Estas acciones se aplican tanto en formatos digitales como físicos, con el objetivo principal de resguardar los activos informáticos frente a amenazas internas y externas. Según los autores, la seguridad de la información no solo requiere el uso de tecnologías avanzadas, sino también la implementación de procedimientos, metodologías y estándares internos que aseguren la protección de los datos dentro de las organizaciones. Esto incluye la implementación de sistemas de gestión que involucren a todos los empleados de la organización, desde los niveles operativos hasta los directivos. Estas acciones están alineadas con el estándar ISO/IEC 27001.

El enfoque integral presentado por Solarte, Enríquez y Benavides (2015) ofrece una perspectiva crucial para el diseño de sistemas de gestión de seguridad de la información en entornos empresariales. Los autores destacan la importancia de realizar diagnósticos y auditorías periódicas para identificar vulnerabilidades y establecer controles que reduzcan los riesgos. Así, se garantiza que la seguridad de la información se integre en una estrategia organizacional que involucre activamente a todos los empleados, fomentando una cultura de seguridad y responsabilidad. Este enfoque no se limita solo a soluciones técnicas.

Sistema de gestión de seguridad – (SGSI).

Se describe el Sistema de Gestión de Seguridad de la Información (SGSI) como un conjunto de normas, procedimientos y medidas destinadas a proteger la disponibilidad, integridad y confidencialidad de la información dentro de una organización, (Coaguila, (2020). De esta manera, se recalca que el SGSI debe adherirse a la norma ISO/IEC 27001, la cual establece directrices para la implementación, mantenimiento y mejora de la seguridad de la información en una entidad. Este sistema es esencial para gestionar los riesgos que afectan a los activos informáticos, basándose en la identificación de amenazas y vulnerabilidades, así como en el tratamiento adecuado de los riesgos para reducir su impacto.

Coaguila, (2020) destaca que el Sistema de Gestión de Seguridad de la Información (SGSI) no se limita solo a aspectos técnicos, sino que también requiere la participación de toda la organización, incluyendo la alta dirección, para que los controles de seguridad sean efectivos. Además, el SGSI debe ser revisado y actualizado periódicamente para asegurar su cumplimiento con los estándares internacionales y su adaptación a las necesidades cambiantes de la organización. Esta metodología de gestión de riesgos facilita la toma de decisiones informadas sobre la protección de los activos informáticos y la garantía de la continuidad operativa.

ISO 27001

Los autores (Torres, Serjino), señalan que la norma ISO 27001 es la mejor colección de mejores prácticas para implementar un Sistema de Administración de Seguridad de la Información, que es vital para proteger la información crítica precisamente. Esta norma es esencial ya que brinda un marco formal para proteger datos sensibles, y si una organización no lo hace, no tiene intención de activos físicos ni financieramente valiosos.

Es vital para una organización que gestiona información de alta confidencialidad, como la DIVATJ de la PNP (Policía Nacional del Perú), y cumple con su responsabilidad como

custodio de la información en términos de confidencialidad, integridad y disponibilidad. También les brinda la certificación una confirmación formal que se obtiene al tiempo que aumenta la confianza de los interesados, obteniendo formalmente.

De esta manera, Torres y Serjino, recomiendan un método metodológico para garantizar la eficacia de la normación. Primero, se propone la realización de la evaluación de riesgos utilizando la metodología MAGERIT, que se invierte para corregir las brechas de seguridad en los sistemas de información. Al mismo tiempo, para lograr facilitar la gestión efectiva de riesgos, debieron desarrollar las políticas y los procesos internos. La capacitación continua del personal es otro criterio importante para poder asegurar que se sigan las prácticas recomendadas y se proteja suficientemente la información confidencial, lo que garantizará el cumplimiento de las leyes correspondientes.

Análisis de riesgos.

Barrientos y Santos, (2023) examinan el concepto de análisis de riesgos como un componente fundamental en la implementación de un sistema de seguridad de la información. Asimismo, lo definen como un proceso que puede ser tanto cuantitativo como cualitativo, destinado a evaluar los posibles riesgos que enfrenta una organización en la protección de sus activos. el primer paso es que este proceso implica la identificación de los activos críticos que requieren protección.

Esta teoría se finaliza con los riesgos que se contrastan con los estándares establecidos para permitir una evaluación consistente y facilitar decisiones informadas acerca de las medidas de seguridad que se deben adoptar. Del mismo modo, los autores enfatizan la importancia de implementar el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) como una herramienta esencial para una gestión de riesgos eficiente. Este ciclo comienza con la fase de planificación, que busca activos críticos y amenazas o vulnerabilidades potenciales.

Posteriormente, durante la fase de ejecución, se implementan controles de seguridad para reducir los riesgos. Se analizan los resultados y se supervisan los incidentes de seguridad durante la fase de verificación para evaluar la efectividad de los controles implementados. Finalmente, durante la fase de acción, se toman medidas correctivas para corregir cualquier error o vulnerabilidad descubierto. El ciclo PDCA, que es iterativo, no solo promueve la mejora continua del sistema de seguridad.

Política de seguridad de la información.

Salcedo, señala la relevancia que existe en cuanto a la necesidad de contar con una política de seguridad de la información para así poder "garantizar la confidencialidad, integridad y disponibilidad de los datos" en una empresa. En cuanto a ello, dada la necesidad para que la política pueda comunicarse de forma formal y clara, "Se logra así el marco donde se indica formalmente los principios básicos para proteger la información en transcurso de cada persona dentro de la empresa, desde la que trabaja, hasta el sistema tecnológico".

En virtud del impacto que posee la seguridad de la información en los procesos esenciales de la organización, es indispensable que la dirección superior esté presente en la observación y cumplimiento de las medidas adecuadas. De igual forma, la implementación de la política de seguridad de la información sigue el ciclo PDCA, el cual es un modelo de gestión de seguridad común que facilita un ciclo continuo de mejora para los sistemas de gestión de seguridad de la información (SGSI).

La etapa de la fase de planificación incluye el desarrollo de la política, la designación de roles y responsabilidades, seguido de la etapa de ejecución abarca la implementación de los controles y procedimientos de seguridad. Luego, en la etapa de verificación, se llevarán a cabo auditorías para evaluar la efectividad de las medidas implementadas. Por último la etapa es la de hacer, que deberá ajustar las políticas y las acciones correctivas deben tomarse para continuar mejorando la seguridad.

2.5 Marco legal.

Para la realización del proyecto fue necesario acoger las normativas legales vigentes en Colombia relacionadas con los Sistemas de Gestión de Seguridad de la Información, las cuales se mencionan a continuación:

Ley 23 de 1982 – (Derechos de autor): Normativa que regula los derechos de autor en Colombia, esta ley establece las disposiciones para la protección de las obras literarias, artísticas y científicas, otorgando derechos morales y patrimoniales a los creadores de dichas obras.

> **Artículo 1-** "Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor". (Congreso de Colombia).

Esta ley es implementada en el proyecto para asegurar que la institución cumpla con la protección de los derechos de autor de cualquier material educativo, software o contenido utilizado. Esto implica la gestión adecuada de las licencias y evitar la violación de derechos de terceros.

Decreto 1008 de 2018: Este decreto establece los lineamientos para la implementación de la Política de Gobierno Digital en Colombia, con el objetivo de promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones (TIC) para mejorar la eficiencia del Estado y la interacción con los ciudadanos.

> **Artículo 2.2.9.1.1.1.** "El presente capítulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y

ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.”

Este decreto se implementará en el proyecto, por el hecho de que reafirma la obligación de las entidades públicas de hacer que la información esté asegurada y aplicar tecnologías seguras. Al hacer un SGSI basado en la ISO 27001, es factible cumplir con este requisito, ya que se asegura el riesgo de confidencialidad, integridad y disponibilidad de la información asociada en su institución educativa.

Ley 1621 de 2013: Normativa que regula las actividades de inteligencia y contrainteligencia en Colombia, con el fin de proteger los derechos humanos y la seguridad nacional, así también busca mejorar la coordinación entre las distintas entidades del Estado para la prevención y lucha contra las amenazas a la seguridad.

> **Articulo 1- “**La presente ley tiene por objeto fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal. Establece los límites y fines de las actividades de inteligencia y contrainteligencia, los principios que las rigen, los mecanismos de control y supervisión, la regulación de las bases de datos, la protección de los agentes, la coordinación y cooperación entre los organismos, y los deberes de colaboración de las entidades públicas y privadas, entre otras disposiciones.” (Congreso de la república de Colombia).

Dentro del contexto del proyecto, esta ley se integra para asegurar la protección de información sensible y estratégica de la institución educativa, y de esta manera ampararla ante posibles amenazas tanto internas como externas.

Ley 527 de 1999: Esta normativa regula aspectos como la equivalencia entre documentos electrónicos y escritos, la validez jurídica de la firma digital y las responsabilidades relacionadas con el uso de estos sistemas.

> “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.”

En el presente proyecto se busca garantizar la integridad y autenticidad de la información a través del uso de firmas digitales, con el fin de implementar procesos seguros para la validación de documentos electrónicos, garantizando que se cumplan los requisitos legales para el manejo de información digital en la institución.

Norma ISO/IEC 27001: Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización, Icontec (2013). De esta forma la ISO 27001 estableces un marco para gestionar y proteger la información confidencial, garantizando la integridad, confidencialidad y disponibilidad de los datos.

Esta norma es el eje central del proyecto, puesto que la implementación de la ISO/IEC 27001 garantizará que el centro educativo Norean gestione la seguridad de la información de manera estructurada y coherente. Por último, el SGSI proporcionará un enfoque sistemático para minimizar los riesgos asociados con el manejo de datos sensibles, asegurando que se cumplan los estándares internacionales.

Ley 1276 de 2008: Esta ley establece el derecho de las personas mayores a recibir una atención adecuada y digna en centros de bienestar, así como la protección de sus datos personales. Aunque su foco principal es la protección social de los adultos mayores, su conexión con la investigación radica en que las instituciones que manejan datos personales de estas personas deben cumplir con medidas de seguridad adecuadas para proteger dicha información.

> **Artículo 1-** “La presente ley tiene por objeto la protección a las personas de la tercera edad (o adultos mayores) de los niveles I y II de Sisbén, a través de los

> Centros Vida, como instituciones que contribuyen a brindarles una atención integral a sus necesidades y mejorar su calidad de vida."

Aporta a la investigación en la medida en que subraya la importancia de garantizar que las instituciones que almacenan datos personales tomen las medidas necesarias para proteger la privacidad y seguridad de la información, alineándose con los principios de la ISO 27001 en cuanto a confidencialidad, integridad y disponibilidad de los datos.

Ley 1581 de 2012: Esta ley otorga a los ciudadanos el derecho fundamental de la protección de sus datos personales, y establece disposiciones para su tratamiento, asegurando que los datos se recojan, almacenen y traten de manera justa y segura. Los titulares de los datos tienen derecho a conocer, actualizar y rectificar la información que se almacena sobre ellos.

> **Artículo 1-** "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."

Es directamente relevante para la implementación del SGSI, ya que regula los derechos de las personas en cuanto a sus datos personales. La investigación debe asegurar que el SGSI cumpla con las disposiciones de esta ley, garantizando que la institución educativa maneje la información de manera que respete los derechos de los titulares. La norma ISO 27001 ofrece el marco adecuado para garantizar que los procedimientos del SGSI se alineen con estas disposiciones legales, lo que refuerza el derecho a la privacidad y protección de los datos personales.

Decreto 1377 de 2013: Este decreto especifica las disposiciones adicionales sobre los derechos de los titulares de los datos personales, incluyendo el consentimiento informado

para la recolección de datos, la rectificación, y la eliminación de la información personal. También establece los requisitos para que las entidades implementen mecanismos adecuados de protección de los datos.

> **Artículo 1-** "El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales."

Esto a cuanto los procedimientos técnicos que deben ser implementados por la institución educativa para cumplir con los derechos de los titulares de datos personales, establecidos en la Ley 1581. La investigación debe considerar cómo integrar estos mecanismos dentro del SGSI, asegurando que las disposiciones técnicas del decreto (como la amonificación de datos y la gestión del consentimiento) sean gestionadas a través de controles de seguridad alineados con ISO 27001.

Ley 1712 de 2014: Esta ley garantiza el derecho de los ciudadanos a acceder a la información pública de manera clara y oportuna. Establece disposiciones sobre cómo las entidades públicas deben poner a disposición del público la información relevante, asegurando que el acceso sea transparente, excepto cuando dicha información esté sujeta a restricciones de seguridad o privacidad.

> **Artículo 1-** "El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información."

Esta ley aporta a la investigación en cuanto a la obligación de la institución educativa de gestionar la información pública de manera segura y responsable, evitando violaciones de seguridad que podrían comprometer la confidencialidad de la información sensible. En este sentido, la norma ISO 27001, a través de su enfoque en la gestión de riesgos y controles de seguridad, asegura que el acceso a la información pública sea seguro, sin poner en riesgo la integridad de la misma ni violar los derechos de privacidad.

Ley Estatutaria 1226 de 2008

Esta ley regula el manejo de la información financiera, crediticia, comercial, de servicios y proveniente de terceros países, y establece los derechos y garantías relacionados con la administración de estos datos personales.

> **Artículo 1-** "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países."

Por ende, la ley también contribuirá a garantizar el cumplimiento de los principios de protección de datos personal en el Sistema de Gestión de Seguridad de la Información, lo cual es un aspecto crítico en la ISO 27001 para garantizar que la información sea privada y segura en la institución educativa.

Decreto 1727 de 2009

Este decreto reglamenta parcialmente la Ley 1266 de 2008, especificando cómo deben funcionar los operadores de bases de datos y los responsables del tratamiento de la información.

> **Artículo 1-** "Para los efectos de lo consagrado en el artículo 14 de la Ley 1266 de 2008, los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, al presentar la información de los titulares deberán adoptar un formato que contenga, como mínimo, los datos requeridos en el presente decreto, según el sector al cual pertenezca la fuente de información. "

Esto lograra proporcionar pautas claras sobre cómo gestionar y actualizar los datos personales almacenados en el SGSI de la institución, asegurando el cumplimiento de las normativas nacionales y alineándose con las buenas prácticas de seguridad de la información.

Ley 1273 de 2009

Esta ley está muy ligada a la norma ISO 27001 ya que el capítulo primero se refiere a "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y el capítulo segundo a "De los atentados informáticos y otras infracciones". Como se puede evidenciar, se hace claramente hincapié a la seguridad de la información.

> **Artículo 1-** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." (Ley 1273, 2009).

Esta ley es fundamental para fortalecer la ciberseguridad del SGSI que se está construyendo. Si se diseñan controles que eviten a toda costa el acceso no autorizado, cumplirá con los requisitos de la ISO 27001, y será leal al mismo tiempo en seguridad de los sistemas de protección y la información.

Ley 1341 de 2009

Esta ley regula la prestación de servicios de tecnologías de la información y las comunicaciones, promoviendo su acceso eficiente y seguro.

> **Artículo 1-** " La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la

protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.“

Refuerza el aspecto tecnológico del SGSI, garantizando que los sistemas que implementaran cumplan con los principios de seguridad, accesibilidad y confiabilidad en la infraestructura de las TIC en la institución.

Decreto 103 de 2015

Este decreto reglamenta la implementación de la Ley de Transparencia y Acceso a la Información Pública (Ley 1712 de 2014), definiendo las obligaciones de las entidades públicas para garantizar el acceso a la información.

> **Artículo 1-** “Este decreto tiene por objeto reglamentar la Ley 1712 de 2014, en lo relativo a la gestión de la información pública”.

Este decreto es crucial para la SGSI ya que logra establecer las condiciones bajo las cuales la información debe estar accesible al público, respetando siempre la confidencialidad y seguridad de los datos sensibles.

Decreto 1078 de 2015

Este decreto consolida y organiza la normativa del sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, y actualiza las regulaciones relacionadas con la infraestructura tecnológica, la ciberseguridad y el manejo de TIC.

> “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”. (Decreto 1078, 2015).

Este decreto proporciona el marco normativo para garantizar que el SGSI que se realice esté alineado con las regulaciones del sector TIC. Asegurando que todos los sistemas tecnológicos y los controles de seguridad que se implementen en la institución cumplan con la normativa actual, especialmente en temas de protección de datos.

CAPITULO 3. ESTRUCTURA METODOLÓGICA

3.1 Tipo de investigación

En el presente proyecto se adopta un enfoque cualitativo con apoyo cuantitativo, dado que la base del análisis se centra en la interacción directa con los participantes y en la interpretación de sus percepciones y prácticas en torno a la gestión de los activos informáticos. Este enfoque cualitativo permite comprender en profundidad la situación actual, apoyándose en entrevistas, listas de chequeo y observación directa, donde la interacción personal para la recopilación de datos es fundamental, como señalan Hernán et al. (2021).

De manera complementaria, se incorporan elementos cuantitativos mediante la aplicación de listas de chequeo y el registro de indicadores de cumplimiento, lo que aporta una visión más objetiva y medible del estado de seguridad de la información en la institución. En este sentido, se emplea un diseño de investigación descriptivo, entendido según Stewart (2022) como una herramienta sistemática utilizada para recopilar y analizar datos de fenómenos de la vida real, con el propósito de describirlos en su contexto natural. Tal como señalan Guevara et al. (2020), “el objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas”.

3.2 Diseño metodológico

La metodología aplicada en el proyecto se basa en una combinación de enfoques cualitativos y cuantitativos. La razón de este diseño metodológico es garantizar un análisis integral durante el desarrollo del sistema de seguridad de la información. De esta manera, se busca abordar de forma efectiva los problemas particulares de la institución educativa, proponiendo la integración de medidas específicas basadas en la norma ISO 27001.

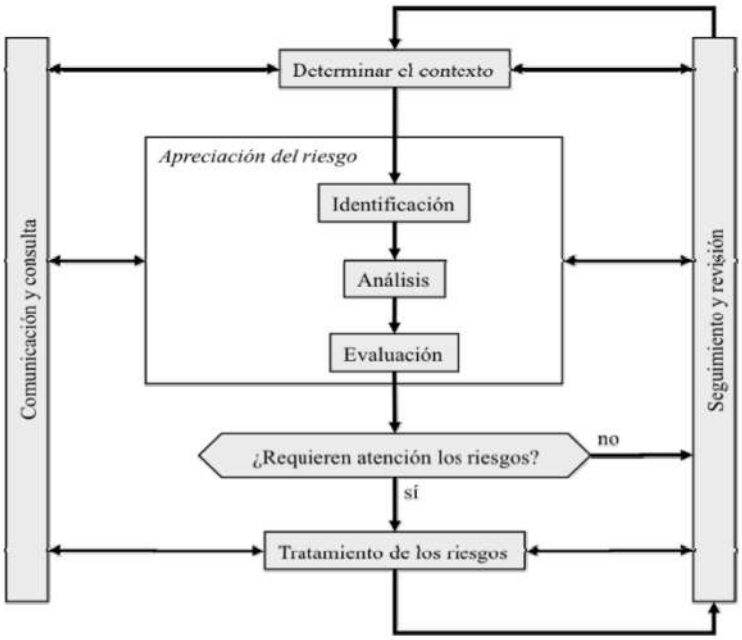
Para el logro de los objetivos establecidos, se implementará, siguiendo las recomendaciones de la ISO 27001, el uso del ciclo continuo PHVA. Según Julia Martins (2024), el Ciclo PDCA, también conocido como Ciclo Deming o PHVA (acrónimo de Planificar-Hacer-Verificar-Actuar), es una estrategia iterativa utilizada para la resolución de problemas, la mejora de la gestión de procesos y la implementación de cambios. En este caso, cada ciclo será utilizado para fortalecer continuamente los procesos de seguridad de la información.

Ilustración 4 Ciclo PHVA

***Fuente**: Méndez (2020); Tomado desde la plataforma LinkedIn.*

Por otro lado, para el análisis de riesgos específicamente, se empleará la metodología sistemática MAGERIT V 3, la cual permitirá identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información en los sistemas de información. Siguiendo la terminología de la norma ISO 31000, MAGERIT responde a lo que se denomina el "Proceso de Gestión de Riesgos" tal como se muestra en la imagen.

Ilustración 5 Proceso de gestión de riesgos



***Fuente**: Margerit V 3.0*

3.3 Operacionalización de las Variables.

Para el desarrollo del proyecto se establecen dos variables principales: una variable independiente, que representa el factor que se interviene o introduce, y una variable dependiente, correspondiente al efecto o resultado derivado de dicha intervención. La operacionalización de estas variables facilita la definición de dimensiones, indicadores e instrumentos de medición.

La variable independiente corresponde a la implementación de los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) basados en la norma ISO/IEC 27001:2022, entendida como la aplicación de controles y directrices orientadas a fortalecer la seguridad del Centro Educativo Norean mediante la identificación de activos, el análisis de riesgos y la definición de políticas y acciones de capacitación.
La variable dependiente hace referencia al nivel de seguridad de la información en la gestión de los activos institucionales, reflejado en la confidencialidad, integridad y

disponibilidad de los datos, así como en el cumplimiento de controles y la disminución de vulnerabilidades tras la aplicación del SGSI.

Tabla 1 Definición y alcance de las variables utilizadas para analizar el impacto de la implementación del SGSI basado en ISO/IEC 27001:2022

Variable	Dimensiones	Indicadores	Técnicas / Instrumentos
Variable Independiente: Implementación de lineamientos del SGSI basados en ISO/IEC 27001:2022	Identificación de activos	Inventario actualizado de activos	Lista de chequeo, entrevistas
	Análisis de riesgos	Existencia de valoración de riesgos; identificación de amenazas y vulnerabilidades	Matriz de riesgos, observación directa
	Controles de seguridad	Porcentaje de controles implementados respecto a la norma	Lista de verificación ISO 27001
	Capacitación	Número de sesiones realizadas y nivel de participación	Registros institucionales

En la siguiente página se continua la tabla.

Tabla 1 (Continuación)

Variable	Dimensiones	Indicadores	Técnicas / Instrumentos
Variable Dependiente: Nivel de seguridad de la información	Confidencialidad	Controles de acceso establecidos; manejo seguro de información	Observación, entrevistas
	Integridad	Procedimientos para la modificación de datos; ausencia de alteraciones	Revisión documental
	Disponibilidad	Accesibilidad a activos; tiempo de recuperación de información	Registros institucionales
	Cumplimiento normativo	Nivel de cumplimiento general del SGSI	Lista de chequeo ISO 27001

Fuente: *Elaborado* por los autores.

3.4 Técnicas para la recolección de datos

Entrevistas semiestructuradas: Se realizarán para poder evaluar los riesgos y necesidades específicas del personal administrativo y los docentes en relación con la seguridad de la información. También es necesario aclarar la percepción de la importancia de la protección de la información y la familiaridad con las políticas institucionales existentes.

Observación directa: se utilizará para evaluar la implementación actual de los procesos de administración de información y la tecnología de la información por parte de la institución.

Encuestas: Se llevarán a cabo para recopilar información sobre el conocimiento y la aplicación de políticas de seguridad entre el personal administrativo y los profesores.

Listas de chequeo: Este instrumento permitirá tener la información que verifica el estado físico y funcional de los equipos de cómputo, dispositivos de red y software de la institución y así identificar posibles fallos o vulnerabilidades.

3.5 Población y Muestra

Población

Para el desarrollo del proyecto, la población objetivo está constituida por el Centro Educativo Norean, dado que los lineamientos y acciones propuestas abarcan a toda la institución. Este grupo incluye a los usuarios que acceden y gestionan activos que contienen información relevante, tanto de los estudiantes como del personal institucional.

Muestra

Conforme a la ISO/IEC 27001:2022, la protección de la información depende de un SGSI orientado a garantizar la confidencialidad, integridad y disponibilidad de los activos. Bajo este criterio, la muestra del proyecto se definió entre los docentes y el personal administrativo, dado que son quienes manejan información institucional de manera directa. En consecuencia, la muestra quedó integrada por el señor Rector y 9 docentes, cuya asistencia se evidencia en el Anexo 10. Asimismo, se aplicaron diversas técnicas de recolección de datos a los participantes, tal como se presenta en los Anexos correspondientes. De esta manera, la muestra estuvo conformada por actores que interactúan directamente con los sistemas de información y participan activamente en los procesos de gestión y protección de los datos institucionales.

CAPITULO 4. DESARROLLO DE OBJETIVOS

4.1. FASE 1: DIAGNOSTICANDO EL ESTADO ACTUAL E IDENTIFICANDO RIESGOS ASOCIADOS A LA DE LA SEGURIDAD DE LA INFORMACIÓN.

Para el desarrollo de la Fase 1, se realizará una breve contextualización de la entidad y los organismos que la conforman. Seguidamente, se realizará una auditoría interna, delimitada por los alcances y separada en actividades específicas, con el fin de diagnosticar el estado actual del centro educativo. De esta manera se mostrarán los resultados obtenidos durante esta primera parte que permitirá avanzar hacia la consecución de nuestro primer objetivo:

“Analizar los riesgos asociados al uso de las tecnologías de la información mediante metodologías que permitan identificar, evaluar y priorizar amenazas, vulnerabilidades e impactos, como base para establecer un diagnóstico del estado actual de la seguridad de la información del centro educativo”.

4.1.1 Contextualización

La Institución Educativa Técnica Norean - Sede Principal, ubicada en el corregimiento de Norean, en Aguachica, Cesar, es una institución oficial de carácter académico con Calendario A, jornada mañana, tarde y fines de semana, y matrícula contratada. Atiende a estudiantes desde preescolar hasta educación media, incluyendo programas para adultos y modalidad virtual asistida.

Su filosofía se basa en la formación integral del estudiante, fomentando valores como liderazgo, equidad, justicia, solidaridad y trabajo en equipo. A través de modelos educativos como Escuela Nueva y Educación Post Primaria, impulsa el desarrollo social y comunitario, promoviendo la paz, la convivencia y el cuidado del medio ambiente, preparando a los estudiantes para aplicar su conocimiento en la solución de problemáticas locales.

4.1.2 Misión y Visión del Centro Educativo.

Misión

El Centro Educativo Norean tiene como misión ofrecer una educación integral que combine los principios del programa PTAFI 3.0, la formación socioemocional a través del programa CRESE, y el desarrollo de centros de interés. Este enfoque busca formar estudiantes completos, críticos y responsables, capaces de enfrentar los retos del mundo actual con valores como el respeto, la reconciliación, la interculturalidad y la resolución pacífica de conflictos. A través de actividades interdisciplinarias y contextualizadas, se fomenta el pensamiento crítico, la investigación y la creatividad, conectando el aprendizaje con la realidad local. Además, se impulsa la participación activa de los estudiantes en la transformación de su comunidad, fortaleciendo la convivencia, la comunicación efectiva y el trabajo colaborativo.

