Maestría en Ciberseguridad

Informe de Investigación previo a la obtención del título de Magíster en Ciberseguridad

Tema: Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando la norma ISO/27001 para la protección de datos en la Unidad Educativa La Inmaculada de la Ciudad de Ambato

Autor: Franklin Vinicio Guamán Muela

Tutores: Ing. Juan Pablo Cuenca Tapia.
Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2024

Certificación de Asesores

Se certifica que:

El informe de investigación "***Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando norma ISO/27001 en la protección de datos para Unidad Educativa La Inmaculada de la Ciudad de Ambato***", de autoría del Señor Ingeniera de Sistemas Franklin Vinicio Guamán Muela, CC:1803439908, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Tecnologías de la Información, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2024.

Ing. Diego Cordero Guzmán. PhD	Ing. Juan Carlos Ortega Castro. Mg
Asesor Científico	Asesor Metodológico

Certificación de Autoría

Certifico que:

"***Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando norma ISO/27001 en la protección de datos para Unidad Educativa La Inmaculada de la Ciudad de Ambato***", es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2024

_____

Ing. Franklin Vinicio Guamán Muela

CC: 1803439908

Agradecimiento

Agradezco profundamente a Dios por permitirme culminar esta etapa tan importante en mi vida. Extiendo mi gratitud a todas las personas que me brindaron su apoyo incondicional, especialmente a mis padres, hermana y amigos, quienes siempre estuvieron a mi lado y nunca dudaron de mis capacidades. También quiero agradecer al Ing. Juan Carlos Ortega, y Ing. Juan Pablo Cuenca Tapia, por su invaluable apoyo en la realización de este trabajo. A mis docentes académicos, quienes durante la Maestría compartieron sus conocimientos y me ayudaron a alcanzar este objetivo, les estoy eternamente agradecido. Por último, gracias a las autoridades de la Unidad Educativa La Inmaculada por abrirme una vez más las puertas de su institución y brindarme su apoyo; sin ellos, nada de esto hubiera sido posible.

Dedicatoria

Este trabajo está dedicado, en primer lugar, a Dios, cuya guía y fortaleza han sido fundamentales en cada paso de este camino. Agradezco infinitamente su presencia en mi vida y la inspiración que me ha brindado.

Con inmenso amor, dedico este esfuerzo a mis padres, quienes han sido mi mayor fuente de apoyo y motivación. Su confianza en mí y su constante aliento me han permitido superar los desafíos y mantenerme firme en la búsqueda de mis sueños. También agradezco profundamente a mi hermana, quien con sus oraciones y cariño ha sido un pilar esencial en mi vida.

Finalmente, quiero expresar mi gratitud a mi pareja, quien ha compartido conmigo este viaje y me ha brindado su amor y amistad incondicional. Su apoyo ha sido invaluable, no solo en los momentos de alegría sino también en los de dificultad.

Gracias a todos por creer en mí y por ayudarme a alcanzar las metas propuestas.

Franklin Vinicio Guamán Muela

Resumen

La rápida evolución de las tecnologías de la información ha transformado la manera en que las organizaciones gestionan y protegen sus datos. En este sentido, la Unidad Educativa La Inmaculada enfrenta varios vulnerabilidad, destacando la falta de políticas de seguridad adecuadas, lo que la hace susceptible a diversas amenazas digitales. El enfoque en crear un manual de seguridad basado en la norma ISO 27001 es crucial, ya que esta norma establece requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) que permite a las organizaciones gestionar de manera efectiva la seguridad de sus datos.

El análisis de los recursos informáticos más vulnerables es un paso esencial para identificar las áreas críticas que requieren atención inmediata. La implementación de medidas preventivas, que se basen en el ciclo P.D.C.A. no solo mejorará la protección de la información, sino que también asegurará la continuidad de las operaciones académicas en un entorno seguro. Además, la integración de medidas contra amenazas específicas como malware, phishing y ransomware es fundamental para mitigar el riesgo y proteger la integridad de los datos.

En resumen, la implementación un SGSI basado en la norma ISO 27001 no solo aborda las vulnerabilidades actuales, sino que también establece un marco de trabajo para la mejora continua en la gestión de la seguridad de la información. Esto es vital para garantizar la confidencialidad, integridad y disponibilidad de los datos en un entorno educativo moderno.

Palabras clave: Gestión, Seguridad de la información, ISO/IEC 27001, Sistema, Vulnerabilidad, Metodología, Modelo, Control, Proceso, Dominio, TIC, PDCA, Riesgo.

Abstract

The rapid evolution of information technologies has transformed the way organizations manage and protect their data. In this sense, La Inmaculada Educational Unit faces several vulnerabilities, highlighting the lack of adequate security policies, which makes it susceptible to various digital threats. The focus on creating a security manual based on the ISO 27001 standard is crucial, as this standard establishes requirements for an Information Security Management System (ISMS) that allows organizations to effectively manage the security of their data.

The analysis of the most vulnerable IT resources is an essential step in identifying critical areas that require immediate attention. The implementation of preventive measures, based on the P.D.C.A. cycle, will not only improve information protection, but will also ensure the continuity of academic operations in a secure environment. In addition, the integration of measures against specific threats such as malware, phishing and ransomware is critical to mitigate risk and protect data integrity.

In summary, implementing an ISMS based on ISO 27001 not only addresses current vulnerabilities, but also establishes a framework for continuous improvement in information security management. This is vital to ensure the confidentiality, integrity and availability of data in a modern educational environment.

Keywords: Management, Information Security, ISO/IEC 27001, System, Vulnerability, Methodology, Model, Control, Process, Domain, ICT, PDCA, Risk.

Índice de contenidos

Contenido

Índice de tabla

Índice Imágenes

Capitulo I. Introducción

En Ecuador, la Ley de Protección de Datos Personales de 2021 ha sido implementada para resguardar la información personal de estudiantes, profesores y personal administrativo en las instituciones educativas. Esta ley establece normativas estrictas relacionadas con el procesamiento y resguardo de datos, tomando como referencia estándares internacionales como el GDPR de la UE. ¿Podrías detallar cómo se está llevando a cabo la implementación de esta ley

en las instituciones educativas de Ecuador y cómo garantizar el cumplimiento de las normativas establecidas para el procesamiento seguro y confidencial de los datos personales?

El impacto del aumento de ciberataques globales en Ecuador es un tema preocupante, especialmente para las instituciones educativas que manejan una gran cantidad de datos personales confidenciales. Los ataques de ransomware, phishing y exfiltración de datos resaltan la urgente necesidad de implementar sistemas de ciberseguridad eficaces para proteger la integridad y confidencialidad de la información.

Los posibles peligros que podrían afectar la privacidad y seguridad de los datos en la Unidad Educativa La Inmaculada en Ambato abarcan la revelación no autorizada de información personal debido a errores humanos, fallas de seguridad o ataques cibernéticos. Estos riesgos pueden agravarse por la presencia de software desactualizado, redes vulnerables, el uso de contraseñas débiles, así como la ausencia de políticas y el incumplimiento de leyes y regulaciones de protección de datos.

Con el fin de llevar a cabo una investigación exhaustiva, es esencial iniciar solicitando permiso a la autoridad competente de la Unidad Educativa La Inmaculada para dar inicio al proceso y gestionar la documentación pertinente en los departamentos de Tecnologías de la Información (TI), inspección general, secretaria y contabilidad. Posteriormente, es necesario generar un listado detallado de los activos de información, con el propósito de identificar los riesgos y vulnerabilidades y así protegerlos debidamente.

Seguidamente, es de vital importancia elaborar políticas y protocolos específicos para los activos identificados como vulnerables. Para concluir, se deberá redactar un documento técnico

dirigido a mitigar las vulnerabilidades detectadas, que incluirá recomendaciones y sugerencias al finalizar el proceso.

En relación con esta investigación, se implementará una propuesta clara y precisa en la Unidad Educativa La Inmaculada para identificar y abordar las vulnerabilidades existentes en sus sistemas de información y las posibles amenazas que comprometan la seguridad de los datos. Se llevará a cabo utilizando los parámetros del modelo de Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001, con el objetivo de establecer políticas de seguridad robustas y estandarizadas para garantizar la protección de la información sensible y cumplir con las normativas internacionales.

1.1. Situación Problemática

En la sociedad actual, la información se transmite principalmente a través de ordenadores e Internet. En el siglo XXI, Internet se ha convertido en una de las herramientas más importantes para la economía, la política y la conexión del ser humano con la sociedad. De esta manera, la vida cotidiana de las personas se ha adaptado a las nuevas tecnologías de la información, abriendo también un nuevo campo para los ataques informáticos, lo cual pone en gran riesgo a la sociedad actual.

Existe una brecha significativa entre la realidad de la ciberseguridad en Latinoamérica y el resto del mundo. En particular, Ecuador se encuentra en primer lugar en Hispanoamérica y en tercer lugar a nivel mundial en términos de ciberataques, con un 2.8% de estos ataques a nivel global. El 49.05% de ellos son provocados por ataques de fuerza bruta a servidores RDP (Remote Desktop Protocol) (Alvarado, 2020).

Según Bogantes (n.d.), las instituciones educativas son un área particularmente atractiva para los ciberatacantes, ya que contienen grandes cantidades de datos e información personal de los estudiantes, profesores y logros profesionales en sus bases de datos.

Partiendo de esta premisa, las instituciones educativas, juntamente con el departamento de Tecnologías de la Información (TI) y las demás dependencias, así como los laboratorios informáticos donde se maneja la información, deben proteger los datos de los estudiantes contra amenazas siempre presentes que pueden representar riesgos extremadamente altos.

1.2. Justificación

El presente proyecto de investigación se puede justificar de forma académica y técnica mediante artículos de la ley del Ministerio de Educación (Mineduc), como son los siguientes: ACUERDO Nro. MINEDUC-MINEDUC-2023-00054-A, que en el Artículo 21 de la Ley Orgánica manifiesta los derechos de los niños, niñas y adolescentes. Además, en la Ley Orgánica de Datos Personales, los artículos 22, 23 y 24 abordan la educación digital y el ejercicio de derechos. También se mencionan los Artículos 40 y 41 relacionados con las amenazas y vulnerabilidades, y las medidas de seguridad.

Para gestionar la seguridad de la información, nos apoyaremos en las normas ISO 27001 en las instituciones educativas, con el objetivo de cumplir con los estándares de ciberseguridad. Los resultados nos permitirán que las instituciones educativas cuenten con normativas, protocolos y políticas para gestionar y proteger sus datos, así como estrategias de seguridad de la información.

En la actualidad, las instituciones educativas no disponen de un Sistema de Gestión de Seguridad de la Información (SGSI) que ayude a gestionar la seguridad de los activos. Por lo

tanto, es necesario aplicar una metodología que permita integrar y organizar de forma ordenada los activos, basándose en las normas ISO 27001.

Este proyecto es factible porque nos permite desarrollar la solución planteada. Al mismo tiempo, gestionar la seguridad de la información basada en la norma ISO 27001 es importante en una empresa u organización, ya que establece mecanismos que mejoran la gestión de la información. La implementación de la norma ISO 27001 en instituciones educativas no solo contribuye a la protección de la información sensible, sino que también fortalece la resiliencia operativa, demuestra el compromiso con la seguridad de la información y contribuye a la construcción de una reputación sólida.

1.3. Objeto de Estudio

El objetivo de la investigación está relacionado con la protección de datos personales, ya que este proyecto específico se centra en las instituciones educativas y está involucrado en la rama de la ciberseguridad. Todas las tareas se realizan en entornos digitales para evitar posibles ciberataques y hackeos. Bajo esta premisa, el entorno operativo de este estudio incluye la infraestructura de activos de información pertenecientes a las instituciones educativas.

Se delimitará el trabajo definiendo el objeto de investigación, para lo cual se utilizará una matriz que abarcará todos los procesos de investigación que se llevarán a cabo. El desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para instituciones educativas, ya sean públicas o privadas, priorizará la protección de la información de los niños, niñas y adolescentes. Esto incluye la información personal de cada estudiante: nombres y apellidos,

domicilio, números de teléfonos convencionales y celulares, cuadro de notas e incluso registros disciplinarios.

El proyecto se basará principalmente en documentos de respaldo de instituciones educativas, donde se manejan los datos personales, y utilizará un modelo de gestión para el proceso de protección de datos sensibles.

1.4. Campo de Acción

El campo de acción tiene como objetivo evaluar los riesgos que pueden surgir en el manejo de datos de una institución educativa (IE). En este contexto, comprenderemos las fases de análisis necesarias para iniciar el desarrollo. Debemos utilizar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas ISO 27001. Para este desarrollo, se emplearán varios ejes temáticos relacionados con la gestión de seguridad que se aplican en las normas ISO.

1.5. Justificación de proyecto

Definir el alcance, los objetivos y las políticas que se deben implementar en la seguridad de la información mediante directrices y procedimientos destinados a garantizar la confidencialidad de los datos en una institución educativa, utilizando el SGSI (Sistema de Gestión de Seguridad de la Información).

Elaborar un inventario de activos de información para identificar los activos críticos que deben ser protegidos.

Realizar investigaciones sobre riesgos y vulnerabilidades relacionadas con los activos críticos de las instituciones educativas, analizando las debilidades de estos activos en cuanto a la confidencialidad de los datos.

Redactar un documento técnico con los informes obtenidos sobre la investigación de riesgos y vulnerabilidades, que debe incluir recomendaciones y sugerencias para la toma de decisiones.

1.6. Objetivos de la Investigación

Para la realización de esta investigación, se plantearon los siguientes objetivos:

1.6.1. Objetivo general

Diseñar un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas ISO 27001, partiendo de los activos y riesgos, con el propósito de proteger los datos de la Unidad Educativa La Inmaculada.

1.6.2. Objetivos específicos

- Solicitar a la autoridad correspondiente de la IE el permiso para iniciar el proceso y manejar la documentación.
- Elaborar un listado de los activos de información en el departamento de Tecnologías de la Información (TI), secretaría y contabilidad para identificar los riesgos y vulnerabilidades y poder resguardarlos.
- Elaborar políticas y protocolos para los activos identificados como vulnerables.
- Presentar un documento técnico para mitigar las vulnerabilidades. Al finalizar el proceso, este documento debe contener recomendaciones y sugerencias.

1.7. Preguntas Científicas

- ¿Cuáles son los riesgos internos y externos en el manejo de la protección de datos en las instituciones educativas?

- ¿Qué papel desempeña el SGSI (Sistema de Gestión de Seguridad de la Información) en la protección de datos para resguardar la información?
- Una vez realizada la evaluación de los riesgos y la vulnerabilidad de los activos, ¿qué se debe conseguir con el informe final?

1.8. Hipótesis

Con el informe de resultados entregado en el análisis de los activos identificados, así como los riesgos y vulnerabilidades que tiene la IE en cuanto a la confidencialidad y la protección de datos, se proporcionará un insumo fundamental para la auditoría en el departamento de Tecnologías de la Información (TI), secretaría, inspección y contabilidad de la Unidad Educativa La Inmaculada.

1.8. Variables

1.8.1. Independientes:

Realizar un inventario de los activos de la Unidad Educativa La Inmaculada y utilizar la herramienta del Sistema de Gestión de Seguridad de la Información (SGSI) basada en las normas ISO 27001.

1.8.2. Dependientes:

- Investigación sobre los activos de datos en cuanto a la utilización de las normas ISO 27001.
- Elaboración de la plantilla sobre los activos de vulnerabilidad basada en las normas ISO 27001.
- Identificación del nivel de confidencialidad de la información sensible que tiene un estudiante en una institución educativa.

1.9. Tabla de Variable

Tabla 1
Operación de las variables

Variable	Concepto	Dimensiones	Indicadores	Tipo de Variable	Escala
Independiente: Inventario de activos de la U.E. La Inmaculada y SGSI.	Identificación y catalogación de los activos de información y herramientas de gestión de seguridad de la información conforme a la norma ISO 27001.	Identificación de activos Clasificación de activos	- Número de activos identificados - Clasificación de activos por categoría	Cuantitativa	Nominal
Dependiente: Investigación sobre los activos de datos y utilización de normas ISO 27001.	Análisis de los activos de datos para determinar su cumplimiento con las normas ISO 27001.	Conformidad con ISO 27001 Estado actual de los activos	- Porcentaje de activos conformes con ISO 27001 -Identificación de brechas de conformidad	Cuantitativa	Porcentual
Dependiente: Elaboración de la plantilla sobre los activos de vulnerabilidad basada en las normas ISO 27001.	Creación de una plantilla que documente las vulnerabilidades de los activos conforme a ISO 27001.	Plantilla de evaluación Registro de vulnerabilidades	- Número de vulnerabilidades documentadas - Compleción de la plantilla	Cualitativa	Ordinal

Fuente Elaborado por el autor basado evidentemente en lo investigado

1.10. Contribuciones de la investigación

1.10.1. Aporte teórico

Desde la perspectiva teórica, este trabajo de investigación proporciona un marco conceptual sólido sobre los Sistemas de Gestión de Seguridad de la Información (SGSI) utilizando las normas ISO 27001, que definen la seguridad de la información en las Unidades Educativas. Incluye la identificación de amenazas, vulnerabilidades y riesgos específicos para las instituciones educativas. Los beneficios de implementar ISO 27001, en términos de

confidencialidad, integridad y disponibilidad de la información, están claramente definidos. Esto nos permitirá mejorar la ciberseguridad y la gestión de la información.

Además, nos permite comprender los riesgos específicos asociados con la protección de datos en el contexto educativo, donde se manejan grandes cantidades de información sensible de estudiantes, docentes, calificaciones y datos financieros.

Es fundamental desarrollar modelos teóricos que integren las mejores prácticas de la ISO 27001 con las necesidades particulares de las instituciones educativas, proporcionando un marco para evaluar y mejorar la seguridad de la información.

1.10.2. Aporte metodológico

El aporte metodológico de esta investigación busca proponer procedimientos que aporten significativamente a la manera en que se implementan y evalúan los SGSI. Se desarrollarán guías y protocolos considerando los recursos y capacidades de las instituciones, creando herramientas de diagnóstico y evaluación que permitan identificar sus puntos débiles en la gestión de la seguridad de la información y medir el cumplimiento con la norma ISO 27001. Esto asegura que los procesos sean adecuados y cumplan con los requisitos, e incluyen fases detalladas de análisis, planificación, implementación y monitoreo. Estos métodos y herramientas evalúan la efectividad de los sistemas de gestión de seguridad de la información, incluyendo auditorías internas, lo cual es crucial para mantener la conformidad con la ISO 27001.

1.10.3. Aporte práctico

Al realizar esta investigación, se aportará un correcto uso de las SGSI con las normas ISO 27001 para mejorar la gestión de la seguridad de la información. Se implementarán medidas de seguridad efectivas que protegen la información sensible contra accesos no autorizados,

ciberataques y otras amenazas. Además, se estandarizarán los procesos y políticas que aseguran una gestión consistente y eficiente de la información, reduciendo el riesgo de brechas de seguridad y garantizando el cumplimiento legal y regulatorio.

1.10.4. Novedad científica

Esta investigación tiene como fin utilizar una de las principales novedades: la adaptación de la norma ISO 27001, abordando desafíos específicos como la gestión de datos de estudiantes y la infraestructura tecnológica disponible. El uso de tecnologías emergentes, como la inteligencia artificial y el blockchain, busca mejorar la protección de datos en las instituciones educativas, proponiendo soluciones innovadoras que podrían ser adoptadas a nivel global.

1.11. Síntesis de la estructura del estado del arte

Para iniciar el presente proyecto, es fundamental entender la Seguridad de Datos a través de diferentes enfoques de varios autores. La seguridad de la información ha evolucionado desde la protección física de dispositivos de almacenamiento hasta la implementación de políticas, procedimientos y controles en sistemas de TI y redes, enfocándose en las personas (Cárdenas et al., 2016). ISO Tools Excellence define la seguridad informática como la implementación de soluciones técnicas para proteger la información, asegurando la integridad y privacidad del sistema informático y preservando las infraestructuras y comunicaciones que soportan las operaciones de una empresa (Figueroa-Suárez et al., 2018).

