

REPÚBLICA DEL ECUADOR



**UNIVERSIDAD TÉCNICA DEL NORTE**



**FACULTAD DE POSGRADO**

**MAESTRÍA EN COMPUTACIÓN MENCIÓN EN SEGURIDAD  
INFORMÁTICA**

**DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA  
UNIDADES EDUCATIVAS DEL CANTÓN ESMERALDAS: ENFOQUE EN LA  
PROTECCIÓN DE DATOS Y RIESGOS.**

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación

AUTOR: Ing, Carlos Alberto Campaña Bone

DIRECTOR: Ing. Henry Patricio Farinango Endara, Msc

IBARRA - ECUADOR

2024

## **DEDICATORIA**

A Dios, por ser mi guía y fuente inagotable de fortaleza, sin Ti nada de esto hubiera sido posible.

A mi amada esposa, Leonela, y a mis hijos, Dubrasska y Asher, quienes fueron mi inspiración diaria. Este trabajo es un reflejo de que todo se puede lograr con el apoyo y el amor de la familia.

A mi madre, por su valentía y dedicación.

A mis hermanos, Sebastián y Odalis, para que nunca dejen de creer en ellos mismos y sepan que, con esfuerzo y dedicación, todo es posible.

A mi suegra, por todo el apoyo brindado. Para mí, te has convertido en una segunda madre.

Y a cada persona e individuo que me dio aliento, ánimo y fuerza para terminar este proyecto de estudio.

## **AGRADECIMIENTOS**

En primer lugar, agradezco a Dios por darme la salud, la sabiduría y la perseverancia necesarias para completar esta etapa de mi vida académica. Su guía ha sido fundamental en cada paso de este camino.

A mi esposa, Leonela, gracias por tu amor, comprensión y apoyo incondicional. Tus palabras de aliento y tu fe en mí han sido el motor que me ha impulsado a seguir adelante.

A mis hijos, Dubrasska y Asher, ustedes son mi mayor motivación. Espero que este logro les muestre que con esfuerzo y dedicación, todo es posible.

A mi tutor Ing. Farinango Endara Henry, asesor Ing. Llumiyinga Gabriel, colegas y amigos que me ofrecieron su tiempo, conocimientos y palabras de ánimo durante este proceso, les estoy eternamente agradecido. Sus contribuciones han sido fundamentales para la realización de este proyecto.

Finalmente, agradezco a la universidad y a todos sus integrantes por brindarme las herramientas y el entorno propicio para llevar a cabo este estudio.



# UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

## BIBLIOTECA UNIVERSITARIA

### AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE



#### 1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
<b>CÉDULA DE IDENTIDAD</b>	0802951921		
<b>APELLIDOS Y NOMBRES</b>	CAMPAÑA BONE CARLOS ALBERTO		
<b>DIRECCIÓN</b>	URB. COSTA VERDE MZ 8 CASA 3		
<b>EMAIL</b>	Ccampana.86@gmail.com		
<b>TELÉFONO FIJO</b>	062010801	<b>TELÉFONO MÓVIL:</b>	0990537953

DATOS DE LA OBRA	
<b>TÍTULO:</b>	DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA UNIDADES EDUCATIVAS DEL CANTÓN ESMERALDAS: ENFOQUE EN LA PROTECCIÓN DE DATOS Y RIESGOS.
<b>AUTOR (ES):</b>	ING. CAMPAÑA BONE CARLOS ALBERTO
<b>FECHA:</b>	03 de junio 2024
SOLO PARA TRABAJOS DE GRADO	
<b>PROGRAMA DE POSGRADO</b>	MAESTRÍA EN COMPUTACION MENCION EN SEGURIDAD INFORMÁTICA
<b>TITULO POR EL QUE OPTA</b>	MAGÍSTER EN COMPUTACIÓN
<b>TUTOR</b>	MSC. FARINANGO ENDARA HENRY





## 2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 15 días del mes de agosto del 2024

### EL AUTOR:

Firma \_\_\_\_\_

Nombre: Ing. Campaña Bone Carlos Alberto



Ibarra, 3 de junio de 2024



Dra.  
Lucía Yépez  
**DECANA FACULTAD DE POSGRADO**

**ASUNTO:** Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado **DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA UNIDADES EDUCATIVAS DEL CANTÓN ESMERALDAS: ENFOQUE EN LA PROTECCIÓN DE DATOS Y RIESGOS**, del maestrante **CAMPAÑA BONE CARLOS ALBERTO**, de la Maestría de Computación Mención En Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	<b>Apellidos y Nombres</b>	<b>Firma</b>
Director	Msc. Farinango Endara Henry	
Asesor	Msc. Llumiquinga Veintimilla Gabriel	