Visión

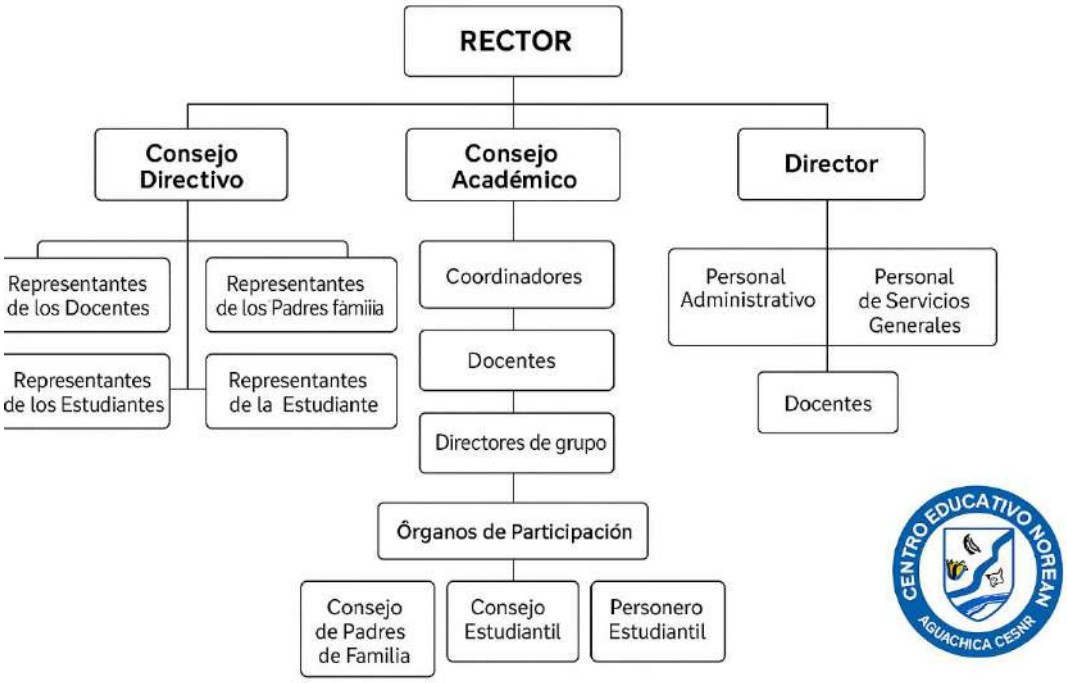
Para el año 2028, el Centro Educativo Norean se proyecta como una institución líder en la formación integral de estudiantes, ofreciendo una educación que combine el desarrollo académico, emocional y ético. A través de la implementación de los programas PTAFI 3.0 y CRESE, así como el desarrollo de centros de interés, se busca formar ciudadanos comprometidos con su comunidad, capaces de afrontar los retos de la vida mediante competencias que les permitan transformar su entorno y contribuir activamente a un futuro más justo, sostenible y humano.

4.1.3 Organigrama del Centro Educativo

El organigrama del Centro Educativo Norean representa la estructura jerárquica y funcional de la institución, destacando las principales instancias que conforman su gobierno escolar. A través de él se evidencia la distribución de responsabilidades y la relación entre los diferentes órganos que orientan la gestión administrativa, académica y

de participación de la comunidad educativa. Esta estructura garantiza una adecuada toma de decisiones, el cumplimiento de los objetivos institucionales y la articulación entre los niveles directivos, docentes, administrativos y estudiantiles.

Ilustración 6 Organigrama del Centro Educativo Norean



Fuente: *Centro Educativo Norean. (2025). Organigrama Institucional. Documento interno del Proyecto Educativo Institucional (PEI), Aguachica, Cesar.*

4.1.4 Auditoría interna

Para obtener resultados transparentes y verídicos se realizará una auditoría interna con el fin de analizar la evaluación orientada al manejo y la protección de los sistemas de información, asimismo la eficiencia de los recursos informáticos disponibles y el desempeño competencial del recurso humano encargado de su gestión.

4.1.4.1 Objetivos de la auditoria

Objetivo General:

Realizar una auditoría interna para evaluar el estado actual de la seguridad de la información en el Centro Educativo Norean de Aguachica, Cesar, identificando vulnerabilidades, riesgos y brechas respecto a la norma ISO 27001, como base para la construcción del Sistema de Gestión de Seguridad de la Información (SGSI).

Objetivos Específicos:

- Identificar vulnerabilidades, amenazas y riesgos que afecten la seguridad de la información, considerando los activos, procesos y sistemas del Centro Educativo Norean.

- Evaluar el cumplimiento y la eficacia de los controles, políticas y procedimientos existentes en relación con los requisitos de la norma ISO 27001.

- Analizar los hallazgos de auditoría y emitir un dictamen sobre el nivel de conformidad con la norma ISO/IEC 27001.

4.1.4.2 Alcance de la auditoria

Es fundamental definir el alcance de la auditoría para precisar el nivel de detalle que se abordará. Con base en ello, se dividirán los objetivos en actividades concretas a realizar dentro de la entidad, considerando las funciones que se auditarán, los elementos específicos que serán objeto de estudio y la profundidad con la que se llevará a cabo la evaluación.

Objetivo 1: Identificar vulnerabilidades, amenazas y riesgos que afecten la seguridad de la información, considerando los activos, procesos y sistemas del Centro Educativo Norean.

Nota: La tabla 2 muestra el plan de actividades que se realizarán para dar cumplimiento al primer objetivo.

Tabla 2 Plan de actividades para la identificación de vulnerabilidades, amenazas y riesgos en los activos, procesos y sistemas del Centro Educativo Norean

Referencia	Actividad o Función	Técnica de evaluación
AS-001	Visita inicial al Centro Educativo Norean para reconocimiento físico y contextual	Observación directa
AS-002	Identificación de activos de información (equipos, documentos, bases de datos)	Entrevista y listas de chequeo
AS-003	Aplicación de instrumentos de recolección de datos sobre amenazas y vulnerabilidades	Entrevistas y encuestas

Elaborado por: Los autores.

Objetivo 2: Evaluar el cumplimiento y la eficacia de los controles, políticas y procedimientos existentes en relación con los requisitos de la norma ISO 27001.

Nota: En la siguiente tabla (Tabla 3), contiene el plan de actividades que se realizarán para dar cumplimiento al segundo objetivo.

Tabla 3 Plan de actividades para evaluar el cumplimiento y la eficacia de los controles, políticas y procedimientos según ISO 27001 en el Centro Educativo Norean.

Referencia	Actividad o Función	Técnica de evaluación
ASS-001	Revisión de documentos institucionales (políticas de seguridad, reglamentos, procedimientos)	Revisión documental
ASS-002	Aplicación de cuestionarios al personal clave para evaluar implementación de controles	Cuestionarios estructurados
ASS-003	Inspección de infraestructura tecnológica y verificación de medidas de protección.	Lista de chequeo.

Elaborado por: Los autores

Objetivo 3: Analizar los hallazgos de auditoría y emitir un dictamen sobre el nivel de conformidad con la norma ISO/IEC 27001.

Nota: La página siguiente contiene la Tabla 4 que muestra el plan de actividades que se realizarán para dar cumplimiento al tercer objetivo.

Tabla 4 Plan de actividades para analizar los hallazgos de auditoría y emitir el dictamen de conformidad según la norma ISO/IEC 27001.

Referencia	Actividad o Función	Técnica de evaluación
ASS-001	Analizar los hallazgos obtenidos en la auditoría.	Informe y análisis de resultados.
ASS-002	Elaborar el dictamen de conformidad con base en los hallazgos.	Documentación técnica.
ASS-003	Presentar los resultados y recomendaciones a la dirección.	Reunión de socialización y entrega del informe.

Elaborado por: Los autores.

4.1.4.3 Plan general de auditoria

Para la elaboración de la auditoría se diseñó un plan de trabajo que permitió organizar, programar y orientar las actividades necesarias para la ejecución del proyecto. Este plan facilitó la definición de objetivos, tareas y responsables, asegurando un desarrollo ordenado y eficiente de las metas propuestas.

En la página siguiente se ilustra la Tabla 5, donde se presenta el plan de trabajo dividido en tres etapas, las cuales representan los objetivos a desarrollar, junto con las actividades y los participantes involucrados en la auditoría. Su finalidad es organizar las tareas según los periodos estimados de cumplimiento.

Tabla 5 Plan de trabajo de la auditoria

ETAPA	DESCRIPCIÓN	ACTIVIDAD	PARCTICIPANTES	PERIODO ESTIMADO
1	Identificar vulnerabilidades, amenazas y riesgos que afecten la seguridad de la información del Centro Educativo Norean.	Identificar activos del centro Educativo por medio de visita al centro Educativo.	Estudiantes investigadoras y director del proyecto, con acompañamiento del Rector.	**Fecha Inicio**
				08/04/2025
				Fecha Final
				15/04/2025
		Aplicar instrumentos de recolección de datos para identificar amenazas y vulnerabilidades	Estudiantes investigadoras, Rector y Docentes colaboradores.	**Fecha Inicio**
				22/04/2025
				Fecha Final
				28/04/2025
		Analizar las respuestas obtenidas por los entrevistados para ir clasificando los hallazgos.	Estudiantes investigadoras bajo orientación del director del proyecto.	**Fecha Inicio**
				12/05/2025
				Fecha Final
				22/05/2025

***Tabla 5**. (Continuación del plan de trabajo en la etapa 2)*

ETAPA	DESCRIPCIÓN	ACTIVIDAD	PARCTICIPANTES	PERIODO ESTIMADO
2	Evaluar el cumplimiento y eficacia de los controles, políticas y procedimientos existentes frente a los requisitos de la norma ISO 27001.	Revisar documentos institucionales (políticas de seguridad, procedimientos, reglamentos internos).	Estudiantes investigadoras y Rector, con orientación del director del proyecto.	**Fecha Inicio**
				23/05/2025
				Fecha Final
				30/05/2025
		Aplicar cuestionarios al personal clave para evaluar el conocimiento y aplicación de los controles establecidos.	Estudiantes investigadoras y Docentes colaboradores.	**Fecha Inicio**
				06/06/2025
				Fecha Final
				10/06/2025
		Analizar los procesos institucionales para detectar riesgos asociados a la seguridad de la información.	Estudiantes investigadoras, director del proyecto y Rector.	**Fecha Inicio**
				11/06/2025
				Fecha Final

Tabla 5. *(Continuación del plan de trabajo en la etapa 3)*

ETAPA	DESCRIPCIÓN	ACTIVIDAD	PARCTICIPANTES	PERIODO ESTIMADO
3	Analizar los hallazgos de auditoría y emitir un dictamen sobre el nivel de conformidad con la norma ISO/IEC 27001	Clasificar y analizar los hallazgos obtenidos durante la auditoría interna.	Estudiantes investigadoras bajo revisión del director del proyecto.	**Fecha Inicio**
				04/09/2025
				Fecha Final
				12/09/2025
		Evaluar el nivel de cumplimiento frente a los requisitos de ISO/IEC 27001	Estudiantes investigadoras y director del proyecto.	**Fecha Inicio**
				19/09/2025
				Fecha Final
				26/09/2025
		Emitir un dictamen técnico con los resultados, resaltando conclusiones y recomendaciones	Estudiantes investigadoras y director del proyecto.	**Fecha Inicio**
				Fecha Final
				07/11/2025

Elaborado por: Los autores.

4.1.4.4 Diseño de los instrumentos aplicados a la auditoria.

Para llevar a cabo la auditoría interna, como parte del desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI), se diseñaron y aplicaron diversos instrumentos de recolección de información, todos orientados a identificar el estado actual de los activos informáticos y las prácticas asociadas a su gestión en la institución educativa.

En este proceso se emplearon tres técnicas principales: entrevistas, listas de chequeo y observación directa, cuyo propósito común fue recopilar información sobre la gestión de los activos informáticos y las medidas de seguridad implementadas.

En cuanto a las entrevistas, se aplicaron tres a los docentes encargados del área de informática, tanto de primaria como de secundaria, así como al rector, por ser el principal representante de la institución. Estas se estructuraron en torno a tres ejes fundamentales: medidas de seguridad, conocimiento de los activos y gestión de riesgos, aplicando las mismas preguntas a cada participante con el fin de obtener una visión unificada sobre el estado actual del colegio en materia de seguridad de la información.

Por otra parte, las listas de chequeo se elaboraron tomando como referencia los controles de la norma ISO/IEC 27001, con el propósito de validar el cumplimiento de buenas prácticas en la protección de activos y la gestión de riesgos. Finalmente, mediante la observación directa, se evaluaron de manera física las condiciones de seguridad, acceso, almacenamiento y uso de los recursos tecnológicos en espacios clave como la sala de sistemas y las oficinas administrativas.

En total, participaron dos docentes de informática y el rector, lo que permitió contar con una muestra representativa de quienes tienen acceso directo y frecuente a los activos informáticos de la institución. La aplicación de entrevistas, listas de chequeo y observación directa posibilitó analizar e interpretar los resultados para obtener un diagnóstico claro sobre la gestión de los activos y las prácticas de seguridad de la información, diagnóstico que sirvió como base para el diseño del sistema de gestión

propuesto. Las entrevistas y sus respuestas se anexan al final del documento (Anexos A, B, C y D).

4.1.4.5 Análisis de los resultados

Luego de organizar las respuestas y la información obtenida mediante la aplicación de los instrumentos (entrevistas, listas de chequeo y observación directa) a los autores consultados (Anexos A, B, C y D), se procedió a realizar el respectivo análisis con el fin de establecer conclusiones e identificar los hallazgos más relevantes relacionados con la gestión de los activos informáticos en la institución.

En cuanto a la identificación de activos, se evidenció que los autores reconocen los dispositivos, servicios e información que manejan, así como la importancia que estos representan para el cumplimiento de los procesos institucionales. No obstante, se identificó un desconocimiento generalizado sobre los riesgos a los que están expuestos dichos activos, así como sobre las salvaguardas o controles necesarios para su adecuada protección.

Adicionalmente, se observó una carencia de buenas prácticas en materia de seguridad de la información, derivada principalmente de la falta de capacitaciones o lineamientos institucionales que orienten al personal en esta temática. Esta situación ha generado un entorno vulnerable, donde los activos se encuentran expuestos, y en algunos casos, los propios actores manifestaron que ya han ocurrido incidentes en los que se ha perdido información relevante.

4.1.4.6 Dictamen.

Aguachica, [26 Mayo 2025]

Señor Rector: Fernando Marín Ariza
Centro Educativo Norean

Con el objetivo de evaluar las prácticas relacionadas con la seguridad de la información en el Centro Educativo Norean se llevó a cabo un proceso de auditoría que incluyó entrevistas, observación directa y listas de chequeo aplicadas al personal docente y directivo. De esta manera la evaluación permitió identificar deficiencias, riesgos y oportunidades de mejora en la gestión de los activos informáticos y la protección de la información.

En cuanto a los hallazgos, se observó que el personal tiene un conocimiento limitado sobre las políticas internas de seguridad, además de la falta de lineamientos formales para el manejo adecuado de información confidencial. Asimismo los docentes admiten que manejan datos sensibles como calificaciones, asistencia y datos personales de los estudiantes, pero se limitan a prácticas básicas como el uso de contraseñas, sin implementar mecanismos adicionales como cifrado o controles de acceso más robustos.

Por otro lado, los activos como computadoras, video beam y televisores digitales están parcialmente organizados, sin embargo no hay un sistema formal de inventario ni protocolos claros para su uso o mantenimiento. De igual forma los respaldos de información se realizan de manera individual, esporádica y sin procedimientos definidos, lo que representa un riesgo significativo para la continuidad operativa. Además, se identificó una fuerte dependencia de plataformas externas como Google Drive, sin claridad sobre sus estándares de protección, lo que, sumado a una conectividad inestable, aumenta la vulnerabilidad de la información almacenada.

Como consecuencia, se presentan riesgos frecuentes como la eliminación accidental de archivos, el uso de equipos obsoletos sin planes de renovación, el almacenamiento de

información en dispositivos personales no protegidos, y la exposición constante a amenazas informáticas por falta de antivirus actualizado o mantenimiento oportuno.

Ante este panorama, se concluye que la institución requiere con urgencia la implementación de un sistema de gestión de seguridad de la información que permita establecer políticas claras, procedimientos definidos y medidas técnicas para proteger la integridad, disponibilidad y confidencialidad de la información. Igualmente, es necesario fortalecer la infraestructura tecnológica, capacitar al personal en buenas prácticas de seguridad, establecer controles efectivos y garantizar la estabilidad de la conectividad, con el fin de construir un entorno informático seguro y funcional para toda la comunidad educativa.

4.2 Análisis de la Gestión de Riesgos

Una vez obtenidos los resultados de la auditoría interna y siguiendo el método establecido, se inicia la fase Planear dentro del ciclo PHVA, donde se realiza el análisis de riesgos mediante la identificación y evaluación de vulnerabilidades y amenazas en los activos de información. Para cumplir con este proceso, se tomó como referencia la metodología Margerit V 3.0, la cual se ha consolidado como una de las principales herramientas para evaluar los riesgos que afectan la integridad, disponibilidad y confidencialidad de la información, según el artículo publicado por el Ministerio de Hacienda de España en 2013.

Partiendo de este enfoque, la metodología Margerit considera tres elementos fundamentales para la gestión de riesgos: activos, amenazas y salvaguardas. A partir de estos componentes, es posible estimar tanto el impacto como el riesgo, lo que permite obtener resultados y conclusiones fundamentadas que alimentarán la fase de tratamiento.
De manera estructurada, Margerit plantea el análisis en los siguientes pasos:

- Determinar los activos relevantes para la organización, su interrelación y su valor, entendiendo este último como el perjuicio o coste que implicaría su degradación
- Identificar las amenazas a las que están expuestos dichos activos
- Analizar las salvaguardas existentes y evaluar su eficacia frente a los riesgos
- Estimar el impacto, definido como el daño ocasionado al activo ante la materialización de una amenaza
- Estimar el riesgo, entendido como el impacto ponderado por la probabilidad de ocurrencia de la amenaza

Esta metodología garantiza un análisis estructurado de los riesgos y facilita la toma de decisiones para la implementación del Sistema de Gestión de Seguridad de la Información alineado con la norma ISO 27001.

4.2.1 Paso 1: Identificación de activos

Podemos definir un activo de información como cualquier elemento que posee valor para la entidad educativa y que requiera información. Siguiendo el formato de la metodología Magerit v 3.0 publicado por el Libro I- Método, se establece como activos relevantes los siguientes:

- **Información y datos:** Datos que materializan la información manejada en el sistema.
- **Servicios**: Funcionalidades esenciales que el sistema presta a la organización.
- **Aplicaciones informáticas (software):** Programas que permiten gestionar la información y automatizar procesos.
- **Equipos informáticos (hardware):** Dispositivos que alojan y procesan datos, aplicaciones y servicios.
- **Instalaciones**: Espacios que albergan equipos informáticos y de comunicación.
- **Recursos administrativos:** Procesos y normativas que garantizan la operatividad del sistema.

- **Recursos humanos:** Personas encargadas de operar y gestionar los sistemas de información.

Según lo acordado en conjunto con los directivos del centro educativo, se determinó que la recolección de información se llevaría a cabo a través de visitas a las instalaciones y entrevistas con los encargados de los procesos, con el propósito de identificar y registrar los activos existentes.

En el proceso de caracterización de los activos de información, se consideró fundamental la colaboración del coordinador, administrativos y profesores, quienes identificaron, valoraron y suministraron información sobre los activos presentes en el centro educativo Norean.

A continuación, en la página siguiente se presenta la **Tabla 6**, la cual incluye la identificación de los activos de información propuestos por MAGERIT.

Nota: La Tabla 6 está conformada por un identificador que funciona como código para representar la categoría del activo, acompañado de una descripción que detalla los elementos incluidos en cada categoría.

Tabla 6 Categoría de activos de información

IDENTIFICADOR	CATEGORIA	DESCRIPCCIÓN
INF	Datos	Contenidos académicos, registros estudiantiles y administrativos.
SW	Software	Sistemas de gestión escolar, plataformas de aprendizaje y bases de datos.
HW	Hardware	Computadores, servidores y dispositivos electrónicos utilizados en la enseñanza.
SVC	Servicios	Funciones operativas y de soporte para la infraestructura tecnológica.
INT	Instalaciones	Espacios físicos que albergan equipos informáticos y redes de comunicación.
RA	Recursos Administrativos	Documentación, normativas y procesos institucionales relacionados con TI.
RH	Recursos Humanos	Personal encargado de operar, administrar y mantener los sistemas tecnológicos.

Fuente: Margerit V 3.0

Nota: En la *Tabla 7* se presenta el inventario de activos de información identificados en el centro educativo Norean.

Tabla 7 Inventario de Activos de Datos/ Información

CATEGORIA	ID	ACTIVO	DESCRIPCIÓN	RESPONSABLE
Datos	INF-01	Registros académicos de estudiantes	Contiene información personal, académica y disciplinaria de los estudiantes.	Coordinación Académica
Datos	INF-02	Informes de docentes	Resúmenes por periodo sobre ejecución de clases y seguimiento pedagógico	Docentes/ Coordinadores
Datos	INF-03	Planes de asignatura	Estructura de contenidos, estrategias y evaluaciones por área	Docentes
Datos	INF-04	Historial de reportes académicos	Boletines, promedios y resultados finales de todos los años	Coordinación Académica
Datos	INF-05	Informes de desempeño docente	Evaluaciones internas, retroalimentación institucional	Rectoría
Datos	INF-06	Base de datos de matrícula	Datos personales y académicos de estudiantes actuales y egresados	Rectoría

En la página siguiente se le da continuidad a la Tabla 6.

Tabla 6. (Continuación)

Inventario de Activos de Datos e información.

CATEGORIA	ID	ACTIVO	DESCRIPCIÓN	RESPONSABLE
Datos	INF-07	Documentos institucionales	Registros de seguimiento y observación del desempeño académico y comportamental de los estudiantes.	Rectoría
Datos	INF-08	Planeaciones y guías de clase	Programación semanal o mensual de actividades pedagógicas	Docentes
Datos	INF-09	Información compartida en Drive institucional	Documentos pedagógicos, planes, informes y recursos subidos a la nube.	Docentes y Coordinación académica
Datos	INF-10	Correos electrónicos institucionales	Envío/recepción de datos académicos, administrativos.	Docentes y Coordinación académica

Elaborado por: Los autores

Tabla 8 Inventario de Activos de Software

CATEGORIA	ID	ACTIVO	FUNCIÓN PRINCIPAL	LICENCIA
Software	SW-01	Plataforma académica WEBCOLEGIOS	Sistema para la gestión académica	Alquiler / SaaS
Software	SW-02	Google Drive	Almacenar, compartir y respaldar documentos institucionales en la nube.	Gratuita
Software	SW-03	Microsoft Office	Elaborar informes, planeaciones, evaluaciones y documentos	No licenciada
Software	SW-04	Sistema Operativo (Windows)	Soporte operativo	Libre
Software	SW-05	Herramientas de videoconferencia	Clases virtuales, reuniones institucionales	Comercial
Software	SW-06	Navegador web	Acceso a contenido educativo en línea	Gratuito
Software	SW-07	SIMAT	Plataforma del MEN para la gestión de matrícula oficial a nivel nacional.	Estatal (Uso autorizado)
Software	SW-08	CloudLabs	Ejecutar simulaciones y prácticas en línea de ciencias y tecnología	Gratuita / limitada

Tabla 8. (Continuación)

Inventario de Activos de Software.

CATEGORIA	ID	ACTIVO	FUNCIÓN PRINCIPAL	LICENCIA
Software	SW-09	Aplicaciones descargadas	Apoyar clases o actividades escolares según cada docente	Gratuita / no oficial
Software	SW-10	Sistema de evaluación	Registrar y calcular calificaciones académicas de los estudiantes	No licenciada

Elaborado por: Los autores

Nota: En la Tabla 9 se presenta el inventario de activos de Hardware identificados en el centro educativo Norean.

Tabla 9 Inventario de Activos de Hardware

CATEGORIA	ID	ACTIVO	CANTIDAD	DEPENDENCIA	OBSERVACÍON
Hardware	HW-01	Computadores portátil (HP)	19	Sala de Informática	Para uso estudiantil en clases de informática
Hardware	HW-02	Router	2	Sala de informática	Conectividad de red para los equipos

Tabla 9. (Continuación)

Inventario de Activos de Hardware.

CATEGORIA	ID	ACTIVO	CANTIDAD	DEPENDENCIA	OBSERVACÍON
Hardware	HW-03	Computadores portátiles	3	Rectoría	Uso administrativo y directivo
Hardware	HW-04	UPS	1	Sala de Informática	Sistema de respaldo eléctrico para protección de equipos de red y cómputo
Hardware	HW-05	USB docentes	8	Docentes	Uso masivo sin control
Hardware	HW-06	Televisor institucional	1	Sala de prescolar	No se usa frecuentemente
Hardware	HW-07	Impresora compartida	1	Rectoría	Uso libre, sin control de impresión
Hardware	HW-08	Videobeam	1	Rectoría	Apoyo audiovisual
Hardware	HW-9	Discos duros externos	2	Rectoría	Sin cifrado, respaldo manual

Elaborado por : Los autores.

Nota: En la Tabla 10 se presenta el inventario de activos de servicios identificados en el centro educativo Norean.

Tabla 10 Inventario de Activos de Servicios

CATEGORIA	ID	ACTIVO	DESCRIPCÍON	ACTIVO RELACIONADO
Servicios	SV-01	Plataforma académica	Servicio contratado para registrar notas, boletines, seguimiento estudiantil	Software académico / información estudiantil
Servicios	SV-02	Servicio de correo institucional	Medio de comunicación entre docentes y administración	Información académica y administrativa
Servicios	SV-03	Capacitación docente	Formación limitada en tecnología y SGSI	Docentes RH-03
Servicios	SV-04	Soporte entre docentes	Ayuda mutua para resolver problemas tecnológicos	Equipos en aula
Servicios	SV-05	Recursos educativos online	Contenido educativo desde plataformas públicas	Navegador SW-05

Tabla 10. (Continuación)

Inventario de Activos de Servicio.

CATEGORIA	ID	ACTIVO	DESCRIPCÍON	ACTIVO RELACIONADO
Servicios	SV-06	Mantenimiento técnico	Reparaciones ocasionales sin contrato	Computadores HW-01, HW-08
Servicios	SV-07	Gestión documental externa	Sin sistema oficial para organizar archivos	SW-01, ADM-03, ADM-04
Servicios	SV-08	CloudLabs	Plataforma educativa externa	SW-04

Elaborado por: Los autores

Nota: En la siguiente Tabla se presenta el inventario de activos de Instalaciones identificados en el centro educativo Norean.

Tabla 11 Inventario de Activos de Instalaciones

CATEGORIA	ID	ACTIVO	ACHIVOS PROTEGIDOS	DESCRIPCION
Instalaciones	INT-01	Sala de informática	Equipos informáticos, red, UPS	Espacio dotado con computadores para prácticas tecnológicas

Tabla 11. (Continuación)

Inventario de Activos de Instalaciones.

Instalaciones	INT-02	Oficina de Rectoría	Computadores, documentos institucionales	Oficina donde se manejan documentos administrativos
Instalaciones	INT-03	Laboratorio de informática	Equipos informáticos, red, UPS	Espacio dotado con computadores para prácticas tecnológicas.
Instalaciones	INT-04	Salón de clase	No	Sin protección de material proyectado
Instalaciones	INT-05	Biblioteca	No	Documentación física sin inventario digital
Instalaciones	INT-06	Cafetería escolar	No aplica	No se almacenan documentos
Instalaciones	INT-07	Zona de cámaras de seguridad	No	Cámaras instaladas sin monitoreo ni respaldo digital

Elaborado por los autores.

Nota: En la Tabla 12 se presenta el inventario de activos de Recursos Administrativos identificados en el centro educativo Norean.