La Seguridad de la Información (SI) utiliza diversas normas, protocolos y políticas para prevenir ataques cibernéticos, protegiendo la confidencialidad, integridad y disponibilidad (CID) de la información, con una gestión orientada a empresas o instituciones. Alarcón et al. (2016) subrayan la importancia de la seguridad en redes y telecomunicaciones, destacando la necesidad de soluciones efectivas para proteger la integridad de la información y asegurar la

confidencialidad de los datos. Existen tres principios que trabajan de la mano para garantizar la solidez dentro de un sistema informático; a esto se le conoce como la Triada de la Seguridad de la Información CID.

Figura 1

Triada CID

Fuente: Pilares de la triada CIA, por Seguridad de la Información (2023), CIA https://ciberseguridad.comillas.edu/content/images/2023/04/piramide-cia-1.png

- **Confidencialidad**: Mantiene la información privada o secreta a salvo de personas no autorizadas. Es crucial para muchas organizaciones.
- **Integridad**: Asegura que la información no sea alterada por usuarios no autorizados, garantizando coherencia y precisión.
- **Disponibilidad**: Permite el acceso seguro a la información. Los sistemas deben estar siempre operativos, evitando interrupciones.

La ciberseguridad protege ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra ataques maliciosos. Su objetivo es prevenir ataques internos y externos, garantizando la protección y seguridad de los datos. La globalización plantea

preocupaciones sobre la ciberseguridad, y es vital respetar los derechos humanos y fomentar la cooperación entre usuarios para evitar violaciones adicionales (Tapia Hernández et al., 2021)

Normas ISO

Las Normas ISO son estándares internacionales para gestionar diferentes áreas de una organización. Implementar un SGSI (Sistema de Gestión de Seguridad de la Información) permite optimizar procesos y asegurar que los sistemas de información estén en perfecto estado. El ciclo PDCA (Planificar, Hacer, Verificar, Actuar) es esencial para evaluar y mejorar proyectos de calidad (La et al., 2020). Existen diferentes grupos de normas:

Gestión de la Calidad: ISO 9001, ISO 16949, ISO 15504, ISO 17025, ISO 20000.

Medio Ambiente y Sostenibilidad: ISO 14001, ISO 50001.

Seguridad: ISO 45001, ISO 27001, ISO 22000.

Innovación y Nuevas Tecnologías: ISO 16600, ISO 166002, ISO 20000.

ISO/IEC 27001: Esta norma proporciona un modelo para crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI. Garantiza la seguridad, confidencialidad e integridad de los datos y sistemas que los procesan. Permite evaluar riesgos y aplicar los controles necesarios, mejorando la competitividad y la imagen de la organización. (Mesquida et al., 2010).

1.12. Análisis de Riesgo

Para realizar un análisis de riesgo de seguridad de la información, primero se identifican los activos más críticos de una organización a través del inventario y valoración de estos activos. Luego, se identifican las amenazas y vulnerabilidades que podrían afectar a dichos activos. Las

amenazas pueden ser de diversos tipos, como hardware, software, organizacionales, humanas, de red o naturales, mientras que las vulnerabilidades pueden ser físicas, naturales, de software, hardware, red o humanas, entre otras.

La norma ISO 27001 establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI) y describe un proceso para identificar, evaluar y tratar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Este proceso incluye la identificación de los activos de información críticos, así como las amenazas y vulnerabilidades asociadas.

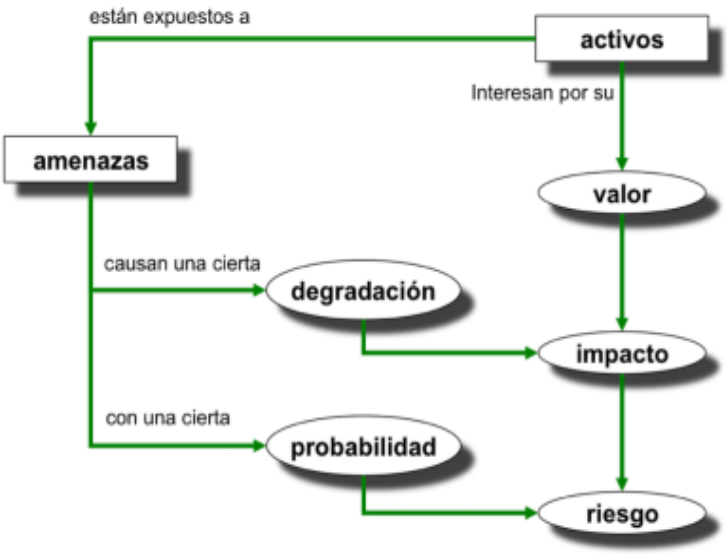
Una vez identificados los riesgos, se evalúan en términos de su probabilidad de ocurrencia y su impacto potencial, utilizando herramientas como matrices de riesgo, o análisis cualitativos y cuantitativos. Esto permite priorizar los riesgos según su severidad y asignar recursos de manera eficiente para mitigarlos.

La ISO 27001 también exige la implementación de controles y medidas para tratar los riesgos identificados, que pueden incluir políticas de seguridad, controles técnicos como el cifrado de datos, capacitación del personal y planes de contingencia y recuperación. Las medidas deben ser proporcionales al nivel de riesgo y revisarse periódicamente.

La gestión de riesgos debe ser un proceso continuo y dinámico, con revisión y auditorías internas regulares para asegurar la eficacia del SGSI. La metodología de análisis de riesgos puede ser cualitativa, cuantitativa o una combinación de ambas, según el detalle y tipo de información disponible, siguiendo los pasos descritos por metodologías como Magerit.

Figura 2

Flujo Metodología MAGERIT

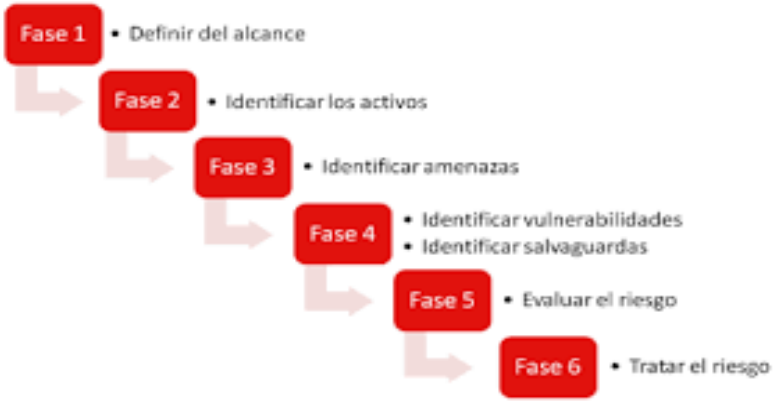


Fuente: Método De Análisis De Riesgos (2020).

Pases del método del análisis de riesgos

Figura 3

Fases de análisis de riesgos



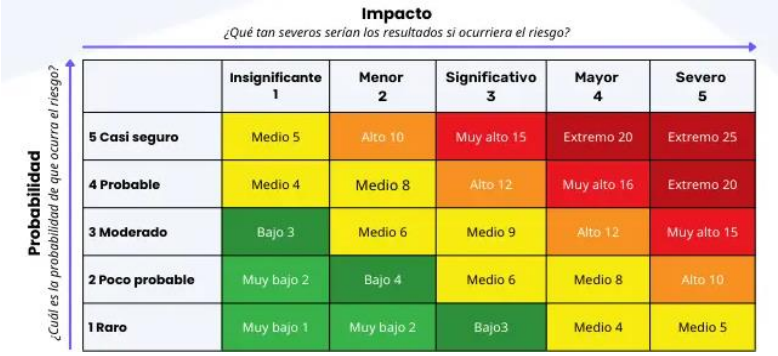
Fuentes: Gestión De Riesgo Metodologías; Fase de Análisis de Riesgo. (P.14)

- **Definir el Alcance:** Identificar las áreas estratégicas a mejorar, como un análisis de riesgo en el entorno PCI DSS o en los procesos de desarrollo.

- **Identificación de activos:** Determinar los activos involucrados, tales como hardware, software, sistemas de comunicación, aplicaciones, instalaciones, personal, proveedores y servicios subcontratados.
- **Identificación de amenazas:** Reconocer las amenazas específicas para cada activo, como daños por fuego, agua, fallos físicos o lógicos, errores del administrador, denegación de servicios, y robo de equipos.
- **Identificación de las salvaguardas:** Analizar las vulnerabilidades de los activos y proponer soluciones para mitigar los riesgos, como actualizar software, configurar alertas e instalar antivirus.
- **Evaluación del riesgo**: Calcular el riesgo basándose en la probabilidad de que ocurra una amenaza y su impacto en el Unidad Educativa. Se puede usar un **método cuantitativo** (Riesgo = Probabilidad x Impacto) o un **método cualitativo** con una matriz de riesgo.

Figura 4

Matriz de riesgos



Fuente: matriz de riesgo 5×5 | SafetyCulture

Para evaluar la seguridad en la Unidad Educativa La Inmaculada, es fundamental considerar las vulnerabilidades y salvaguardas existentes. Una vez calculado el riesgo, se deben tratar aquellos que excedan el límite establecido; Para ello, se utilizan los siguientes criterios:

- **Método cualitativo:** Tratar los riesgos con un valor mayor a 5.
- **Método cuantitativo:** Atacar los riesgos clasificados como “Medio” o superiores.

Las estrategias para tratar el riesgo incluyen:

- **Transferir el riesgo:** Contratar a un proveedor de servicios para procesar los datos sensibles, como los de tarjetas de clientes.
- **Eliminar el riesgo:** Suprimir los datos innecesarios, como eliminar los datos de tarjetas de clientes si no son estrictamente necesarios.
- Asumir el riesgo: En caso de que implementar soluciones como bases de datos segmentadas sean muy costosas, se documenta y se asume el riesgo.
- Implantar medidas de mitigación: Desarrollar proyectos específicos para reducir el riesgo en cada activo, incluyendo escaneos de seguridad externos e internos trimestrales para identificar y resolver vulnerabilidades.

El análisis de riesgo es crucial para la Unidad Educativa La Inmaculada, ya que proporciona información valiosa y ayuda a implementar medidas de mitigación para mejorar la seguridad. Se recomienda a las U.E. realizar estos proyectos para equilibrar el coste, la importancia del activo y el nivel del riesgo.

1.13. Identificar y ordenar las amenazas

La Unidad Educativa La Inmaculada se enfrenta a una serie de desafíos que ponen en riesgo tanto su seguridad como su operatividad. Entre estos desafíos destacan los ataques cibernéticos, que pueden tomar diversas formas, como malware, phishing o ransomware, comprometiendo la confidencialidad, integridad y disponibilidad de los datos académicos y personales de estudiantes y personales. Además, la institución está expuesta a riesgos físicos, como robos, donde las instalaciones pueden ser vandalizadas o bienes valiosos sustraídos, así como a la violencia escolar, que abarca desde el ciberacoso hasta peleas, representando una amenaza significativa para la seguridad tanto física como psicológica. de la comunidad educativa.

Para mitigar estos riesgos, La Unidad Educativa La Inmaculada debe implementar estrategias integrales de seguridad que aborden tanto las amenazas cibernéticas como los desafíos físicos y sociales. Esto puede incluir la adopción de medidas de seguridad informática robustas, como firewalls y programas antivirus actualizados, así como la implementación de protocolos de seguridad física, como sistemas de vigilancia y acceso restringido. Además, es fundamental promover una cultura escolar de respeto y tolerancia, fomentando la empatía y el diálogo para prevenir la violencia escolar y promover un ambiente seguro y saludable para todos los miembros de la comunidad educativa.

1.14. Realizar un análisis del impacto en la organización

El análisis de impacto en la Unidad Educativa utilizando un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 implica identificar y evaluar los riesgos y las consecuencias de posibles incidentes de seguridad de la información. Este análisis es esencial para implementar medidas de control y mitigación adecuadas, garantizando la protección de la información y la continuidad de las actividades educativas.

En la investigación en la unidad educativa, de acuerdo con el impacto basado en el análisis e identificación de activos involucrados, es un proceso clave, considerando su impacto a escala cuantitativa en la organización, siguiendo las normas ISO 27001.

Cada amenaza tendrá un nivel de impacto basado en su Nivel de Vulnerabilidad, que a su vez estará condicionado al nivel asociado a cada dimensión del activo. Así, obtenemos un nivel de impacto asociado a cada dimensión (Confidencialidad, Disponibilidad e Integridad) del activo.

Figura 5

Niveles de Impacto de las Amenazas

Tabla 1 Valores Impacto

Valor de Vulnerabilidad de la amenaza	VALORES DE DE LAS DIMENSIONES DE LOS ACTIVOS 0 No Aplicable 1 Incidental 2 Menor 3 Moderado 4 Importante 5 Extremo					
	0	1	2	3	4	5
0 - Deterioro Menor / inexistente	0	0	0	0	0	0
1 - Deterioro Perceptible / Bajo	0	1	2	3	4	5
2 - Deterioro Grave / medio	0	2	3	4	5	6
0 - Deterioro Catastrófico / Alto	0	3	4	5	6	7

Fuente. (ISO/IEC 27001:2013, 2020)

1.15. Crear un plan de respuesta y recuperación

El plan de respuesta y recuperación basado en un Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo la norma ISO 27001, debe centrarse en la identificación de riesgos, la implementación de controles y la preparación para incidentes. Un análisis de riesgos exhaustivo es crucial para identificar amenazas a la información confidencial, como datos de estudiantes y procesos administrativos. Se deben establecer controles de seguridad, como cifrado de datos, controles de acceso y copias de seguridad periódicas, de acuerdo con las directrices ISO 27001, para mitigar los riesgos y proteger la integridad, la confidencialidad y la disponibilidad de la información.

En la fase de recuperación, contar con un plan de continuidad en la Unidad Educativa y un plan de recuperación ante desastres es vital para restaurar sistemas y datos críticos en caso de un incidente de seguridad. Procedimientos claros, comunicación efectiva con las partes interesadas, capacitación del personal sobre políticas de seguridad y medidas de respuesta a incidentes son esenciales para una respuesta rápida y eficiente. Las pruebas periódicas del plan garantizan la eficacia y permiten ajustes, manteniendo un ciclo de mejora continua según los principios de la ISO 27001.

1.16. Probar el plan y refinar el análisis

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 en la Unidad Educativa implica desarrollar un plan de seguridad integral. Este plan debe abarcar políticas, procedimientos y controles para salvar la información educativa, asegurando su integridad, confidencialidad y disponibilidad. Es crucial identificar los activos de información, evaluar los riesgos asociados y establecer controles adecuados para mitigar estos riesgos. La participación activa de todas las partes interesadas, incluidos el personal

administrativo, los profesores y los estudiantes, es vital para garantizar la eficacia y relevancia de las medidas de seguridad.

Una vez que el plan esté implementado, perfeccionar el análisis es vital para mejorar continuamente las estrategias de seguridad. Este proceso de perfeccionamiento incluye una revisión periódica de los controles implementados, un seguimiento constante de los incidentes de seguridad y una evaluación de la eficacia de las políticas. Se deben realizar auditorías internas para confirmar el cumplimiento de la norma ISO 27001 e identificar áreas de mejora. La retroalimentación de las auditorías y la experiencia práctica deben alimentar el ciclo de mejora continua, fortaleciendo el SGSI y alineándolo con las amenazas y desafíos emergentes en el panorama educativo.

1.17. Marco teórico

Los proyectos de investigación realizados por el Ing. Wilson Enrique Cuenca León en 2019 y por Carlos Alonso Santamaría Calucho en 2022 abordan la gestión de la seguridad de la información en el contexto de las instituciones educativas. Cuenca León enfoca su investigación en la aplicación de la norma ISO/IEC 27001 en instituciones de educación superior en Machala, destacando la falta de implementación de controles, políticas o estándares para una adecuada gestión de la seguridad de la información, a pesar de contar con activos físicos e información.

Por otro lado, Santamaría Calucho aborda el control de seguridad en una plataforma educativa institucional, resaltando la escasez de fundamentación teórica y metodológica en ciberseguridad y gestión de seguridad en plataformas educativas y organizaciones. Ambos estudios destacan la importancia de la gestión de seguridad de la información en cumplimiento de leyes y estándares como la Ley Orgánica de Seguridad Digital, el Acuerdo Ministerial 006-

2021 y la Ley Orgánica de Protección de Datos Personales, así como la necesidad de un enfoque. crítico y propositivo para abordar estos desafíos.

Sistema de gestión de seguridad de la información (SGSI). El Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto organizado de procesos, políticas, estándares y procedimientos establecidos para gestionar de manera integral la seguridad de la información en una empresa. Su principal objetivo es proteger la confidencialidad, integridad y disponibilidad de la información.

Las características del SGSI incluyen su enfoque integral que aborda tecnología, procesos, personas y la infraestructura física; un enfoque basado en el riesgo que identifica, evalúa y gestiona proactivamente los riesgos de seguridad de la información; un ciclo de mejora continua que utiliza procesos como el Planificar-Hacer-Verificar-Actuar (PDCA); la participación activa de la alta dirección para liderar la implementación del SGSI; y el foco en mantener los principios fundamentales de confidencialidad, integridad y disponibilidad de la información.

Ciclo Deming o PDCA. - El ciclo PDCA de Deming. Sin embargo, la realidad empresarial, especialmente en Occidente, muestra un fuerte dominio de Do (hacer), mientras que las partes P, C y A del ciclo no son tan aplicadas (Costas, sf).

ISO/27001.- El texto presenta una visión general sobre la norma ISO/27001 y los sistemas de gestión de seguridad de la información (SGSI). Según (Baldecchi, 2014), la ISO/27001 establece un marco para la protección de la información en una organización, centrándose en tres atributos clave: confidencialidad, integridad y disponibilidad.

La seguridad de la información (SI) se define como la protección de los datos de una empresa u organización contra amenazas internas y externas, con el objetivo de minimizar daños, impulsar oportunidades de negocio, asegurar el retorno de la inversión, mantener la continuidad del negocio y promover una cultura ética. El SGSI logra esto mediante una estructura definida que incluye la gestión de riesgos, políticas, procesos, procedimientos, controles, revisiones y mejoras.

La ISO tiene como misión promover la estandarización a nivel mundial en áreas relacionadas con esta norma, facilitando el intercambio de servicios y bienes y fomentando la cooperación en los ámbitos intelectual, económico, científico y tecnológico (Cuenca León, 2019).

El SGSI se basa en una triada de seguridad de la información: confidencialidad, integridad y disponibilidad. La confidencialidad garantiza que la información esté disponible solo para personas autorizadas, la integridad asegura la exactitud y validez de la información, protegiéndola contra modificaciones no autorizadas, y la disponibilidad garantiza el acceso y uso de los servicios cuando sean solicitados por personas autorizadas.

Figura 6

Confidencialidad, integridad y disponibilidad

Fuente. Carlos A Martínez Development Manager en Olimpia IT

Institución Educativa. Las instituciones educativas fiscomisionales son establecimientos educativos de derecho privado con apoyo estatal que brindan un servicio educativo complementario al del Estado ecuatoriano cuando la oferta fiscal es insuficiente para atender un sector geográfico y/o a necesidades educativas especializadas, asociadas o no a una discapacidad (Espinosa & De Educación, n.d.)

1.18. Tipos de Instituciones Educativas

Por Moreno et al. (2018) se ha afirmado lo siguiente: Las instituciones educativas se clasifican, de acuerdo a su fuente principal de financiamiento, en públicas, privadas y fiscomisionales. A continuación, se define a cada uno de estos tipos según las respectivas normativas nacionales (Asamblea Nacional Constituyente, 2008; LOEI, 2011).