Tabla 12 Inventario de Activos de Recursos Administrativos

CATEGORIA	ID	ACTIVO	USUARIO	DESCRIPCION
Recursos Administrativos	RA-01	Archivador metálico	Rector	Mueble de almacenamiento de documentos físicos.
Recursos Administrativos	RA-02	Portátil	Rector	Equipos utilizado para gestionar planeaciones, reportes y documentación interna.
Recursos Administrativos	RA-03	Cronograma académico	Rector	Calendario institucional que detalla fechas clave de evaluaciones y reuniones.
Recursos Administrativos	RA-04	Formato de asistencia	Rector	Documento utilizado para registrar asistencia del personal docente y directivo.
Recursos Administrativos	RA-05	Contratos y convenios	Rectoría	Documentos legales sin respaldo digital
Recursos Administrativos	RA-06	Registro de inventario	Rectoría	Anotado manualmente, sin respaldo
Recursos Administrativos	RA-07	Plan de mejoramiento	Rectoría	Documento en papel, sin control de cumplimiento
Recursos Administrativos	RA-08	Presupuesto	Rectoría	Archivo Excel editable sin control

Elaborado por . Los autores.

Nota: En la página siguiente se encuentra la Tabla 13 que presenta el inventario de activos de Recursos Humanos identificados en el centro educativo Norean.

Tabla 13 Inventario de Activos de Recursos Humanos

CATEGORIA	ID	ACTIVO	DESCRIPCIÓN	ROL
Recursos Humanos	RH-01	Rector	Directivo encargado de la gestión general del colegio	Dirección y toma de decisiones
Recursos Humanos	RH-02	Docente de Informática /Bachillerato	Impartición de clases relacionadas con tecnología	Formación tecnológica
Recursos Humanos	RH-03	Docente de Informática /Primaria	Generación y uso de información académica y planes de clase	Apoyo académico en ciencias
Recursos Humanos	RH-04	Docentes	Gestiona bienestar y casos disciplinarios	Bienestar estudiantil
Recursos Humanos	RH-05	Rector	Maneja archivos, certificados y matrículas	Personal administrativo
Recursos Humanos	RH-06	Estudiantes	Generan y manipulan información sin formación SGSI	Usuarios finales
Recursos Humanos	RH-07	Servicios generales	Limpieza, apoyo logístico y mantenimiento	Operativo

Elaborado por: Los autores.

4.2.1 Paso 2: Valoración de activos

Una vez identificados los activos del Centro Educativo Norean, se procede a realizar su valoración aplicando la metodología MAGERIT versión 3 (Libro 1, Método).

Esta metodología establece que el valor de un activo no depende de su costo económico o de su estado físico, sino del perjuicio que ocasionaría su pérdida o afectación. El propósito de esta valoración es determinar la necesidad de protección de cada activo, entendiendo que su valor está en la información que maneja y en los servicios que presta a los demás elementos del sistema.

El valor de un activo se mide en función del impacto que tendría su afectación en los procesos de la institución. En este sentido, los activos con mayor dependencia o repercusión en otros servicios adquieren un valor superior, pues su pérdida podría interrumpir actividades esenciales o exponer información sensible.

De acuerdo con MAGERIT v3, para determinar el valor de un activo se deben analizar varias dimensiones de seguridad, que permiten identificar los posibles perjuicios derivados de incidentes:

- **Confidencialidad:** perjuicio causado por la revelación no autorizada de información.

- **Integridad**: perjuicio por modificación, corrupción o destrucción no autorizada de datos o servicios.

- **Disponibilidad:** perjuicio por la falta de acceso o utilización del activo cuando se requiere.

Una vez determinadas las dimensiones de seguridad, se estima el impacto que tendría su pérdida o afectación, considerando factores como el coste de reposición, lucro

cesante, pérdida de operatividad, sanciones legales o daños colaterales (a personas, otros activos o el entorno).

Para esta valoración se adopta una escala cualitativa ordinal de 1 a 5 (*Tabla 14*), que permite asignar valores de impacto de forma objetiva y establecer la criticidad de los activos, sirviendo como base para definir las salvaguardas y medidas de protección adecuadas.

Tabla 14 Criterios de valoración de los activos

Valor	Descripción del impacto
1 – Muy Bajo	El impacto es irrelevante; la afectación no genera consecuencias sobre los procesos ni sobre otros activos.
2 – Bajo	La afectación genera una perturbación menor, recuperable sin pérdida significativa de información ni de servicio.
3 – Medio	El incidente afecta el funcionamiento normal y requiere acciones correctivas, aunque no compromete la operación total.
4 – Alto	La afectación interrumpe servicios críticos o causa pérdida significativa de datos o reputación institucional.
5 – Muy Alto	La pérdida del activo implica la paralización de servicios esenciales, violación grave de la confidencialidad o sanciones legales.

Elaborado por: Los autores basado en Margerit V3.0

Nota: En la siguiente Tabla (*Tabla 15*) se muestra la valoración de los activos en función de su nivel de criticidad, el cual se determina a partir de tres dimensiones clave: confidencialidad, integridad y disponibilidad.

Tabla 15 Valoración de los activos según el nivel de criticidad

		DIMENSIONES			
TIPO	**ACTIVO**	**CONFI**	**INTEGR**	**DISPON**	**CRITICIDAD**
INF	Registros académicos de estudiantes / Base de datos de matrícula	5	5	5	5 – Muy Alta
INF	Informes de docentes / Informes de desempeño docente	4	5	4	5 – Muy Alta
INF	Historial de reportes académicos / Documentos institucionales	4	5	4	5 – Muy Alta
INF	Información compartida en Drive institucional / Correos electrónicos institucionales	4	4	4	5 – Muy Alta
SW	Plataforma WEBCOLEGIOS	5	5	5	5 – Muy Alta
SW	Google Drive institucional	4	5	5	5 – Muy Alta
SW	Microsoft Office / Sistema operativo	3	4	4	4 – Alta

Tabla 16. (Continuación)

Valoración de los activos según el nivel de criticidad.

TIPO	ACTIVO	CONFI	INTEGR	DISPON	CRITICIDAD
SW	CloudLabs / SIMAT	4	4	5	5 – Muy Alta
HW	Computadores portátiles / Sala de informática	4	4	5	5 – Muy Alta
HW	Router / Infraestructura de red	3	4	5	5 – Muy Alta
HW	UPS / Discos duros externos	3	4	5	5 – Muy Alta
SV	Correo institucional	4	4	5	5 – Muy Alta
SV	Soporte técnico / Mantenimiento	3	4	5	5 – Muy Alta
SV	Gestión documental externa	5	5	4	5 – Muy Alta
INT	Sala de informática	3	4	5	5 – Muy Alta
INT	Oficina de Rectoría / Secretaría	5	5	4	5 – Muy Alta
INT	Laboratorio de informática	3	4	5	5 – Muy Alta

Tabla 16. (Continuación)

Valoración de los activos según su nivel de criticidad.

TIPO	ACTIVO	CONFI	INTEGR	DISPON	CRITICIDAD
RA	Contratos y convenios	5	5	4	5 – Muy Alta
RA	Presupuesto / Registros financieros	5	5	4	5 – Muy Alta
RA	Archivadores institucionales	3	4	4	4 – Alta
RH	Rector y equipo directivo	5	5	4	5 – Muy Alta
RH	Docentes	4	5	4	5 – Muy Alta
RH	Estudiantes	4	4	4	5 – Muy Alta

Elaborado por los autores

El análisis evidenció que la mayoría de los activos poseen una criticidad muy alta, especialmente aquellos relacionados con la gestión académica, bases de datos institucionales, plataformas digitales y equipos de infraestructura. Esta condición refleja una alta dependencia tecnológica y la necesidad de fortalecer los controles de acceso, copias de seguridad y medidas de protección física y lógica. En consecuencia, se requiere una gestión integral de activos que asegure su confidencialidad, integridad y disponibilidad conforme a los principios de la norma ISO 27001.

4.3 ENFOQUE NORMATIVO PARA LA GESTÍON DE RIESGOS

La metodología aplicada para el análisis de riesgos se basa en los principios establecidos por las normas ISO/IEC 27001 e ISO 31000, las cuales orientan el proceso hacia la identificación, evaluación, tratamiento y seguimiento de los riesgos que afectan la seguridad de la información. Estas directrices permiten definir niveles aceptables de riesgo, de acuerdo con las necesidades y el entorno particular de la institución.

Esta articulación normativa se representa en la (Ilustración 3), donde se ilustra cómo interactúan los elementos que componen el sistema de gestión de seguridad de la información.

La integración de estas normas fortalece el enfoque adoptado en este proyecto, asegurando que el análisis y manejo de riesgos se realicen de manera metódica, conforme a estándares internacionales y adaptada a la realidad del centro educativo.

El proceso incluye las siguientes etapas clave:

- Detección de amenazas potenciales.
- Reconocimiento de vulnerabilidades existentes.
- Identificación y caracterización de los riesgos.
- Cálculo de la probabilidad de ocurrencia.
- Evaluación del impacto sobre los activos de información.

4.3.1 Identificación de las amenazas y vulnerabilidades.

Para esta fase, se realizó una evaluación de las amenazas y vulnerabilidades que podrían afectar los activos de información de la institución. Para identificar las amenazas, se consideró su clasificación según el origen, contemplando las siguientes categorías:

- Naturales, como terremotos o inundaciones.
- Ambientales o industriales, como fallas eléctricas o contaminación.
- Técnicas, derivadas de errores en el diseño o implementación de software o hardware.
- Humanas accidentales, causadas por descuidos u omisiones.
- Deliberadas, con la intención de dañar o acceder de forma indebida a los sistemas.

En cuanto a las vulnerabilidades, se identificaron como debilidades que podrían ser aprovechadas por dichas amenazas. De esta manera, estas pueden encontrarse tanto en los procesos tecnológicos como en los procedimientos operados por el personal.

Una vez finalizada la identificación, los resultados se organizaron y se presentan la Tabla 16, lo cual permite continuar con el análisis del riesgo.

Tabla 16 Identificación de Amenazas y vulnerabilidades

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
INF-01	Registros académicos de estudiantes	✓ Contraseñas débiles ✓ Archivos sin cifrado ✓ Acceso sin control	✓ Acceso no autorizado ✓ Pérdida o robo de información ✓ Modificación de calificaciones

Tabla 16. (Continuación)

Identificación de Amenazas y vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
INF-02	Informes de docentes	✓ Almacenamiento en equipos personales ✓ Sin control de versiones ✓ Falta de respaldo	✓ Divulgación no autorizada ✓ Pérdida de documentos ✓ Alteración de contenidos
INF-03	Planes de asignatura	✓ Documentos editables sin restricción. ✓ Copias desactualizadas	✓ Confusión en clases ✓ Uso indebido por terceros
INF-04	Historial de reportes académicos	✓ Documentos almacenados sin cifrado ✓ Falta de respaldo periódico	✓ Alteración de históricos ✓ Acceso no autorizado
INF-05	Informes de desempeño docente	✓ Almacenamiento en carpetas compartidas ✓ Permisos abiertos	✓ Fuga de información confidencial ✓ Uso para acoso o presión
INF-06	Base de datos de matrícula	✓ Permisos mal configurados Sin copias de seguridad cifradas	✓ Ransomware Suplantación de identidad Acceso por personal no autorizado
INF-07	Documentos institucionales	✓ Almacenados solo en papel ✓ Sin respaldo digital	✓ Daños físicos (fuego, humedad) ✓ Pérdida o robo

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
INF-08	Planeaciones y guías de clase	✓ No hay control de cambios Sin trazabilidad	✓ Uso indebido Alteración del material
INF-09	Información en Drive institucional	✓ Enlaces compartidos sin restricción ✓ Falta de políticas de uso	✓ Fuga de datos ✓ Eliminación por error ✓ Acceso externo
INF-10	Correos electrónicos institucionales	✓ Sin verificación en dos pasos Contraseñas simples ✓ Uso desde dispositivos no seguros	✓ Phishing ✓ Suplantación de identidad ✓ Acceso a datos personales o confidenciales
SW-05	Videoconferencia (Zoom, Meet)	✓ Enlaces públicos ✓ Sin autenticación ✓ Uso en dispositivos personales	✓ Ingreso no autorizado ✓ Escucha o grabación maliciosa
SW-06	Navegador web	✓ Sin filtros de contenido ✓ Descargas automáticas habilitadas	✓ Ingreso a sitios maliciosos ✓ Descarga de malware
SW-07	SIMAT	✓ Claves débiles ✓ Uso compartido de usuario	✓ Acceso indebido a información confidencial ✓ Falsificación de datos

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
SW-08	CloudLabs	✓ Depende completamente del internet ✓ Almacenamiento externo	✓ Pérdida de progreso académico ✓ Interrupción de actividades
SW-09	Aplicaciones descargadas	✓ No oficiales ✓ Instaladas sin control ni validación	✓ Malware ✓ Pérdida de datos ✓ Inestabilidad del sistema
SW-10	Sistema de evaluación	✓ Sin cifrado ✓ No hay trazabilidad de cambios	✓ Alteración de notas ✓ Eliminación de evaluaciones
HW-01	Computador portátil (HP)	✓ Sin contraseña ✓ Datos sin cifrado ✓ Sin antivirus	✓ Robo físico ✓ Pérdida total de datos
HW-02	Router	✓ Contraseña débil ✓ Sin actualización de firmware	✓ Intervención de red ✓ Robo de datos en tránsito
HW-03	Computadores portátiles	✓ Obsoletos ✓ Lentos ✓ Software desactualizado	✓ Caídas del sistema ✓ Exposición a malware

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
HW-04	UPS	✓ Sin mantenimiento ✓ Baterías descargadas	✓ Apagones que causen pérdida de datos o daños en equipos
HW-05	USB docentes	✓ Sin cifrado ✓ Virus portables ✓ Uso compartido	✓ Propagación de malware ✓ Pérdida de información
HW-06	Televisor institucional	✓ Exposición pública ✓ Sin protección física	✓ Daños por manipulación ✓ Uso indebido
HW-07	Impresora compartida	✓ Sin restricciones de impresión ✓ No requiere autenticación	✓ Fugas de información ✓ impresa
HW-08	Videobeam	✓ Desprotección física ✓ Uso sin registro	✓ Robo Daños por mal uso
HW-09	Discos duros externos	✓ Sin cifrado ✓ Portabilidad sin control	✓ Robo ✓ Exposición de ✓ datos personales
SE-01	Plataforma académica	✓ No tiene respaldo local ✓ Depende 100% de internet	✓ Caída del servicio ✓ Fuga de datos académicos

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
SE-02	Correo institucional	✓ Sin autenticación 2FA ✓ Claves débiles ✓ Uso personal	✓ Phishing ✓ Suplantación ✓ Acceso a información sensible
SE-03	Capacitación docente	✓ No se realiza periódicamente ✓ No hay seguimiento	✓ Desconocimiento de riesgos digitales ✓ Uso indebido de TIC
SE-04	Soporte entre docentes	✓ No formalizado ✓ No hay registro de incidentes	✓ Soluciones incorrectas ✓ Daños a equipos o datos
SE-05	Recursos educativos online	✓ Sin validación de sitios ✓ Sin restricciones en navegadores	✓ Acceso a contenido malicioso ✓ Descarga de virus
SE-06	Mantenimiento técnico	✓ No hay contrato ✓ No se documentan intervenciones	✓ Fallas constantes ✓ Pérdida de información
SE-07	Gestión documental externa	✓ No hay control de versiones ✓ No está cifrada	✓ Modificación o pérdida de archivos oficiales
SE-08	CloudLabs	✓ Uso depende de internet ✓ No hay guía institucional	✓ Interrupción de clases ✓ Pérdida de progreso académico

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
INS-06	Cafetería escolar	✓ No aplica a activos de información	✓ Riesgo físico general, no afecta SGSI
INS-07	Zona de cámaras de seguridad	✓ Sin respaldo de grabaciones ✓ Monitoreo limitado	✓ No registro en caso de incidente ✓ Manipulación de dispositivos
INS-08	Bodega institucional	✓ Acceso sin control ✓ Equipos abandonados sin inventario	✓ Reutilización insegura ✓ Pérdida de activos tecnológicos
INS-09	Espacios comunes	✓ Sin control de uso de TIC portátiles ✓ Equipos sin supervisión	✓ Robo ✓ Daño físico de herramientas escolares
ADM-01	Archivador metálico	✓ Sin llave o con acceso abierto ✓ Documentos físicos sin respaldo digital	✓ Pérdida por extravío o daño ✓ Fuga de información
ADM-02	Portátil	✓ Sin antivirus ✓ Almacenamiento sin cifrado ✓ Uso personal e institucional	✓ Robo ✓ Acceso no autorizado ✓ Pérdida total de archivos

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
ADM-03	Cronograma académico	✓ Editable por cualquier usuario ✓ Sin control de versiones	Confusión de actividades Alteración no autorizada
ADM-04	Formato de asistencia	✓ Firmas manuales, sin trazabilidad digital	✓ Suplantación de firmas ✓ Pérdida o falsificación
ADM-05	Contratos y convenios	✓ Solo versión física ✓ Sin respaldo cifrado	✓ Pérdida o daño irreparable ✓ Divulgación indebida
ADM-06	Registro de inventario	✓ Anotaciones manuales ✓ Sin sistema de control digital	✓ Omisiones involuntarias Manipulación intencional
ADM-07	Plan de mejoramiento	✓ Cambios sin registro de aprobación No se guarda cronológicamente	✓ Modificación maliciosa ✓ Pérdida de trazabilidad institucional
ADM-08	Presupuesto	✓ Archivos sin contraseña ✓ Editable libremente	✓ Alteración de cifras ✓ Uso indebido de recursos

Tabla 16. (Continuación)

Identificación de Amenazas y Vulnerabilidades.

ID	ACTIVO	VULNERABILIDADES	AMENAZAS
RH-01	Rector	✓ No tiene respaldo cifrado ✓ Accede a todos los sistemas	✓ Suplantación Pérdida de decisiones institucionales
RH-02	Docente de Informática Bachillerato	✓ Maneja TIC sin protocolo SGSI ✓ Usa software no oficial	✓ Infección por malware ✓ Fugas de datos académicos
RH-04	Docentes	✓ Almacenamiento en USB sin cifrado Uso personal de Drive	✓ Pérdida o filtración de planeaciones y notas
RH-05	Estudiantes	✓ Sin formación en ciberseguridad ✓ Acceden sin supervisión	✓ Acceso a contenido malicioso ✓ Robo de cuentas o suplantación
RH-06	Servicios generales	✓ Acceso físico a oficinas y aulas ✓ Sin capacitación básica en SGSI	✓ Pérdida accidental de documentos ✓ Ingreso no autorizado a salas

Elaborado por: Los autores

4.3.2 Valoración de amenazas.

Una vez identificados los activos de información y sus respectivas amenazas, se procede a valorar el nivel de impacto que podría generar cada amenaza sobre las dimensiones fundamentales de seguridad: confidencialidad, integridad y disponibilidad (CID). Esta valoración se expresa en porcentajes que reflejan el grado de afectación estimado que tendría la amenaza sobre cada una de estas dimensiones.

Esta metodología se fundamenta en los lineamientos propuestos por la Metodología MAGERIT (Ministerio de Hacienda y Administraciones Públicas, 2012), la cual proporciona una estructura estandarizada para la estimación de riesgos en sistemas de información. Esta valoración permite establecer el grado de severidad de las amenazas identificadas sobre los activos críticos del Centro Educativo Norean de Aguachica, como insumo para la posterior evaluación del riesgo.

Posteriormente, para determinar el nivel de impacto de cada amenaza se realiza el cálculo del promedio de afectación, sumando los valores porcentuales asignados a cada dimensión (confidencialidad, integridad y disponibilidad) y dividiendo entre tres, de la siguiente manera:

Ecuación 1

$$Promedio = \frac{Confidencialidad(\%) + Integridad(\%) + Disponibilidad(\%)}{3}$$

Fuente: Elaborado por los autores basado en Margerit V 3.0

A continuación, la Tabla 17 presenta la clasificación utilizada para asignar los valores de impacto según el promedio de afectación, estableciendo su correspondencia con la escala definida y el nivel cualitativo asociado.

Tabla 17 Escala de clasificación del impacto

Promedio de afectación(%)	Escala	Nivel cualitativo
0%	1	Nulo
1% - 25%	2	Bajo
26% - 50%	3	Medio
51% - 75%	4	Alto
76% - 100%	5	Muy alto

Elaborado por los autores basado en la metodología Margerit V 3.0.

Posteriormente, se presenta la tabla (*Tabla 18)* con la valoración de amenazas y vulnerabilidades, donde se incluyen los activos evaluados, las amenazas asociadas, los porcentajes de afectación por dimensión (confidencialidad, integridad y disponibilidad), el promedio obtenido, y su correspondiente nivel cualitativo de impacto. Esta información es el punto de partida para realizar la matriz de riesgo.

Tabla 18 Valoración de amenazas y vulnerabilidades sobre activos de información

CATEGORÍA DE AMENAZA	AMENAZAS INCLUIDAS	C	I	D	NIVEL	ACTIVOS AFECTADOS
Acceso no autorizado	Acceso indebido, acceso externo, cuentas sin control, acceso sin roles definidos	100%	100%	50%	Alto / Muy Alto	Bases de datos, plataformas, documentos, correos
Eliminación o pérdida de información	Eliminación accidental, pérdida de archivos, sin respaldo, daño físico	50%	100%	100%	Alto	Documentos, Drive, hardware
Manipulación o alteración	Edición sin autorización, cambios sin trazabilidad, falsificación de datos	25%	100%	50%	Alto	Registros, reportes, historiales
Divulgación no autorizada	Difusión sin permiso, exposición, fuga de información	100%	75%	50%	Alto	Documentos, informes, contratos
Robo de información o equipos	Robo de equipos, pérdida con información sensible	100%	60%	100%	Muy Alto	Portátiles, discos duros, Videobeam

Tabla 18. (Continuación)

Valoración de amenazas y vulnerabilidades sobre activos de información

CATEGORÍA DE AMENAZA	AMENAZAS INCLUIDAS	C	I	D	NIVEL	ACTIVOS AFECTADOS
Malware / software malicioso	Virus, spyware, macros, software no oficial	50%	100%	75%	Alto / Muy Alto	Equipos, Office, navegadores
Falta de actualizaciones / vulnerabilidades	Sistema desactualizado, vulnerabilidades sin parche	50%	100%	75%	Muy Alto	SO, routers, salas de informática
Interrupción del servicio	Caídas, fallos de conexión, suspensión	25%	50%	100%	Medio / Alto	Plataformas, CloudLabs
Configuración débil / red	Configuración débil, acceso no autorizado a la red	75%	100%	100%	Muy Alto	Router, red interna
Exposición o riesgo físico	Documentos expuestos, equipos mal ubicados	50%	75%	75%	Alto	Archivos físicos, cámaras, bodegas
Gestión documental deficiente	Archivos sin respaldo, inventarios sin registro	**75%**	**100%**	**75%**	Muy Alto	Biblioteca, contratos, archivos

Tabla 18. (Continuación)

Valoración de amenazas y vulnerabilidades sobre activos de información.

CATEGORÍA DE AMENAZA	AMENAZAS INCLUIDAS	C	I	D	NIVEL	ACTIVOS AFECTADOS
Exposición o riesgo físico	Documentos expuestos, equipos mal ubicados	**50%**	**75%**	**75%**	Alto	Archivos físicos, cámaras, bodegas
Gestión documental deficiente	Archivos sin respaldo, inventarios sin registro	**75%**	**100%**	**75%**	Muy Alto	Biblioteca, contratos, archivos
Uso inadecuado / operacional	Uso sin autenticación, dispositivos no seguros	**75%**	**75%**	**50%**	Alto	Docentes, estudiantes, administrativos
Grabación / privacidad	Grabación sin consentimiento	**100%**	**75%**	**50%**	Alto	Videoconferencias, clases

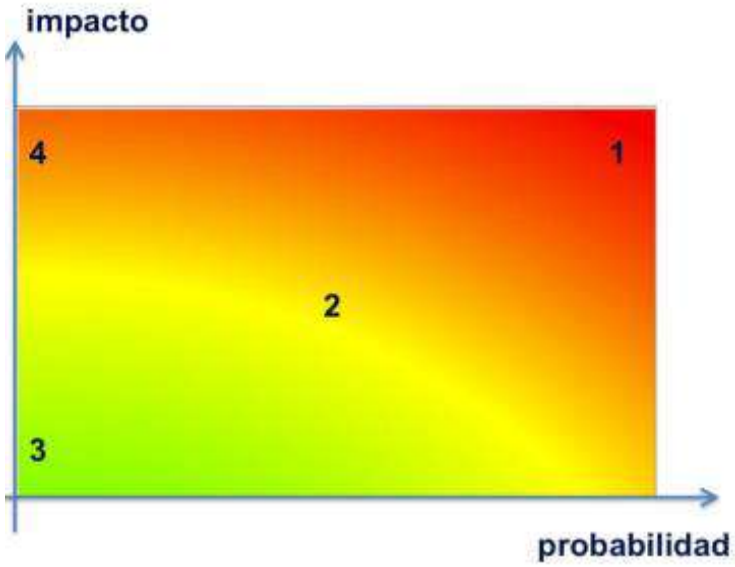
Elaborado por los autores

La valoración permitió identificar un alto nivel de exposición a riesgos, principalmente derivados del acceso indebido, ransomware, pérdida de información y errores humanos. Los activos críticos, como la base de datos de matrícula, correos institucionales y equipos portátiles, presentan impactos significativos sobre la seguridad de la información. De ello se desprende la necesidad de reforzar controles técnicos, establecer autenticación multifactor y promover la concienciación en ciberseguridad, garantizando la trazabilidad de los procesos institucionales.

4.3.3 Determinación del riesgo.

En este punto se determina el nivel de riesgo correspondiente a cada uno de los activos y amenazas previamente identificados y valorizados. Para ello se aplicó la metodología MAGERIT v3.0, la cual establece dos dimensiones fundamentales para el cálculo del riesgo:

Ilustración 7 El riesgo en función del impacto y la probabilidad



Fuente: Tomado desde Margerit V. 3.0

El impacto representa el daño que podría sufrir un activo ante la materialización de una amenaza, mientras que la probabilidad corresponde a la posibilidad de que dicha amenaza ocurra efectivamente, estimada cualitativamente según el contexto, la frecuencia de exposición, el uso del activo y las vulnerabilidades identificadas.

Ecuación 2

$$Riesgo = Impacto\ x\ Probabilidad$$

Fuente: Elaborado por los autores basado en Margerit V 3.0

Donde:

Impacto: Proviene del análisis acumulado o repercutido sobre el activo afectado.

Probabilidad : Corresponde al valor asignado según la clasificación establecida en la Tabla 19.

Tabla 19 Niveles de probabilidad

VALOR	FRECUENCIA ESTIMADA	DESCRIPCIÓN CUALITATIVA
1	Muy rara / Improbable	El evento casi nunca ocurre. No se tienen antecedentes conocidos.
2	Poco frecuente	Podría ocurrir eventualmente. Ha ocurrido de manera aislada.
3	Ocasional	Sucede cada cierto tiempo. Hay antecedentes conocidos.
4	Frecuente	Se presenta con regularidad. Suele ocurrir al menos una vez al año.
5	Muy frecuente / Casi segura	Ocurre constantemente. Se espera que ocurra varias veces al año.

Elaborado por los autores basado en MARGERIT v3

Para el tratamiento de los riesgos, se establecieron zonas basadas en la relación entre la probabilidad de ocurrencia y el impacto del evento, dado que a mayor impacto y probabilidad, mayor será el nivel de riesgo. Para este análisis se aplicó la metodología MAGERIT v3.0, la cual clasifica los niveles de riesgo mediante una escala numérica complementada con zonas de color que permiten una interpretación rápida y una adecuada priorización. La Tabla 20 presenta dicha clasificación.

Tabla 20 Clasificación de Riesgos

IMPACTO	PROBABILIDAD	VALOR DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN
Alto (4 o 5)	Muy probable (4 o 5)	16 +	Rojo	Riesgo crítico. Requiere acción inmediata.
Medio (3)	Muy probable (4 o 5)	11 a 15	Naranja	Riesgo significativo. Priorizar control.
Alto (4 o 5)	Poco probable (1 o 2)	6 a 10	Amarillo	Riesgo manejable. Controlar puntualmente.
Bajo (1 o 2)	Poco probable (1 o 2)	1 a 5	Verde	Riesgo aceptable. No requiere acción urgente.

Elaborado por los autores basado en la metodología Margerit v3

En la siguiente tabla (Tabla 21) se presentan los resultados de la evaluación del riesgo, ya clasificados. El valor de impacto corresponde a los resultados obtenidos en la valoración de amenazas, mientras que la probabilidad fue determinada con base en los antecedentes y la frecuencia con la que estos eventos se han presentado en la institución educativa, según la información recopilada a través de entrevistas.

Tabla 21 Determinación del nivel de riesgo según su impacto y probabilidad

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Registros académicos de estudiantes	Crítico		Riesgo elevado por manipulación o eliminación no autorizada.
Informes de docentes	Alto		Requiere control de acceso y respaldo regular.
Planes de asignatura	Crítico		Riesgo alto por eliminación accidental o edición no autorizada.
Historial de reportes académicos	Crítico		Riesgo de alteración o robo de información sensible.
Informes de desempeño docente	Crítico		Riesgo por fuga o modificación no autorizada de información.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad. .

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Base de datos de matrícula	Crítico		Riesgo máximo por pérdida o alteración masiva de datos.
Documentos institucionales	Alto		Vulnerables por pérdida física o acceso no controlado.
Planeaciones y guías de clase	Alto		Riesgo por eliminación o difusión indebida.
Información en Drive institucional	Alto		Amenaza por enlaces públicos sin control ni respaldo.
Correos electrónicos institucionales	Medio		Riesgo moderado de phishing o interceptación.
Plataforma académica WEBCOLEGIOS	Crítico		Riesgo alto por caída o falsificación de datos.
Google Drive	Crítico		Riesgo de eliminación accidental y accesos externos.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad.

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Microsoft Office	Medio		Posible pérdida de archivos o malware por macros.
Sistema operativo (Windows)	Alto		Riesgo por vulnerabilidades sin parches.
Videoconferencia (Zoom, Meet)	Medio		Riesgo por accesos indebidos o grabaciones no consentidas.
Navegador web	Crítico		Riesgo alto por descargas o sitios maliciosos.
SIMAT	Crítico		Riesgo crítico por acceso no autorizado a datos estudiantiles.
CloudLabs	Crítico		Riesgo por pérdida de prácticas o accesos sin roles definidos.
Aplicaciones descargadas	Medio		Riesgo por software no oficial o virus.
Computador portátil (HP)	Alto		Riesgo por robo o fallos sin respaldo.
Router	Medio		Riesgo por configuración débil o falta de actualización.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad.

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
UPS	Bajo		Riesgo aceptable por fallos eléctricos ocasionales.
USB docentes	Alto		Riesgo por pérdida o propagación de malware.
Televisor institucional	Medio		Riesgo físico por mal uso.
Impresora compartida	Bajo		Riesgo bajo por exposición de documentos.
Videobeam	Bajo		Riesgo físico por robo o mal manejo.
Discos duros externos	Crítico		Riesgo alto por pérdida o daño sin respaldo.
Plataforma académica (general)	Crítico		Riesgo de accesos indebidos o cuentas compartidas.
Correo institucional	Medio		Riesgo moderado por suplantación o links maliciosos.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad.

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Capacitación docente	Medio		Riesgo por desactualización en temas de ciberseguridad.
Soporte entre docentes	Medio		Riesgo por falta de trazabilidad o soluciones informales.
Recursos educativos online	Crítico		Riesgo alto por enlaces inseguros o caducados.
Mantenimiento técnico	Crítico		Riesgo por fallas recurrentes sin diagnóstico.
Gestión documental externa	Alto		Riesgo por pérdida o duplicación de información.
Sala de informática	Crítico		Riesgo por equipos obsoletos y accesos no controlados.
Oficina de Rectoría	Alto		Riesgo por documentos sin cifrar ni respaldo digital.
Laboratorio de informática	Medio		Riesgo por uso de software no oficial o USB sin control.
Salón de clase	Alto		Riesgo físico por pérdida de materiales o falta de control.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad.

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Cafetería escolar	Bajo		Riesgo aceptable, sin impacto directo informativo.
Zona de cámaras de seguridad	Medio		Riesgo por falta de respaldo o ubicación inadecuada.
Bodega institucional	Bajo		Riesgo bajo por falta de custodia y ventilación.
Espacios comunes	Medio		Riesgo físico o pérdida de archivos móviles.
Archivador metálico	Alto		Riesgo por robo o daño de documentación física.
Portátil	Alto		Riesgo por pérdida o uso compartido sin autenticación.
Cronograma académico	Medio		Riesgo por modificaciones sin respaldo.
Formato de asistencia	Medio		Riesgo por manipulación de registros o firmas.
Contratos y convenios	Medio		Riesgo por divulgación no autorizada o falta de respaldo.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad.

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Registro de inventario	Medio		Riesgo por manipulación o falta de digitalización.
Plan de mejoramiento	Alto		Riesgo por cambios sin trazabilidad.
Presupuesto	Medio		Riesgo por archivos editables sin protección.
Rector	Alto		Riesgo por divulgación no autorizada o falta de formación.
Docente de Informática (Bachillerato)	Crítico		Riesgo alto por uso de dispositivos sin protección.
Docente de Informática (Primaria)	Alto		Riesgo por manejo inseguro de archivos o plataformas.
Docentes	Medio		Riesgo por mal uso de plataformas o correos.
Estudiantes	Medio		Riesgo por acceso a cuentas ajenas o manipulación.

Tabla 21. (Continuación)

Determinación del nivel de riesgo según su impacto y probabilidad.

ACTIVO	NIVEL DE RIESGO	ZONA DE COLOR	INTERPRETACIÓN GENERAL
Servicios generales	Bajo		Riesgo bajo por daños físicos no intencionales.

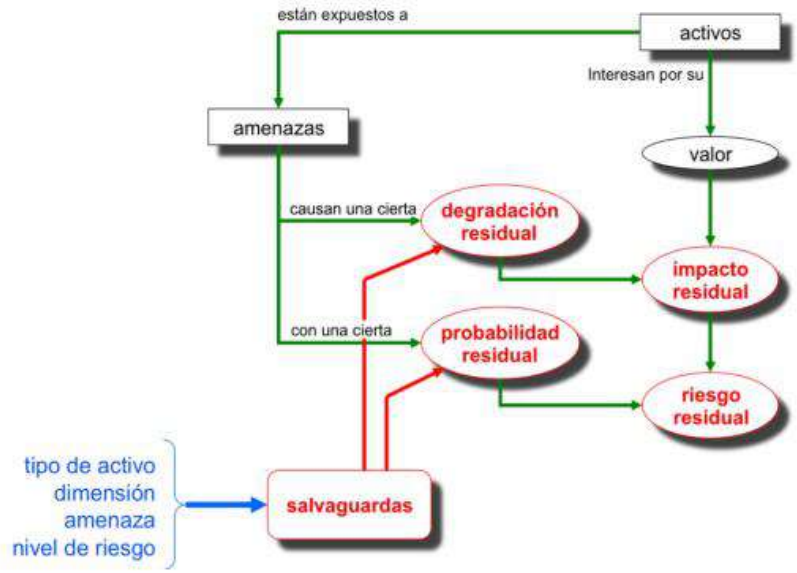
Fuente: Elaborada por los autores.

4.3.4 Salvaguardas.

De acuerdo con la metodología MAGERIT v3, las salvaguardas son medidas de protección o contramedidas implementadas con el fin de reducir la probabilidad de materialización de una amenaza o mitigar su impacto sobre los activos de información. Estas medidas pueden ser de tipo técnico, organizativo, físico o administrativo, y tienen como propósito principal preservar las tres dimensiones esenciales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Dentro del marco de un Sistema de Gestión de Seguridad de la Información (SGSI), las salvaguardas constituyen los mecanismos operativos y estratégicos que permiten proteger los activos críticos, prevenir incidentes y asegurar la continuidad de las operaciones. Su adecuada selección e implementación debe basarse en el nivel de riesgo identificado, garantizando una respuesta proporcional y efectiva frente a las amenazas detectadas.

Ilustración 8 Elementos del análisis del riesgo residual



Fuente: Tomado desde Margerit V 3.0

Según MAGERIT, las salvaguardas pueden clasificarse de la siguiente manera:

- **Preventivas (PR):** Reducen la probabilidad de amenazas. *Ejemplo:* uso de contraseñas seguras, control de acceso a salas de informática.
- **Correctivas (CR):** Permiten recuperar la operatividad tras un incidente. *Ejemplo:* copias de seguridad en discos externos, plan básico de recuperación.
- **Detectivas (DC):** Identifican y notifican eventos. *Ejemplo:* revisión periódica de registros, supervisión de uso de equipos.
- **Disuasorias (DI):** Desincentivan la materialización de amenazas. *Ejemplo:* carteles de advertencia, presencia visible de cámaras.
- **Compensatorias (CO):** Sustituyen un control principal. *Ejemplo:* doble revisión manual de notas o documentos.

Para valorar la eficacia de las salvaguardas se utilizó la escala de niveles propuesta en MAGERIT, que va desde L0 (inexistente) hasta L5 (optimizado):

Tabla 22 Eficacia y madurez de las salvaguardas

FACTOR	NIVEL	SIGNIFICADO
0%	L0	Inexistente
	L1	Inicial/ ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Fuente: Elaborado por los autores basado en Magerit V3.0

La selección de salvaguardas debe guiarse por el principio de proporcionalidad, priorizando los activos de mayor valor, los riesgos más probables y la cobertura que ofrecen las medidas de protección.

Se consideran dos posibles exclusiones en este proceso:

- **No aplica:** cuando la salvaguarda no corresponde al activo, amenaza o dimensión evaluada.
- **No se justifica:** cuando la medida resulta desproporcionada frente al riesgo.

El resultado es una declaración de aplicabilidad, que consolida las salvaguardas pertinentes y se convierte en la base del sistema de protección.

Con base en el análisis de riesgos realizado y en las entrevistas y visitas efectuadas, se identificaron los activos críticos, las amenazas a las que están expuestos, sus vulnerabilidades y las salvaguardas que deben aplicarse.

A continuación, se presenta la tabla con las medidas de protección propuestas:

Tabla 23 Identificación y clasificación de salvaguardas

TIPO DE ACTIVO	AMENAZAS	SALVAGUARDA 01	SALVAGUARDA 02	EFICACIA ACTUAL
INF – Información	Acceso indebido, eliminación accidental, manipulación/ alteración, divulgación no autorizada, edición sin trazabilidad, pérdida por error humano.	Implementar políticas de clasificación de la información y controles de acceso basados en roles para garantizar que únicamente usuarios autorizados accedan, modifiquen o eliminen registros sensibles.	Establecer un plan integral de respaldo automático en la nube con control de versiones y auditoría de modificaciones, asegurando recuperación en caso de incidentes.	L0 – L2

Tabla 23. (Continuación)

Identificación y clasificación de salvaguardas

TIPO DE ACTIVO	AMENAZAS	SALVAGUARDA 01	SALVAGUARDA 02	EFICACIA ACTUAL
SW – Software	Robo de información, eliminación accidental, acceso indebido, modificación no autorizada, fuga de información, ransomware, pérdida de datos, documentos sin trazabilidad.	Implementar cifrado de extremo a extremo en reposo y tránsito, junto con una gestión robusta de identidades y roles para proteger datos sensibles en las aplicaciones.	Diseñar un sistema de recuperación ante desastres con backups programados y auditorías periódicas de seguridad, garantizando continuidad y trazabilidad.	L0 – L2
HW – Hardware	Acceso externo no autorizado, robo de equipos, phishing por correo, pérdida de dispositivos USB, fallos eléctricos, eliminación de carpetas sin respaldo, daños físicos o mecánicos.	Aplicar medidas de seguridad física y lógica como firewalls, autenticación multifactor, cifrado completo de dispositivos y políticas estrictas de contraseñas.	Establecer un programa de mantenimiento preventivo con UPS, reguladores eléctricos, sistemas de rastreo y borrado remoto para minimizar pérdidas por incidentes físicos.	L0 – L2

Tabla 23. (Continuación)

Identificación y clasificación de salvaguardas

TIPO DE ACTIVO	AMENAZAS	SALVAGUARDA 01	SALVAGUARDA 02	EFICACIA ACTUAL
SE – Servicios	Interceptación de correos, acceso indebido a plataformas, caídas de sistema, falsificación de datos académicos, enlaces compartidos sin restricción, eliminación accidental.	Adoptar autenticación multifactor en plataformas críticas y firma digital en registros académicos, reforzando la trazabilidad y la legitimidad de la información.	Implementar servidores redundantes y planes de continuidad del negocio que incluyan políticas de permisos y caducidad de enlaces compartidos.	L0 – L2
INS – Instalaciones	Pérdida de archivos por error, falta de cifrado, instalación de software no oficial, vulnerabilidades sin parches, ingreso no autorizado a videoconferencias, fallos de red, acceso a sitios maliciosos.	Establecer políticas de whitelisting y actualización periódica de software, junto con cifrado de archivos sensibles y control de accesos en sesiones de videoconferencia.	Diseñar un plan de redundancia de red y filtrado web con proxies, complementado con copias automáticas para garantizar disponibilidad y seguridad de la información.	L0 – L2

Tabla 23. (Continuación)

Identificación y clasificación de salvaguardas

TIPO DE ACTIVO	AMENAZAS	SALVAGUARDA 01	SALVAGUARDA 02	EFICACIA ACTUAL
ADM – Recursos Administrativos	Malware/spyware, instalación de extensiones inseguras, suplantación de usuarios, errores en bases de datos, interrupción de servicios en la nube, falta de políticas claras, pérdida de prácticas, acceso indebido a datos estudiantiles.	Implementar soluciones de ciberseguridad con antivirus avanzado, control estricto de descargas y autenticación multifactor en sistemas administrativos.	Desarrollar un plan de continuidad institucional con respaldos automáticos de bases de datos y auditorías periódicas de accesos y permisos.	L0 – L2
RH – Recursos Humanos	Uso de software no oficial, infecciones por virus, incompatibilidad de sistemas, uso de dispositivos sin clave, robo de portátiles, fallos de sistema sin respaldo, mal uso de plataformas, acceso indebido de estudiantes, desconocimiento en ciberseguridad.	Aplicar políticas de uso aceptable de software y dispositivos, incluyendo cifrado en portátiles, bloqueo automático de sesiones y contraseñas robustas.	Establecer un programa continuo de capacitación en ciberseguridad y respaldo automático de archivos, complementado con auditorías técnicas periódicas.	L0 – L2

Fuente: Elaborado por los autores.

4.4 FASE 2: DISEÑO DEL PROTOCOLO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) ALINEADO A LA POLÍTICA DE GOBIERNO DIGITAL.

4.4.1 Introducción

La información constituye uno de los activos más valiosos de cualquier organización, incluida la comunidad educativa. En el caso del Centro Educativo Norean, la gestión, protección y disponibilidad de los datos académicos y administrativos resultan esenciales para garantizar la continuidad de los procesos formativos y la confianza de estudiantes, docentes y personal administrativo.

La presente Política de Seguridad de la Información surge como resultado de la auditoría tecnológica inicial realizada en la sala de informática, donde se identificaron deficiencias en controles físicos, lógicos y administrativos. Dichos hallazgos justifican la necesidad de establecer lineamientos claros y efectivos que orienten a la institución hacia una gestión responsable y segura de la información.

Este documento se encuentra fundamentado en los principios de la norma ISO/IEC 27001 y en la Política de Gobierno Digital del MinTIC, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de los activos de información institucionales, mediante la implementación de políticas alineadas a las mejores prácticas internacionales.

4.4.2 Objetivos

Objetivo General.

Establecer las directrices necesarias para proteger los activos de información y los recursos tecnológicos del Centro Educativo Norean, promoviendo su correcto uso y garantizando la protección de los datos frente a amenazas internas y externas.

Objetivos Específicos

1. Establecer lineamientos para el acceso, uso, monitoreo y mantenimiento de los recursos informáticos, con el fin de reducir riesgos y prevenir incidentes de seguridad.

2. Fomentar la cultura de seguridad de la información en la comunidad educativa, mediante actividades de formación, sensibilización y promoción de buenas prácticas.

3. Elaborar una propuesta básica de procedimientos para la gestión de incidentes de seguridad, que permita identificar, registrar y comunicar eventos relevantes dentro de la institución.

4.4.3 Alcance

La presente política aplica a toda la comunidad educativa del Centro Educativo Norean, así como a todos los recursos tecnológicos y activos de información de la institución, incluyendo equipos, redes, software, plataformas académicas, bases de datos y documentos físicos o digitales.

De este modo, su alcance cubre no solo la sala de informática, sino también los procesos de uso, almacenamiento, transmisión y gestión de la información en todas las áreas del colegio, garantizando la confidencialidad, integridad y disponibilidad de los datos, en cumplimiento de la ISO/IEC 27001 y la Política de Gobierno Digital del MinTIC**.**

4.4.4 Glosario.

- **Activo de información:** Recurso valioso para la institución, como equipos, bases de datos, plataformas o documentos.

- **Confidencialidad:** Garantía de que solo personas autorizadas pueden acceder a la información.

- **Disponibilidad:** Que los sistemas y datos estén accesibles cuando se necesiten.

- **Integridad:** Que la información no sea modificada o dañada sin permiso.

- **SGSI:** Conjunto de políticas y reglas para proteger la información de la institución.

- **Incidente de seguridad:** Cualquier problema que afecte la información, como un virus, pérdida de archivos o acceso indebido.

- **Amenaza:** Situación o evento que puede causar un daño a la información (ejemplo: un apagón o un virus).
- **Vulnerabilidad:** Debilidad que puede ser aprovechada por una amenaza, como no tener antivirus o usar contraseñas débiles.

4.4.5 Dominios de seguridad y políticas específicas.

En cumplimiento con los lineamientos establecidos por la Norma **ISO/IEC 27001**, el Centro Educativo Norean define las siguientes políticas de seguridad de la información, de carácter obligatorio y permanente, aplicables a todos los miembros de la comunidad educativa, incluyendo directivos, docentes, administrativos, estudiantes, contratistas y terceros con acceso a los activos de información de la institución.

El propósito de estas políticas es establecer un marco que garantice la protección, gestión y control adecuado de la información, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad.

Dominio 1: Organización de la Seguridad de la Información.

Este dominio se enfoca en establecer una estructura organizativa clara que defina las responsabilidades, roles y autoridad en materia de seguridad de la información. Busca garantizar que existan políticas, procedimientos y mecanismos de coordinación que fortalezcan la gestión y el cumplimiento de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI).

I. La política de seguridad será obligatoria para todos los miembros de la comunidad educativa.

II. La Rectoría será la máxima autoridad responsable de su cumplimiento y supervisión.

III. Se establecerán roles y responsabilidades en la protección de la información.

IV. Cualquier incidente de seguridad deberá reportarse inmediatamente al coordinador académico o responsable TIC.

V. Los dispositivos tecnológicos asignados (computadores, tabletas, proyectores, etc.) deberán usarse únicamente con fines educativos o administrativos.

VI. Los equipos institucionales deberán contar con configuraciones de seguridad básicas (contraseñas, bloqueo de pantalla, antivirus, etc.).

VII. Ningún miembro de la institución está autorizado a modificar o manipular los equipos sin autorización previa.

Dominio 2: Seguridad de los recursos humanos.

Este dominio se enfoca en implementar medidas orientadas a asegurar que el personal comprenda y asuma sus responsabilidades en materia de seguridad de la información antes, durante y después de su vinculación con la institución. Además, promueve la capacitación, la concientización y el compromiso con la confidencialidad de los datos institucionales.

I. El personal administrativo y docente deberá firmar un acuerdo de confidencialidad para proteger los datos institucionales.

II. Se realizarán jornadas de sensibilización y capacitación en seguridad digital para estudiantes, docentes y administrativos al menos una vez por año.

III. El incumplimiento de esta política podrá acarrear sanciones disciplinarias.

IV. En caso de retiro de personal, se suspenderán inmediatamente sus accesos a sistemas y redes institucionales.

V. Todo docente o administrativo deberá devolver los equipos o materiales tecnológicos asignados al finalizar su relación laboral.

VI. Se promoverá entre estudiantes la ética digital y el uso responsable de la información en internet y redes sociales.

Dominio 3: Gestión de activos.

Este dominio se enfoca en identificar, clasificar, registrar y proteger todos los activos de información, incluyendo equipos, software, bases de datos y documentos físicos o digitales. Su propósito es garantizar que cada activo sea adecuadamente administrado y protegido de acuerdo con su valor e importancia para la organización.

I. La institución llevará un inventario actualizado de equipos de cómputo, software, licencias, bases de datos y documentos físicos y digitales.

II. Cada activo de información tendrá un responsable asignado.

III. Los datos institucionales no podrán almacenarse en dispositivos personales.

IV. La clasificación de la información se hará bajo criterios de confidencialidad, integridad y disponibilidad.

V. Los medios de almacenamiento removibles deberán ser protegidos y, al finalizar su uso, destruidos o borrados de manera segura.

VI. Todo documento académico o administrativo deberá estar identificado y resguardado adecuadamente.

Dominio 4: Control de acceso.

Este dominio se enfoca en establecer medidas que regulen y limiten el acceso a la información, sistemas y recursos tecnológicos, asegurando que solo personas autorizadas puedan utilizarlos según sus funciones. Busca prevenir accesos indebidos, proteger la confidencialidad y evitar el uso inadecuado de los recursos institucionales.

I. Todos los computadores institucionales deberán estar protegidos con contraseña segura.

II. Las contraseñas serán personales, intransferibles y deberán cambiarse cada tres meses.

III. Los equipos se bloquearán automáticamente tras 5 minutos de inactividad.

IV. El acceso a sistemas institucionales será autorizado únicamente por la Rectoría o el área administrativa.

V. El uso compartido de credenciales está prohibido.

VI. Se fomentará la creación de contraseñas robustas (mínimo 10 caracteres con mayúsculas, minúsculas, números y símbolos).

VII. No se permitirá instalar software sin autorización previa.

Dominio 5: Seguridad física y del entorno.

Este dominio se enfoca en proteger las instalaciones, equipos y entornos físicos donde se procesa o almacena la información institucional. Incluye medidas para prevenir daños,

pérdidas o accesos no autorizados, así como controles de ingreso a las áreas críticas y mecanismos de protección ante amenazas ambientales o humanas.

I. El acceso a las salas de informática y oficinas administrativas será controlado y registrado.

II. Los equipos deberán mantenerse alejados de riesgos físicos como agua, fuego, polvo, humedad o vandalismo.

III. Está prohibido consumir alimentos o bebidas en salas de informática y oficinas donde se ubiquen equipos.

IV. El personal no podrá trasladar equipos sin autorización de la Rectoría.

V. Todos los puestos de trabajo deberán mantenerse organizados y sin documentos sensibles expuestos.

VI. Los equipos deberán contar con sistemas de respaldo energético (UPS) para evitar pérdida de datos en cortes eléctricos.

VII. Cada seis meses se realizarán mantenimientos preventivos de los equipos de cómputo.

Dominio 6: Seguridad de las operaciones.

Este dominio se enfoca en establecer procedimientos que garanticen que las operaciones tecnológicas y administrativas se desarrollen de manera segura y controlada. Comprende la gestión de respaldos, la protección contra software malicioso, la supervisión de incidentes y el mantenimiento de la integridad de los sistemas durante su funcionamiento diario.

I. Todo equipo institucional deberá contar con software antivirus actualizado.

II. Los archivos descargados deberán verificarse antes de abrirse.

III. Queda prohibida la instalación de programas no autorizados.

IV. Se implementarán copias de seguridad periódicas de la información académica y administrativa.

V. Todo cambio en los equipos o sistemas deberá ser aprobado y registrado por la Rectoría o área administrativa.

VI. Se restringirá el uso de dispositivos extraíbles no autorizados.

VII. El personal docente y administrativo deberá reportar cualquier anomalía en los sistemas informáticos.

Dominio 7: Seguridad de las comunicaciones.

Este dominio se enfoca en asegurar la protección de la información que se transmite a través de redes internas o externas, evitando accesos no autorizados, alteraciones o pérdidas de datos. Contempla el uso seguro de correos electrónicos, redes inalámbricas, servicios en línea y medios digitales institucionales.

I. El servicio de internet institucional será utilizado exclusivamente para fines académicos y administrativos.

II. El acceso a páginas web con contenido inadecuado (violencia, pornografía, drogas, hacking, etc.) estará bloqueado.

III. El correo institucional será el único medio autorizado para comunicaciones oficiales.

IV. No se permitirá compartir datos confidenciales a través de correos personales o redes sociales.

V. Se deberán eliminar correos sospechosos o de remitentes desconocidos.

VI. El uso de aplicaciones de mensajería instantánea estará restringido a actividades educativas aprobadas.

VII. La institución deberá implementar medidas de separación de redes (docentes, estudiantes, administrativos).

Dominio 8: Adquisición, desarrollo y mantenimiento de sistemas.

Este dominio se enfoca en garantizar que la seguridad de la información sea considerada desde la etapa de diseño, desarrollo, implementación y mantenimiento de los sistemas. Busca prevenir vulnerabilidades mediante controles de validación, pruebas de seguridad, gestión de cambios y documentación técnica actualizada.

I. Todo software adquirido deberá cumplir con requisitos de seguridad y licencia legal.

II. Nuevos sistemas o actualizaciones deberán ser probados en un entorno de prueba antes de implementarse.

III. No se permitirá el uso de software pirata o sin licencia.

IV. Se documentarán las configuraciones y cambios realizados en sistemas institucionales.

V. Todo sistema educativo o administrativo deberá incorporar controles de seguridad básicos.

Dominio 9: Relación con proveedores.

Este dominio se enfoca en establecer medidas que aseguren que los proveedores externos que acceden a la información o recursos tecnológicos cumplan con los mismos estándares de seguridad que la institución. Incluye la firma de acuerdos de confidencialidad, la evaluación de riesgos y la supervisión del cumplimiento de las políticas de seguridad.

I. Todo proveedor que tenga acceso a información del colegio deberá firmar acuerdos de confidencialidad.

II. La institución verificará la seguridad de los servicios contratados (software, mantenimiento, soporte técnico, etc.).

III. La información compartida con proveedores será únicamente la necesaria y estará protegida bajo contrato.

IV. Se realizará un seguimiento a la gestión de los proveedores que manejen datos sensibles.

Dominio 10: Gestión de Incidentes de Seguridad.