Públicas: Financiadas con fondos públicos, incluyendo instituciones fiscales, municipales, y de las Fuerzas Armadas y Policía Nacional. La educación es laica y gratuita para los beneficiarios. La comunidad puede utilizar las instalaciones para actividades culturales,

deportivas, etc. Privadas: Financiadas con fondos privados, administradas por personas naturales o jurídicas de derecho privado. La educación puede ser religiosa o laica, y no es gratuita para los estudiantes. Deben obtener autorización de la autoridad educativa nacional y están sujetas a su control y supervisión. Fiscomisionales: Financiadas con fondos públicos y privados. Pueden ser de derecho privado y religiosas o laicas. Sus promotores pueden ser congregaciones u órdenes religiosas.

NIVELES DE EDUCACIÓN Según LOEI (2023), se afirma lo siguiente: Se entiende por "aprobación" en los subniveles de educación básica media, básica superior y bachillerato al logro de los objetivos de aprendizaje definidos para una unidad, programa de asignatura o área de conocimiento, fijados para cada uno de los grados, cursos, subniveles y niveles correspondientes del Sistema Nacional de Educación (LOEI, 2023). Según LOES (2018), se afirma lo siguiente: La Ley Orgánica de Educación Superior (LOES) señala en su artículo 344 de la Sección Primera, Educación, del Título VII del Régimen del Buen Vivir de la Constitución de la República del Ecuador, determina que el sistema nacional de educación comprenderá las instituciones, programas, políticas, recursos y actores del proceso educativo, así como acciones en los niveles de educación inicial, básica y bachillerato, y estará articulado con el Sistema de Educación Superior (LOES, 2018)

PROTECCIÓN DE DATOS Según (Ordoñez, 2017), se afirma lo siguiente: Con la evolución de la tecnología, la sociedad se ha enfrentado a importantes desafíos a la hora de proteger ciertos intereses jurídicamente salvaguardados a través del concepto de privacidad. Estos intereses requieren ahora una protección más específica e integral, proporcionada por el derecho a la protección de datos o a la autodeterminación informativa.

DERECHO DE LA PROTECCIÓN DE LOS DATOS (Rodotà, 1997) se afirma lo siguiente: El primero está mencionado en el artículo 7, que en resumen reproduce el esquema del artículo 8 del Convenio Europeo de Derechos Humanos. El segundo, recogido en el artículo 8 de la Carta, consagra el carácter autónomo del derecho fundamental, distinto del derecho a la tutela de la vida privada.

EJERCICIO DE DERECHO .- Según (LOPDP, 2021) se afirma lo siguiente: El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales. Según RLOPDP (2023), se afirma lo siguiente: La vulnerabilidad de los datos en el Artículo 24 de la notificación de la vulneración de seguridad. - De conformidad con la ley, el responsable del tratamiento deberá notificar a las autoridades de la protección de datos personales y la agencia de regulación y control de telecomunicaciones.

Capítulo II. Diagnostico Situacional

El análisis situacional para el desarrollo de sistemas de protección de datos con estándares ISO 27001 implicó la implementación de un proceso metodológico que ayudó a identificar activos con el fin de salvaguardar los datos de estudiantes y docentes en caso de que la información estuviera cifrada durante un ataque de ciberdelito, garantizando así la protección de datos.

2.1. Enfoque:

El proyecto de investigación adoptó un enfoque cuali-cuantitativo. Se emplearon parámetros de medición en la variable independiente, junto con juicios de valor sobre la aplicación de las normas ISO/27001 en la gestión de Sistemas de Información (SI). La fuente principal de información fue los activos y recursos tecnológicos del Departamento de Tecnologías de la Información (TI) y la Secretaría de la Unidad Educativa La Inmaculada.

2.2. Modalidad básica de la investigación.

Investigación Aplicada.

El presente proyecto de investigación tiene como enfoque buscar estrategias y políticas que permitan mejorar la seguridad de la información que posee la Institución Educativa en cuanto a la protección de datos.

Investigación Bibliográfica.

La investigación bibliográfica se fundamentó en artículos científicos, sitios web, investigaciones previas, revistas y legislación existente para desarrollar un marco teórico sobre el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 y su impacto en los procesos de sistemas informáticos.

2.3. Nivel o tipo de investigación.

Experimental:

El enfoque experimental de la investigación implicó la aplicación de la gestión del Sistema de Información a través del SGSI en procesos de análisis de datos. Se utilizó el estándar ISO 27001 para observar los resultados y establecer la situación actual de la confidencialidad de la información.

Descriptiva:

La investigación descriptiva se llevó a cabo para explorar en profundidad el problema, sus causas, sus consecuencias y las dificultades que enfrentó.

Explicativa:

La investigación adoptó una perspectiva explicativa, ya que logró fundamentar de manera convincente la relevancia de la gestión de sistemas de información en los protocolos de seguridad mediante el empleo de la norma ISO 27001.

Población y Muestra:

La investigación se centró en el personal del departamento de Tecnologías de la Información (TI), Secretaría, Contabilidad e Inspección General de la Institución Educativa de la Ciudad de Ambato, específicamente en la Unidad Educativa La Inmaculada. Dado que el tamaño de la población era inferior a 60, no fue necesario realizar un muestreo.

2.4. Metodología

La presente investigación se fundamenta en los estándares de las siguientes normas para su análisis detallado

2.4.1. Norma ISO /IEC 27001

La norma ISO/IEC 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) en el contexto de los riesgos de seguridad de la información que enfrenta una empresa. Esta norma proporciona un marco para que las organizaciones desarrollen políticas y procedimientos para proteger la confidencialidad, integridad y disponibilidad de la información que poseen.

2.4.2. Norma ISO / IEC 27701:2019

Por otro lado, la ISO/IEC 27701:2019 es una extensión de la norma ISO/IEC 27001, que se enfoca específicamente en la gestión de la privacidad de la información, proporcionando pautas para las organizaciones sobre cómo gestionar los riesgos relacionados con la privacidad y cómo cumplir con requisitos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

2.4.3. Norma ISO /IEC 27001:2020

La norma ISO/IEC 27001:2020 es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Fue desarrollada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

2.4.4. Normas ISO 27005:2008

Normas ISO 27005:2008 es una norma internacional que proporciona directrices para la gestión de riesgos de seguridad de la información dentro de una organización. Está diseñado para ayudar a las organizaciones a establecer un marco y un proceso sistemático para identificar, analizar y gestionar los riesgos relacionados con la seguridad de la información.

La norma ISO/27001 se basa en el ciclo de Deming, también conocido como PDCA(Gobierno Electrónico de Ecuador, (s/f), n.d.) Planificar-Hacer-Verificar-Actuar). Según la publicación del Ministerio de Telecomunicaciones, cada fase se define de la siguiente manera:

- **Planificar**: Comprender el contexto de la organización y las partes interesadas, establecer objetivos y asignar los recursos necesarios para el proyecto.
- **Hacer**: Implementar lo planificado, incluyendo el análisis y la evaluación de riesgos, así como la elaboración y ejecución del plan de comunicación.
- **Verificar**: Controlar y medir la efectividad de los procesos del negocio, monitoreando y revisando los resultados para asegurar el alineamiento con los objetivos y proteger la confidencialidad, integridad y disponibilidad de los datos.
- **Actuar**: Realizar mejoras continuas, identificando desviaciones de los objetivos planteados por la institución.

2.5. Elaboración de actividades para la protección de datos

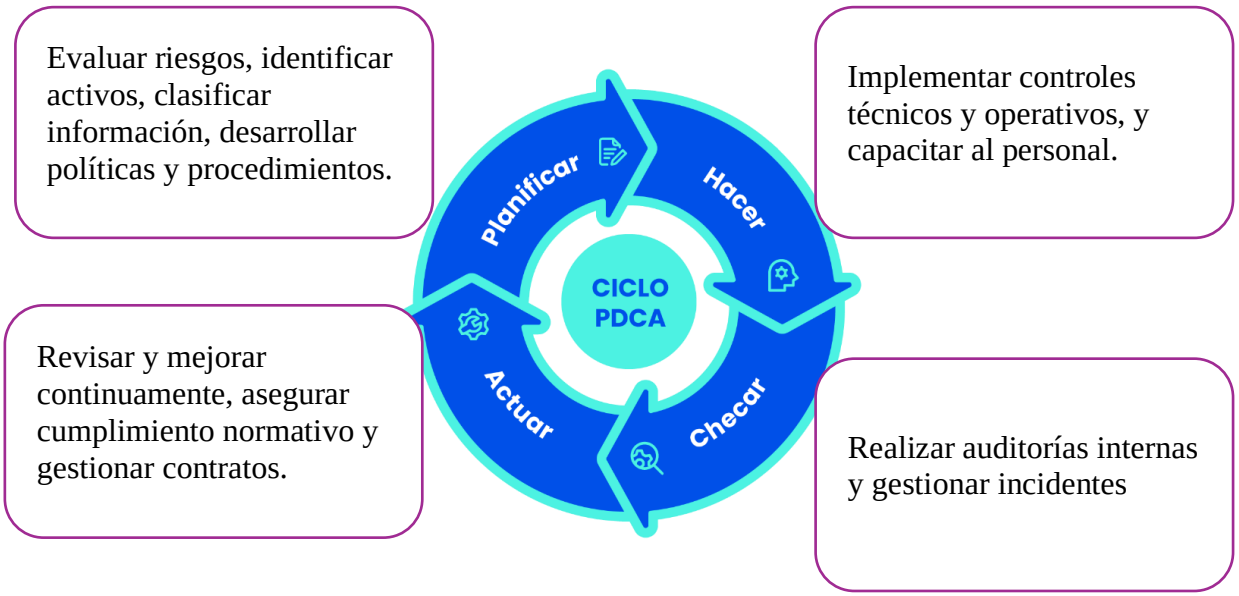
La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 en una Unidad Educativa La Inmaculada implica una serie de actividades y controles destinados a proteger los datos de estudiantes, personales y otros actores involucrados. Aquí tienes una lista detallada de actividades que puedes considerar:

- Siguiendo la metodología establecida, nos hemos basado en la norma ISO 27001 para orientar nuestras acciones dentro del ciclo de Deming, específicamente en el punto 2.2. Esta normativa nos proporciona un marco sólido para definir y ejecutar las actividades necesarias, garantizando así la efectividad y la seguridad en nuestros procesos.
- Diagramar la red sobre la infraestructura tecnológica de UELI.

- Identificar y evaluar los riesgos a los que están expuestos los datos e información en la institución.
- Listar todos los activos de información, incluyendo hardware, software, bases de datos y documentos físicos y digitales.
- Clasificar la información según su nivel de sensibilidad y criticidad (pública, interna, confidencial).
- Crear políticas claras que establezcan cómo se debe manejar y proteger la información.
- Establecer y mantener procedimientos de respaldo y recuperación de datos.
- Asegúrese de que todos los sistemas y aplicaciones estén actualizados con sus respectivas licencias y con los últimos parches de seguridad; utilizar antivirus en cada departamento.
- Mantener un registro de todos los incidentes de seguridad, sus causas y las acciones tomadas para resolverlos.
- Evaluación de desempeño.
- Mejora continua.

Figura 7

Ciclo de Deming para las actividades de la protección de datos



Fuente Elaborado por el autor basado evidentemente en lo investigado

Todas estas actividades se detallarán en el capítulo III del presente proyecto de investigación

2.6. Estructura Organizacional.

2.6.1. Contexto de la organización.

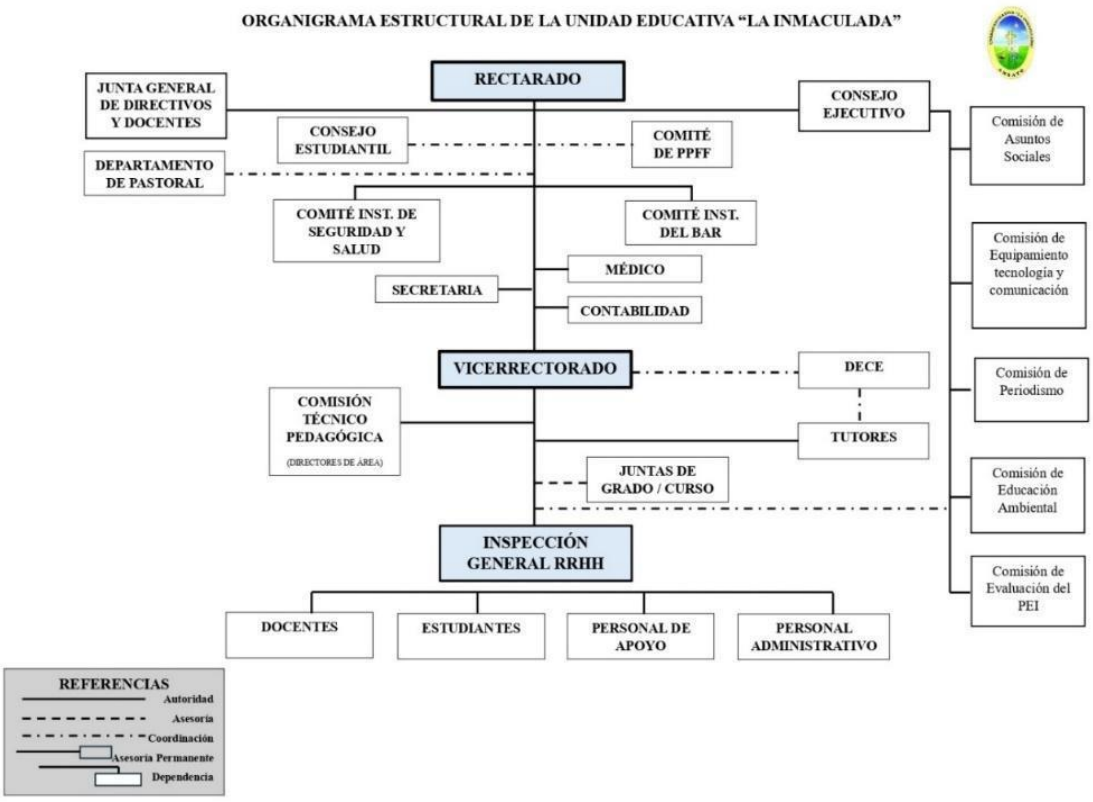
La Unidad Educativa La Inmaculada, ubicada en el sector de Miraflores en Ambato, es una destacada institución con 61 años de trayectoria en la educación, consolidándose como un referente en la región. Su estructura organizativa incluye un rectorado, un vicerrectorado y una inspección general, los cuales aseguran la implementación de políticas educativas efectivas y el desarrollo integral de sus estudiantes. El equipo administrativo está conformado por nueve personas, mientras que el plantel cuenta con 46 docentes capacitados y ocho miembros del personal de apoyo, quienes juntos crean un ambiente educativo propicio.

La infraestructura de la institución incluye dos laboratorios de computación, internet y cámaras de vigilancia para la seguridad. El rectorado supervisa varios comités y personal clave, mientras que el vicerrectorado gestiona la comisión técnico-pedagógica y el departamento de Consejería Estudiantil (DECE). La inspección general, además de sus tareas habituales, apoya en la gestión de recursos humanos, asegurando una armoniosa colaboración entre docentes, estudiantes y personal administrativo, todo orientado al logro de los objetivos institucionales.

A continuación, se detalla la estructura organizacional de la Unidad Educativa La Inmaculada.

Figura 8

Organigrama funcional de la UELI



Fuente Elaborado por el autor basado evidentemente en lo investigado

2.6.2 FODA.

Tabla 2

FODA

Fortaleza	Oportunidades	Debilidades	Amenazas
F1.- Conciencia sobre la importancia de la protección de datos. F2. Acceso a recursos educativos. F3.- Apoyo de la dirección. F4.- Profesionales capacitados. F5.- Imagen y posicionamiento institucional.	**O1.** Participación en redes educativas. **O2.** Colaboración con expertos externos. **O3.** Provisión de un servicio educativo de calidad y calidez para los estudiantes de la ciudad.	D1. Ausencia de conciencia sobre la seguridad de la información. D2. Carencia de políticas para la gestión de la información. D3. Falta de directrices para la generación de contraseñas de acceso a la información. D4. Documentos en formato físico sin respaldo digital. D5. Ausencia de políticas para la eliminación de documentos.	A1. Pérdida de estudiantes que eligen otras instituciones. A2. Robo de información. A3. Acceso físico no autorizado a la institución. A4. Ciberataques en el centro educativo.

Fuente Elaborado por el autor basado evidentemente en lo investigado

2.6.3 Partes interesada.

Rectorado: El rector/a es el máximo responsable administrativo y académico de la institución educativa. Supervisa todas las actividades, establece políticas, dirige la implementación del plan estratégico y representa a la institución ante la comunidad educativa y otras entidades.

Vicerrectorado: Los vicerrectores son designados por el rector y actúan como sus principales colaboradores, su función es apoyar al rector en la gestión y coordinación de las actividades correspondientes a su área.

Inspector General: El inspector general es responsable de supervisar y evaluar el funcionamiento de la institución educativa, así como el cumplimiento de los programas académicos y las normativas establecidas por el Ministerio de Educación y otras autoridades pertinentes. También brinda asesoramiento y apoyo al cuerpo docente para mejorar la calidad educativa.

Secretario/a: El secretario/a es el encargado de la gestión administrativa y documental de la institución educativa. Entre sus responsabilidades se encuentran la redacción y archivo de actas, la atención a la correspondencia oficial, la coordinación de trámites administrativos y la organización de la agenda del rector y otros directivos.

Contadora: La contadora se encarga de la gestión financiera y contable de la institución educativa. Esto incluye la elaboración de presupuestos, la gestión de ingresos y egresos, la presentación de informes financieros, la supervisión del cumplimiento de obligaciones fiscales y la planificación económica a corto y largo plazo.

Técnico de Tecnologías de la Información (TI): El Técnico de TI es responsable de la gestión y mantenimiento de la infraestructura tecnológica de la institución educativa. Esto incluye la administración de redes, sistemas y bases de datos, la implementación de soluciones tecnológicas para mejorar los procesos educativos y administrativos, y la garantía de la seguridad

de la información. También puede estar a cargo del desarrollo e implementación de estrategias digitales para la enseñanza y el aprendizaje.

2.7. Análisis del entorno actual

En el contexto actual de la Unidad Educativa La Inmaculada, resulta fundamental establecer un Sistema de Gestión de Seguridad de la Información (SGSI) robusto con el fin de proteger eficazmente la gran cantidad de datos sensibles que maneja, tales como información de estudiantes, docentes, calificaciones y datos financieros. Para garantizar esta protección, se requiere una infraestructura mínima que incluya una arquitectura de seguridad integral compuesta por firewalls avanzados, sistemas de detección y prevención de intrusiones (IDS/IPS), encriptación tanto de datos en tránsito como en reposo, así como soluciones de respaldo. y recuperación ante desastres.