Este dominio se enfoca en definir y aplicar procedimientos para la detección, análisis, respuesta y aprendizaje frente a incidentes que afecten la seguridad de la información. Su propósito es minimizar el impacto de los eventos, restaurar la operación normal y fortalecer la prevención de futuras amenazas.

I. El Centro Educativo Norean establecerá procedimientos formales para la identificación, registro y atención de incidentes.

II. Todo miembro de la comunidad educativa deberá reportar incidentes inmediatamente.

III. Los incidentes serán analizados y documentados para prevenir su recurrencia.

IV. Se elaborarán planes de respuesta ante emergencias que puedan comprometer los sistemas.

V. Se promoverá el aprendizaje a partir de cada incidente para fortalecer la seguridad institucional.

Dominio 11: Cumplimiento.

Este dominio se enfoca en garantizar que la institución cumpla con las leyes, normas, políticas internas y requisitos contractuales relacionados con la seguridad de la información. Abarca la protección de datos personales, el respeto de los derechos de autor, el uso legal del software y la aplicación de medidas correctivas en caso de incumplimiento.

I. El colegio garantizará el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales.

II. Todo software utilizado deberá contar con su licencia de uso.

III. El acceso a datos sensibles estará limitado únicamente a personas autorizadas.

IV. El incumplimiento de esta política podrá acarrear sanciones disciplinarias.

V. La Rectoría y coordinación académica serán responsables de supervisar el cumplimiento de las políticas.

4.5 FASE 3: ESTABLECIMIENTO DE CONTROLES DE SEGURIDAD Y ENUNCIADO DE APLICABILIDAD (SoA) BASADOS EN LA NORMA ISO/IEC 27001.

En esta fase se elaboró el Enunciado de Aplicabilidad (SoA), mediante el cual se seleccionaron y justificaron los controles de la norma ISO/IEC 27001 pertinentes para el Centro Educativo, tomando como referencia los riesgos identificados y las políticas definidas en fases anteriores.

De igual forma, se vinculó cada salvaguarda con los controles de seguridad reconocidos internacionalmente, dejando constancia de aquellos que fueron aplicables y de los que no, junto con su respectiva justificación.

Así, el SoA se consolidó como documento fundamental del Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la coherencia entre riesgos, salvaguardas, políticas y controles, y sirviendo de guía para la implementación de medidas de protección en la institución.

Tabla 24 Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.5	**Políticas de seguridad de la información**		
A.5.1	Directrices para la gestión de la seguridad de la información	**Si**	Se aplica el control para definir los lineamientos generales que orienten la gestión de la seguridad dentro del colegio.
A.5.1.1	Políticas para la seguridad de la información	**Sí**	Se aplica el control, puesto que es necesario establecer políticas institucionales que definan las directrices y responsabilidades para la protección de los activos de

			información, aprobadas por la dirección y comunicadas a todo el personal.
A.5.1.2	Revisión de las políticas de seguridad de la información	**Sí**	Se aplica para asegurar la actualización continua de las políticas según los cambios tecnológicos o estructurales del colegio, garantizando su eficacia y adecuación.
A.5.2	Roles y responsabilidades organizacionales	**Si**	Se aplica para definir claramente las funciones del rector, los docentes y los responsables del manejo de información en la institución.
A.5.2.1	Definición de funciones y responsabilidades en seguridad de la información	**Sí**	Se aplica el control para asignar responsabilidades específicas relacionadas con la gestión y cumplimiento del SGSI.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.5.3	Contacto con autoridades	**Sí**	Se aplica el control para garantizar la comunicación oportuna con autoridades competentes ante incidentes o requerimientos legales.
A.5.4	Contacto con grupos de interés especial	**No**	No aplica, la institución no pertenece a grupos técnicos ni foros especializados en seguridad de la información.

A.5.5	Amenazas a la seguridad de la información	**Sí**	Se aplica, ya que es necesario mantener un proceso de identificación continua de amenazas internas y externas.
A.5.6	Planificación de la seguridad de la información	**Sí**	Se aplica para integrar los objetivos de seguridad dentro de la planificación institucional y garantizar la mejora continua del SGSI.
A.5.7	Inventario de activos de información	**Sí**	Se aplica, ya que se requiere identificar y registrar todos los equipos, software y datos institucionales.
A.5.8	Uso aceptable de los activos	**Sí**	Se aplica para definir reglas sobre el uso correcto de los recursos informáticos y tecnológicos del colegio.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.5.9	Devolución de activos	**Sí**	Se aplica, dado que el personal debe devolver los equipos asignados al finalizar su vinculación o uso temporal.
A.5.10	Clasificación y etiquetado de la información	**Sí**	Se aplica para establecer niveles de clasificación según la sensibilidad y criticidad de los datos.
A.5.11	Manejo de medios	**Sí**	Se aplica, ya que se deben implementar medidas seguras para el transporte, almacenamiento y eliminación de medios físicos y digitales.
A.5.12	Requisitos legales, reglamentarios y contractuales	**Sí**	Se aplica, pues la institución debe garantizar el cumplimiento normativo en materia de protección de datos personales y propiedad intelectual.
A.5.13	Derechos de propiedad intelectual	**Sí**	Se aplica para asegurar el uso legítimo de software y material digital dentro del entorno académico.
A.5.14	Protección de registros	**Sí**	Se aplica, ya que los registros académicos y administrativos deben conservarse íntegros y confidenciales.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.5.15	Privacidad y protección de datos personales	**Sí**	Se aplica en cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales.
A.5.16	Revisión independiente del SGSI	**No**	No aplica, la institución no dispone de personal o entidad externa designada para revisiones independientes.
A.6	**Controles de personas**		
A.6.1	Responsabilidades antes, durante y después del empleo	**Si**	Se aplica, ya que el personal debe mantener la confidencialidad y las buenas prácticas en todo momento.
A.6.1.1	Selección de personal	**Sí**	Se aplica el control, ya que se deben verificar antecedentes y asegurar compromisos de confidencialidad antes de la vinculación laboral o contractual.
A.6.1.2	Términos y condiciones de empleo	**Sí**	Se aplica, puesto que los contratos deben incluir cláusulas sobre responsabilidades y uso adecuado de la información institucional.
A.6.1.3	Responsabilidades posteriores al empleo	**Sí**	Se aplica, dado que la obligación de confidencialidad se mantiene una vez finalizada la relación laboral o contractual.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.6.2	Concienciación, educación y formación en seguridad de la información	**Si**	Se aplica, porque es necesario mantener programas de formación y campañas de concienciación en seguridad de la información.
A.6.2.1	Capacitación y sensibilización del personal	**Sí**	Se aplica, porque es necesario mantener programas de formación y campañas de concienciación en seguridad de la información.
A.6.3	Procesos disciplinarios relacionados con la seguridad	**Si**	Se aplica, ya que deben existir medidas disciplinarias frente a violaciones de las políticas o prácticas inseguras.
A.6.3.1	Sanciones por incumplimiento de políticas	**Sí**	Se aplica, ya que deben existir medidas disciplinarias frente a violaciones de las políticas o prácticas inseguras.
A.7	**Controles físicos**		
A.7.1	Seguridad de las instalaciones	**Si**	Se aplica el, dado que el Centro Educativo cuenta con áreas donde se alojan equipos y materiales sensibles. Es necesario implementar medidas básicas de seguridad física como mantener los espacios cerrados, restringir el acceso al personal autorizado y supervisar el uso de los equipo para prevenir daños, robos o accesos no permitidos.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.7.1.1	Seguridad de las áreas donde se alojan los sistemas	**Sí**	Se aplica el control, ya que es necesario proteger las zonas donde se encuentran equipos críticos, como la sala de informática y oficinas administrativas.
A.7.1.2	Controles de acceso físico	**Sí**	Se aplica para restringir el ingreso únicamente a personal autorizado, previniendo accesos no permitidos.
A.7.1.3	Protección contra amenazas físicas y ambientales	**Sí**	Se aplica, pues deben adoptarse medidas de prevención ante incendios, humedad o fallas eléctricas que puedan afectar los equipos.
A.7.1.4	Seguridad en el uso de equipos	**Sí**	Se aplica, ya que los equipos informáticos deben manipularse siguiendo prácticas seguras que eviten daños o pérdida de información.
A.7.1.5	Eliminación o reutilización segura de equipos	**Sí**	Se aplica, puesto que los dispositivos deben limpiarse o destruirse adecuadamente antes de su reasignación o desecho.
A.7.2	Protección de la información en entornos físicos	**Si**	Se aplica para evitar accesos indebidos o exposición de información sensible dentro de las instalaciones.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.7.2.1	Política de escritorio limpio y pantalla bloqueada	**Sí**	Se aplica el control para prevenir la exposición de información confidencial y accesos indebidos durante y después del uso de los equipos.
A.8	**Controles tecnológicos**		
A.8.1	Gestión de configuración	**Sí**	Se aplica, ya que se deben mantener configuraciones seguras y actualizadas en los equipos informáticos para evitar vulnerabilidades.
A.8.2	Gestión de la capacidad	**No**	No aplica, debido a que la infraestructura tecnológica es limitada y no requiere monitoreo de capacidad continuo.
A.8.3	Protección contra malware	**Sí**	Se aplica el control, puesto que los equipos deben contar con software antivirus actualizado y medidas de detección de amenazas.
A.8.4	Copias de seguridad	**Sí**	Se aplica, dado que es necesario realizar respaldos periódicos de la información académica y administrativa.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.8.5	Registro de eventos y monitoreo	**No**	No aplica, ya que la institución no dispone de sistemas automáticos de monitoreo o auditoría de eventos.
A.8.6	Sincronización de tiempo	**No**	No aplica, porque los equipos no requieren sincronización centralizada de reloj.
A.8.7	Control de instalación de software	**Sí**	Se aplica para restringir la instalación de programas no autorizados en los equipos institucionales.
A.8.8	Gestión de vulnerabilidades técnicas	**Sí**	Se aplica, pues se deben identificar y corregir vulnerabilidades detectadas en sistemas operativos o aplicaciones.
A.8.9	Gestión de cambios	**Sí**	Se aplica el control para documentar, aprobar y verificar los cambios realizados en los sistemas o configuraciones.
A.8.10	Seguridad en las redes	**Sí**	Se aplica, ya que las redes institucionales deben protegerse mediante contraseñas seguras y protocolos de cifrado.
A.8.11	Seguridad en los servicios de red	**Sí**	Se aplica el control para asegurar el correcto funcionamiento, filtrado y control de acceso a los servicios de red.

Tabla 24. (Continuación)

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

NÚM.	CONTROL	APLICA	JUSTIFICACIÓN
A.8.12	Seguridad en la transferencia de información	**Sí**	Se aplica para proteger los datos transmitidos por medios digitales mediante cifrado o canales seguros.
A.8.13	Uso aceptable de los servicios de comunicación	**Sí**	Se aplica, ya que regula el uso responsable de internet, correo electrónico y redes institucionales.
A.8.14	Desarrollo y mantenimiento seguro de software	**No**	No aplica, ya que la institución no desarrolla ni mantiene sistemas informáticos propios.
A.8.15	Seguridad en la relación con proveedores	**Sí**	Se aplica para asegurar que los proveedores cumplan con acuerdos de confidencialidad y medidas de seguridad.
A.8.16	Gestión de incidentes de seguridad de la información	**Sí**	Se aplica, puesto que deben existir procedimientos formales para registrar, analizar y responder ante incidentes.
A.8.17	Continuidad de la seguridad de la información	Si	Aplica, porque permite mantener la protección de la información y asegurar la continuidad del servicio ante cualquier interrupción.

Tabla 24. Continuación

Establecimiento y Enunciado de Aplicabilidad (SoA) de los Controles de Seguridad según la Norma ISO/IEC 27001.

A.8.18	Cumplimiento con requisitos legales y normativos	**Sí**	Se aplica para garantizar el cumplimiento de la normativa vigente sobre protección de datos y derechos de autor.

CONCLUSIONES

El proyecto desarrollado en el Centro Educativo Norean permitió diagnosticar el estado actual de la seguridad de la información institucional, evidenciando la ausencia de políticas y procedimientos formales orientados a la protección de los datos. No obstante, se identificó una infraestructura tecnológica básica y un equipo docente y administrativo dispuesto a fortalecer la cultura de seguridad digital dentro del entorno educativo.

A través de la identificación y clasificación de los activos de información entre ellos datos, software, hardware, servicios, instalaciones y recursos humanos se logró establecer un panorama claro de las vulnerabilidades y amenazas que afectan la confidencialidad, integridad y disponibilidad de la información. Mediante la aplicación de la metodología de análisis de riesgos MAGERIT v3.0, se valoraron los riesgos y se determinaron los niveles de impacto y probabilidad asociados, lo cual permitió priorizar la identificación de controles técnicos y administrativos que mitiguen los riesgos críticos detectados.

En el proceso de diseño del Sistema de Gestión de Seguridad de la Información (SGSI), alineado a la norma ISO/IEC 27001:2022, se formularon políticas, procedimientos y lineamientos que facilitan la protección, gestión y asignación de responsabilidades sobre los activos de información. Este modelo se constituye como una herramienta fundamental para el fortalecimiento institucional, promoviendo una gestión organizada y responsable de los datos académicos y administrativos.

El cumplimiento de los objetivos planteados se evidencia en la realización del diagnóstico, la evaluación de riesgos, la definición de políticas y la propuesta de un modelo de SGSI aplicable al contexto educativo. Asimismo, el proyecto contribuye a generar conciencia sobre la importancia de la privacidad y confidencialidad de la información, considerando los aspectos legales, técnicos, organizativos y culturales que inciden en la seguridad institucional.

La investigación resalta que la construcción de un marco integral de gestión de la seguridad no solo podría reducir los riesgos de pérdida o filtración de información, sino que también fortalece la confianza, la ética y la sostenibilidad dentro de la comunidad educativa. En un contexto en el que las amenazas cibernéticas son cada vez más sofisticadas, este proyecto sienta las bases para que las instituciones educativas adopten un enfoque preventivo y resiliente frente a los incidentes de seguridad.

En síntesis, el estudio desarrollado en el Centro Educativo Norean trasciende la mera necesidad técnica de proteger los datos, convirtiéndose en una propuesta estratégica que fomenta una cultura institucional de seguridad, responsabilidad y transparencia. Su integración efectiva permitirá garantizar la continuidad, la reputación y la confianza de la comunidad educativa, consolidando un modelo sostenible de protección de la información acorde con las exigencias de la era digital.

RECOMENDACIONES

1. Es fundamental fortalecer las competencias del personal administrativo, docente y directivo en materia de seguridad de la información mediante programas de formación continua que promuevan el uso responsable de los sistemas tecnológicos, la correcta gestión de los datos personales y la prevención de riesgos digitales. Del mismo modo, resulta necesario fomentar una cultura organizacional basada en la ética, la responsabilidad y la confidencialidad, que contribuya a consolidar el compromiso institucional con la protección de la información y la seguridad digital.

2. Se recomienda formalizar políticas internas orientadas a la protección y manejo adecuado de la información, alineadas con la norma ISO/IEC 27001:2022. Dichas políticas deben establecer directrices claras sobre el acceso, almacenamiento y tratamiento de los datos, garantizando el cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás disposiciones legales relacionadas con la protección de datos personales.

3. Es necesario fortalecer la infraestructura tecnológica del Centro Educativo Norean mediante controles técnicos y administrativos como respaldos de seguridad, autenticación multifactor y auditorías internas. Además, se debe implementar un proceso de mejora continua del SGSI con revisiones periódicas que evalúen su eficacia y adapten las medidas ante nuevas amenazas. Finalmente, se recomienda designar un comité responsable de garantizar el cumplimiento de políticas, estándares y la actualización constante de los procedimientos de seguridad.

4. Se sugiere adoptar la metodología MAGERIT v3.0 de manera continua para evaluar y gestionar los riesgos asociados a los sistemas de información. Esta herramienta facilitará la detección temprana de amenazas, la priorización de

riesgos y la aplicación de medidas preventivas que reduzcan su impacto en la operación institucional.

POSIBLES COLABORADORES EN LA INVESTIGACIÓN.

A continuación, para el desarrollo de este proyecto de investigación, se contará con la colaboración especialistas en gestión de seguridad de la información, auditores de TI con experiencia en la norma ISO/IEC 27001 y consultores en estrategias tecnológica.

Director	Erney Alberto Ramírez Camargo
Codirector	Wilfer Escalante
Población objetivo	Centro Educativo Norean, Aguachica Cesar

Fuente: Los autores.

RECURSOS DISPONIBLES.

Para el desarrollo de este proyecto de investigación, se dispondrá de herramientas tecnológicas como computadores de rendimiento, softwares especializados, al igual que documentos físicos normativos y guías de implementación que servirán como referencia esencial para garantizar la precisión y el cumplimiento de los estándares establecidos.

Elementos	Cantidad	Valor Unitario	Valor total
Computador portátil	2	$2’000.000	$4’000.000
Papelería	1	50.000	50.000
CD	2	5.000	5.000
TOTAL			4.055.000

Fuente: Los autores.

CRONOGRAMA DE ACTIVIDADES

Tabla 25 Cronograma de actividades de la realización del proyecto

OBJETIVOS ESPECÍFICOS	ACTIVIDADES	SEMANA

Identificar el estado actual de la seguridad de la información la Institución Educativa.	✓ Revisión de la infraestructura tecnológica actual. ✓ Entrevistas con el personal clave de la institución para entender los procesos actuales de seguridad. ✓ Revisión de políticas y procedimientos actuales. ✓ Análisis del manejo de la información y accesos a los datos sensibles.	**1-2**
Analizar los riesgos asociados al uso de las tecnologías de la Información a partir de metodologías para la identificación, análisis y evaluación de amenazas, vulnerabilidades e impactos.	✓ Selección de la metodología de análisis de riesgos. ✓ Identificación de activos de información. ✓ Identificación de amenazas y vulnerabilidades para cada activo. ✓ Evaluación del impacto y la probabilidad de ocurrencia de los riesgos. ✓ Documentación de los resultados del análisis de riesgos.	**3-4**
Definir el alcance y las políticas del Sistema de Gestión de Seguridad de la información (SGSI) para los procesos soportados por la Institución Educativa.	✓ Identificación de los procesos y áreas que serán cubiertos por el SGSI. ✓ Definición de los límites y el alcance del sistema. ✓ Redacción de las políticas de seguridad de la información (confidencialidad, integridad, disponibilidad). ✓ Establecimiento de roles y responsabilidades dentro del SGSI. ✓ Validación de las políticas con las autoridades de la institución.	**5-6**

Diseñar un sistema de gestión de la seguridad de la información (SGSI) para la Institución educativa alineados a la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y Comunicación MinTIC.	✓ selección de los controles de seguridad. ✓ Elaboración de procedimientos para la gestión de incidentes de seguridad. ✓ Diseño del plan de continuidad de negocio y recuperación ante desastres. ✓ Documentación de los procesos del SGSI. ✓ Alineación del diseño con la Política de Gobierno Digital y la ISO 27001. ✓ Revisión y ajustes finales del diseño con el equipo de TI de la institución.	**7-8**

Fuente: Elaboración propia.

REFERENCIAS

Barcia, G. (2023). IMPLEMENTACIÓN DEL ESTÁNDAR ISO/IEC 27001 PARA LA SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD EDUCATIVA FISCAL CULTURA MACHALILLA. *UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ*. Obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/5917/1/BARCIA%20BAQUE%20GABRIEL%20ALEXANDER.pdf

Barrera, J. (2019). *PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDADEDUCATIVA NUESTRA SEÑORA DE FÁTIMA.* Quito. Obtenido de https://repositorio.uisrael.edu.ec/bitstream/47000/1901/1/UISRAEL-EC-SIS-378.242-2019-008.pdf

Bleeping Computer. (2023). *Cuáles son las consecuencias de recibir un ciberataque y cómo prevenirlo.* WIN Empresas. Obtenido de https://winempresas.pe/blog/cuales-son-las-consecuencias-de-recibir-un-ciberataque-y-como-prevenirlo

Cajamarca, Ron, & Chamorro, G. (2023). Evaluación del nivel de seguridad informáticadesplegadoen los institutos de educación superior de la red RIT II. *Revista Conectividad*. Obtenido de https://revista.ister.edu.ec/ojs/index.php/ISTER/article/view/49/91

Castillo, F. (2023). Plan de implementación de un Sistema de Gestión de Seguridad de la Información SGSI para el Colegio Universitario de Cartago. *Universidad CENFOTEC*. Obtenido de https://repositorio.ucenfotec.ac.cr/bitstream/handle/123456789/518/PIA02-Castillo%20Molina%20Frank.pdf?sequence=1&isAllowed=y

Check Point. (2023). *Ciberseguridad.* Obtenido de https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

Correa, M. (2023). Modelo de sistema de gestión de seguridad de la información para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la informac. *Universidad estatal de milagro* . Obtenido de https://repositorio.unemi.edu.ec/bitstream/123456789/6971/1/ALEX%20AVILA%20COELLO.pdf

Estalla, L., & Morales, M. (2024). *Propuesta de un sistema de gestíon de seguridad de la informacíon basado en la nprma 27001 para la agencia de compras de las fuerzas armandas,2023.* Callao. Obtenido de https://repositorio.unac.edu.pe/bitstream/handle/20.500.12952/8903/TESIS%20-%20ESTALLA-MORALES.pdf?sequence=1&isAllowed=y

Fernandez, P. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.* Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf

Forbes Colombia. (2024). Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM. *Forbes Staf*.

Forbes Staff. (2024). Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM. *Forbes Colombia*. Obtenido de https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica

Franco, A. (2024). PLAN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA COLOMBIANA DE INGENIERIA CIVIL CIBJO SAS BIC. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/63286/afrancoco.pdf?sequence=1&isAllowed=y

Gallego, N., & Gonzales, J. (2021). DISEŃO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) PARA UNA EMPRESA DEL SECTOR INDUSTRIAL BASADO EN LA NORMA ISO/IEC 27001:2013. *UNIVERSIDAD EL BOSQUE*. Obtenido de https://repositorio.unbosque.edu.co/server/api/core/bitstreams/8ec7beba-8849-4fad-a7da-ba91a3077254/content

Garcia, R. (2020). Propuesta de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO 27001 para la Oficina de Tecnologías de Información del Gobierno Regional Piura. *UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE*. Obtenido de https://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/20296/CONFIDENCIALIDAD_INFORMACION_GARCIA_CRUZ_RODOLFO_AUGUSTO.pdf?sequence=1&isAllowed=y

Gaviria, J., Villamizar, A., Soto, D., & Reyes, A. (2023). Buenas prácticas en la gestión en seguridad. *Revista Ibérica de Sistemas e Tecnologias de Informação*. Obtenido de https://www.proquest.com/openview/1f29f74f4cdb6807b3ee1246f95400f8/1?pq-origsite=gscholar&cbl=1006393

Gomez, Y., & Montaña, D. (2020). Diseño del sistema de gestión de la seguridad de la información para el sistema de pedidos web de la empresa panamericana outsourcing s.a. basado en la norma iso iec 27001:2013. *UNIVERSIDAD PILOTO*

DE COLOMBIA . Obtenido de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8207/Trabajo%20de%20Grado.pdf?sequence=1

Guerrero, D., Navarro, A., Lizcano, R., & Felizzola, L. (2019). Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, seccional Aguachica. *Universidad Popular del Cesar*. Obtenido de https://repositorioinstitucional.ufpso.edu.co/bitstream/handle/20.500.14167/1373/CUERPO%20DEL%20TRABAJO%20-%20PROYECTO%20DE%20GRADO_removed.pdf?sequence=1&isAllowed=y

Guevara, E., Delagdo, D., & Mendoza, A. (2022). Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001. Obtenido de file:///C:/Users/Usuario/Downloads/RISI15-1_011_Guevara.pdf

Guzman, J., & Garcia, H. (2023). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS CRÍTICOS DE LA EMPRESA STAR S.A.S BAJO LA NORMA ISO 27001:2013ORANGE.* Bogotá: Universidad Piloto de Colombia. Obtenido de file:///C:/Users/Usuario/Documents/Proyecto%20de%20grado/Proyectos/Disen%CC%83o%20de%20SGSI%20Orange%20Star%20Sas.pdf

Moya, J. (2023). La importancia de la seguridad informática en la educación digital. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8977055

Muñoz, E., & Palmera, L. (2019). PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA FQ TECNOLOGIAS S.A.S, BASADO EN LA NORMA ISO 27001:2013. *UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA* . Obtenido de https://repositorioinstitucional.ufpso.edu.co/bitstream/handle/20.500.14167/1382/Cuerpo%20del%20trabajo%20-%20PLANEACI%c3%93N%20DEL%20SISTEMA%20DE%20GESTI%c3%93N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACION%20PARA%20LA%20EMPRESA%20FQ%20TECNOLOGIAS%20S.A_remov

Obando, J. (2024). Ciberseguridad en Colombia: panorama completo de su estado en 2023. *Link Tic*. Obtenido de https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

Osorio, J. (2022). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001:2013 PARA EL ÁREA DE TECNOLOGÍA EN LAUNIDAD ADMINISTRATIVA ESPECIAL CUERPO OFICIAL DE BOMBEROS DE BOGOTÁ. *UNIVERSIDAD PILOTO DE COLOMBIA*. Obtenido de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12339/Final%20SGI%20Bomberos%20con%20norma%20%284%29.pdf?sequence=1&isAllowed=y

Ospina, J. (2023). DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL FONDO DE EMPLEADOS FEBIMBO EN EL ÁREA DE TECNOLOGÍA. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/56674/jcospinar.pdf?sequence=4&isAllowed=y

Pando, F. (2024). Análisis de vulnerabilidades para empresas: ¿Cómo se realiza? *Digixem*. Obtenido de https://www.itmastersmag.com/noticias-analisis/analisis-de-vulnerabilidades-cual-es-su-importancia/

Rodriguez, J., & Ruiz, A. (2021). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TALENTO HUMANO DE LA SECRETARÍA DE EDUCACIÓN DE FUSAGASUGÁ BASADO EN LA NORMA NTC-IEC ISO 27001:2013.* Bogotá: UNIVERSIDAD PILOTO DE COLOMBIA . Obtenido de https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9854/DISE%c3%91O%20DE%20UN%20SISTEMA%20DE%20GESTI%c3%93N%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%c3%93N%20PARA%20EL%20%c3%81REA%20DE%20TALENTO%20HUMANO%20DE%20LA%20SECRETAR%c3%8dA%20DE%20EDU

Ruiz, Estrada, & Sanchez. (2020). PROPUESTA DE UN MODELO DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA INSTITUCIONES EDUCATIVAS. Obtenido de file:///C:/Users/Usuario/Downloads/Dialnet-PropuestaDeUnModeloDeUnSistemaDeGestionDeCalidadEn-7812303.pdf

Suarez, L. (2021). SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001:2015- EN LA EMPRESA MAGDANIEL LTDA. EN EL DISTRITO ESPECIAL, TURÍSTICO Y CULTURAL DE RIOHACHA. *UNIVERSIDAD DE LA GUAJIRA*. Obtenido de https://repositoryinst.uniguajira.edu.co/bitstream/handle/uniguajira/407/89.TRABAJO%20DE%20GRADO%20AGOSTO%20LUZ%20DARIS%20SUAREZ.pdf?sequence=1&isAllowed=y

Suarez, L. (2024). Ciberseguridad en Colombia ¿cuáles son los riesgos a los que se enfrenta el país? Obtenido de https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/#:~:text=Seg%C3%BAn%20el%20Centro%20Cibern%C3%A9tico%20de,del%2079%20%25%20respecto%20a%202021.