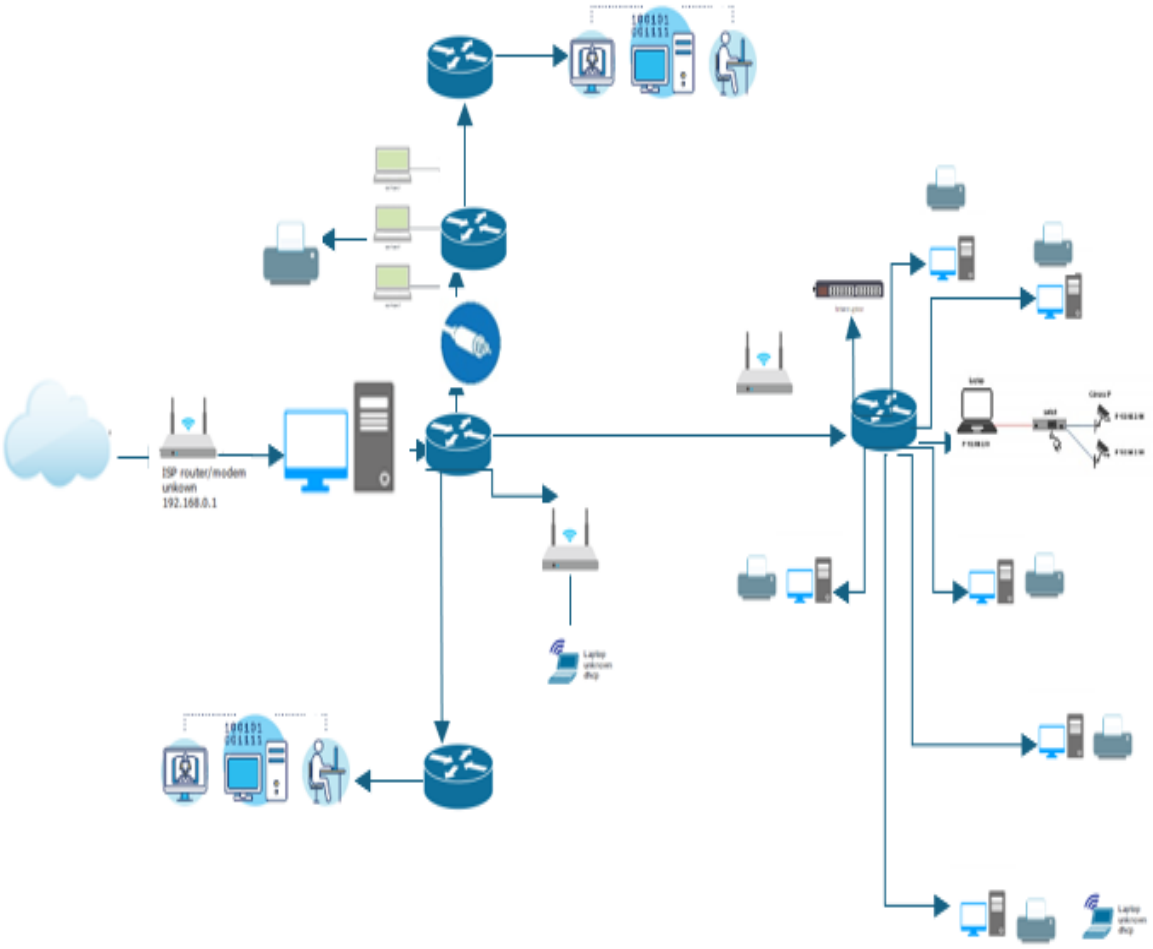
Además, es esencial implementar políticas de gestión de accesos y autenticación multifactor (MFA) para garantizar que únicamente el personal autorizado tenga acceso a la información crítica. Ante el creciente riesgo de ciberataques que podrían comprometer la infraestructura actual, se hace necesario llevar a cabo una evaluación continua de vulnerabilidades y actualizar periódicamente las medidas de seguridad, con el objetivo de mitigar posibles brechas y asegurar la resiliencia del sistema.

2.8. Diagrama de red actual de los activos en la protección datos

El diagrama siguiente ofrece una visión general de los dispositivos con el propósito de identificar todos los activos y realizar un análisis de riesgos e impacto, teniendo en cuenta un potencial ciberataque.

Figura 9

Diagrama de red actual de los activos en la protección datos



Fuente Elaborado por el autor basado evidentemente en lo investigado

2.9. Metodología para levantamiento del inventario de activos de información y evaluación del riesgo de seguridad de la información

La metodología que se utilizará para realizar el análisis de riesgos en el presente proyecto es la norma ISO/IEC 27005:2008, la cual proporciona directrices para gestionar el riesgo en la seguridad de la información dentro de una organización. Esta norma da soporte a los requisitos

de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001. También se contará con la ayuda de la norma ISO/IEC 27001:2013 y los controles definidos en la norma ISO/IEC 27002:2013.

2.9.1. Identificación de Activos

Los activos son todos los elementos que una organización posee para el tratamiento de la información, incluyendo hardware, software, recursos humanos, entre otros. **(Anexos 3)** Es importante agrupar estos activos según la función que desempeñan en el manejo de la información y en la protección de datos. La Unidad Educativa La Inmaculada cuenta con diversos activos esenciales para el desarrollo de sus actividades, tales como:

2.9.1.1. Servicios

Correo Electrónico Corporativo: Es un servicio de correo electrónico proporcionado por una organización para el uso interno y externo de sus empleados y miembros, generalmente utilizando un dominio personalizado de la empresa.

Sitio Web: Es un conjunto de páginas web accesibles a través de Internet que suelen estar relacionadas con un dominio específico y que contienen información, imágenes, vídeos u otros contenidos.

Sistemas de Gestión Académica: El Sistema de Gestión Académica (SGA) es una herramienta tecnológica creada para asistir a las instituciones educativas en la administración y organización de sus tareas tanto administrativas como académicas de manera eficaz. Este tipo de sistema facilita y automatiza una gran cantidad de procesos y funciones dentro de las unidades educativas.

2.9.1.2. Datos e Información

- **Base de datos**. - Una base de datos es un conjunto organizado de datos, generalmente almacenados y accesibles electrónicamente desde un sistema informático.
- **Código fuente. -** Por código fuente se entiende todo texto legible por un ser humano y redactado en un lenguaje de programación determinado.
- **Manual de procedimiento.** - Un manual de procedimientos es un documento que detalla una serie de instrucciones paso a paso para realizar tareas y operaciones específicas dentro de una organización.
- **Políticas de privacidad.** - Son documentos legales que establecen cómo una organización recopila, utiliza y protege la información personal de los usuarios que interactúan con sus servicios o sitio web.
- **Documentos físicos. -** Son documentos impresos en papel que contienen información escrita o gráfica.
- **Documentos contables**. - Son registros financieros que documentan transacciones comerciales, ingresos, gastos y otros aspectos económicos de una organización.

2.9.1.3. Aplicaciones de Software

- **Windows:** Es un sistema operativo desarrollado por Microsoft, utilizado ampliamente en computadoras personales.
- **Sistemas Linux:** Se refiere a los sistemas operativos basados en el núcleo Linux, que son conocidos por su robustez, seguridad y flexibilidad, y son utilizados en una amplia gama de dispositivos y servidores.
- **Microsoft Office:** Es una suite de aplicaciones de productividad (como Word, Excel, PowerPoint, etc.) desarrollada por Microsoft.

- **Adobe Macromedia:** Se refiere a productos y tecnologías desarrollados por Macromedia, que fue adquirida por Adobe, como Flash y Dreamweaver.
- **Software gratuito**: Son programas de computadora que se distribuyen sin costo alguno y permiten a los usuarios utilizar, estudiar, modificar y redistribuir el software según los términos de su licencia.
- **Koinor**: Es un sistema de contabilidad para el manejo de ingresos y egresos, gastos que maneja la institución.
- **Antivirus**: Es un software diseñado para detectar, prevenir y eliminar software malicioso (malware) como virus, gusanos, troyanos, etc.
- **UniFi**: Es una marca y plataforma de productos de redes y comunicaciones desarrollada por Ubiquiti Networks, que incluye dispositivos para redes Wi-Fi, switches y cámaras IP, entre otros.

2.9.1.4. Equipos Informáticos

- **Router**: Equipo que permite redireccionar el servicio recibido por la operadora de telefonía a la central interna a través de la red local.
- **Switch Cisco**: Equipo que administra el flujo de la red interna y gestiona las VLAN creadas para el servicio SIP recibido de la telefonía y la central telefónica.
- **Servidores de BD:** Donde se almacena toda la información para cargar el sistema y, a su vez, mantiene la información para reportes de incidentes.
- **Red de datos:** Está conformada por cableado estructurado Cat 6A y cables de fibra para conexión vertical.

- **Red WiFi:** Es una red de área local inalámbrica que permite la conexión de dispositivos mediante tecnología WiFi, utilizando un enrutador o punto de acceso inalámbrico.

2.9.1.5. Recurso Humano

- **Padre de Familia:** Es la persona responsable de cuidar y educar a sus hijos. Su papel es vital para el bienestar de los niños, ofreciendo apoyo emocional, financiero y educativo.
- **Estudiantes:** Personas que asisten a escuelas para aprender. Se dedican al estudio y participan en actividades académicas guiadas por maestros.
- **Personal administrativo**: Empleados que apoyan en instituciones educativas y organizaciones. Se encargan de gestionar recursos humanos, finanzas, logística y mantenimiento de instalaciones.
- **Encargado de TI:** Responsable de gestionar y mantener los sistemas informáticos en una organización. Incluye administración de redes, soporte técnico, seguridad informática e implementación de tecnologías innovadoras.
- **Autoridades en el contexto educativo:** Son líderes y administradores responsables de gestionar instituciones educativas, como directores y supervisores.

2.9.2 Codificación y etiquetado de activos

De acuerdo con cada tipo de activo, se etiquetará la lista de activos identificados en este caso de estudio como resultado de la concatenación del área a la que pertenece el activo, más el tipo, el año actual y un número secuencial.

2.9.2.1. Etiquetación Área

Tabla 3

Etiqueta de las diferentes áreas

Área	Identificación
Secretaria	SEC
Contabilidad	CON
Tecnología	TIC
Inspección	INS

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla # 3 se detallan las áreas donde se investigarán los activos. Cada área desempeña un rol específico y esencial dentro de la Unidad Educativa, y cuenta con identificaciones únicas que facilitan su reconocimiento y referencia

2.9.2.2. Etiquetación Tipo de Activo

Tabla 4

Etiqueta para los tipos de activos

Activo	Identificación
Recurso humano	RRHH
Servicios	SERV
Datos e Información	DEI
Aplicaciones de Software	APS
Equipos Informáticos	EQU
Redes de Comunicación	RDC

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #4 se enumeran los distintos tipos de activos que la Unidad Educativa podría poseer, cada uno de ellos identificado con una etiqueta específica diseñada para facilitar su gestión y análisis.

2.9.3 Análisis de riesgos

Frente a una posible amenaza, como un ataque cibernético, ahora tenemos la capacidad de llevar a cabo un análisis utilizando los parámetros de frecuencia y el nivel de vulnerabilidad.

2.9.3.1. Criterios para la valoración de activos

La ISO 27005:2008 establece un método para evaluar cualitativamente los activos de información. Se utilizan términos como bajo, medio y alto. La elección del término depende de los requisitos de seguridad de la Institución Educativa.

Se ha implementado un sistema de evaluación cualitativa de activos de información según la norma ISO 27001. Se utilizan clasificaciones de bajo, medio y alto, basadas en requisitos de seguridad específicos de la Institución Educativa.

La valoración de los activos se realizó con base a la siguiente tabla:

Tabla 5

Valoración de los activos

Nivel de Valor	Valor	Criterio
1	No aplica	No aplica criterio de importancia para el activo
2	Muy Bajo	El activo afecta procesos.
4	Bajo	El activo puede afectar una tarea aislada de la operación o del proceso.
6	Medio	El activo puede afectar de forma parcial una operación o un proceso.
8	Alto	Uno o varios procesos pueden ser seriamente afectados.
10	Crítico	La organización se ve seriamente afectada y puede generar sanciones elevadas y afectar la credibilidad de la organización y sus procesos

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #5 se presentan los valores críticos de los activos, los cuales pueden evaluarse según el análisis de riesgos, utilizando las normas ISO 2700.

2.9.3.2. Valoración de activos por tipo

A continuación, se presentan los activos de información con su respectiva valoración de acuerdo con la tabla presentada previamente. Estos resultados fueron obtenidos en base al formato detalla en el del **ANEXO 4** donde se separa por el tipo de activo y la valoración final, que es el promedio dado por la valoración individual sobre la confidencialidad, integridad y la disponibilidad.

Tabla 6

Valoración de activos de Redes de comunicación

Tipo de activo	Descripción del Activo	Valoración del activo
Redes de comunicación	Redes de fibra óptica:	6
	Red LAN	4

	Redes de comunicación	6
	Antena Direccional	6

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #6 se describen los activos de las redes de comunicación junto con sus valores críticos, los cuales están en niveles específicos. Se identificaron tres activos con un valor de (4) y un activo con un valor de (6).

Tabla 7
Valoración de activos de Equipos Informáticos

Tipo de activo	**Descripción del Activo**	**Valoración del activo**
Equipos Informáticos	Router	4
	Switch cisco	4
	Servidores de BD	8
	Red de datos	6
	Antena Direccional	4
	Red Wifi.	4

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #7 se detallan los tipos activos de los equipos informáticos junto con sus valores críticos. Se identificaron cuatro activos con un valor medio de (4), un activo con un valor (6) y un activo con un valor alto de (8).

Tabla 8

Valoración de activos de Aplicaciones de Software

Tipo de activo	Descripción del Activo	Clasificación
Software	Windows	8
	Linux	4
	Microsoft Office	4
	Softwares gratuitos	4
	Koinor	6
	Facturación electrónica	6
	Aplicaciones Web	6
	Software del biometrico	6
	Sistema de Gestión de Video	6
	Antivirus	6
	UniFi	6
	Firewall	8

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #8 se detallan los tipos de activos relacionados al software junto con sus valores críticos. Se identificaron tres activos con un valor bajo de 4, siete activos con un valor medio de (6) y dos activos con un valor alto de (8).

Tabla 9

Valoración de activos de personas

Tipo de activo	Descripción del Activo	Valoración del activo
Personal	Encargado de TI	6
	Contadora	4
	Auxiliar de contabilidad	2
	Padre de Familia	1
	Estudiantes	1
	Secretaria	4
	Inspector General	6

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #9 se detallan los tipos de activos relacionados con el personal que trabaja en la Unidad Educativa, junto con sus valores críticos. Se identificaron dos activos con valor no aplica 1, un activo con valor Muy bajo (2), dos activos con valor bajo (4) y dos activos con valor medio (6).

Tabla 10

Valoración de activos de infraestructura

Tipo de activo	Descripción del Activo	Valoración del activo
Instalaciones	Edificio	6
	Instalación eléctrica	6
	Antena Direccional	4
	Red de datos	4

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #10 se detallan los tipos de activos relacionados con los activos de infraestructura que trabaja en la Unidad Educativa, junto con sus valores críticos. Se identificaron dos activos con valor bajo (4), dos activos con valor medio (6).

Tabla 11

Valoración de activos de Datos e información

Tipo de activo	Descripción del Activo	Valoración del activo
Datos e Información	Manual de procedimiento	4
	Base de datos	8
	Documentación TI	4
	Registros	6
	Documentos Físicos	8
	Documentos Contables	6
	Informes de auditoría	4
	Grabaciones de Vigilancia	6
	Políticas de Seguridad	8

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #11 se detallan los tipos de activos relacionados con los activos de Datos e información que trabaja en la Unidad Educativa, junto con sus valores críticos. Se identificaron dos activos con valor bajo (4), tres activos con valor medio (6) y 3 activos con valor alto (8).

2.10. Clasificación del activo de información

Un incidente de seguridad de la información puede variar en impacto según el activo involucrado. Considerando esto, se ha evaluado cada activo determinando el nivel de daño que un incidente podría causar en términos de confidencialidad, integridad y disponibilidad, evaluados de forma independiente.

Para clasificar los activos, se usaron los siguientes criterios:

- **Confidencial**: Información privada, accesible únicamente por personal autorizado.
- **Uso Interno:** Información con acceso controlado, disponible solo para personal interno.
- **Pública**: Información accesible para usuarios internos y externos.

A continuación, se enumeran los activos según su clasificación definitiva:

Tabla 12

Clasificación de activos de redes de comunicación

Tipo de activo	Descripción del Activo	Clasificación
Redes de comunicación	Redes de fibra óptica:	Confidencial
	Red LAN	Uso Interno
	Redes de comunicación	Uso Interno
	Antena Direccional	Uso Interno

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #12 se detallan los activos de redes de comunicación que se manejan en la Unidad Educativa, junto con su clasificación correspondiente. Se identificaron tres activos clasificados para (uso interno) y uno clasificado como (Confidencial).

Tabla 13

Clasificación de activos de equipos informáticos

Tipo de activo	Descripción del Activo	Clasificación
Equipos Informáticos	Router	Confidencial

	Switch cisco	Confidencial
	Servidores de BD	Confidencial
	Red de datos	Interno
	Antena Direccional	Confidencial
	Red Wifi.	Interno
	Firewall	Confidencial

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #13 se detallan los activos de los equipos informáticos que se manejan en la Unidad Educativa, junto con su clasificación correspondiente. Se identificaron dos activos clasificados para (uso interno) y cinco activos clasificados como (Confidencial).

Tabla 14

Clasificación de activos de aplicaciones de software

Tipo de activo	Descripción del Activo	Clasificación
Aplicaciones de Software	Windows	Uso Interno
	Linux	Uso Interno
	Microsoft Office	Uso Interno
	Softwares gratuitos	Uso Interno
	Software de Contabilidad Koinor	Confidencial
	Facturación electrónica	Confidencial
	Aplicaciones Web	Uso Interno
	Software del biometrico	Confidencial
	Sistema de Gestión de Video	Confidencial
	UniFi	Confidencial
	Antivirus	Uso Interno

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #14 se detallan los activos de aplicación de software que se manejan en la Unidad Educativa, junto con su clasificación correspondiente. Se identificaron siete activos clasificados para (uso interno) y cinco clasificados como (Confidencial).

Tabla 15

Clasificación de activos de datos e información

Tipo de activo	Descripción del Activo	Clasificación
Datos e Información	Manual de procedimiento	Uso Interno
	Base de datos	Confidencial
	Documentación TI	Uso Interno
	Registros	Uso Interno
	Documentos Físicos	Confidencial
	Documentos Contables	Confidencial
	Informes de auditoría	Uso Interno
	Grabaciones de Vigilancia	Confidencial
	Políticas de Seguridad	Uso Interno

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #15 se detallan los activos de datos informativos que se manejan en la Unidad Educativa, junto con su clasificación correspondiente. Se identificaron cinco activos clasificados para (uso interno) y cuatro clasificados como (Confidencial).

2.11. Importancia del activo de información

La fórmula proporcionada para calcular el valor total de un activo de información es:

$$Valor\ Total = \frac{VD + VI + VD}{3}$$

Donde:

- **VD**: Valor de Disponibilidad
- **VI**: Valor de Integridad
- **VD**: Valor de Confidencialidad

Paso a Paso para la Valoración

- **Identificación de los Activos de Información**: Identificar todos los activos de información dentro de la organización.
- **Evaluación de la Disponibilidad (VD)**: Determinar el impacto y la importancia de que la información esté disponible cuando se necesite.
- **Evaluación de la Integridad (VI)**: Evaluar la importancia de que la información sea precisa y no esté alterada.
- **Evaluación de la Confidencialidad (VC)**: Evaluar la necesidad de que la información sea accesible solo para las personas autorizadas.
- **Cálculo del Valor Total**: Aplicar la fórmula para obtener un valor promedio que refleje la importancia global del activo de información.

El valor obtenido se coteja con la siguiente escala:

- **Prescindible:** Existe una baja probabilidad de que la falla de este activo cause pérdidas en la Unidad Educativa.
- **Importante:** Hay una probabilidad media de que la falla de este activo pueda causar pérdidas en la Unidad Educativa.
- **Grave:** La probabilidad de que la falla de este activo cause pérdidas en la Unidad Educativa es alta.

En la siguiente tabla se detalla la importancia de cada activo:

Tabla 16

Importancia de activos de redes de comunicación

Tipo de activo	Descripción del Activo	Importancia
Redes de comunicación	Redes de fibra óptica	Grave
	Red LAN	Grave
	Redes de comunicación	grave
	Antena Direccional	Importante

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #16 se detallan los activos de redes de comunicación utilizados en la Unidad Educativa. Según su importancia, se identifican tres activos valorados como 'graves' y un activo valorado como 'importante'.

Tabla 17

Importancia de activos de equipos informáticos

Tipo de activo	Descripción del Activo	Importancia
Equipos Informáticos	Router	Grave
	Switch cisco	Grave
	PC Servidores de BD	Grave
	Central Telefónica	Importante
	Wifi.	Importante

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #17 se detallan los activos de los equipos informáticos utilizados en la Unidad Educativa. Según su importancia, se identifican tres activos valorados como “graves” y dos activos valorados como “importante”.

Tabla 18

Importancia de activos de Aplicaciones de Software

Tipo de activo	**Descripción del Activo**	**Importancia**
Aplicaciones de Software	Windows	Grave
	Linux	Grave
	Microsoft Office	Importante
	Adobe Macromedia	Prescindible
	Softwares gratuitos	Prescindible
	Software de contabilidad Koinor	Grave
	Facturación electrónica	Grave
	Software del biométrico	Grave
	Sistema de Gestión de Video	Importante
	Antivirus	Importante
	UniFi	Grave
	Aplicaciones Web	Importante

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #18 se detallan los activos de las aplicaciones de software que son utilizados en la Unidad Educativa. Según su importancia, se identifican seis activos valorados como “graves”, cuatro activos valorados como “importante” y dos activos valorados como “prescindibles”

Tabla 19

Importancia de activos de datos e información

Tipo de activo	Descripción del Activo	Importancia
Datos e Información	Manual de procedimiento	Importante
	Base de datos	Grave
	Documentación TI	Grave
	Registros	Grave
	Documentos Físicos	Importante
	Documentos Contables	Importante
	Informes de auditoría	Grave
	Grabaciones de Vigilancia	Grave
	Políticas de Seguridad	Importante

Fuente Elaborado por el autor basado evidentemente en lo investigado

En la Tabla #19 se detallan los activos de datos de información que son utilizados en la Unidad Educativa. Según su importancia, se identifican cinco activos valorados como 'graves', cuatro activos valorados como 'importante'.

2.12. Lista de activos con mayor riesgo

De acuerdo con las valoraciones realizadas, se obtuvo que los activos cuya pérdida supondría un riesgo grave son los siguientes:

Tabla 20
Lista de activos con mayor riesgo

Activos con mayor riesgo
Redes de fibra óptica
Red LAN
Redes de comunicación
Router
PC Servidores de BD
Windows Linux Actualización
Software del biométrico
UniFi
Base de datos
Documentación TI
Registros
Grabaciones de Vigilancia

Fuente Elaborado por el autor basado evidentemente en lo investigado

2.13. Catálogo de amenazas

Existen numerosos catálogos de amenazas en los cuales se basará el catálogo de amenazas comunes NTE INEN-ISO/IEC 27005:2012 en el (**Anexo 1**) de catálogos de amenazas.

De acuerdo con el alcance planteado sobre los ciberataques globales, también han impactado a Ecuador. Ataques como ransomware, phishing a la infraestructura de la organización, y considerando que dentro del catálogo de amenazas no existe un registro puntual con esta descripción, pero por la naturaleza de la amenaza se ha considerado el segmento de "**Compromiso de la información** " para enmarcar los ciberataques.

2.14. Frecuencia o Probabilidad de ocurrencia

Al evaluar la amenaza de ciberataques, se analiza la posibilidad de que ocurran o la frecuencia con la que podrían manifestarse, asignándoles un valor según su grado dentro de una escala determinada.

Tabla 21.

Matriz Térmica de Riesgos.

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

Fuente: Adaptada matriz de riesgo (Mintel, 2022a)

2.15. Nivel de Vulnerabilidad

El nivel de vulnerabilidad evalúa las posibles consecuencias de la pérdida de información si la amenaza llegara a materializarse. Se centra en determinar el impacto que sufriría la organización una vez que la amenaza se concreta.

2.16. Evaluación de riesgos

Figura 10

Evaluación de Riesgos

	Riesgo Muy Alto. Requiere medidas de prevención de manera urgente. El inicio de un proyecto requiere de la aplicación de medidas preventivas urgentes
	Riesgo Alto. Las medidas preventivas son obligatorias. Se debe tener el control de las variables de riesgo durante el proceso del proyecto.
	Riesgo Medio. Estudiar económicamente si hay la posibilidad de introducir medidas preventivas para poder reducir el nivel de riesgo. En caso de no ser posible, hay que mantener las variables controladas.
	Riesgo Bajo. Se vigilará, aunque no requiere medidas preventivas iniciales.

Fuente: Adaptada matriz de riesgo (Mintel, 2022a)

Se realiza una evaluación comparativa entre la estimación del riesgo y un criterio de riesgo predefinido para determinar su relevancia. La evaluación numérica del riesgo se fundamenta en la valoración de los activos de información, el impacto generado por posibles amenazas y la probabilidad de que se aproveche una vulnerabilidad

2.17. Fórmula para calcular el grado de riesgo

Grado de Riesgo=Probabilidad × 1Impacto

Donde:

La **probabilidad** es la posibilidad de que ocurra un evento no deseado.

El **impacto** es la magnitud del daño o consecuencia si el evento ocurre.

Según el resultado obtenido para el nivel de riesgo, se crea la siguiente tabla para evaluar de manera cualitativa los niveles de riesgo de los activos, utilizando la matriz térmica indicada en la tabla 21

Tabla 22

Nivel de riesgo

NIVEL DE RIESGO		
1	3	BAJO
4	9	MEDIO
10	1	ALTO
15	25	MUY ALTO

Fuente: Adaptada matriz de riesgo (Mintel, 2022

2.18. Tratamiento de riesgos

Según el nivel de riesgo identificado en cada activo, se proponen las siguientes medidas para analizar cómo abordar esos riesgos. Estas propuestas se basan en el documento "**Formato Referencial_Matriz de Evaluación de Riesgos de Seguridad de la Información (EGSI-V2)**" publicado por el MINTEL en su sitio web (Mintel, 2022b)

Tabla 23

Tratamiento del riesgo

OPCIONES DE TRATAMIENTO	
MITIGAR, REDUCIR O MODIFICAR EL RIESGO	Selección de uno o varios controles para reducir el riesgo a un nivel aceptable para la institución ej. Implementar políticas de control de acceso
EVITAR EL RIESGO	Eliminar la actividad de alto riesgo o cambiar las condiciones bajo las cuales la actividad es operada (remover el riesgo)
TRANSFERIR O DESVIAR EL RIESGO	Trasferir el riesgo a otra entidad interna o externa mediante: el traspaso de la gestión del activo y/o del riesgo, pólizas de seguros o tercerización seguros, etc., para cambiar o compartir la responsabilidad de la pérdida.
ACEPTAR O RETENER EL RIESGO	Tomar la decisión de aceptar las consecuencias de un riesgo en particular, es decir, no se realiza ninguna acción respecto al riesgo

Fuente: Adaptada matriz de riesgo (Mintel, 2022a)

Según la vulnerabilidad de cada activo, se establece una escala para decidir la acción adecuada para manejar el riesgo.

Tabla 24

Riesgo Residual

RIESGO RESIDUAL		
1	3	ACEPTAR
4	2 7	MITIGAR / EVITAR / TRANSFERIR

Fuente: Adaptada matriz de riesgo (Mintel, 2022a)

Para llevar a cabo un análisis que respalde la propuesta en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando las directrices de la norma

ISO 27001, se tienen en cuenta los activos previamente identificados como críticos y susceptibles de ser vulnerables a ciberataques dentro del ámbito definido.

Tabla 25.

Activos con mayor riesgo en ciberataque

Activos con mayor riesgo en ciberataque
Pc
Dispositivos Móviles
Laptop
Huellas Dactilares
Cámaras de Vigilancia
Red Interna
Software del biométrico
Firewall
Correo Electrónico Corporativo
Mantenimiento / Actualización
Documentación TI
Documentos Físicos
Grabaciones de Vigilancia
Políticas de Seguridad
Base de Datos
Backup

Fuente Elaborado por el autor basado evidentemente en lo investigado

A continuación, se detalla más exhaustivamente cada uno de los activos en el (**Anexo 5**) titulado "Análisis, Tratamiento y Evaluación del Riesgo". Este anexo evalúa los controles de seguridad que pueden ser implementados en los activos con mayor vulnerabilidad ante ciberataques, considerando diversos tipos de amenazas conforme a la norma ISO/IEC 27002:2013.

Según los resultados obtenidos, para mitigar los riesgos de nivel muy alto, es crucial tener en cuenta el dominio de control A.12 enfocado en la seguridad operativa. Dentro de este dominio, se destacan los objetivos de control A.12.2, que aborda la protección contra código malicioso, y A.12.3, que se centra en la realización de copias de seguridad.

Capítulo III. Propuesta

3.1 Datos Informativos.

- **Tema**: Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando la norma ISO/27001 para la protección de datos en la Unidad Educativa La Inmaculada de la ciudad de Ambato
- **Institución**: Unidad Educativa La Inmaculada
- **Provincia**: Tungurahua
- **Cantón**: Ambato
- **Dirección**: Avenida Miraflores y Margaritas
- **Beneficiarios**: Rectora, Vicerrectora; Técnico de sistemas, Personal administrativo (secretaría, contabilidad e Inspección General)
- **Responsable**: Ing. Franklin Vinicio Guamán Muela
- **Director**: Ing. Juan Pablo Cuenca, Mg.

3.2 Antecedentes de la Propuesta.

El activo principal de una unidad educativa es la información. Esta debe ser confidencial, inalterada, accesible y libre de interrupciones. La Unidad Educativa La Inmaculada tiene un departamento de tecnologías de la información que gestiona y protege la información de los estudiantes y docentes.

El departamento de TI, la secretaría, la contabilidad y la inspección no han establecido estándares de gestión de seguridad, lo que pone en riesgo la confiabilidad de los servicios de TI. La organización maneja información administrativa y académica crítica. Pueden producirse demoras significativas en tiempo y costos si ataques externos o la pérdida de datos interrumpen estos procesos.

3.3. Introducción.

Con el propósito de administrar la seguridad de la información en la Unidad Educativa L Inmaculada, se presenta la necesidad de instaurar un modelo básico de SGSI. Este modelo busca unificar los procesos hacia un objetivo común en la gestión de la seguridad de la información.

3.4. Objetivo.

El propósito de esta investigación es informar a las autoridades de la Unidad Educativa La Inmaculada sobre las pautas y acciones necesarias para establecer un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema tiene como objetivo reducir las vulnerabilidades y amenazas relacionadas con la seguridad de la información en la protección de datos de la Institución, siguiendo las normas ISO 27001. La implementación de estas normas incrementará la confiabilidad en la Institución.

3.5 Justificación.

Tras un análisis realizado durante el proceso de recogida de activos y considerando la necesidad de garantizar una adecuada gestión de la seguridad de la información para la protección de datos y la calidad de los servicios informáticos de la Unidad Educativa La Inmaculada, resulta imprescindible la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/27001. Esto es crucial debido a la falta de metodologías para contrarrestar los ataques externos. El objetivo es evaluar el impacto de la información en la institución educativa.

La presente investigación contempla la implementación de un SGSI para salvaguardar la información, alineándose a los estándares establecidos en la norma ISO/27001. El enfoque incluye una estrategia de mejora continua de los procesos de gestión de seguridad de la información en la institución educativa. Además, la propuesta es factible con el apoyo de las autoridades, el departamento de TI, la secretaría, contabilidad, inspección general y el personal para la recolección de la información necesaria.

3.6. Alcance

El propósito de esta investigación es abarcar los procesos institucionales vinculados con la gestión de la protección de datos por parte de todo el personal administrativo. Su cumplimiento es obligatorio para todos los que laboran, incluyendo tanto al personal docente y administrativo como al personal externo que colabore con bienes o servicios en la institución educativa.

3.7. Control del instructivo

Este documento pertenece exclusivamente a la Unidad Educativa La Inmaculada. Su distribución o reproducción está prohibida sin el permiso previo de los responsables, quienes se

encargarán de supervisar y controlar su distribución para evitar modificaciones o actualizaciones no autorizadas.

3.8. Compromiso de la dirección

La administración de la Unidad Educativa La Inmaculada está dedicada a la seguridad de la información y a la protección de datos, adoptando plenamente los principios establecidos en la norma ISO 27001. Esta norma actúa como una guía de buenas prácticas que especifica los objetivos de control y las medidas recomendadas para garantizar la seguridad de la información. La institución se compromete a proteger sus activos de información frente a amenazas mediante una gestión de riesgos adecuada, el cumplimiento de requisitos legales, la adopción de mejores prácticas y la implementación de controles adaptados a la realidad del centro educativo y su entorno.

3.9. Requisitos legales y/o reglamentarios.

Para implementar el Sistema de Gestión de Seguridad de la Información (SGSI), la Unidad Educativa La Inmaculada debe cumplir con las disposiciones establecidas en el marco legal y normativo correspondiente a la ley de protección de datos.

3.10. Análisis de Factibilidad.

3.10.1. Factibilidad Técnica.

Técnicamente, la propuesta de investigación es completamente viable, dado los medios técnicos que necesita, como la infraestructura de computadoras en el departamento de TI, las herramientas técnicas con las que se desarrollará, el acceso de los usuarios y el soporte de datos e información. La implementación del sistema de gestión de seguridad de la información (SGSI) basado en los estándares de seguridad informática ISO 27001 se llevará a cabo en el departamento de tecnología de la información (TI), el departamento de contabilidad, el

departamento de secretaría y el departamento de inspección general en la Unidad Educativa Inmaculada para la protección de datos. Se incluye la especificación ISO/IEC 27001 y la documentación que implementa el SGSI.

3.10.2. Factibilidad Operativa.

El proyecto es operativamente viable gracias al apoyo de la Unidad Educativa La Inmaculada, que permitirá al personal de la institución colaborar con la información necesaria y los resultados de la investigación. Para lograr los objetivos propuestos, se implementará el sistema de gestión de seguridad de la información de acuerdo con las normas ISO 27001, con el apoyo de la Rectora y los empleados del departamento de Tecnologías de la Información (TI), Secretaría, Contabilidad e Inspección General. Los procedimientos desarrollados en un documento describen el proceso a seguir en el desarrollo de métodos que garanticen el cumplimiento de ISO/IEC 27001:2013.

3.10.3. Factibilidad Organizacional.

El proyecto actual es factible desde un punto de vista organizacional, ya que la rectora y el encargado del departamento de TI de la institución están interesados en disponer de medidas para mejorar la gestión de la seguridad de la información.

3.11. Propuesta de Solución

La implementación de esta investigación es económicamente beneficiosa porque se lleva a cabo de acuerdo con la norma. Se eligió la fase de la norma ISO/IEC 27001. El personal asume la responsabilidad, y la institución educativa asume la responsabilidad del tiempo del personal involucrado en el desarrollo de la propuesta.

3.12. Fundamentación.

El principal objetivo de un sistema de gestión de seguridad de la información es mejorar la gestión de seguridad de los datos personales frente a los diversos riesgos, amenazas y vulnerabilidades que enfrentan las tecnologías actuales. Con la ayuda de estos sistemas, se puede prevenir la información sobre estos ataques, ya que permiten un análisis detallado de cómo afrontar estos ataques utilizando sus métodos, documentación y otras herramientas, ayudando así a prevenir, mitigar y, en la mayoría de los casos, eliminar amenazas específicas (ISO27000.es, 2012).

Toda la información se puede enviar a procesos y sistemas de procesamiento. Hoy en día, la información es el activo más importante de cualquier organización. Por tanto, su confidencialidad, integridad y disponibilidad son factores decisivos para la consecución de las metas y objetivos fijados. Una adecuada gestión de la información puede conducir al éxito organizacional, mientras que una gestión ineficaz, sin herramientas y mecanismos adecuados de protección de datos, tendrá consecuencias negativas (ISO27000.es, 2012).

3.13. Responsable

Compromiso del Departamento de Tics.

El departamento de TI de la Unidad Educativa La Inmaculada debe demostrar su dedicación al establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para proteger la información. Es necesario definir los objetivos de seguridad de la información y asignar roles específicos a cada empleado de la Unidad Educativa, quienes serán responsables de gestionar ciertos activos. Para alcanzar el objetivo de mejora continua en la Unidad Educativa, es esencial que la autoridad máxima esté informada sobre el cumplimiento de los objetivos de seguridad de la información.

Gestión de los recursos

- Garantizar que las políticas de seguridad de la información respalden el cumplimiento de la misión y visión de la Unidad Educativa La Inmaculada.
- Identificar y cumplir con los requisitos legales y reglamentarios, así como con las obligaciones de seguridad establecidas en los contratos, o mantener un nivel adecuado de seguridad mediante la correcta aplicación de todos los controles implementados.
- Asegurar que todo el personal esté consciente de la importancia de la seguridad de la información.

3.14. Ventajas que obtendrá la Unidad Educativa La Inmaculada al poner en marcha un Sistema de Gestión de Seguridad de la Información (SGSI). Aplicando las Normas ISO 27001

- Reducir el riesgo de pérdida de información en la institución, incluyendo robos y alteraciones por manipulación.
- Desarrollar una metodología clara y concisa para gestionar la seguridad de la información.
- Implementamos medidas de seguridad para garantizar que solo el personal autorizado tenga acceso a la información dentro de cada departamento.
- Facilitar la identificación clara de incidentes relacionados con la gestión de la seguridad de la información dentro de la institución.
- Contar con un SGSI que brinda a la Unidad Educativa La Inmaculada una garantía para padres de familia y estudiantes, demostrando su compromiso con la confidencialidad, la seguridad de la información y la protección de datos.

3.15. Procedimiento de Comunicación de las Políticas de Seguridad

- El personal del departamento de TI de la Unidad Educativa La Inmaculada, consciente del uso constante de los recursos de información por parte de los usuarios que acceden a diversos servicios descritos en este documento, ha decidido transmitir las normas básicas de comportamiento para el uso adecuado de los equipos de cómputo y otros recursos tecnológicos e informáticos.

3.16. Políticas de seguridad aplicando SGSI:

- Las políticas de seguridad de la información (SGSI) se centran en mitigar el riesgo de incidentes de seguridad. Estas políticas establecen las normas fundamentales para la operación de los recursos informáticos de la organización. El objetivo principal del diseño de estas políticas es reducir y eliminar diversos factores de riesgo, especialmente aquellos que pueden llevar a la ocurrencia de incidentes.

3.17. Políticas de seguridad.

- La Unidad Educativa La Inmaculada enfatiza la importancia de los Sistemas de Gestión de Seguridad de la Información (SGSI) para proteger los datos como un activo estratégico. El mal uso de los activos de información puede poner en peligro la continuidad institucional o causar daños significativos. El personal, terceros y empleados deben conocer los protocolos de seguridad para evitar acciones disciplinarias. Se implementarán controles de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los activos de información en consonancia con la visión, misión y estándares legales de la institución en la protección de datos.

3.18. Políticas

Todas las autoridades de la institución deben cumplir con estas normas, las cuales buscan asegurar que se implementen medidas para proteger los datos dentro de la Unidad Educativa La Inmaculada.

3.18.1. Políticas de la seguridad de la información

Tabla 26.

Políticas de la seguridad de la información

Código		A.5. A.5.1.1 A.5.1.2	
Fecha de versión		2013	
Responsable			
Aprobado por		Rectorado -Consejo Ejecutivo	
Nivel de confidencialidad		Alta	
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El objetivo de esta política de alto nivel es establecer las normas y procedimientos para la gestión de la seguridad de la información en la Institución Educativa.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: Mensualmente.

Actividades destinadas a comprobar y ejecutar la política incluyen:

1. Asegurarse de que la información esté adecuadamente respaldada en dispositivos electrónicos o almacenada en servicios en la nube como Amazon Cloud Drive, Box, Dropbox, Google Drive, OneDrive o iCloud.
2. Actualizar regularmente las contraseñas del personal administrativo, docente y demás empleados de la Unidad Educativa La Inmaculada.
3. Supervisar que no se descarguen archivos de origen desconocido en las computadoras institucionales.
4. Garantizar que el acceso a la información en computadoras ubicadas en áreas como Secretaría, Contabilidad e Inspección esté restringido solo al personal autorizado.
5. Verificar que el ingreso de calificaciones sea realizado por el docente y, en caso de modificación de calificaciones, que se realicen con la debida autorización del Rectorado.