Ureche, M. (2017). DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA BASADAS EN LA NORMA NTC-ISO-IEC 27001:2013 PARA LA UNIVERSIDAD DE CARTAGENA CENTRO TUTORIAL MOMPOX BOLÍVAR. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD*. Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/12027/19772159.pdf?sequence=1&isAllowed=y

Vargas, G. (2020). Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT. *Universidad Mayor de San Andrés*. Obtenido de C:/Users/Usuario/Downloads/Gonzalo+Diego+Vargas+Ramos.pdf

ANEXOS

Anexo 1 Autorización institucional para la realización del proyecto de grado.

A continuación, se presenta la carta emitida por el rector del Centro Educativo Norean, donde se otorga la autorización oficial a las estudiantes de la Universidad Popular del Cesar, programa de Ingeniería de Sistemas, para llevar a cabo el proyecto de grado titulado “Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado a la norma ISO/IEC 27001:2022”, dentro de las instalaciones de la institución.

Aguachica, Cesar 20/03/2025

Señores:
COMITÉ DE PROYECTOS DE GRADO
Facultad de Ingenierías y Tecnológicas
Programa de Ingeniería de Sistemas
Universidad Popular Del Cesar

Cordial Saludo respetados Ingenieros,

Me permito informarle que los estudiantes: **Paula Andrea Garnica Molinares** y **Doris Natalia Bautista Romero,** se encuentran autorizados por esta entidad para realizar su proyecto de grado, titulado **"Construcción de un sistema de gestión de seguridad de la información alineado a la norma ISO 27001 para el Centro educativo Norean, del Municipio de Aguachica Cesar"**, Aclaro de antemano que el desarrollo del proyecto no genera ningún vínculo laboral con la entidad.

Atentamente,

20/03/2025

Fernando Marin Ariza
CC No. 12458145 de San Alberto, Cesar
Rector

CENTRO EDUCATIVO NOREAN CESAR
Dirección: km 10, Norean, Vía Aguachica
Teléfono móvil: 305 3538325
Correo institucional: eenorean@educacioncesar.gov.co

Fuente: *Centro Educativo Norean (2025).*

Anexo 2 Formato de la entrevista

Este anexo contiene las entrevistas aplicadas al rector y a dos docentes del Centro Educativo Norean, como parte del diagnóstico inicial para la construcción del Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001.

Objetivo:

Recopilar información sobre los activos de información, prácticas actuales de seguridad, riesgos identificados y nivel de conocimiento del personal institucional, con el fin de identificar vulnerabilidades y establecer una línea base para el diseño del SGSI.

ENTREVISTAS DE DIAGNÓSTICO Y ANÁLISIS PARA LA CONSTRUCCIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL CENTRO EDUCATIVO NOREAN.

1. OBJETIVO:

Obtener información detallada y contextual sobre los activos utilizados en el centro Educativo Norean.

2. INTRODUCCIÓN:

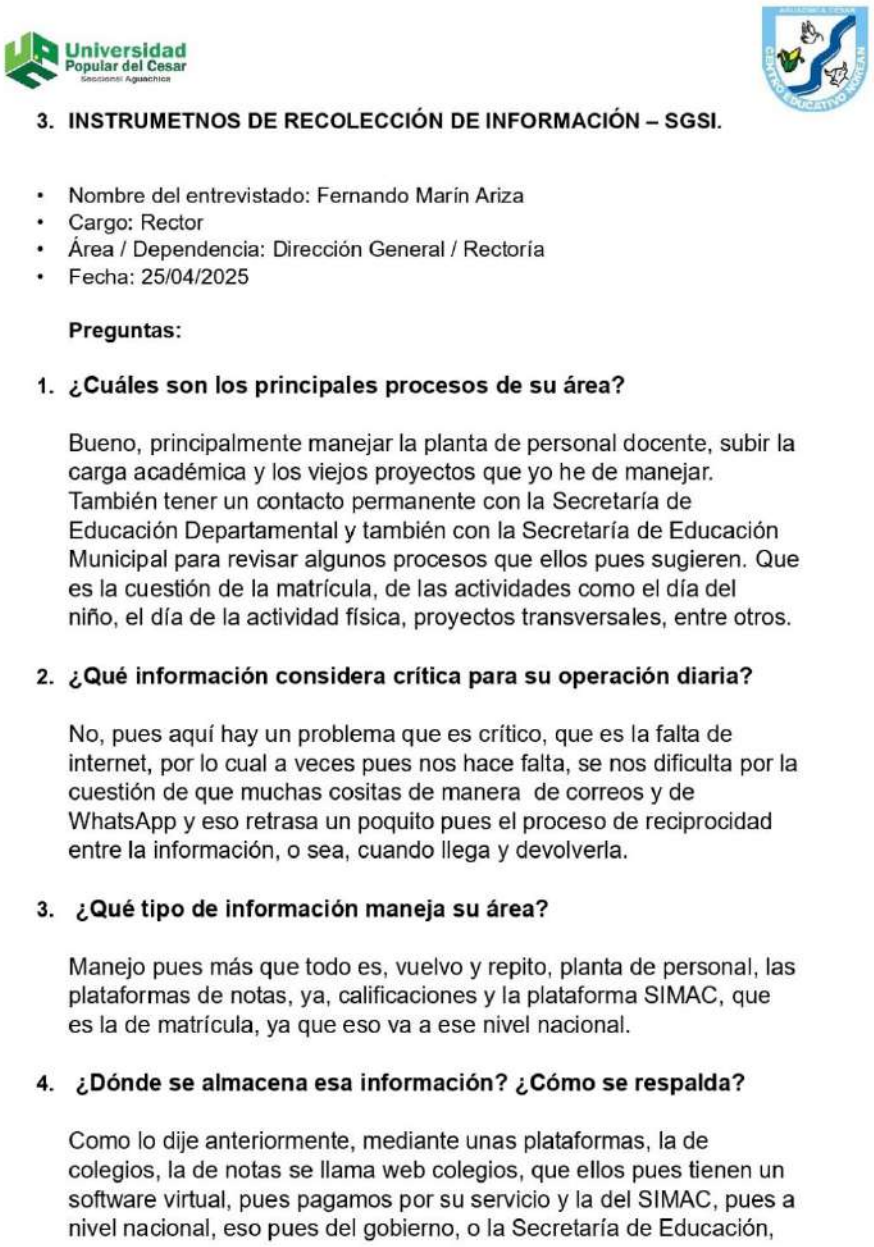
Como parte del proceso de construcción del Sistema de Gestión de Seguridad de la Información (SGSI) para el Centro Educativo Norean del municipio de Aguachica, Cesar, se ha diseñado una serie de entrevistas dirigidas al personal de distintas áreas de la institución. Estas entrevistas tienen como propósito recolectar información clave sobre los activos de información, las prácticas actuales de seguridad, los riesgos identificados, y el nivel de conocimiento y compromiso del personal frente a la protección de la información.

La recolección de esta información permitirá realizar un diagnóstico detallado de la situación actual, identificar vulnerabilidades y establecer las bases necesarias para la implementación de políticas, controles y procedimientos que fortalezcan la seguridad de la información conforme a los requisitos de la norma ISO 27001. La participación activa y sincera de los entrevistados es fundamental para el éxito de este proyecto.

Fuente: *los autores.*

Anexo 3 Primera entrevista al señor Rector (Fernando Marín Ariza).

Entrevista 01. Objetivo: Obtener información detallada y contextual sobre los activos utilizados en el centro Educativo Norean.



Universidad Popular del Cesar
Seccional Aguachica

3. INSTRUMETNOS DE RECOLECCIÓN DE INFORMACIÓN – SGSI.

- Nombre del entrevistado: Fernando Marín Ariza
- Cargo: Rector
- Área / Dependencia: Dirección General / Rectoría
- Fecha: 25/04/2025

Preguntas:

1. **¿Cuáles son los principales procesos de su área?**

   Bueno, principalmente manejar la planta de personal docente, subir la carga académica y los viejos proyectos que yo he de manejar. También tener un contacto permanente con la Secretaría de Educación Departamental y también con la Secretaría de Educación Municipal para revisar algunos procesos que ellos pues sugieren. Que es la cuestión de la matrícula, de las actividades como el día del niño, el día de la actividad física, proyectos transversales, entre otros.

2. **¿Qué información considera crítica para su operación diaria?**

   No, pues aquí hay un problema que es crítico, que es la falta de internet, por lo cual a veces pues nos hace falta, se nos dificulta por la cuestión de que muchas cositas de manera de correos y de WhatsApp y eso retrasa un poquito pues el proceso de reciprocidad entre la información, o sea, cuando llega y devolverla.

3. **¿Qué tipo de información maneja su área?**

   Manejo pues más que todo es, vuelvo y repito, planta de personal, las plataformas de notas, ya, calificaciones y la plataforma SIMAC, que es la de matrícula, ya que eso va a ese nivel nacional.

4. **¿Dónde se almacena esa información? ¿Cómo se respalda?**

   Como lo dije anteriormente, mediante unas plataformas, la de colegios, la de notas se llama web colegios, que ellos pues tienen un software virtual, pues pagamos por su servicio y la del SIMAC, pues a nivel nacional, eso pues del gobierno, o la Secretaría de Educación,

Fuente: *los autores.*

Anexo 3. (Continuación)

Primera entrevista al señor Rector

pues lo tiene a disposición de cada uno de los colegios de la nación, no solamente del departamento, del municipio y no de la nación.

5. **¿Qué aplicaciones utiliza para realizar sus tareas?**

   Word, Excel, PowerPoint, más que todas esas tres.

6. **¿Es software institucional, propio o externo (en la nube)?**

   Es externo en la nube.

7. **¿Qué equipos tecnológicos están asignados a su área?**
   computadores, videobi, tableros electrónicos también

8. **¿Hay servidores, equipos de red u otros dispositivos relevantes?**

   Hay uno, pero no es muy bueno el servicio, es satelital, pero no. Lo arreglan y dura dos días el servicio.

9. **¿Dependen de servicios externos (internet, hosting, correo, etc.)?**

   Sí, el correo, WhatsApp.

10. **¿Qué sucede si ese servicio se interrumpe?**
    Lo que está pasando, el problema de la comunicación, Estamos tratando de comprar uno, pero ha habido dificultades.
11. **¿Quiénes tienen acceso a la información crítica?**
    Yo y un docente.
12. **¿Reciben capacitación en seguridad de la información?**
    No, hasta ahora escucho eso.
13. **¿Existen manuales o políticas que regulen el uso de la información?**
    Como tal, no. Se supone que debería haber uno, pero no lo tenemos.
14. **¿Dónde se encuentran y quién los gestiona?**
    Como tal, no hay.

Fuente: *los autores.*

Anexo 4 Segunda entrevista al señor Rector

ENTREVISTA DE DIAGNÓSTICO INICIAL SOBRE SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Conocer el estado actual de la gestión de la seguridad de la información en el Centro Educativo Norean.

- Nombre del entrevistado: Fernando Marín Ariza
- Cargo: Rector
- Área / Dependencia: Dirección General / Rectoría
- Fecha: 25/04/2025

Preguntas:

1. ¿Qué importancia tiene la información en su área para el cumplimiento de las funciones diarias?

   A ver, es muy importante pues sobre todo las dos plataformas, la que es de nota y la que es de matrícula porque nos mantienen informados o nos mantenemos al día con lo que es en la cuestión de notas pues con las calificaciones de los estudiantes los padres de familia pueden también averiguar y mirar su nota en la plataforma de los colegios y el profesor constantemente está subiendo sus calificaciones y sus actividades. En cuanto a la ELSIMA pues tenemos una relación constante con el ministerio y con la secretaría de cuántos niños tenemos, cuántos se han retirado, cuántos se han desertado y cuántos se han matriculado en cada uno de los grados.

2. ¿Cómo se maneja actualmente la protección de información en su área?

   Pues eso nos dan un usuario una contraseña que se cambia más o menos cada tres meses.

3. ¿Existen procedimientos para el manejo de información confidencial?

   Puede ser, sí, claro. Sí, sí. Y en el caso por ejemplo de los archivos de la institución pues solamente se le entregan al que firmo la matrícula, en el caso de las carpetas y eso, solamente, no se le entregan al tercero.

4. ¿Qué tipo de incidentes de seguridad han ocurrido en los últimos años?

   Bueno soy nuevo en este colegio, pero si se robaron dos ventiladores

5. ¿Cómo se responde ante un incidente que compromete la información?

   No, a mí me corcho porque no me ha pasado ningún tipo de incidente

6. ¿Cuenta su área con respaldos periódicos de información? ¿Con qué frecuencia?

Fuente: *los autores.*

Anexo 4. (Continuacíon)

Segunda entrevista al señor Rector.

¿Con respaldos? Pues sí, vuelvo y le repito, tenemos una plataforma que ya está en una nube y nos guardan toda la información. ¿Y cada cuanto hacen como una copia de seguridad de esa información? Cada año.

7. ¿Quién define las políticas o lineamientos de seguridad en su dependencia?

   Si, yo como director.

8. ¿Qué barreras o dificultades enfrenta para proteger la información?

   Ninguna

9. ¿Se han realizado auditorías o revisiones internas sobre seguridad de información?

   No

10. ¿Qué mejoras considera necesarias en el tratamiento de la información?

    ¿Mejoras? Pues no sé, creo yo. Pues como no tenemos un proceso en ese tema, en esa rama, la verdad no sabría decirle nada. Podría ser como tener un manual de seguridad de información. Ah, sí, como hacer un manualcito.O hacer como una capacitación a los docentes y al área administrativa sobre eso.

Fuente: *los autores.*

Anexo 5 Tercera entrevista al señor Rector

ENTREVISTA TÉCNICA SOBRE ACTIVOS DE INFORMACIÓN Y RIESGOS.

Objetivo: Identificar activos de información, su valor, y riesgos asociados.

- Nombre del entrevistado: Fernando Marín Ariza
- Cargo: Rector
- Área / Dependencia: Dirección General / Rectoría
- Fecha: 25/04/2025

Preguntas:

1. ¿Cuáles son los principales activos de información que maneja su área?

   Lo que es esto, certificado de notas, especialmente certificado de notas y las matrículas de los estudiantes en cada uno de los grados y las sedes.

2. ¿Dónde se almacenan físicamente y lógicamente esos activos?

   No, físicamente no están. Hasta el año 2023 se entregaron un libro, inclusive no lo entregaron, Pero están en una nube de los archivos, pero sí se entregaron físicamente, pero no lo entregaron. Pero ahorita los almacenan en toda la nube.

3. ¿Se realiza respaldo de la información? ¿Qué método se utiliza?

   Pues se paga por el servicio.

4. ¿Quiénes tienen acceso a los activos de información críticos?

   El rector y el profesor.

5. ¿Se utiliza cifrado o protección especial en los archivos sensibles?

   Los cifrados no. Simple y sencillamente un usuario y una contraseña, uno sube y baja el archivo.

6. ¿Qué tipo de amenazas internas o externas identifica sobre los activos?

   No, en este momento no.

7. ¿Con qué frecuencia se actualizan los equipos o software que contienen información?

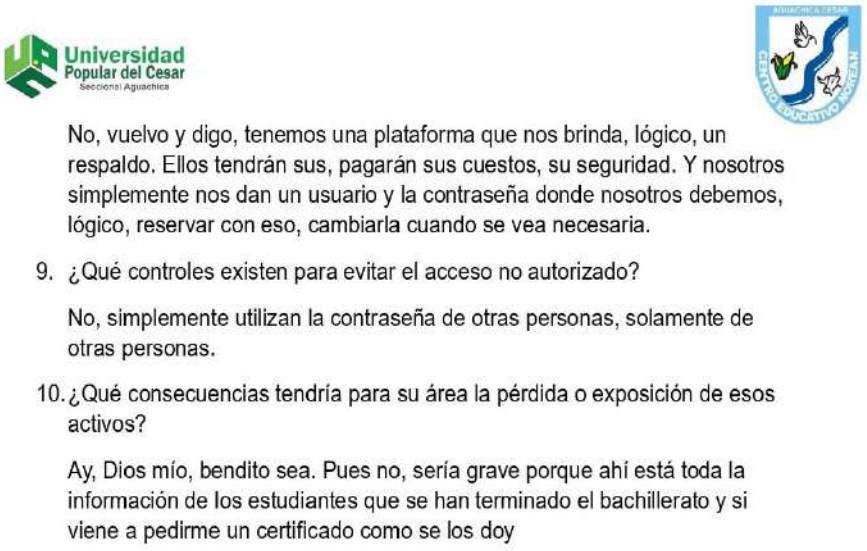
   No, no tenemos un programa de actualización de los equipos, la verdad.Sí, cada año. Legalmente es cada año, le va a hacer mantenimiento.

8. ¿Cómo se asegura la integridad de la información (evitar alteraciones no autorizadas)?

Fuente: *los autores.*

Anexo 5. (Continuación)

Tercera entrevista al señor Rector



No, vuelvo y digo, tenemos una plataforma que nos brinda, lógico, un respaldo. Ellos tendrán sus, pagarán sus cuestos, su seguridad. Y nosotros simplemente nos dan un usuario y la contraseña donde nosotros debemos, lógico, reservar con eso, cambiarla cuando se vea necesaria.

9. ¿Qué controles existen para evitar el acceso no autorizado?

   No, simplemente utilizan la contraseña de otras personas, solamente de otras personas.

10. ¿Qué consecuencias tendría para su área la pérdida o exposición de esos activos?

    Ay, Dios mío, bendito sea. Pues no, sería grave porque ahí está toda la información de los estudiantes que se han terminado el bachillerato y si viene a pedirme un certificado como se los doy

Fuente: *Los autores*

Anexo 6 Cuarta entrevista al señor Rector

ENTREVISTA SOBRE CONCIENCIA Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Evaluar el nivel de conocimiento y conciencia del personal sobre seguridad de la información.

- Nombre del entrevistado: Fernando Marín Ariza
- Cargo: Rector
- Área / Dependencia: Dirección General / Rectoría
- Fecha: 25/04/2025

Preguntas:

1. ¿Ha recibido capacitación formal sobre seguridad de la información?

   Como tal, no. Solamente de archivo. ¿De archivo? De archivo, que vamos a dar más archivar, que ya se debe archivar y ya no se debe guardar más.

2. ¿Conoce las políticas internas de protección de datos del Centro Educativo Norean?

   No.

3. ¿Cuáles son las principales amenazas de seguridad de información que conoce?

   No, pero tengo entendido que virus, pues, virus informáticos que por equipo ya abrieron un enlace, entonces pueden afectar o dañar los equipos o borrar la información.

4. ¿Qué medidas personales toma para proteger la información en su trabajo diario?

   No, meterme en lo que no conozco y no abrir todas las cosas que le llegan a uno que no conoce de dónde viene.

5. ¿Sabe identificar un correo electrónico o archivo sospechoso?

   Pues sí, al no ser una persona que uno no conozca ni nada de esas cosas. Normalmente se usa el correo institucional es aparte, ahí solamente llegan las cosas de la institución. Nada más, No llegan, no se reciben cosas de otro sitio

6. ¿Cómo protegería información confidencial en caso de trabajar fuera de la institución?

   Pues no, porque siempre uno carga el equipo para lado y lado. La seguridad va en el computador o a través del computador.

Fuente: Los autores

Anexo 6.(Continuación)

Cuarta entrevista al señor Rector

Universidad Popular del Cesar
Seccional Aguachica

7. ¿Con qué frecuencia cambia sus contraseñas de acceso?

   Esa es la que más se cambia, la del SIMAC es cada tres meses. Cada tres meses.

8. ¿Sabe a quién reportar un incidente de seguridad (pérdida de datos, acceso indebido)?

   Ni idea.

9. ¿Qué tan fácil o difícil le resulta aplicar las buenas prácticas de seguridad en su trabajo?

   Pues fácil no lo veo, es que no las aplicamos. Simple y sencillamente uno lo hace como empíricamente, lo que uno sabe, lo que uno hace por las redes, lo que uno ve que le dicen, no haga esto, no haga esto,

10. ¿Qué recomendaciones o sugerencias daría para mejorar la seguridad de la información en la institución?

    Bueno, yo creo que una capacitación para uno pues para tener conocimiento de eso y de qué tipo de riesgos hay y cómo lo pueden afectar a uno, porque uno la verdad no sabemos que hay virus, pero no nos han enseñado qué es lo que pasa y cómo es que se puede contraer.

Fuente: *los autores.*

Anexo 7 Entrevista al Docente de Primaria (Juan Barraza)

5. **¿Qué aplicaciones utiliza para realizar sus tareas?**

   Los tres, el Word, el CED y PowerPoint.
6. **¿Es software institucional, propio o externo (en la nube)?**

   Es externo en la nube, Sí, en el Google Drive, pues externo como tal, no, porque Google Drive nos permite tener un acceso propio y predeterminado. Nosotros tenemos acceso a ese, pero sin embargo es de ellos, es un servidor prácticamente.

7. **¿Qué equipos tecnológicos están asignados a su área?**
   Los computadores y el videobi.

8. **¿Hay servidores, equipos de red u otros dispositivos relevantes?**

   Pues hay un servidor, pero no sirve.
9. **¿Dependen de servicios externos (internet, hosting, correo, etc.)?**

   Sí, el internet Y tenemos, el año pasado tuvimos una licencia con CloudLabs, pues tenemos laboratorios virtuales, pero cuando no tenemos acceso a internet, los computadores están ahí con los laboratorios en nada.

10. **¿Qué sucede si ese servicio se interrumpe?**

    Pues como no hay servicio, pues no se tiene internet y es lo que está pasando ahora. Es lo que pasa estamos limitados en nuestro conocimiento.

11. **¿Quiénes tienen acceso a la información crítica?**
    El rector y mi persona junto con los otros.

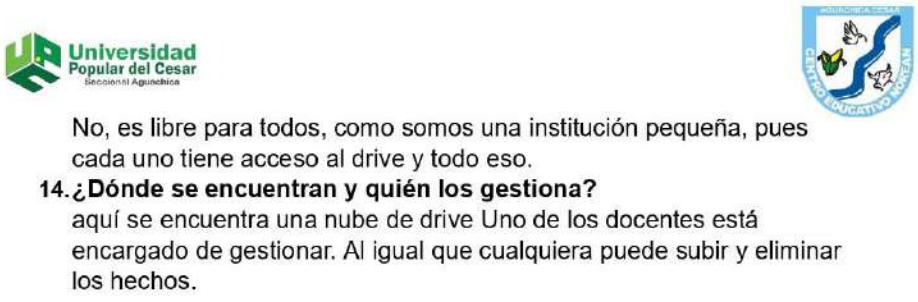
12. **¿Reciben capacitación en seguridad de la información?**
    No.

13. **¿Existen manuales o políticas que regulen el uso de la información?**

Fuente: *los autores.*

Anexo 7. (Continuación)

Entrevista al docente de primaria.



No, es libre para todos, como somos una institución pequeña, pues cada uno tiene acceso al drive y todo eso.

14. **¿Dónde se encuentran y quién los gestiona?**
aquí se encuentra una nube de drive Uno de los docentes está encargado de gestionar. Al igual que cualquiera puede subir y eliminar los hechos.

Fuente: Los autores

Anexo 7. (Continuación)

Entrevista al docente de primaria.

Universidad Popular del Cesar
Seccional Aguachica

3. INSTRUMETNOS DE RECOLECCIÓN DE INFORMACIÓN – SGSI.

- Nombre del entrevistado: Juan
- Cargo: Profesor
- Área / Dependencia: Docente de Informática en Educación Primaria
- Fecha: 25/04/2025

Preguntas:

1. **¿Cuáles son los principales procesos de su área?**

   Como estoy en la básica primaria, pues lo principal es que los estudiantes aprendan el funcionamiento de lo que es la parte ofimática. Para el caso de los estudiantes de primaria, como apenas están adiestrándose, están en parte de sensibilización con lo que es la computación, lo primordial es que ellos aprendan la seguridad con información en cuanto a cómo encender el computador, cómo guardar un archivo, qué tiene que ver con la información que ellos realizan, los trabajos y demás. Muy importante es la parte del procesador de texto, de Word, porque es uno de los, digamos, de los principales o del eje fundamental de la informática para que los estudiantes realicen escritos, cartas, informaciones y demás.
2. **¿Qué información considera crítica para su operación diaria?**

   Operación, o sea, para el desarrollo de las clases. Sí, sería, pues el internet. Sí, uno de los, de los, sí, el internet. Sin embargo, pues como docente desde ahora, pues he utilizado otra estrategia, lo que es el caso de utilizar herramientas ofimáticas, offline, perdón, como el caso de los, de los paquetes de Microsoft y de Colombia Red
3. **¿Qué tipo de información maneja su área?**

   Como te digo, he recorrido información que tenga que ver más que todo con la parte offline, tiene que ver el procesador de texto de Word, PowerPoint, el CED y las cápsulas de Colombia Aprende
4. **¿Dónde se almacena esa información? ¿Cómo se respalda?**

   En las clases de informática, pues se le han enseñado a los estudiantes a cómo guardar archivos, como son, como son los paquetes de Microsoft, pues esto es lo que permite el explorador de texto guardar, copiar y almacenar archivos.

Anexo 7. (Continuación)

ENTREVISTA DE DIAGNÓSTICO INICIAL SOBRE SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Conocer el estado actual de la gestión de la seguridad de la información en el Centro Educativo Norean.

- Nombre del entrevistado: Juan
- Cargo: Profesor
- Área / Dependencia: Docente de Informática en Educación Primaria
- Fecha: 25/04/2025

Preguntas:

1. ¿Qué importancia tiene la información en su área para el cumplimiento de las funciones diarias?

   Es importante que los estudiantes, entre compañeros y con los estudiantes se manejen la información para que logremos los objetivos que se crean en el área o a nivel institucional.

2. ¿Cómo se maneja actualmente la protección de información en su área?

   Por medio de Google Drive, los estudiantes utilizan la nube para subir información. Asimismo, por medio de memorias, en este caso USB.

3. ¿Existen procedimientos para el manejo de información confidencial?

   No.

4. ¿Qué tipo de incidentes de seguridad han ocurrido en los últimos años?

   Digamos, no de inseguridad. Más que todo de desconocimiento. Algunos compañeros han sucedido con el Google Drive que por error o equivocación, eliminan algunos archivos de otros compañeros en la opción de eliminar, porque todos tenemos acceso a la información.

5. ¿Cómo se responde ante un incidente que compromete la información?

   Con un plan b que seria la memoria USB que si se elimino el archivo se puede subir de nuevo.

6. ¿Cuenta su área con respaldos periódicos de información? ¿Con qué frecuencia?

   Por periodo, cada tres meses

7. ¿Quién define las políticas o lineamientos de seguridad en su dependencia?

   Independientes, somos autónomos en ese sentido

8. ¿Qué barreras o dificultades enfrenta para proteger la información?

   Pues primero el internet, porque como no tenemos internet aquí, no tenemos acceso a subirlo de forma inmediata a la nube, entonces tenemos que llegar a la casa, o a veces se nos puede eliminar la información cuando son documentos en línea

9. ¿Se han realizado auditorías o revisiones internas sobre seguridad de información?

   No

10. ¿Qué mejoras considera necesarias en el tratamiento de la información?