Documentos de referencia

- Directrices técnicas según la normativa NTC-ISO/IEC 27001:2013.
- Informe detallado del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).
- Proceso para evaluar y manejar riesgos.
- Declaración que establece la aplicabilidad.

3.18.2. Política de clasificación de la información

Tabla 27.

Política de clasificación de la información

Código		A.6.2 A.11.2.6.	
Fecha de versión		2013	
Responsable			
Aprobado por		Rectorado -Consejo Ejecutivo	
Nivel de confidencialidad		Alta	
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El propósito de este documento es asegurar que la información esté protegida de manera adecuada en relación con la confidencialidad de la información.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: Cada trimestre

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Asegurarse de que los equipos de la institución no se conecten a redes inalámbricas públicas o desconocidas.
- Validar que todo el software instalado en los equipos tenga la licencia correspondiente (Office, Windows, antivirus).
- Verificar que el acceso a los equipos requiera un usuario y contraseña.
- Garantizar que la información sensible en los equipos institucionales no esté accesible para estudiantes u otras personas no autorizadas.

- Realizar el borrado seguro de la información o la destrucción física de dispositivos de almacenamiento cuando son entregados por empleados que dejan la institución, antes de ser reasignados.
- Realizar verificaciones para contar el número de computadoras en la institución.
- Clasificar adecuadamente la información según el esquema siguiente.

Según su confidencialidad.

De acuerdo con su nivel de confidencialidad, la información se categoriza de la siguiente manera:

- **Reservada**: información que, si se divulga sin autorización, podría dañar los intereses o la reputación de la institución.
- **Institucional:** información que los empleados de la institución deben conocer para realizar sus funciones**.**
- **Pública**: información que es de dominio público y se puede entregar o difundir sin restricciones.

Según su Integridad

La información se clasificará según su nivel de integridad de la siguiente manera:

- 4.- No se puede reparar y provoca pérdidas graves para la institución.
- 3.- Difícil de reparar y causa pérdidas significativas.
- 2.- Reparación posible, ocasiona pérdidas leves.
- 1.- No afecta la operación y es fácilmente reparable.

Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.6.2 y A.11.2.6

- Política de seguridad de la información
- Política de clasificación de la información.

3.18.3. Políticas de claves

Tabla 28.

Políticas de claves

Código		A.9.2.1, A.9.2.2, A.9.2.4, A9.3.1, A9.4.3	
Fecha de versión		2013	
Responsable			
Aprobado por		Rectorado -Consejo Ejecutivo	
Nivel de confidencialidad		Alta	
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El objetivo del presente documento es establecer reglas para garantizar la gestión y utilización seguras de las claves.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: Cada trimestre

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Asegurarse de que las contraseñas para el acceso al sistema académico de la institución tengan entre 8 y 16 caracteres y combinen letras mayúsculas, minúsculas y números.
- Confirme que los administradores de estas contraseñas no las guarden ni las escriban en lugares visibles donde personas no autorizadas puedan hacer mal uso de ellas.
- Garantizar que los nombres de usuario no se repitan.
- Realizar el cambio de contraseña en el período estimado (una vez al mes) para evitar problemas de accesos no autorizados.

Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
- Política de seguridad de la información
- Declaración de aceptación de los documentos del SGSI.

3.18.4. Políticas de control de acceso

Tabla 29.

Políticas de control de acceso

Código			A.9.1.1, A.9.1.2, A9.2.1, A.9.2.Z, A.9.2.3, A9.2.4, A,9.2.5 A.9.2.6, A9.3.1, A.9.4.1, A.9.4.3
Fecha de versión			2013
Responsable			
Aprobado por			Rectorado -Consejo Ejecutivo
Nivel de confidencialidad			Alta
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

Establecer normas de acceso para distintos sistemas, equipos, instalaciones y datos según las necesidades de la institución y las exigencias de seguridad.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: trimestral

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Se debe verificar que todos los docentes tengan acceso adecuado a todos los sectores físicos de la institución, con excepción del rectorado, vicerrectorado, administración, recursos humanos, y secretaría y contabilidad, los cuales solo pueden ser ingresados por una persona autorizada.
- Además, se debe asegurar que los empleados de la institución, al utilizar computadoras con acceso a Internet proporcionado por la institución, tengan restricciones que incluyan:
    - No utilizar mensajería instantánea comercial.
    - No usar correo electrónico no autorizado.
    - No descargar archivos personales.
    - No conectarse a sitios no autorizados.
    - No acceder a sitios de pornografía.
- No utilizar ningún servicio que comprometa la seguridad de la red o afecte su rendimiento.
- Es fundamental bloquear las páginas no autorizadas en los navegadores y verificar regularmente que no hayan sido desbloqueadas.

- Además, se debe asegurar que el acceso a información específica esté restringido solo al personal autorizado y establecer privilegios de acceso al sistema académico de la institución.
- Finalmente, se debe instruir a cerrar sesión y apagar los equipos cuando no estén en uso.

Documentos de referencia

- Norma ISO 27001, clausulas A9.1.1, A.9.1.2, A9.2.1, A.9.2.2, A.9.2.4, A.9.2.5, A.9.2.6, A9.3.1, A.9.4.1, A.9.4.3
- Política de seguridad de la información.
- Declaración de aplicabilidad.
- Política de clasificación de la información.

3.18.5. Políticas de eliminación y destrucción

Tabla 30.

Políticas de eliminación y destrucción

Código	A.9.1.1, A.9.1.2, A9.2.1, A.9.2.Z, A.9.2.3, A9.2.4, A,9.2.5 A.9.2.6, A9.3.1, A.9.4.1, A.9.4.3		
Fecha de versión	2013		
Responsable			
Aprobado por	Rectorado -Consejo Ejecutivo		
Nivel de confidencialidad	Alta		
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El objetivo del presente documento es garantizar que la información almacenada en equipos y soportes sea borrada o eliminada de forma segura.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: Mensual

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Todos los datos y software con licencia almacenados en medios móviles (como CD, DVD, unidades USB, tarjetas de memoria, discos duros externos, almacenamiento en la nube y en formato papel), así como en todos los dispositivos que utilicen medios de almacenamiento (incluyendo computadoras de escritorio, portátiles, teléfonos móviles, etc.), deben ser eliminados o los soportes deben ser destruidos antes de ser devueltos o reutilizados.
- Es necesario asegurarse de que se destruya completamente la información que no sea necesaria para evitar la redundancia y posibles confusiones dentro de la institución.
- Verificar que se elimine por completo la información de los empleados que ya no trabajen en la institución (tales como contraseñas, nombres de usuario y hojas de vida).

Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.8.3.2, A.11.2.7.
- Política de seguridad de la información.
- Política de clasificación de la información.
- Inventario de activos.

3.18.6. Políticas de pantallas y escritorio

Tabla 31.

Políticas de pantallas y escritorio

Código		A.11.2.8 y A.11.2.9.	
Fecha de versión		2013	
Responsable			
Aprobado por		Rectorado -Consejo Ejecutivo	
Nivel de confidencialidad		Alta	
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El propósito de este documento es establecer normas destinadas a prevenir el acceso no autorizado a la información en los lugares de trabajo, así como a las instalaciones y equipos compartidos.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: semanalmente

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Asegurarse de que todos los documentos impresos y soportes de almacenamiento de datos estén guardados de manera segura bajo llave cuando el personal no esté presente en su puesto de trabajo, especialmente fuera del horario laboral.
- Verificar que en los equipos solo se encuentre información y programas autorizados oficialmente. Eliminar cualquier información o programas no autorizados según la política establecida para la eliminación y destrucción.
- Configurar los equipos para que la sesión se bloquee y el protector de pantalla se active automáticamente después de cinco (5) minutos de inactividad.
- Asegurarse de que la información sensible impresa no quede disponible y se almacene inmediatamente después de ser impresa.

Documentos de referencia

- Norma ISO/IEC 27001, clausulas A 11.2.8 y A.11.2.9.
- Política de seguridad de la información.
- Política de clasificación de la información.

3.18.7. Procedimientos para trabajo en áreas seguras

Tabla 32.

Procedimientos para trabajo en áreas seguras

código	A.11.2.8 Y A.11.2.9.
Fecha de versión	2013
Responsable	
Aprobado por	Rectorado -Consejo Ejecutivo
Nivel de confidencialidad	Alta
Historial de modificaciones	

Historia	Versión	Responsable	Descripción de la Modificación
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El objetivo de este documento es establecer las normas fundamentales de conducta en las zonas seguras.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: Mensual.

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Asegurarse de que solo las personas autorizadas utilicen los equipos de cada departamento administrativo, como la secretaría, contabilidad, Inspección General y el Departamento de TI.
- Garantizar que la información crítica, como boletines de calificaciones y registros de estudiantes y personal de la Unidad Educativa La Inmaculada, esté almacenada de manera segura.
- Verificar la implementación de medidas de seguridad en áreas clave, como la secretaría, contabilidad, Inspección General y el departamento de TI, con el fin de proteger la información en caso de desastres naturales.
- Designar responsables específicos para cada área de la institución, quienes asegurarán la integridad y disponibilidad de dichas áreas solo para personas autorizadas.

Documentos de referencia

- Norma ISO/IEC 27001, clausulas A 11.1.5

- Política de control de acceso
- Inventario de activos

3.18.8. Procedimientos para gestión de incidentes de seguridad

Tabla 33.

Procedimientos para gestión de incidentes de seguridad

Código		A.7.2.3, A16.1.1, A.16.1.2, A.16.1.8, A.16.1.4, A.16.1.5, A16.1.6, A,16.1.7	
Fecha de versión		2013	
Responsable			
Aprobado por		Rectorado -Consejo Ejecutivo	
Nivel de confidencialidad		Alta	
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El propósito de este documento es asegurar que se detecten prontamente eventos y vulnerabilidades de seguridad, y que se actúe rápidamente para responder a incidentes de seguridad.

Responsable de asegurar que esta política se cumpla: Rectorado - Consejo Ejecutivo.

Frecuencia con la que se implementa la política: cada trimestre.

Actividades destinadas a comprobar y ejecutar la política incluyen:

- Es esencial que todos los empleados, proveedores o terceros que interactúen con información y/o sistemas dentro de la institución reporten cualquier debilidad, incidente o evento que potencialmente pueda resultar en un incidente de seguridad.
- La persona responsable de sancionar al personal que intencionalmente cause un incidente de seguridad debe estar claramente identificada.
- En caso de cualquier confusión relacionada con el ingreso de grado ocurso, es necesario informar a la administración para obtener la autorización y hacer las correcciones necesarias antes de que surja cualquier problema con el Ministerio de Educación.
- Es esencial mantener registros de evidencia de todos los incidentes de seguridad de la información.

Documentos de referencia

- Norma ISO/IEC 27001, A.7.2.3, A.16.1.1, A16.1.2, A16.1.3, A.16.1.4, A.16.1.5, A16.1.6, A.16.1.7
- Política de seguridad de la información.
- Inventario de activos.

3.18.9. Políticas de transferencia de información

Tabla 34.

Políticas de transferencia de información

Código	A.13.2.1, A.13.2.2.
Fecha de versión	2013
Responsable	
Aprobado por	Rectorado -Consejo Ejecutivo
Nivel de	Alta

confidencialidad			
Historial de modificaciones			
Historia	**Versión**	**Responsable**	**Descripción de la Modificación**
			Descripción básica de los documentos

Fuente Elaborado por el autor basado evidentemente en lo investigado

Objetivo

El propósito de este documento es garantizar la protección de la información y el software al ser compartidos tanto dentro como fuera de la organización.

Responsable de asegurar que esta política se cumpla: Rectorado.

Frecuencia con la que se implementa la política: mensual.

Actividades destinadas a comprobar y ejecutar la política incluyen:

Es importante asegurarse de que toda la información institucional que se comparta a través de los siguientes canales electrónicos cumpla con la autorización del Rectorado. Además, ningún administrativo deberá intercambiar información confidencial sin la debida autorización de la máxima autoridad correspondiente.

Documentos de referencia

- Norma ISO/IEC 27001, A.13.2.1. A.13.2.2.
- Política de seguridad de la información
- Política de seguridad para proveedores

3.19. Planificación del SGSI

Para el establecimiento y ejecución del Sistema de Gestión de Seguridad de la Información utilizando las normas ISO 27001, se definen las siguientes fases:

- Elaboración de la documentación del sistema.
- Implementación del sistema.
- Evaluación del sistema mediante auditorías internas y externas.
- Mejora continua de la efectividad del sistema a través del análisis de datos.

3.20. Control de documentos.

Los responsables de estas acciones son el Rectorado y el Consejo Ejecutivo. Según lo especificado, este control debe llevarse a cabo mensualmente para asegurar que la documentación esté actualizada y para tener claridad sobre qué documentos posee la entidad educativa en caso de una auditoría. Se recomienda seguir un formato específico para esta actividad.

Tabla 35.

Control de documentos

Código del doc.	Nombre del doc.	Responsable	Fecha de revisión	Ubicación

Fuente Elaborado por el autor basado evidentemente en lo investigado

3.21. Establecimiento del SGSI

El establecimiento y ajuste del Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo definir los mecanismos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información. Esto garantiza la protección de los datos de estudiantes, padres de familia y empleados de la institución educativa, así como la información generada en los procesos de calificaciones, asegurando la eficiencia y transparencia en los procesos institucionales.

Para lograrlo, se implementarán los siguientes procedimientos:

- Identificar, gestionar y tratar los riesgos de seguridad de la información relevante para la institución, siguiendo la metodología de identificación, análisis y evaluación de riesgos, utilizando Magerit.
- Gestionar los incidentes relacionados con la seguridad de la información.
- Divulgar y mantener disponibles las políticas y procedimientos de seguridad para que sean comprendidos y utilizados por los empleados de la institución.
- Capacitar a los empleados en temas de seguridad de la información para fortalecer sus valores éticos y garantizar su compromiso con la protección de los activos de información.
- Asegurar la disponibilidad de los activos de información para aquellos que los requieran y estén debidamente autorizados.
- Garantizar el suministro de los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.

3.22. Proceso para llevar a cabo una auditoría interna

Responsable: Departamento Administrativo

Frecuencia con que se debe realizar este control: Trimestral

Procedimientos

- Elaborar un calendario de auditorías que detalle las fechas, los departamentos, los procesos y el personal autorizado para llevar a cabo la actividad.
- Coordinar con el personal la disponibilidad del departamento para llevar a cabo la auditoría.

- Conducir la auditoría, recopilando la información requerida según un cuestionario o parámetros definidos por la gerencia.
- Mantener al gerente del proceso informado sobre las áreas problemáticas que requieren revisión.

Figura 11.

Formato Para Auditoria Internas

Fecha:					
N ° de auditoria					
Parámetros	**Proceso**	**Área**	**Fecha de inicio**	**Fecha de finalización**	**Tiempo de duración de auditoria**

Fuente Elaborado por el autor basado evidentemente en lo investigado

3.23. Elaborar directrices para la detección y gestión de los riesgos.

Responsable: Rectorado, Consejo Ejecutivo

Frecuencia con la que se debe realizar este control: Trimestral

Procedimiento

Si se detecta algún riesgo en la Unidad Educativa La Inmaculada, se realizará la clasificación de la siguiente manera.:

Tabla 36.

Directrices para la detección y gestión de los riesgos

Medida	Descripción
Evitar riegos	Evitar riesgos implica tomar acciones para eliminar la posibilidad de que ocurra un evento adverso. Esto se logra dejando de realizar una actividad específica que conlleva el riesgo. Por ejemplo, una empresa podría decidir no almacenar datos sensibles en sus servidores para evitar el riesgo de una violación de datos.
Reducir el riesgo	Reducir el riesgo significa implementar medidas que disminuyan la probabilidad de que ocurra un evento adverso o que minimicen el impacto de dicho evento si llega a ocurrir. Esto puede incluir la instalación de software de seguridad, la capacitación del personal en prácticas de seguridad o la implementación de políticas de contraseñas fuertes.
Dispersar y atomizar el riesgo	Dispersar y atomizar el riesgo implica distribuirlo entre diferentes áreas o partes de la organización para que ningún evento adverso único tenga un impacto catastrófico. Esto puede incluir la diversificación de proveedores, la replicación de datos en diferentes ubicaciones o la implementación de políticas de redundancia.
Transferir el riesgo	Transferir el riesgo consiste en pasar la responsabilidad del riesgo a otra entidad,

	como una compañía de seguros. Esto se logra a través de contratos, seguros o acuerdos de servicio en los que otra organización acepta manejar y asumir el riesgo. Por ejemplo, contratar un seguro cibernético para cubrir los costos asociados con una violación de datos.
Asumir el riesgo	Asumir el riesgo significa aceptar el riesgo y las posibles consecuencias de un evento adverso. Esto puede ser una decisión estratégica cuando el costo de mitigar el riesgo es mayor que el impacto potencial del riesgo mismo. En estos casos, la organización está preparada para enfrentar y gestionar las consecuencias si el riesgo se materializa.

Fuente Elaborado por el autor basado evidentemente en lo investigado

3.24. Redacción procedimientos para medidas correctivas

Responsable: Rectorado y Consejo Ejecutivo

Frecuencia con la que se debe realizar este control: Trimestral

Procedimientos

En caso de identificarse riesgos en la Unidad Educativa La Inmaculada, se llevarán a cabo acciones correctivas siguiendo el formato recomendado.:

Figura 12.

Formato para medidas correctivas

Responsable	
Fecha:	
Tema:	
Personas que participan en la acción y coordinador:	
Descripción del problema que se quiere eliminar o evitar.	
Acciones precedentes o primeras acciones adoptadas	
Causa o causas que genera el problema o que lo pueden generar	
Soluciones que atacan las causas del problema, posibles acciones	
Acciones correctivas/ preventivas finalmente realizadas, incluyendo fecha	
Acciones que se efectuarán para verificar la eficacia de las soluciones implantadas, fechas y responsables.	
Resultados obtenidos conclusiones	
Firma de responsables	

Fuente Elaborado por el autor basado evidentemente en lo investigado

3.25. Responsabilidades y supervisión (Proceso para implementar acciones correctivas).

Es fundamental definir roles y responsabilidades para apoyar y cumplir con la política de seguridad de la información. A continuación, se presentan los roles y responsabilidades pertinentes:

Las Autoridades de la Unidad Educativa muestran su compromiso con el sistema de gestión de seguridad de la información mediante las siguientes acciones:

- **Definir y establecer la política y los objetivos de seguridad de la información**: Asegurarse de que todos los empleados de la Unidad Educativa estén al tanto de ellos.
- **Implementar el Sistema de Gestión de Seguridad de la Información (SGSI)**: Evaluar su efectividad dentro de la Unidad Educativa para fomentar la mejora continua.
- **Asignar responsabilidades y delegar tareas**: Especificar funciones y designar a los responsables correspondientes.
- **Determinar criterios de aceptación de riesgos de seguridad de la información**: Establecer los niveles de riesgo aceptables.
- **Promover el cumplimiento**: Asegurar que los empleados sigan las normas, requisitos y regulaciones aplicables para garantizar la seguridad de la información.

3.26. Gestión de recursos

Las autoridades de la Unidad Educativa tendrán la responsabilidad de asegurar los recursos necesarios para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Para ello, deben garantizar los siguientes aspectos:

- **Presupuesto**: asignar los fondos necesarios para asegurar la implementación, mantenimiento y mejora del SGSI.
- **Personal especializado:** organizar capacitaciones y campañas de concienciación para los empleados de la institución sobre el uso adecuado, protección y seguridad de la información.

3.27. Medición y mejora

La Unidad Educativa La Inmaculada desarrolla y establece los procedimientos necesarios para revisar y mejorar el SGSI, con el objetivo de:

- Garantizar la efectividad del Sistema de Gestión de Seguridad de la Información.
- Maximizar la eficiencia del SGSI

3.28. Revisión por parte de la dirección

Cada año, las autoridades de la institución llevarán a cabo una revisión del SGSI con el objetivo de:

- Garantizar su eficacia.
- Evaluar la necesidad de modificar el SGSI.
- Ajustar los objetivos y políticas si no cumplen con los requisitos del SGSI.

Para cumplir con estos objetivos, las directivas de la institución se basarán en los resultados de revisiones anteriores, la retroalimentación de los responsables de los procesos, la información, los informes sobre afectaciones y medidas correctivas, así como en las recomendaciones de mejora del comité SGSI.

Como resultado de esta revisión, y si es necesario, se implementarán acciones para:

- Mejorar la eficiencia del SGSI.
- Ajustar normas, políticas y procedimientos en respuesta a cambios internos o del entorno, requisitos del negocio, marco legal y criterios de aceptación de riesgos.
- Actualizar la evaluación de riesgos.
- Actualizar el plan de tratamiento de riesgos.
- Solicitar nuevos recursos.

Los resultados de esta revisión deben registrarse en un acta que se archivará en la institución y se comunicarán al comité SGSI, el cual se encargará de supervisar el cumplimiento de los acuerdos y cambios definidos.

3.29. Mejora

Las autoridades de la Unidad Educativa deben promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Para lograrlo, gestionarán los recursos e insumos necesarios, basándose en los resultados de las evaluaciones realizadas.

Asimismo, deben definir y establecer acciones y procedimientos correctivos para eliminar y asegurar que no se repitan las causas que provocan fallos en el SGSI. Además, deben establecer acciones y procedimientos preventivos para anticiparse a posibles situaciones que puedan generar fallos en el SGSI y prevenir su recurrencia.

Todas estas acciones deben ser adecuadamente documentadas y presentadas al comité del SGSI para su revisión, aprobación e implementación.

3.30. Términos y Condiciones de Contratación

Después de elegir a un nuevo empleado, se formalizará un contrato legal que incluirá cláusulas de confidencialidad que el empleado, tanto a nivel individual como corporativo, deberá respetar. Este contrato requerirá que el empleado acepte los términos y condiciones, comprometiéndose a seguir las políticas de seguridad del Departamento de Tecnologías de la Información. El modelo del "Acuerdo de Confidencialidad" está adjunto como **(Anexo 6).**

Acuerdo de Confidencialidad

Antes de que los usuarios puedan utilizar los recursos tecnológicos de la institución, deben comprometerse formalmente a mantener la confidencialidad y seguridad de los sistemas

de información. Este compromiso se formaliza mediante el acuerdo de confidencialidad **(Anexo 6)**. Una vez cumplido este requisito, se les proporciona una cuenta de usuario, una contraseña para acceder a la red y los privilegios necesarios para la instalación de soluciones de autenticación biométrica.

- Los dispositivos electrónicos propiedad de la institución no deben ser usados para actividades personales, como acceder a redes sociales o correos electrónicos no relacionados con el trabajo.
- Es obligatorio que todos los usuarios envíen información exclusivamente a través de sus cuentas de correo electrónico institucionales.
- Cada usuario que forme parte del personal interno será responsable del uso adecuado de los equipos de cómputo asignados para sus labores, incluyendo la prevención de infecciones por virus.
- Queda estrictamente prohibida la descarga de archivos desde Internet que puedan ser considerados pornográficos, difamatorios o racistas, así como videos, música u otros contenidos que violen los principios éticos y las buenas prácticas, a menos que sea necesario para el desempeño de funciones administrativas específicas.

3.31 Devolución de activos:

Al implementar este control, los custodios de activos cumplirán con las siguientes pautas:

Si un empleado saliente trabajó con tecnología o información administrativa relacionada con su trabajo dentro de la Unidad Educativa La Inmaculada, deberá informarlo al departamento donde laboró mediante documentación.

Toda la información de la Unidad Educativa La Inmaculada en los equipos de cómputo del empleado será eliminada.

Devolución general de equipos:

El formulario “Inventario de Hardware y Software de Computadores” se encuentra en el (**Anexo 7).**

3.32. Control De Accesos.

Los usuarios dispondrán de una identificación única (nombre de usuario) para acceder a los sistemas pertinentes, junto con un elemento de autenticación (contraseña) destinado al uso personal y confidencial de los recursos tecnológicos necesarios para sus tareas. Esta política cubre los aplicativos implementados hasta la fecha de emisión de este documento. Los empleados recibirán una identificación personal única y su contraseña correspondiente, asignada por el responsable del departamento de tecnologías de la información (TI).

Cada usuario es responsable de los mecanismos de control de acceso que se les otorgan, es decir, el nombre de usuario y la contraseña necesarios para acceder al sistema, al grupo de trabajo y/o al dominio de red **(Anexo 8).**

3.33. Copias de seguridad de la información.

La información debe ser respaldada de manera precisa y sin errores. Un miembro del personal del departamento de TI será designado para esta responsabilidad. Las copias de seguridad se harán en ubicaciones adecuadas, siguiendo procedimientos específicos según la criticidad y confidencialidad de los sistemas, y todas estarán cifradas. La información se almacenará en dispositivos de gran capacidad, como discos duros extraíbles o servidores. Estas copias se realizarán en momentos de baja actividad, utilizando formularios de control para las

copias diarias, semanales y mensuales. Sistemas específicos, como el de control biométrico de RR.HH., tendrán frecuencias de respaldo establecidas. Los registros detallados de las copias de seguridad se encuentran en el **(Anexo 9.)**

Conclusiones

La norma ISO 27001 proporciona directrices cruciales para la gestión de la seguridad de la información mediante la evaluación y tratamiento de riesgos, amenazas y vulnerabilidades que afectan los datos en los centros educativos. Este estándar ofrece instrucciones detalladas sobre cómo preservar la seguridad de los equipos informáticos en la Unidad Educativa La Inmaculada.

En la Unidad Educativa La Inmaculada se ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de asegurar la protección de la información en los departamentos administrativos, centrándose en mantener la confidencialidad, disponibilidad e integridad de los datos. Se han establecido políticas de seguridad y gestión de activos de TI, además de medidas y controles específicos que garantizan la protección adecuada de la información.

Todos los departamentos administrativos deben adoptar un sistema de gestión de seguridad de la información en cumplimiento con la norma ISO 27001. Aunque la Unidad Educativa La Inmaculada no puede ofrecer una seguridad absoluta, asegura el cumplimiento de los estándares y las mejores prácticas establecidas por la norma ISO 27001. Esto es fundamental para que el Sistema de Gestión de Seguridad de la Información opere de manera efectiva y exitosa.

Recomendaciones

Se sugiere a las autoridades de la Unidad Educativa La Inmaculada, en colaboración con el Consejo Ejecutivo, ampliar la implementación de políticas de seguridad informática desde el departamento de Tecnologías de la Información hacia todos los empleados, con el fin de que se mantengan al día con respecto a los temas y normas en seguridad de la información.

Se sugiere que el Rectorado y el encargado del Departamento de TI lleven a cabo revisiones periódicas, cada seis meses, del sistema de gestión de seguridad de la información para asegurar su mejora constante y su adecuación a las innovaciones tecnológicas.

Se sugiere a las autoridades del centro educativo, incluyendo a la Rectora y al Consejo Ejecutivo, que lleven a cabo la capacitación del personal del Departamento de Tecnologías de la Información en la norma de seguridad de información ISO/27001. Este proceso no debe considerarse un gasto, sino una inversión. Los beneficios derivados de la implementación de esta norma se reflejarán en la gestión de la seguridad de la información en la Unidad Educativa La Inmaculada.

Bibliografía

Baldecchi, R. (2014). Implementación efectiva de un SGSI ISO 27001. *Implementación Efectiva de Un SGSI ISO 27001.*, 1–30. www.sonda.com

Bogantes, A. (n.d.). *El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados*.

Cárdenas, S., Martínez, A., & Becerra, A. (2016). *Vista de Gestión de seguridad de la información: revisión bibliográfica*. https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/epi.2016.nov.10/32176

Costas, J. (n.d.). *Entender_el_Ciclo_PDCA_de_mejora_continu*.

Cuenca León, W. E. (2019). *Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala*. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/29844

Espinosa, A. X., & De Educación, A. M. (n.d.). *NORMATIVA PARA REGULAR EL FUNCIONAMIENTO DE LAS INSTITUCIONES EDUCATIVAS FISCOMISIONALES DEL ECUADOR * (CODIFICACIÓN NO OFICIAL) †*. www.educacion.gob.ec

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo Del Conocimiento*, *2*(12), 145. https://doi.org/10.23857/pc.v2i12.420

Gobierno Electrónico de Ecuador. (s/f). (n.d.). *Ciclo de Deming (PDCA) – Gobierno Electrónico de Ecuador*. Retrieved June 23, 2024, from https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

LOES. (2018). *LEY ORGANICA DE EDUCACION SUPERIOR, LOES*. www.lexis.com.ec

LOPDP. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*.

Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001. *REICIS*, *6*(3), 24–35.

Ordoñez, L. (2017). *La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración*. 1–19.

Rodotà, S. (1997). *CDP_19-20: Democracia y protección de datos*.

Tapia Hernández, E. F., Ruiz Canizales, R., & Vega Páez, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Misión Jurídica*, *20*, 142–158. https://doi.org/10.25058/1794600x.1912

Anexo

Anexos 1 Catalogo de amenazas / vulnerabilidades

CATALOGO DE AMENAZAS / VULNERABILIDADES Fuente: NTE INEN-ISO/IEC 27005:2012		
EJEMPLOS DE VULNERABILIDADES EN DIVERSAS ÁREAS DE SEGURIDAD / EJEMPLOS DE AMENAZAS QUE PUEDEN EXPLOTAR ESTAS VULNERABILIDADES		
Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos

	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información

	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado

Referencia: ISO/IEC 27005:2008

Anexo 2 Iso27001 Dominios y Controles

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

 Octubre-2013

Anexo 3 Información de los Activos

SOFTWARE	Software de contabilidad Koinor	Departamento TIC-UELI	Encargado de TI	Autoridad	6	6	4	8	8	5	6,25	38,50
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Facturación electrónica	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,5	4	8	8	5	6,25	33,00
				Responsable TIC	8		8	8	8	5	7,25	
				Comisión	4		4	2	8	5	4,75	
				Auditor Interno	4		4	6	8	5	5,75	
							5,00	6,00	8,00	5,00	6,00	
	Software del biométrico	Departamento TIC-UELI	Encargado de TI	Autoridad	4	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Sistema de Gestión de Video	Departamento TIC-UELI	Encargado de TI	Autoridad	4	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	UniFi	Departamento TIC-UELI	Encargado de TI	Autoridad	2	4	4	8	8	5	6,25	25,67
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Aplicaciones Web	Departamento TIC-UELI	Encargado de TI	Autoridad	4	4,66667	4	8	8	5	6,25	29,94
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Firewall	Departamento TIC-UELI	Encargado de TI	Autoridad	4	4,66667	4	8	8	5	6,25	29,94
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Antivirus	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	10		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
SERVICIO	Correo Electrónico Corporativo	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Sitio Web	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
SERVICIO							5,33	7,33	8,00	5,00	6,42	
	Proveedor de Internet	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Mantenimiento / Actulización	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
INFRAESTRUCTURA	Red de área local e inalámbrica	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Red de Fibra optica	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Redes de comunicación	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Antena Direccional	Departamento TIC-UELI	Encargado de TI	Autoridad	8	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
HUMANO	**ESTUDIANTES**	**ESTUDIANTES**	**ESTUDIANTES**	Autoridad	6	5,5	4	8	8	5	6,25	33,00
				Responsable TIC	8		8	8	8	5	7,25	
				Comisión	4		4	2	8	5	4,75	
				Auditor Interno	4		4	6	8	5	5,75	
							5,00	6,00	8,00	5,00	6,00	
	PERSONAL ADMINISTRATIVO	FUNCIONARIOS	FUNCIONARIOS	Autoridad	6	6,66667	4	8	8	5	6,25	42,78
				Responsable TIC	10		8	8	8	5	7,25	
				Auditor Interno	4		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	SOPORTE	SOPORTE	SOPORTE	Autoridad	6	5,5	4	8	8	5	6,25	33,00
				Responsable TIC	8		8	8	8	5	7,25	
				Experto	4		4	2	8	5	4,75	
				Auditor Interno	4		4	6	8	5	5,75	
							5,00	6,00	8,00	5,00	6,00	
							5,00	6,00	8,00	5,00	6,00	
	ROUTERS (HW	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Switch cisco	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Central Telefónica	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Wifi	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	SISTEMAS OPERATIVOS WINDOWS	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5	4	8	8	5	6,25	32,08
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	1		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	SISTEMAS OPERATIVOS LINUX	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5	4	8	8	5	6,25	32,08
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	1		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Microsoft Office	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Adobe Macromedia	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5,33333	4	8	8	5	6,25	34,22
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	2		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	
	Softwares gratuitos	Departamento TIC-UELI	Encargado de TI	Autoridad	6	5	4	8	8	5	6,25	32,08
				Responsable TIC	8		8	8	8	5	7,25	
				Auditor Interno	1		4	6	8	5	5,75	
							5,33	7,33	8,00	5,00	6,42	

ERAC N	O PONDERADO	IÓN PONDERADA
%	1,80	23,3625
%	8,80	
%	4,80	
%	2,40	
%	**4,45**	

Anexo4. Lista de Valores de los Activos de información

Listado y valoración de los activos de información

Nro. Activo	Tipo de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
							C	I	D	VA
A1	Personal	Personal administrativo	Empleados que gestionan tareas administrativas dentro de la organización.	Gestión y administración de tareas y procesos internos de la organización	Físico	Secretaria, contadora , Inspección General	1	1	1	1.00
A2	Hardware	pc	Computadoras personales utilizadas por el personal para realizar diversas tareas laborales.	Uso general para tareas administrativas y de oficina	Físico	Secretaria, contadora , Inspección General	3	2	2	2.33
A3	Hardware	Memoria Flash	Dispositivos de almacenamiento portátil utilizados para guardar y transferir datos.	Almacenamiento y transferencia de datos portátiles	Físico	Secretaria, contadora , Inspección General	3	3	3	3.00
A4	Hardware	Dispositivos Móviles	Teléfonos inteligentes y tabletas utilizados por el personal para comunicación y acceso a datos.	Comunicación móvil y acceso a aplicaciones y servicios corporativos	Físico	Secretaria, contadora , Inspección General	2	2	2	2.00
A5	Hardware	Laptop	Computadoras portátiles utilizadas por el personal para trabajo móvil y	Trabajo móvil y remoto, tareas administrativas	Físico	Departamento de Tic	2	2	2	2.00
A6	Hardware	Impresora	Dispositivos utilizados para imprimir documentos y otros materiales necesarios.	Impresión de documentos administrativos y contables	Físico	Secretaria, contadora , Inspetor	1	1	2	1.33
A7	Hardware	Huellas Dactilares	Datos biométricos utilizados para autenticar la identidad del personal.	Control de acceso y seguridad	Físico	Inspección	2	2	1	1.67
A8	Hardware	Cámaras de Vigilancia	Dispositivos de seguridad utilizados para monitorear y grabar actividades dentro y fuera de las instalaciones.	Monitoreo y seguridad de instalaciones	Físico	Departamento de Tic	1	2	1	1.33
A9	Redes	Red de área local e inalámbrica	Infraestructura de red que permite la conexión y comunicación de dispositivos dentro de la organización.	Conectividad y comunicación dentro de la organización	Físico	Departamento de Tic	1	2	1	1.33
A10	Redes	Red Interna	Infraestructura de red interna que facilita la comunicación y el intercambio de datos entre dispositivos.	Infraestructura de red para servicios y aplicaciones internas	Físico	Infratructura	1	1	2	1.33
A11	Redes	Antena Direccional	Dispositivo de comunicación que mejora la señal de red en una dirección específica.	Comunicación de largo alcance y enlaces punto a punto	Físico	Infratructura	2	2	2	2.00
A12	Redes	Red de Comunicación	Infraestructura que soporta la comunicación interna y externa de la organización.	Comunicación de datos y voz dentro y fuera de la organización	Físico	Infratructura	1	2	3	2.00
A13	Software	Software del biometrico	Aplicaciones utilizadas para gestionar y autenticar datos biométricos del personal.	Gestión de datos biométricos y control de acceso	Digital	Inspección	2	2	2	2.00
A14	Software	Aplicaciones	Programas informáticos utilizados por el personal para realizar tareas específicas.	Herramientas de productividad y gestión	Digital	Secretaria, contadora , Inspección General	1	1	2	1.33
A15	Software	Software de Gestión	Aplicaciones utilizadas para la administración y gestión de diversos aspectos de la organización.	Gestión de recursos y operaciones empresariales	Digital	Departamento de Tic, Secretaria . Inspección General	1	1	1	1.00
A16	Software	Software de Contabilidad	Programas informáticos utilizados para llevar la contabilidad y las finanzas de la organización.	Gestión financiera y contable	Digital	Contabilidad	2	3	2	2.33
A17	Software	**Firewall**	Dispositivo o software que protege la red de accesos no autorizados y ciberataques.	Seguridad perimetral y protección contra amenazas externas	Digital	Departamento de Tic	3	3	3	3.00
A18	Software	Sistema de Gestión de Video	Software utilizado para gestionar y almacenar grabaciones de cámaras de vigilancia.	Gestión y almacenamiento de grabaciones de vigilancia	Digital	Departamento de Tic	2	2	3	2.33
A19	Software	Correo Electrónico Corporativo	Servicio de email utilizado para la comunicación interna y externa de la organización.	Comunicación interna y externa	Digital	Departamento de Tic	1	1	3	1.67
A20	Software	Sitio Web	Página web oficial de la organización utilizada para la comunicación y promoción en línea.	Presencia en línea y comunicación con clientes y partes interesadas	Digital	Departamento de Tic	2	1	1	1.33
A21	Software	Proveedor de Internet	Empresa que proporciona el servicio de conexión a internet.	Conectividad a internet	Físico	Departamento de Tic	2	1	1	1.33
A22	Software	Mantenimiento / Actulización	Actividades y procedimientos destinados a mantener y actualizar los sistemas y dispositivos.	Mantenimiento y actualización de sistemas y equipos TI	Lógico	Departamento de Tic	3	3	3	3.00
A23	Datos	Documentación TI	Registros y manuales relacionados con la infraestructura y sistemas tecnológicos de la organización.	Registro y documentación de procesos y sistemas de TI	Físico-Digital	Secretaria, Inspección	2	2	2	2.00
A24	Datos	Documentos Físicos	Archivos en papel que contienen información relevante para la	Almacenamiento y gestión de documentos impresos	Físico	Secretaria, contadora , Inspección General	2	2	2	2.00
A25	Datos	Documentos Contables	Registros financieros y contables en formato físico o digital.	Registro y gestión de información financiera y contable	Físico-Digital	Secretaria, contadora , Inspección General	2	2	2	2
A26	Datos	Informes de auditoría	Documentos que detallan los resultados de auditorías internas y externas.	Evaluación y verificación de conformidad y cumplimiento	Físico-Digital	Secretaria, contadora , Inspección General	3	3	3	3
A27	Datos	Grabaciones de Vigilancia	Videos capturados por las cámaras de seguridad.	Almacenamiento y revisión de videos de seguridad	Físico-Digital	Secretaria, contadora , Inspección General	1	3	3	3
A28	Datos	Políticas de Seguridad	Normativas y procedimientos implementados para proteger la información y los activos de la organización.	Directrices y normas para la protección de la información	Digital	Departamento de Tic	3	3	3	3
A29	Datos	Base de Datos	Colección organizada de datos almacenados electrónicamente.	Almacenamiento y gestión de datos críticos	Digital	Departamento de Tic	2	2	3	3
A30	Datos	Backup	Copias de seguridad de datos y sistemas importantes para prevenir pérdida de información.	Copias de seguridad y recuperación de datos	Digital	Departamento de Tic	3	3	3	3
A31										
A32										