    Yo digo que una de las mejoras es más que todo el servidor que se está utilizando, pues porque Google Drive no es tan efectivo a la hora de guardar información.

Fuente: *los autores.*

Entrevista 03.

ENTREVISTA TÉCNICA SOBRE ACTIVOS DE INFORMACIÓN Y RIESGOS.

Objetivo: Identificar activos de información, su valor, y riesgos asociados.

- Nombre del entrevistado: Juan
- Cargo: Profesor
- Área / Dependencia: Docente de Informática en Educación Primaria
- Fecha: 25/04/2025

Preguntas:

1. ¿Cuáles son los principales activos de información que maneja su área?

   Sí, el portátil, el videobi, que es el reproductor de audio, también, y el televisor digital.

2. ¿Dónde se almacenan físicamente y lógicamente esos activos?

   Hay unos que son personales, en el caso de los docentes, cada uno tiene uno personal y para los estudiantes, tenemos una maleta, un maletín, donde se depositan todos esos elementos, lo que son el televisor digital, puesto en la sala de informática, todo eso y todo lo que haya guardado en la sala de informática.

3. ¿Se realiza respaldo de la información? ¿Qué método se utiliza?

   Pues cada docente maneja su propia información y si queremos, por ejemplo, en el caso del rector, que es el encargado de revisar la información de los demás, pues él se va al drive, pues cada uno monta la información. Básicamente, montamos lo que queremos que él vea.

4. ¿Quiénes tienen acceso a los activos de información críticos?

   El rector.

5. ¿Se utiliza cifrado o protección especial en los archivos sensibles?

   No.

6. ¿Qué tipo de amenazas internas o externas identifica sobre los activos?

   En el caso de algunos compañeros, ellos pues es de conocimiento para todos de que ellos les suministren la contraseña, y el usuario, digamos, al hijo o al familiar, para que le ayude a subir archivos, porque de pronto lo desconocen, entonces podría ser eso podría ser una amenaza.

7. ¿Con qué frecuencia se actualizan los equipos o software que contienen información?

Fuente: *los autores.*

La verdad es que hace rato que están desactualizados. Incluso hay unos computadores que son Windows 7. Hay unos muy obsoletos. Entonces, ¿no es como cada año? No, no hay periodicidad, No hay un periodo.

8. ¿Cómo se asegura la integridad de la información (evitar alteraciones no autorizadas)?

   No hay un mecanismo que regule esa parte.

9. ¿Qué controles existen para evitar el acceso no autorizado?

   No, pues como te digo, si yo le suministro la contraseña al usuario, a mi hijo o a mi hija, pues él tiene acceso a eso también.

10. ¿Qué consecuencias tendría para su área la pérdida o exposición de esos activos?

    Pues prácticamente, si se pierden los archivos, pues se pierde todo el trabajo. Por eso el rector utilizó el plan B de utilizar unos discos duros, donde se guarda información para en esos casos donde por error o por equivocación se elimine, pues se puedan subir nuevamente.

Fuente: *los autores.*

Entrevista 04.

ENTREVISTA SOBRE CONCIENCIA Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Evaluar el nivel de conocimiento y conciencia del personal sobre seguridad de la información.

- Nombre del entrevistado: Juan
- Cargo: Profesor
- Área / Dependencia: Docente de Informática en Educación Primaria
- Fecha: 25/04/2025

Preguntas:

1. ¿Ha recibido capacitación formal sobre seguridad de la información?

   No.

2. ¿Conoce las políticas internas de protección de datos del Centro Educativo Norean?

   No.

3. ¿Cuáles son las principales amenazas de seguridad de información que conoce?

   Pueden ser como virus, maliciosos, o cuando se descarga algún archivo más que todo cuando descargamos, como somos docentes, pues estamos en internet siempre buscando recursos, y a veces como no sabemos cuáles son las fuentes conflictuales de descarga, pues podemos caer en no tanto por, digamos, a propósito, sino que nada más por descargar un recurso podemos pecar en descargar un virus.

4. ¿Qué medidas personales toma para proteger la información en su trabajo diario?

   Una de las medidas es actualizar el disco duro, es decir, tener dos reservas de información, una en el computador oficial y otra en un disco aparte extraído

5. ¿Sabe identificar un correo electrónico o archivo sospechoso?

   Si.

6. ¿Cómo protegería información confidencial en caso de trabajar fuera de la institución?

Fuente: *los autores.*

Utilizando una cuenta de Google Drive, pero que sea del colegio, o sea, protegiéndola con él, no sé cómo le llamarían eso que en el momento de compartir, pues solo compartir en privado, exactamente, solo tener acceso. Acceso privado.

7. ¿Con qué frecuencia cambia sus contraseñas de acceso?

   Cada dos o tres años.

8. ¿Sabe a quién reportar un incidente de seguridad (pérdida de datos, acceso indebido)?

   No.

9. ¿Qué tan fácil o difícil le resulta aplicar las buenas prácticas de seguridad en su trabajo?

   Pues después de que las conozca, muy fácil.

10. ¿Qué recomendaciones o sugerencias daría para mejorar la seguridad de la información en la institución?

    Pues aquí en la institución, de que los compañeros, pues aprendan primeramente a manejar lo que son los sistemas de la información, porque hay unos, digamos que son por su edad, y eso pues desconocen muchas partes de mi lógica. Pero sería bueno que cada uno manejara un Drive personal con su contraseña, y hacer uso de unas contraseñas seguras. Como el caso de cambiar contraseñas con un tiempo mucho más corto.

Fuente: *los autores.*

Anexo 8 Entrevista al Docente de Bachillerato (José Luis Zafra Duarte)

Entrevista 01

Fuente: *los autores.*

Universidad Popular del Cesar Seccional Aguachica	**CONSTRUCCIÓN DE UN SISTEMA DE GESTÍON DE SEGURIDAD DE LA INFORMACION ALINEADO A LA NORMA ISO 27001 PARA EL CENTRO EDUCATIVO NOREAN DE AGUACHICA CESAR.**	
	FORMATO: ENTREVISTA SEMIESTRUCTURADA	
	FECHA: 28 ABRIL 2025	**Página 3 de 11**

4.1 ENTREVISTA DE ACTIVOS UTILIZADOS DENTRO DEL AREA DEPENDIENTE.

- **Nombre del entrevistado**: José Luis Zafra Duarte
- **Cargo**: Docente de Bachillerato
- **Área / Dependencia:** Sala de informática

INTERROGANTES:

a) ¿Cuáles son los principales procesos de su área?

Docencia y coordinación de proyectos transversales (ambientales, democraciaticos), proyectos de ciencias naturales y tecnología, manejo del SIMAC, matrículas para estudiantes nuevos, observación y comportamiento.

b) ¿Qué información considera crítica para su operación diaria?

El manejo de guías de trabajo desde Google Drive y la proyección de presentaciones y videos.

c) ¿Qué tipo de información maneja su área?

Planes de asignatura, listas de asistencia y planillas de notas.

d) ¿Dónde se almacena esa información? ¿Cómo se respalda?

Se almacena de forma física y digital, esta última desde una plataforma institucional, además de respaldos físicos.

e) ¿Qué aplicaciones utiliza para realizar sus tareas?

Teach, Canva, Correo, Drive, aplicaciones de video y herramientas de Office.

f) ¿Es software institucional, propio o externo (en la nube)?

El software es externo, pero está administrado por docentes y profesores.

g) ¿Qué equipos tecnológicos están asignados a su área?

Computadores portátiles y pantallas inalámbricas.

h) ¿Hay servidores, equipos de red u otros dispositivos relevantes?

Sí, hay algunos dispositivos relevantes.

i) ¿Dependen de servicios externos (internet, hosting, correo, etc.)?

Sí, dependemos del internet para acceder a nuestras tareas, aunque presenta deficiencias en la cobertura.

j) ¿Qué sucede si ese servicio se interrumpe?

Utilizamos recursos propios como respaldo.

k) ¿Quiénes tienen acceso a la información crítica?

Las credenciales de acceso están restringidas al rector y al administrador.

l) ¿Reciben capacitación en seguridad de la información?

No.

m) ¿Existen manuales o políticas que regulen el uso de la información?

No.

n) ¿Dónde se encuentran y quién los gestiona?

No se ha recibido esa información.

Fuente: *los autores.*

Entrevista 02.

Universidad Popular del Cesar Seccional Aguachica	CONSTRUCCIÓN DE UN SISTEMA DE GESTÍON DE SEGURIDAD DE LA INFORMACION ALINEADO A LA NORMA ISO 27001 PARA EL CENTRO EDUCATIVO NOREAN DE AGUACHICA CESAR.	
	FORMATO: ENTREVISTA SEMIESTRUCTURADA	
	FECHA: 28 ABRIL 2025 — Página 5 de 11	

4.2 ENTREVISTA DE DIAGNÓSTICO INICIAL SOBRE SEGURIDAD DE LA INFORMACIÓN.

INTERROGANTES

a) **¿Qué importancia tiene la información en su área para el cumplimiento de las funciones diarias?**

La información es fundamental, ya que manejo notas, asistencias e información de los estudiantes, lo cual es esencial para la gestión académica y el seguimiento del desempeño.

b) **¿Cómo se maneja actualmente la protección de información en su área?**

Se hacen copias de seguridad de la información que se encuentra guardada en línea, principalmente en Google Drive.

c) **¿Existen procedimientos para el manejo de información confidencial?**

No, actualmente no hay procedimientos establecidos para ello.

d) **¿Qué tipo de incidentes de seguridad han ocurrido en los últimos años?**

Durante la pandemia se borró información desde el Drive, el proveedor anterior no entregó la información que tenía, además hubo un incendio que ocasionó la pérdida de archivos físicos.

e) **¿Cómo se responde ante un incidente que compromete la información?**

En general, se intenta recuperar lo que estaba respaldado previamente por el docente, pero no hay un procedimiento formal establecido.

Fuente: *los autores.*

f) **¿Cuenta su área con respaldos periódicos de información y con qué frecuencia?**
Sí, realizo respaldos cada mes.

g) **¿Quién define las políticas o lineamientos de seguridad en su dependencia?**

El rector es quien toma esas decisiones.

h) **¿Qué barreras o dificultades enfrenta para proteger la información?**

Existe una falta de conocimiento u orientación sobre cómo mantener la información segura en línea.

i) **¿Se han realizado auditorías o revisiones internas sobre seguridad de información?**

No, no se han realizado auditorías ni revisiones.

j) **¿Qué mejoras considera necesarias en el tratamiento de la información?**
(No se obtuvo respuesta específica para esta pregunta, pero podría sugerirse incluir capacitación en seguridad digital y creación de procedimientos de respaldo).

Fuente: *los autores.*

Entrevista 03.

Universidad Popular del Cesar Seccional Aguachica	CONSTRUCCIÓN DE UN SISTEMA DE GESTÍON DE SEGURIDAD DE LA INFORMACION ALINEADO A LA NORMA ISO 27001 PARA EL CENTRO EDUCATIVO NOREAN DE AGUACHICA CESAR.	
	FORMATO: ENTREVISTA SEMIESTRUCTURADA	
	FECHA: 28 ABRIL 2025	Página 7 de 11

4.3 ENTREVISTA TÉCNICA SOBRE ACTIVOS DE INFORMACIÓN Y RIESGOS.

INTERROGANTES

a) ¿Cuáles son los principales activos de información que maneja su área?

Manejo información esencial como las notas académicas, registros de asistencia, observadores, calificaciones y datos personales de los estudiantes.

b) ¿Dónde se almacenan físicamente y lógicamente esos activos?

Los documentos físicos se encuentran guardados en la rectoría, mientras que los archivos digitales se almacenan en el Drive y en la plataforma institucional.

c) ¿Se realiza respaldo de la información? ¿Qué método se utiliza?

En la mayoría de los casos, suelo hacer copias de seguridad por mi cuenta, guardando la información en otros espacios digitales para prevenir pérdidas.

d) ¿Quiénes tienen acceso a los activos de información críticos?

En la plataforma solo los autorizados por el administrador

e) ¿Se utiliza cifrado o protección especial en los archivos sensibles?

No utilizo ningún tipo de cifrado ni medidas especiales de protección en los archivos sensibles.

Fuente: *los autores.*

f) ¿Qué tipo de amenazas internas o externas identifica sobre los activos?

Una de las amenazas más evidentes es que cualquier persona podría acceder a la información almacenada en el Drive o en los archivadores, ya que no hay un control riguroso.

g) ¿Con qué frecuencia se actualizan los equipos o software que contienen información?

Los equipos y programas que utilizo suelen actualizarse una vez al año, aunque no siempre es de manera constante.

h) ¿Cómo se asegura la integridad de la información (evitar alteraciones no autorizadas)?

No cuento con un proceso claro o definido para asegurar la integridad de la información, lo que representa una debilidad en el manejo de los datos.

i) ¿Qué controles existen para evitar el acceso no autorizado?

En la plataforma, el acceso está restringido únicamente a quienes son autorizados por el administrador. En el caso de los documentos físicos, se guardan bajo llave en la rectoría.

j) ¿Qué consecuencias tendría para su área la pérdida o exposición de esos activos?

La pérdida o exposición de esta información generaría retrasos significativos, ya que implicaría rehacer informes semanales y mensuales, afectando directamente el desarrollo de las actividades.

Fuente: *los autores.*

Entrevista 04.

Universidad Popular del Cesar Seccional Aguachica	CONSTRUCCIÓN DE UN SISTEMA DE GESTÍON DE SEGURIDAD DE LA INFORMACION ALINEADO A LA NORMA ISO 27001 PARA EL CENTRO EDUCATIVO NOREAN DE AGUACHICA CESAR.	
	FORMATO: ENTREVISTA SEMIESTRUCTURADA	
	FECHA: 28 ABRIL 2025	Página 9 de 11

4.4 ENTREVISTA SOBRE CONCIENCIA Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

INTERROGANTES

a) **¿Ha recibido capacitación formal sobre seguridad de la información?**

No, hasta el momento no he recibido ninguna capacitación formal relacionada con la seguridad de la información.

b) **¿Conoce las políticas internas de protección de datos del Centro Educativo Norean?**

No tengo conocimiento de que existan políticas internas específicas sobre la protección de datos dentro del Centro Educativo.

c) **¿Cuáles son las principales amenazas de seguridad de información que conoce?**

Considero que una de las principales amenazas es que la información no se encuentra en un sitio seguro, lo que permite que cualquier persona pueda acceder fácilmente a ella.

d) **¿Qué medidas personales toma para proteger la información en su trabajo diario?**

Generalmente hago copias de seguridad de la información, tanto en formato físico como digital, para asegurarme de tener respaldo en caso de pérdida o daño.

e) **¿Sabe identificar un correo electrónico o archivo sospechoso?**

No tengo conocimientos claros sobre cómo identificar correos o archivos sospechosos, lo cual es una limitación en temas de seguridad.

Fuente: *los autores.*

f) **¿Cómo protegería información confidencial en caso de trabajar fuera de la institución?**

Cuando trabajo fuera de la institución, procuro utilizar el mismo computador de siempre y trato de trabajar en línea sin recurrir a información impresa o física.

g) **¿Con qué frecuencia cambia sus contraseñas de acceso?**

No suelo cambiar mis contraseñas con frecuencia, ya que no tengo el hábito ni la costumbre de hacerlo regularmente.

h) **¿Sabe a quién reportar un incidente de seguridad (pérdida de datos, acceso indebido)?**

No tengo claro el protocolo de reporte, por lo general, si ocurre algo relacionado con seguridad, lo informo directamente al rector.

i) **¿Qué tan fácil o difícil le resulta aplicar las buenas prácticas de seguridad en su trabajo?**

Me resulta complicado aplicarlas, ya que tengo conocimientos básicos sobre el tema y a veces no sé por dónde empezar.

j) **¿Qué recomendaciones o sugerencias daría para mejorar la seguridad de la información en la institución?**

Considero que sería útil implementar otra herramienta distinta al Drive para almacenar la información, y además capacitar al personal en buenas prácticas que fortalezcan la integridad y seguridad de los datos.

Anexo 9 Lista de asistencia de Docentes.

AUDITORÍA INTERNA EN EL CENTRO EDUCATIVO NOREAN

Fecha : 8 de Abril del 2025

Responsables: Doris Natalia Bautista Romero / Paula Andrea Garnica Molinares

N.°	Nombre del Docente	Cargo	Firma
1	Juan Alberto Alvarez B.	Docente	
2	EMILIO NIZ ARIAS	Docente	
3	Claudia Ramones	Docente	
4	Jesús Lizcano Poveda	Docente	
5	José Luis Zafra O.	Docente	
6	Martin Galeza G.	Docente	
7	Javier A Carranza L	Docente	Javier Carranza
8	M. Alejandra Vanegas Rivero	docente	
9	Fernando Mora M	Rector	

CAPACITACION BUENAS PRACTICAS EN LA SEGURIDAD DE LA INFORMACIÓN

Fecha : 6 de Junio del 2025

Responsables: Doris Natalia Bautista Romero / Paula Andrea Garnica Molinares

N.°	Nombre del Docente	Cargo	Firma
1	Juan Alberto Alvarez B.	Docente	
2	EMILIO DIAZ ARIAS	Docente	
3	Claudia Quiñones	Docente	
4	Jesús Lizcano Posada	Docente	
5	José Luis Zafra	Docente	
6	Martin Galeza G.	Docente	
7	Javier A. Carranza leon	Docente	JavierCarranza
8	M. Alejandra Vanegas R.	Docente	
9	Fernando Murcia A	Rector	

Universidad

ELABORACIÓN DEL INFORME DE RIESGOS Y PROPUESTA DOCUMENTAL

Fecha : 17 de Septiembre del 2025

Responsables: Doris Natalia Bautista Romero / Paula Andrea Garnica Molinares

N.°	Nombre del Docente	Cargo	Firma
1	Juan Alvarez Barraza	Docente	
2	EMILIO NIZARIAS	Docente	
3	Claudia Ramos	Docente	
4	Jesus Lizcano Poveda	Docente	
5	José Luis Zafra Ovalle	Docente	
6	Martin Galeano G	Docente	
7	Javier A Carrascal	Docente	Javier Carrascal
8	M. Alejandra Venegas R.	Docente	
9	Fernando Ibarra A	Rector	

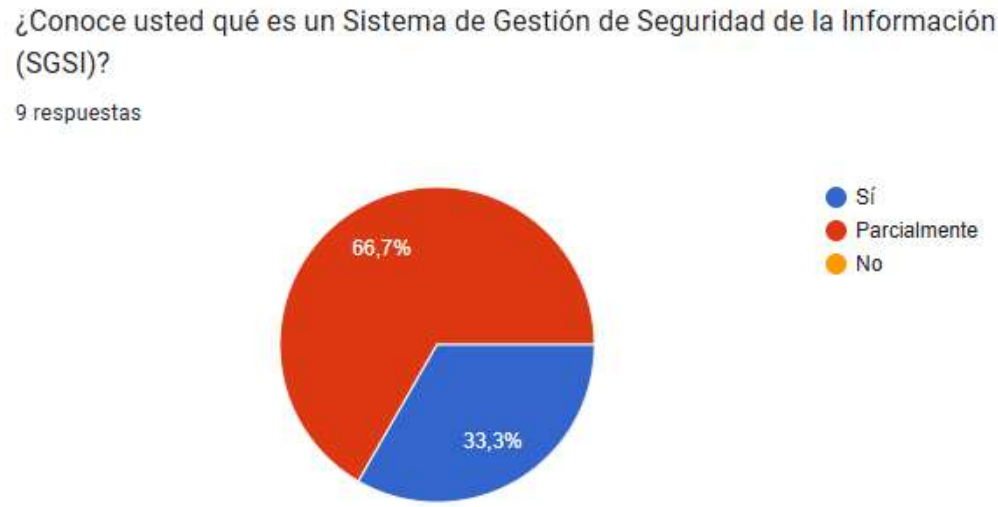
Anexo 10 Encuesta sobre percepción y prácticas de seguridad de la información en el Centro Educativo Norean.

Objetivo de la encuesta:

Evaluar el nivel de conocimiento, percepción institucional y satisfacción frente a la capacitación recibida sobre buenas prácticas de seguridad de la información.

Resultados e interpretación:

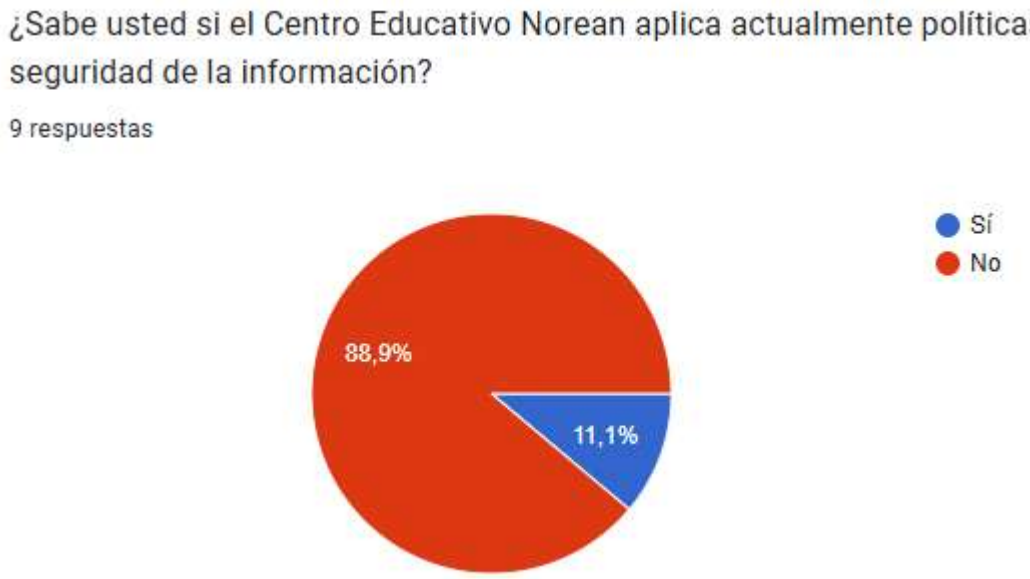
1. ¿Conoce usted qué es un Sistema de Gestión de Seguridad de la Información (SGSI)?



Fuente el autor.

Análisis:
La mayoría de los encuestados (66,7%) tienen solo un conocimiento parcial del concepto de SGSI, lo cual refleja la necesidad de profundizar en capacitaciones. Sin embargo, un 33,3% ya conoce el término, lo que constituye una base para fortalecer la cultura institucional en seguridad de la información.

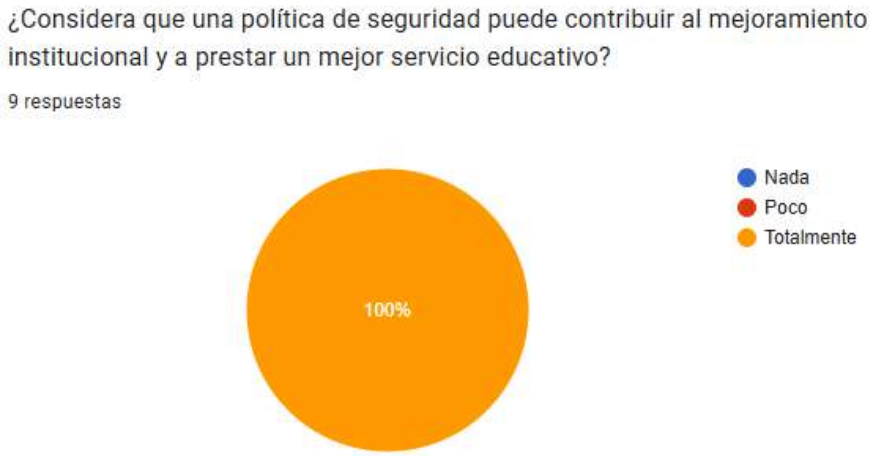
2. ¿Sabe usted si el Centro Educativo Norean aplica actualmente políticas de seguridad de la información?



Fuente el autor.

Análisis:
Existe una percepción generalizada (88,9%) de que en el colegio no se aplican políticas de seguridad de la información. Esto evidencia una brecha importante entre la normativa y la práctica, reforzando la urgencia de implementar un SGSI formal en la institución.

3. ¿Considera que una política de seguridad puede contribuir al mejoramiento institucional y a prestar un mejor servicio educativo?



Fuente el autor.

Análisis:

El consenso es absoluto: todos los encuestados reconocen que la política de seguridad fortalece la institución y mejora la calidad del servicio educativo. Este resultado es positivo porque asegura la aceptación institucional para la implementación del SGSI.

4. ¿En su labor diaria aplica prácticas como el uso seguro de contraseñas, respaldo de información o manejo responsable de datos personales?

Fuente el autor.

Análisis:

Más de la mitad (55,6%) aplican prácticas seguras, aunque un 33,3% lo hace solo de forma ocasional y un 11,1% no las aplica. Esto demuestra que, aunque existen buenas prácticas, aún hay debilidades en la constancia y disciplina digital que deben ser abordadas con capacitaciones y controles.

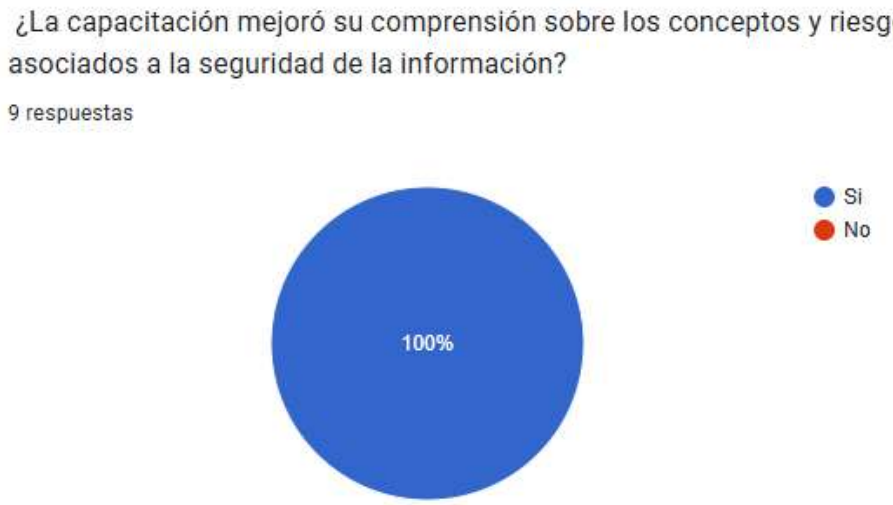
5. ¿Qué tan preparado considera que está el personal de la institución para enfrentar incidentes que afecten la seguridad de la información?

Fuente el autor.

Análisis:

El 88,9% del personal considera que está poco o nada preparado para enfrentar incidentes de seguridad. Esto constituye un riesgo alto para la institución, pues ante un ataque o pérdida de datos, la reacción sería limitada. Se evidencia la necesidad de protocolos de actuación e instrucción técnica al personal.

6. ¿La capacitación mejoró su comprensión sobre los conceptos y riesgos asociados a la seguridad de la información?