Anexo 5 Tratamiento y Evaluación de Riesgos

Análisis de Riesgos				Evaluación de Riesgos						Tratamiento de Riesgos							
				Impacto	Probabilidad												
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual
A1	Personal administrativo	Phishing, ingeniería social	Falta de conciencia en seguridad	1,00	1	2	Políticas de seguridad y formación continua	2,00	BAJO	ACEPTAR	CONTROL PREVENTIVO	A.7 Seguridad de los Recursos Humanos A.7.2.2 Responsabilidades de la seguridad antes, durante y después del empleo	2	3	6,00	MEDIO	INACEPTABLE
A2	pc	Malware, ransomware	Falta de actualizaciones de seguridad	1,00	3	3	Antivirus y actualizaciones periódicas	9,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.9 Control de Acceso A.9.2.1 Registro de usuarios	2	2	4,00	MEDIO	INACEPTABLE
A3	Memoria Flash	Pérdida física, robo	Falta de cifrado de datos	1,00	2	2	Cifrado de datos y políticas de uso	4,00	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.8 Gestión de Activos A.8.1.3 Uso aceptable de activos	3	3	9,00	ALTO	INACEPTABLE
A4	Dispositivos Móviles	Robo, pérdida, malware móvil	Falta de autenticación segura	2,33	2	2	Cifrado de datos y autenticación multifactor	9,33	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.6 Organización de la Seguridad de la Información A.6.2.1 Política de uso de dispositivos móviles	3	3	9,00	ALTO	INACEPTABLE
A5	Laptop	Robo, pérdida, malware	Falta de cifrado de disco duro	2,33	2	2	Seguridad física y cifrado de disco	9,33	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.9 Control de Acceso A.9.4.1 Uso de dispositivos de usuario	2	3	6,00	MEDIO	INACEPTABLE
A5	Laptop	Robo, pérdida, malware	Falta de cifrado de disco duro	2,33	2	2	Seguridad física y cifrado de disco	9,33	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.9 Control de Acceso A.9.4.1 Uso de dispositivos de usuario	2	3	6,00	MEDIO	INACEPTABLE
A6	Impresora	Acceso no autorizado, interceptación de impresión	Falta de configuraciones seguras	2,33	1	1	Red segura y control de acceso	2,33	BAJO	ACEPTAR	NO APLICA CONTROL	A.11 Seguridad Física y del Entorno A.11.2.6 Seguridad de equipos fuera de las instalaciones	1	2	2,00	BAJO	ACEPTABLE
A7	Huellas Dactilares	Robo de identidad, falsificación	Falta de autenticación multifactorial	3,00	3	3	Sistemas biométricos avanzados y monitoreo	27,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.18 Cumplimiento A.18.1.5 Protección de datos personales	2	2	4,00	MEDIO	INACEPTABLE
A8	Cámaras de Vigilancia	Acceso no autorizado, interceptación de transmisión	Falta de actualizaciones de firmware	3,00	2	2	Monitoreo y protección física	12,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.11 Seguridad Física y del Entorno A.11.1.4 Zonas de seguridad y controles de acceso físico	2	2	4,00	MEDIO	INACEPTABLE
A9	Red de área local e inalámbrica	Ataques de sniffing, DoS	Configuraciones débiles de contraseña	2,00	2	2	Cifrado WPA3 y segmentación de red	8,00	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.13 Seguridad en las Comunicaciones A.13.1.1 Políticas de seguridad de la red	3	3	9,00	ALTO	INACEPTABLE
A10	Red Interna	Acceso no autorizado, escuchas	Falta de segmentación de red	2,00	3	3	Control de acceso y auditorías	18,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.13 Seguridad en las Comunicaciones A.13.1.3 Separación en las redes	3	2	6,00	MEDIO	INACEPTABLE
A11	Antena Direccional	Interferencia, acceso no autorizado	Falta de detección de intrusiones	2,00	2	2	Cifrado de la señal	8,00	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.13 Seguridad en las Comunicaciones A.13.1.2 Controles de red	2	2	4,00	MEDIO	INACEPTABLE
A12	Red de Comunicación	Intercepción de datos, spoofing	Falta de cifrado de datos	1,33	2	2	Cifrado de extremo a extremo	5,33	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.13 Seguridad en las Comunicaciones A.13.1.1 Políticas de seguridad de la red	3	3	9,00	ALTO	INACEPTABLE

A13	Software del biometrico	Falsificación, manipulación de datos	Falta de pruebas de seguridad del software	1,67	3	3	Actualizaciones y parches regulares	15,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.14 Adquisición, desarrollo y mantenimiento de sistemas de información A.14.1.2 Principios de seguridad en el desarrollo de sistemas de información	2	2	4,00	MEDIO	INACEPTABLE
A14	Aplicaciones	Inyección de código, vulnerabilidades conocidas	Falta de parches de seguridad	1,67	2	2	Pruebas de seguridad y revisiones de código	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.14 Adquisición, desarrollo y mantenimiento de sistemas de información A.14.2.1 Procedimientos seguros de desarrollo de software	2	2	4,00	MEDIO	INACEPTABLE
A15	Software de Gestión	Acceso no autorizado, vulnerabilidades de software	Falta de políticas de acceso	1,33	2	2	Gestión de parches y actualizaciones	5,33	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.12 Seguridad de las Operaciones A.12.1.2 Procedimientos de gestión de cambios	2	2	4,00	MEDIO	INACEPTABLE
A16	Software de Contabilidad	Manipulación de datos, accesos no autorizados	Falta de auditorías regulares	1,33	2	2	Políticas de contraseñas y autenticación	5,33	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.12 Seguridad de las Operaciones A.12.1.3 Capacidades de registro de eventos	2	2	4,00	MEDIO	INACEPTABLE
A17	**Firewall**	Ataques de evasión, configuraciones débiles	Falta de actualizaciones de reglas	1,33	3	3	Configuración segura y monitoreo continuo	12,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.13 Seguridad en las Comunicaciones A.13.1.1 Políticas de seguridad de la red	3	2	6,00	MEDIO	INACEPTABLE
A18	Sistema de Gestión de Video	Acceso no autorizado, interceptación de video	Falta de autenticación fuerte	1,33	2	1	Cifrado y segmentación de red	2,67	BAJO	ACEPTAR	CONTROL CORRECTIVO	A.13 Seguridad en las Comunicaciones A.13.1.2 Controles de red	2	2	4,00	MEDIO	INACEPTABLE
A19	Correo Electrónico Corporativo	Phishing, malware adjunto	Falta de filtrado de correo electrónico	1,33	3	3	Filtros de spam y capacitación a usuarios	12,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.13 Seguridad en las Comunicaciones A.13.2.3 Protección de la información en tránsito	3	3	9,00	ALTO	INACEPTABLE
A20	Sitio Web	SQL Injection, XSS	Falta de escaneos de vulnerabilidades	1,33	2	3	Servicios anti-DDoS y monitoreo	8,00	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.14 Adquisición, desarrollo y mantenimiento de sistemas de información A.14.1.3 Protección de transacciones en servicios de aplicaciones	3	2	6,00	MEDIO	INACEPTABLE
A21	Proveedor de Internet	Interrupciones de servicio, ataque de red	Falta de monitoreo de red	2,00	1	1	Contratos SLA y redundancia	2,00	BAJO	ACEPTAR	NO APLICA CONTROL	A.15 Relaciones con Proveedores A.15.1.1 Políticas de seguridad de la información para relaciones con proveedores	2	2	4,00	MEDIO	INACEPTABLE
A22	Mantenimiento / Actulización	Interrupción de servicio, actualizaciones defectuosas	Falta de pruebas antes de implementar	2,00	3	3	Políticas y procedimientos claros	18,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.12 Seguridad de las Operaciones A.12.5.1 Instalación de software en sistemas operativos	2	2	4,00	MEDIO	INACEPTABLE
A23	Documentación TI	Acceso no autorizado, pérdida física	Falta de control de acceso físico	2,00	3	3	Cifrado y control de acceso	18,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.8 Gestión de Activos A.8.2.3 Clasificación de la información	2	2	4,00	MEDIO	INACEPTABLE

A24	Documentos Físicos	Robo, pérdida, acceso no autorizado	Falta de almacenamiento seguro	2,00	3	3	Almacenamiento seguro y control de acceso	18,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.8 Gestión de Activos A.8.3.1 Gestión de soportes removibles	1	2	2,00	BAJO	ACEPTABLE
A25	Documentos Contables	Manipulación de datos, acceso no autorizado	Falta de trazabilidad de cambios	1,33	2	2	Almacenamiento seguro y control de acceso	5,33	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.8 Gestión de Activos A.8.3.2 Eliminación segura de soportes	1	2	2,00	BAJO	ACEPTABLE
A26	Informes de auditoría	Acceso no autorizado, alteración	Falta de protección de integridad	1,00	1	3	Almacenamiento seguro y control de acceso	3,00	BAJO	ACEPTAR	CONTROL PREVENTIVO	A.16 Gestión de Incidentes de Seguridad de la Información A.16.1.1 Responsabilidades y procedimientos	2	2	4,00	MEDIO	INACEPTABLE
A27	Grabaciones de Vigilancia	Acceso no autorizado, eliminación no autorizada	Falta de encriptación de almacenamiento	2,33	2	2	Almacenamiento seguro y control de acceso	9,33	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.18 Cumplimiento A.18.1.4 Protección de registros	2	2	4,00	MEDIO	INACEPTABLE
A28	Políticas de Seguridad	Incumplimiento, falta de actualización	Falta de conciencia y entrenamiento	3,00	1	3	Almacenamiento seguro y control de acceso	9,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.5 Políticas de Seguridad de la Información A.5.1.1 Políticas para la seguridad de la información	2	2	4,00	MEDIO	INACEPTABLE
A29	Base de Datos	SQL Injection, acceso no autorizado	Falta de encriptación de datos sensibles	2,33	2	2	Actualizaciones regulares y gestión de parches	9,33	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	A.14 Adquisición, desarrollo y mantenimiento de sistemas de información A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	3	3	9,00	ALTO	INACEPTABLE
A30	Backup	Pérdida, acceso no autorizado a copias	Falta de pruebas de restau	1,67	3	2	Copias de seguridad regulares y almacenamiento	10,00	ALTO	MITIGAR / EVITAR / TRANSFERIR	CONTROL CORRECTIVO	A.12 Seguridad de las Operaciones A.12.3.1 Procedimientos de copia de seguridad	3	3	9,00	ALTO	INACEPTABLE

UNIDAD EDUCATIVA "LA INMACULADA"
Ambato Ecuador
Av.Miraflores 1.156 y Margaritas www.lainmaculada.edu.ec Telf. (03)2823988

Anexo 6: Acuerdo de Confidencialidad

Ambato, a _____ de _____ 20___

Yo,_____, portador de la C.C:_____, empleado de la Unidad Educativa La Inmaculada, desempeñando a la fecha el cargo de _____ en el Área de _____ bajo la modalidad de contrato _____ suscribo el presente Acuerdo de Confidencialidad de la Información, asumiendo que:

1. Comprendo que la información no publica asociada con el personal y la institución tienen el carácter de confidencial, por tanto, me comprometo a estar sujeto y utilizarla solo para los fines que mis responsabilidades como empleado de la Unidad Educativa La Inmaculada lo requiera.

2. Ser consciente de la responsabilidad de no poner en riesgo la confidencialidad, integridad y disponibilidad de la información que gestiona la Unidad Educativa La Inmaculada. A su vez me comprometo a cumplir los procedimientos de gestión de seguridad de la información que concierne a mis funciones descritas en el documento de las POLITICAS DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

3. Cumplir con las disposiciones relacionadas a las POLITICAS DE SEGURIDAD DE LA INFORMACIÓN(SGSI) en lo que se refiere a su utilización y difusión.

4. Comprende que no cumplir con las disposiciones del presente acuerdo podría implicar penalizaciones por parte de la Unidad Educativa La Inmaculada y las leyes vigentes.

Firma del empleado

_____
NOMBRES Y APELLIDOS
CEDULA DE CIUDADANÍA

Firma del responsable de la Seguridad de la Información

_____
NOMBRES Y APELLIDOS
CEDULA DE CIUDADANÍA

UNIDAD EDUCATIVA "LA INMACULADA"
Ambato Ecuador
Av.Miraflores 1.156 y Margaritas www.lainmaculada.edu.ec Telf. (03)2823988

Anexo 7: Formulario de inventario de hardware y software de computadoras

Nombre del Computador	
Dirección IP	
Mascara de Subred	
Nombre de Dominio	
Localización física del Computador	
Modelo del Microprocesador	
Marca de Computador	
Modelo de Computador	
Número de procesadores	
Velocidad Procesador	
Sistema Operativo	
Versión de Sistema Operativo	
Memoria RAM	
Capacidad de Almacenamiento	

Lineamientos de uso de los equipos:

- No ingresar con alimentos ni bebidas.
- No fumar.
- Tener el equipo conectado a un UPS para evitar variaciones de voltaje.
- No realizar cambios sobre el software.
- No realizar cambios o mantenimiento sobre el hardware.
- Conservar los equipos en óptimas condiciones.

UNIDAD EDUCATIVA "LA INMACULADA"
Ambato Ecuador
Av.Miraflores 1.156 y Margaritas www.lainmaculada.edu.ec Telf. (03)2823988

Anexo 8: Formulario de Creación de Usuarios y Responsabilidades de Contraseñas

SOLITUD DE ACCESO A SISTEMAS DE INFORMACIÓN	
Datos Generales	
Departamento:	
Datos del Usuario	
Apellido y Nombre del Solicitante:	
Cargo:	Telf.:
Correo Electrónico:	
Perfil de usuario a crear	
Sistema de Información:	
Usuario:	
Contraseña:	
Obligaciones del Usuario	
La clave o contraseña es de uso personal y no puede ser otorgada a otro empleado por ningún motivo. Para realizar cambios de perfiles de usuario se debe comunicar con el Departamento TI de la Unidad Educativa la Inmaculada En caso de que el empleado sea suspendido temporal o definitivamente de su cargo, se deberá informar de manera inmediata al administrador de usuarios. El empleado debe cerrar su sesión de usuario cuando no esté en uso.	
Firmas	
Cargo: **Fecha:** **Solicitante:**	**Cargo:** **Fecha:** **Autoriza:**
Observaciones:	

UNIDAD EDUCATIVA "LA INMACULADA"
Ambato Ecuador
Av.Miraflores 1.156 y Margaritas www.lainmaculada.edu.ec Telf. (03)2823988

Anexo 9: Formato para el Registro De Backups.

Código:

Versión:					
Fecha de Actualización:					
Elaborado por:					
Sistema de información	**Tipo de Backups**	**Tiempo del Backups**	**Medio de Almacena miento**	**Lugar de Almacena miento**	**Persona que lo genera**

Glosario

- **SGSI/ISMS**: Conjunto de políticas para proteger la información, garantizando confidencialidad, integridad y disponibilidad.
- **ISO/IEC 27001**: Norma internacional para gestionar la seguridad de la información.
- **Principios CIA**:
    - **Confidencialidad**: Información accesible solo a autorizados.
    - **Integridad**: Información precisa y completa.
    - **Disponibilidad**: Información accesible cuando se necesita.
- **SOA (Statement of Applicability)**: Documento que especifica los controles de seguridad aplicables.
- **Ciclo PDCA**: Ciclo de mejora continua en la gestión de la seguridad.
- **Evaluación y Gestión de Riesgos (RA y RM)**: Identificación y mitigación de riesgos de seguridad.
- **SOC (Security Operations Center)**: Unidad centralizada que monitorea la seguridad.
- **IAM (Identity and Access Management)**: Gestión del acceso a recursos.
- **MFA (Multi-Factor Authentication)**: Autenticación con múltiples verificaciones.
- **SIEM (Security Information and Event Management)**: Análisis en tiempo real de alertas de seguridad.
- **CISO (Chief Information Security Officer)**: Responsable de la seguridad de la información.
- **GDPR (General Data Protection Regulation)**: Reglamento de protección de datos de la UE.
- **BACKUP**: Copia de seguridad para recuperación de datos.

- **Desastre, Amenaza y Activo**: Eventos disruptivos, causas potenciales y elementos de valor.
- **Auditoría y Ciberseguridad**: Evaluación de cumplimiento y protección contra ataques.
- **Plan de Continuidad**: Procedimientos para recuperar operaciones tras interrupciones.
- **Seguridad de la información**: Protección de confidencialidad, integridad y disponibilidad de la información.
- **Análisis Preliminar de Riesgos (ARP)**: Identificación de riesgos en el diseño de productos/servicios.
- **Phishing**: Obtención de información sensible mediante engaño.
- **Malware**: Software malicioso que daña sistemas.
- **Ransomware**: Malware que exige rescate para liberar archivos encriptados.
- **Spyware**: Recopila información sin consentimiento.
- **Adware**: Publicidad no deseada y recopilación de datos de navegación.
- **Ingeniería social**: Manipulación para revelar información confidencial.
- **Ataques DDoS**: Saturación de tráfico para inhabilitar servicios en línea.
- **Man-in-the-Middle (MitM)**: Interceptación de comunicaciones.
- **Vulnerabilidades de software**: Fallos explotables que permiten acceso no autorizado.
- **Exfiltración de datos**: Transferencia no autorizada de datos.
- **Acoso cibernético**: Intimidación o amenazas en medios electrónicos.
- **Robo de identidad**: Uso fraudulento de información personal.
- **Shadow IT**: Uso de aplicaciones no aprobadas, generando riesgos.
- **Cifrado**: Protección de datos mediante conversión en código.

Universidad Católica de Cuenca

Ambato, 10 de febrero del 2024.

Mg. Sor Esthela Chicaiza
RECTORA DE LA UNIDAD EDUCATIVA LA INMACULADA
Presente. –

De mi consideración:

Me place extenderle un cordial saludo y al mismo tiempo dirigirme a usted con el objeto de solicitar muy respetuosamente que mi persona yo, **Franklin Vinicio Guamán Muela** con cedula de Identidad **1803439908** estudiante de la Maestría de Ciberseguridad de la **Universidad Católica de Cuenca** me permita realizar el tema de Tesis de grado en su prestigiosa Institución.

El tema a desarrollar es **Desarrollo *de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando norma ISO/27001 en la protección de datos para la Unidad Educativa La Inmaculada de la Ciudad de Ambato;*** *me permita tener el acceso* a la información que permite desarrollar el proyecto de trabajo de grado. el cual contribuirá positivamente la protección de datos

Por la gentil atención a la presente solicitud, le anticipo mis sinceros agradecimientos.

Atentamente,

Ing. Franklin Vinicio Guamán M.
C.I. 1803439908
Estudiante de la Maestría Ciberseguridad
UCACUE

10-02-2024
Mg. Esthela Chicaiza
Recibido

UNIDAD EDUCATIVA "LA INMACULADA" AMBATO RECTORADO

Universidad Católica de Cuenca

Ambato, 10 de febrero del 2024.

Mg. Sor Esthelita Chicaiza
RECTORA DE LA UNIDAD EDUCATIVA LA INMACULADA
Presente. -

De mi consideración:

Reciba un cordial saludo. Por medio del presente, me permito dirigirme a usted con el propósito de solicitar su autorización para llevar a cabo el levantamiento de activos de la información en la protección de datos en los departamentos de Sistemas, Contabilidad, Secretaría e Inspección General para la realización del tema de Tesis de la Maestría en su prestigiosa Institución.

El objetivo de esta actividad es realizar un inventario detallado de todos los activos de información, con el fin de garantizar su adecuada protección y cumplir con las normativas vigentes en materia de seguridad de la información y protección de datos personales. Este levantamiento nos permitirá identificar, clasificar y evaluar los activos, así como establecer las medidas de seguridad necesarias para proteger la información sensible y confidencial de la institución

Por la favorable atención que se dé al presente anticipo mis sinceros agradecimientos.

Atentamente,

Ing. Franklin Vinicio Guamán M.
C.I. 1803439908
Estudiante de la Maestría Ciberseguridad
UCACUE

10-02-2024
Mg. Esthela Chicaiza
Recibido

AMBATO
RECTORADO