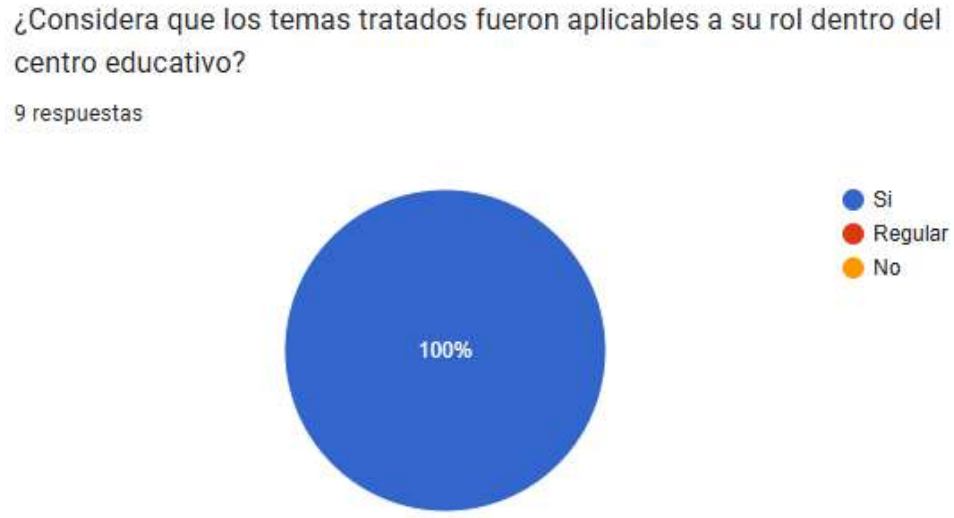


Fuente el autor.

Análisis:

Todos los participantes afirman que la capacitación recibida mejoró su comprensión, lo cual valida la efectividad de los procesos de sensibilización realizados en el colegio. Esto muestra que la capacitación es un medio clave para cerrar las brechas detectadas en preguntas anteriores.

7. ¿Considera que los temas tratados fueron aplicables a su rol dentro del centro educativo?



Fuente el autor.

Análisis:

El 100% de los encuestados considera que la capacitación fue aplicable a sus funciones dentro del

colegio. Esto significa que el diseño de los contenidos fue pertinente y tuvo ***impacto práctico*** *en la comunidad educativa.*

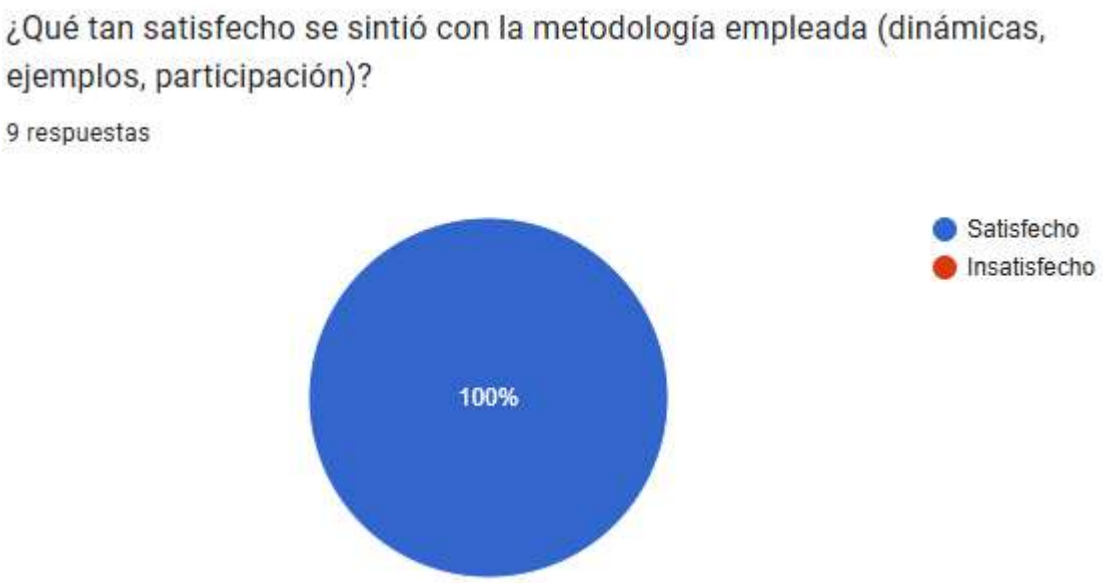
8. ¿Cómo califica la claridad y organización del contenido presentado?

Fuente el autor.

Análisis:

El 100% de los encuestados calificó la claridad y organización del contenido como excelente. Esto refleja que la capacitación estuvo estructurada de manera ordenada, comprensible y acorde a las necesidades de los participantes, generando una percepción positiva en todos los asistentes.

9. ¿Qué tan satisfecho se sintió con la metodología empleada (dinámicas, ejemplos, participación)?

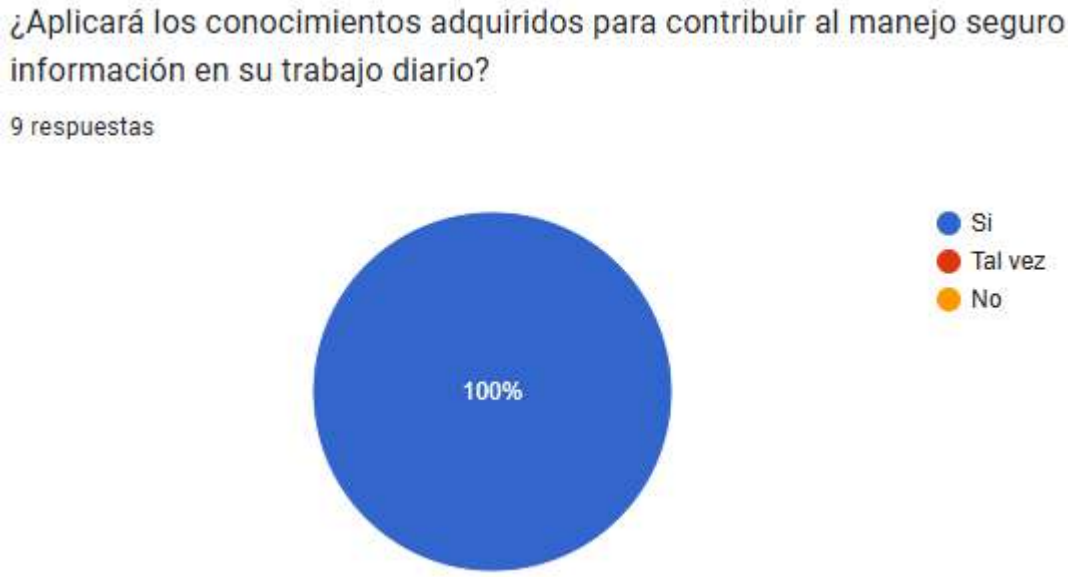


Fuente el autor.

Análisis:

La totalidad de los participantes manifestó estar satisfechos con la metodología utilizada. Esto evidencia que las dinámicas, ejemplos y espacios de participación fueron efectivos para lograr la comprensión y el interés en la capacitación.

10. ¿Aplicará los conocimientos adquiridos para contribuir al manejo seguro de la información en su trabajo diario?

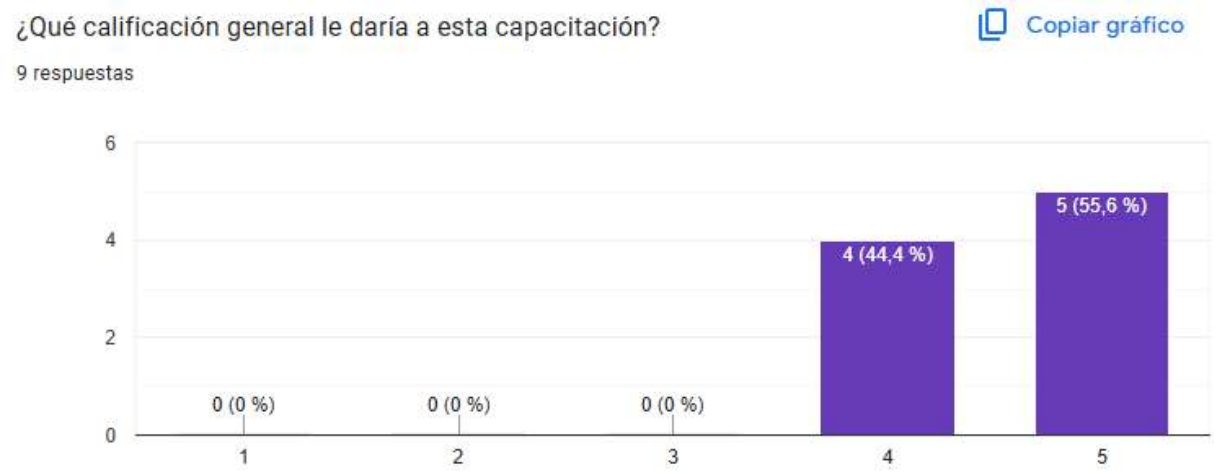


Fuente el autor.

Análisis:

El 100% de los encuestados indicó que aplicará los conocimientos adquiridos en sus actividades diarias. Esto demuestra que el contenido fue pertinente, práctico y alineado con las funciones laborales de los asistentes, lo cual favorece la mejora en la seguridad de la información institucional.

11. ¿Qué calificación general le daría a esta capacitación?

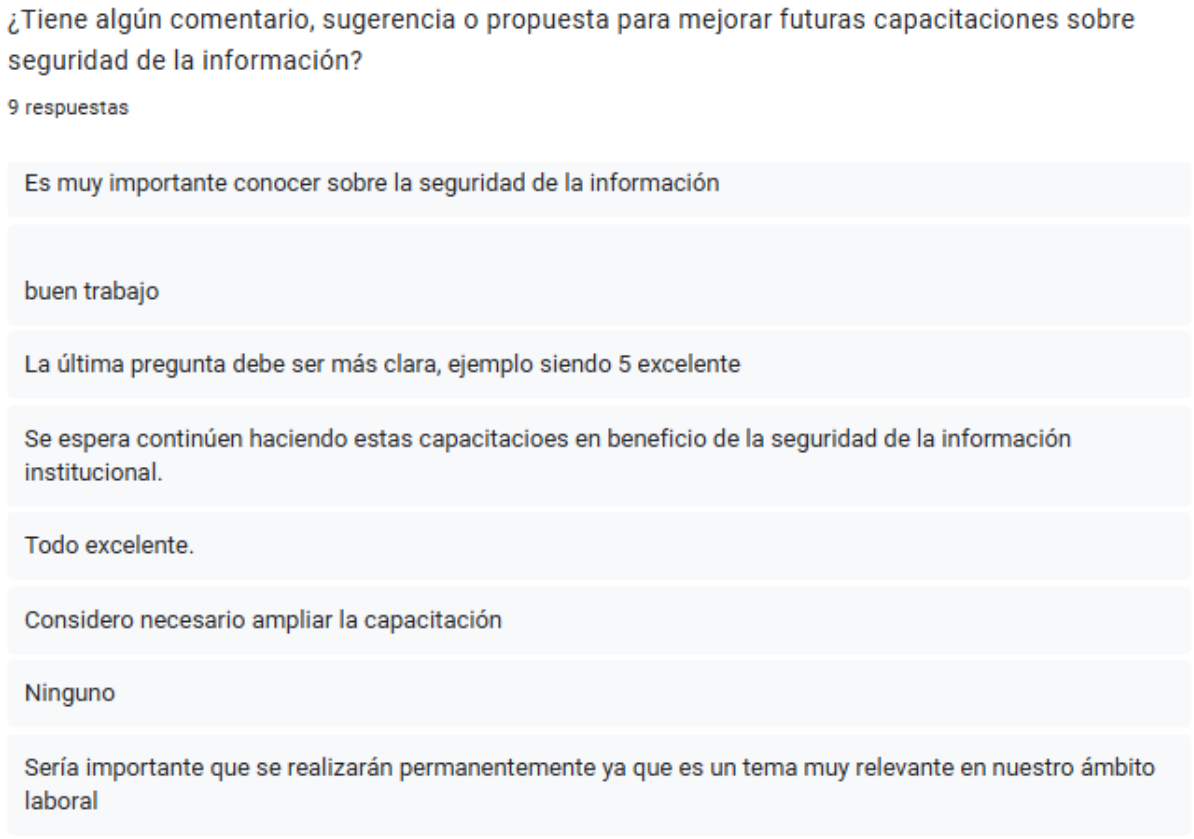


Fuente el autor.

Análisis:

La mayoría de los participantes calificó la capacitación con la nota más alta (5), y el resto con 4. Esto refleja una valoración muy positiva en términos de calidad y utilidad. Aunque todos se mostraron satisfechos, un grupo pequeño identificó oportunidades de mejora para alcanzar un nivel de excelencia aún mayor.

12. ¿Tiene algún comentario, sugerencia o propuesta para mejorar futuras capacitaciones sobre seguridad de la información?



Fuente el autor.

Análisis:

Los comentarios reflejan una alta satisfacción con la capacitación, destacando su relevancia y utilidad. Las sugerencias giran en torno a la necesidad de profundizar en los temas, mantener estas iniciativas de formación y mejorar la formulación de las preguntas de evaluación para evitar ambigüedades.

Anexo 11 Registro de asistencia de los docentes participantes en las capacitaciones y encuestas.

Fuente: Los autores

Anexo 12 Informe de Capacitación

INFORME DE CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO/IEC 27002.

Introducción

En el marco del proyecto “Construcción de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado a la Norma ISO/IEC 27001 para el Centro Educativo Norean”, se llevó a cabo una jornada de capacitación dirigida al personal administrativo y docente, fundamentada en la norma internacional ISO/IEC 27002. Esta norma proporciona directrices para establecer controles y buenas prácticas orientadas a la protección de la información, la gestión de riesgos y el fortalecimiento de la cultura de seguridad digital en las organizaciones.

La actividad tuvo como propósito no solo impartir conocimientos técnicos, sino también sensibilizar a los docentes y administrativos sobre la importancia del manejo responsable de los datos, las plataformas digitales y los dispositivos tecnológicos, fomentando comportamientos seguros ante los riesgos del entorno digital actual.

Objetivos de la capacitación

Objetivo general:

Fortalecer las competencias del personal docente y administrativos del Centro Educativo Norean en materia de seguridad de la información, conforme a las directrices de la norma ISO/IEC 27002, promoviendo una cultura institucional de protección y gestión responsable de los activos informáticos.

Objetivos específicos:

1. Concientizar al personal docente sobre los riesgos asociados al tratamiento de la información institucional.

2. Socializar las principales políticas y controles de seguridad propuestos en la ISO/IEC 27002.

3. Promover hábitos seguros en el uso de contraseñas, plataformas digitales y manejo de datos sensibles.

4. Evaluar la percepción del personal sobre la utilidad y aplicabilidad de los contenidos impartidos.

Temáticas abordadas

I. Durante la jornada se desarrollaron los siguientes temas:

II. Introducción a la seguridad de la información.

III. Fundamentos del SGSI y su importancia en el contexto educativo.

IV. Principios básicos de la norma ISO/IEC 27002.

V. Clasificación y control de activos de información.

VI. Gestión de accesos y contraseñas.

VII. Uso seguro de Internet y del correo institucional.

VIII. Prevención y manejo de incidentes de seguridad.

IX. Recomendaciones prácticas para el aula digital y la protección de datos personales.

La metodología combinó la exposición teórica con actividades prácticas y ejercicios de reflexión, utilizando material audiovisual, ejemplos reales y dinámicas participativas.

Desarrollo de la jornada

1. La capacitación se desarrolló de forma presencial en las instalaciones del Centro Educativo Norean. Se aplicó una metodología activa basada en:

2. Exposiciones con apoyo de diapositivas informativas.

3. Análisis de casos reales de incidentes de seguridad.

4. Ejercicios grupales para identificar buenas y malas prácticas.

5. Espacios de retroalimentación y aclaración de dudas.

Al cierre, se aplicó una encuesta de satisfacción con el fin de evaluar la percepción de los participantes frente a la claridad, relevancia y aplicabilidad de los contenidos abordados.

Resultados de la capacitación

Perfil de los asistentes:

El grupo estuvo conformado principalmente por docentes con amplia trayectoria educativa, muchos de ellos de edad avanzada. A pesar de sus limitaciones técnicas iniciales, mostraron gran disposición para aprender sobre temas de ciberseguridad y manejo seguro de la información.

Relevancia del tema:

El 100% de los participantes consideró la temática altamente pertinente, tanto en el ámbito laboral como personal. Durante la jornada, compartieron experiencias relacionadas con intentos de fraude digital, suplantación de identidad y acceso no autorizado a sus cuentas personales, lo cual generó un valioso espacio de reflexión y aprendizaje.

Contenido y actualización:

El 95% manifestó que el contenido fue actualizado, relevante y coherente con las nuevas exigencias tecnológicas. La norma ISO/IEC 27002 fue percibida como un marco práctico para orientar políticas de protección de datos institucionales.

Claridad y metodología:

El 98% de los asistentes destacó la claridad del facilitador y la aplicabilidad de los ejemplos utilizados, valorando el enfoque empático y didáctico que facilitó la comprensión de conceptos técnicos.

Aplicación práctica:

El 92% expresó sentirse más preparado para aplicar las prácticas aprendidas, reconociendo la necesidad de modificar hábitos inseguros como el uso de contraseñas débiles o la apertura de correos sospechosos.

Propuestas de mejora:

El 65% de los docentes sugirió extender la capacitación a toda la comunidad educativa, incluyendo personal administrativo y estudiantes, para fortalecer la cultura institucional de seguridad digital.

Comentarios destacados de los participantes

I. “Esta capacitación me hizo entender cómo pueden robarme a través del celular o el correo; ya me pasó una vez con el banco.”
II. “Muy buena explicación, todo claro y con palabras que uno entiende. Gracias por tenernos en cuenta, a nuestra edad también se aprende.”
III. “Sería bueno que nos enseñen también cómo proteger el celular y reconocer mensajes falsos.”

Estos testimonios reflejan el impacto positivo de la jornada y la necesidad de continuar con procesos formativos adaptados al perfil del personal docente.

Conclusiones

La capacitación representó una experiencia significativa en el proceso de fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) del Centro Educativo Norean.
Se logró incrementar la conciencia del personal docente frente a los riesgos digitales y reforzar las prácticas seguras en el manejo de la información.

El espacio de aprendizaje permitió consolidar una cultura institucional orientada a la protección de los datos, alineada a los principios de confidencialidad, integridad y disponibilidad. Además, fomentó la participación activa y el compromiso del personal para continuar con acciones formativas en materia de ciberseguridad educativa.

En términos generales, la jornada contribuyó a sentar las bases para un proceso continuo de mejora, prevención y responsabilidad digital dentro del contexto académico.

Recomendaciones

1. Fortalecer la continuidad de las capacitaciones: implementar un plan anual de formación docente en seguridad de la información, con sesiones progresivas y adaptadas al nivel tecnológico de los participantes.

2. Fomentar la práctica aplicada: incorporar talleres prácticos sobre temas de alta relevancia, como la gestión de contraseñas, seguridad en dispositivos móviles y prevención de fraudes digitales.

3. Establecer canales de apoyo técnico: crear un punto de contacto institucional para la atención de incidentes o dudas relacionadas con la ciberseguridad.

4. Extender el alcance de las jornadas: incluir al personal administrativo, estudiantes y padres de familia para consolidar una cultura de seguridad transversal en toda la comunidad educativa.

5. Evaluar el impacto y mejora continua: aplicar instrumentos de evaluación antes y después de cada capacitación, con el fin de medir el grado de apropiación y realizar ajustes pertinentes a los contenidos.

Anexo 13 Evidencia de encuestas de satisfacción

Copias escaneadas de encuestas de satisfacción.

CAPACITACIÓN ISO/IEC 27002 CENTRO EDUCATIVO NOREAN.

Datos del Asistente

Nombre completo: Martin Galezo Guerra

Cargo:

☐ Administrativo ☒ Docente ☐ Otro: _____

Correo electrónico: mgalezoguerra@gmail.com.

Encuesta de Satisfacción.

Esta encuesta tiene como objetivo conocer tu opinión sobre la capacitación en buenas prácticas de seguridad de la información. Tus respuestas nos ayudarán a mejorar futuras actividades formativas y asegurar que sean útiles, claras y aplicables en tu entorno laboral.

1. ¿El tema desarrollado fue relevante y aplicable a tu entorno laboral?

☐ En desacuerdo ☐ Neutral ☒ De acuerdo

2. ¿Consideras que el contenido fue actualizado y alineado con buenas prácticas?

☐ En desacuerdo ☐ Neutral ☒ De acuerdo

3. ¿El facilitador explicó con claridad los conceptos clave?

☐ En desacuerdo ☐ Neutral ☒ De acuerdo

4. ¿Las actividades o ejemplos prácticos te ayudaron a entender el tema?

☒ Sí ☐ Parcialmente ☐ No

5. ¿El tiempo asignado al tema fue suficiente?

☐ Sí ☐ Parcialmente ☐ No

6. ¿Sientes que ahora puedes aplicar lo aprendido en tu trabajo?

☒ Sí ☐ Parcialmente ☐ No

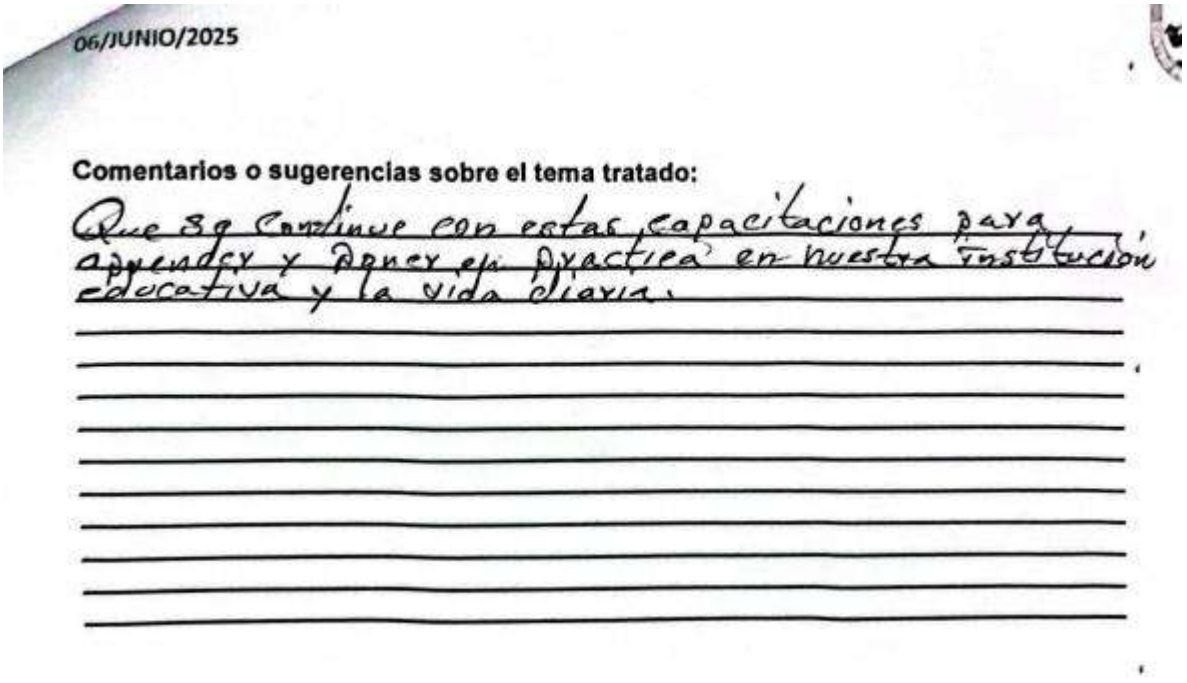
7. ¿Recomendarías incluir este tema en futuras capacitaciones?

☒ Sí ☐ No ☐ No estoy seguro/a

8. ¿Cómo calificarías este módulo temático?

☐ Excelente ☒ Bueno ☐ Regular ☐ Deficiente

Fuente: *los autores.*


06/JUNIO/2025

Comentarios o sugerencias sobre el tema tratado:

Que se continue con estas capacitaciones para aprender y poner en practica en nuestra institución educativa y la vida diaria.

Fuente: *los autores.*

CAPACITACIÓN ISO/IEC 27002 CENTRO EDUCATIVO NOREAN.

Datos del Asistente

Nombre completo: Josi Bernarda Guillen M

Cargo:

☐ Administrativo ☒ Docente ☐ Otro: _____

Correo electrónico: Josibernarda2020@gmail.com

Encuesta de Satisfacción.

Esta encuesta tiene como objetivo conocer tu opinión sobre la capacitación en buenas prácticas de seguridad de la información. Tus respuestas nos ayudarán a mejorar futuras actividades formativas y asegurar que sean útiles, claras y aplicables en tu entorno laboral.

1. ¿El tema desarrollado fue relevante y aplicable a tu entorno laboral?

☐ En desacuerdo ☐ Neutral ☒ De acuerdo

2. ¿Consideras que el contenido fue actualizado y alineado con buenas prácticas?

☐ En desacuerdo ☐ Neutral ☒ De acuerdo

3. ¿El facilitador explicó con claridad los conceptos clave?

☐ En desacuerdo ☐ Neutral ☒ De acuerdo

4. ¿Las actividades o ejemplos prácticos te ayudaron a entender el tema?

☐ SI ☒ Parcialmente ☐ No

5. ¿El tiempo asignado al tema fue suficiente?

☐ SI ☒ Parcialmente ☐ No

6. ¿Sientes que ahora puedes aplicar lo aprendido en tu trabajo?

☒ SI ☐ Parcialmente ☐ No

7. ¿Recomendarías incluir este tema en futuras capacitaciones?

☒ SI ☐ No ☐ No estoy seguro/a

8. ¿Cómo calificarías este módulo temático?

☐ Excelente ☒ Bueno ☐ Regular ☐ Deficiente

06/JUNIO/2025

Comentarios o sugerencias sobre el tema tratado:

Excelente presentación

Fuente: *los autores.*

Registro fotográfico de visitas y capacitaciones

El siguiente registro fotográfico presenta la evidencia visual de las actividades realizadas durante el desarrollo del proyecto en el Centro Educativo Norean, incluyendo la visita institucional, la auditoría interna, las capacitaciones y la interacción con los docentes. Las imágenes fueron tomadas por las autoras como parte del trabajo de campo y se emplean exclusivamente con fines académicos.

Figura 1. Auditoría interna en el Centro Educativo Norean

En la imagen se observa a una de las autoras del proyecto junto con un docente del Centro Educativo Norean durante la primera visita institucional. Esta jornada correspondió a la fase de auditoría interna, en la cual se realizó la identificación de activos, la evaluación del estado de la infraestructura y el análisis del nivel de conocimiento de los docentes en materia de seguridad de la información.

Fuente: *Fotografías tomadas por las autoras durante el trabajo de campo (2025).*

Figura 2. Primera capacitación sobre seguridad de la información en el Centro Educativo Norean

En las siguientes imágenes se evidencia la realización de la primera capacitación sobre seguridad de la información y las buenas prácticas implementadas. Esta actividad tuvo como propósito analizar los posibles riesgos a los que la institución puede estar expuesta y fortalecer el conocimiento del personal docente sobre la protección de los activos de información.

Fuente: *Fotografías tomadas por las autoras durante el trabajo de campo (2025).*

Figura 3 . Elaboración del informe de riesgos y propuesta documental

En esta etapa se elaboró un informe detallado sobre los riesgos asociados a la seguridad de la información, acompañado de un borrador del documento que será entregado a la institución. Este material servirá como base para que, con la participación de los directivos, se implementen las acciones correctivas y preventivas correspondientes dentro de la entidad.

Fuente: *Fotografías tomadas por las autoras durante el trabajo de campo (2025).*