# ÍNDICE DE CONTENIDOS

CAPITULO I .....	14
1. EL PROBLEMA.....	14
1.1. Introducción.....	14
1.2. Problema de investigación.....	15
1.3. Interrogantes de la investigación .....	17
1.4. Objetivos de la investigación.....	18
1.4.1. Objetivo general.....	18
1.4.2. Objetivos específicos.....	18
1.5. Justificación .....	18
1.6. Hipótesis de Trabajo .....	19
1.7. Hipótesis Alternativa .....	20
1.8. Variables Independiente .....	20
1.9. Variables Dependiente.....	20
CAPÍTULO II .....	21
2. MARCO REFERENCIAL.....	21
2.1. Antecedentes.....	21
2.2. Marco Teórico .....	22
2.2.1. Sistemas de Gestión de Seguridad de la Información .....	22
2.2.2. Normas/Estándares ISO27001 .....	22
2.2.3. Análisis de metodologías.....	24
2.2.4. Seguridad De La Información .....	32
2.2.5. Implementación De Medidas De Seguridad .....	34
2.2.6. Ciberseguridad.....	34
2.2.7. Tipos De Amenazas y Vulnerabilidades.....	35
2.2.8. Protección De Datos .....	36
2.3. Marco Legal.....	37
CAPÍTULO III.....	39
3. MARCO METODOLÓGICO .....	39
3.1. Descripción del área de estudio .....	39
3.2. Enfoque y Tipo de Investigación.....	42
3.3. Recolección de información .....	42
3.4. Procesamiento de la información.....	43
3.5. Metodología de investigación.....	43
3.5.1. Fase 1 – Situación Actual (UESDC) .....	44
3.5.2. Fase 2 – Sistema de Gestión Documental / Preparación SGSI.....	46

3.5.3.	Fase 3 - Análisis de Riesgo.....	50
3.5.3.1.	Identificación de los Activos .....	51
3.5.3.2.	Identificación de Amenazas.....	59
3.5.3.3.	Valoración de amenazas .....	69
3.5.3.4.	Estimación del impacto.....	71
3.5.3.5.	Riesgo Aceptable .....	72
3.5.3.6.	Riesgo Residual .....	73
3.5.3.7.	Activos críticos para la unidad Educativa .....	75
3.5.4.	Fase 4 – Plan de Seguridad de la Información .....	76
3.5.5.	Fase 5 - Resultados .....	77
3.5.5.1.	De los Riesgos .....	77
3.5.5.2.	Generales .....	80
4.	CAPITULO IV .....	84
4.1.	RESULTADOS Y DISCUSIÓN .....	84
	CONCLUSIONES Y RECOMENDACIONES .....	99
	CONCLUSIONES .....	99
	RECOMENDACIONES.....	99
	BIBLIOGRAFÍA .....	101
	ANEXOS	104
	ANEXO A: CONTROL DE SEGURIDAD DE LA INFORMACIÓN .....	104
	ANEXO B: VALORACION DE LAS AMENAZAS DE LOS ACTIVOS DE LA UESDC .....	115
	ANEXO C: VALORACION DE LAS AMENAZAS DE LOS ACTIVOS DE LA UESDC APLICADOS SALVAGUARDA .....	122
	ANEXO D: PLAN DE SEGURIDAD DE INFORMACION .....	130
	ANEXO E: ENCUESTA REALZIADA AL PERSONAL ADMINISTRATIVO Y DOCENTE DE LA UESDC	134

## ÍNDICE DE TABLAS

TABLA 1 RESUMEN DE LAS NORMAS ISO-27000 .....	23
TABLA 2 RESUMEN DE REVISIÓN BIBLIOGRÁFICA .....	25
TABLA 3 COMPARACIÓN DE METODOLOGÍAS TRATAMIENTO DE VULNERABILIDADES.....	29
TABLA 4 COMPARACIÓN DE METODOLOGÍAS TRATAMIENTO DE AMENAZAS.....	30
TABLA 5 RESUMEN DE AMENAZAS Y VULNERABILIDADES SEGÚN MAGERIT .....	35
TABLA 6 UNIDADES EDUCATIVAS SELECCIONADAS .....	39
TABLA 7 VALORACIÓN DE CONTROLES .....	46
TABLA 8 TIPO DE ACTIVO .....	51
TABLA 9 INVENTARIOS DE ACTIVOS.....	52
TABLA 10 VALORES DE CRITICIDAD .....	54
TABLA 11 VALORACIÓN DE ACTIVOS SEGÚN SU CRITICIDAD.....	55
TABLA 12 AMENAZAS DATOS [D] – [E], [A].....	59
TABLA 13 AMENAZAS SERVICIOS [S] – [E], [A].....	60
TABLA 14 AMENAZAS APLICACIONES DE SOFTWARE [SW] - [I], [E], [A] .....	61
TABLA 15 AMENAZAS EQUIPOS INFORMÁTICOS [HW] - [N], [I], [E], [A] .....	63
TABLA 16 AMENAZAS PERSONAL[P] - [E], [A].....	64
TABLA 17 AMENAZAS REDES DE COMUNICACIÓN [COM] - [I], [E], [A].....	64
TABLA 18 AMENAZAS SOPORTE DE INFORMACIÓN [MEDIA] - [N], [I], [E], [A] .....	66
TABLA 19 EQUIPAMIENTO AUXILIAR [AUX] - [N], [I], [E], [A] .....	67
TABLA 20 AMENAZAS INSTALACIONES [L] - [N], [I], [E], [A] .....	68
TABLA 21 DEGRADACIÓN DEL VALOR .....	69
TABLA 22 PROBABILIDAD DE OCURRENCIA .....	69
TABLA 23 VALORACIÓN DE AMENAZAS DATOS/INFORMACIÓN [D] .....	70
TABLA 24 VALORACIÓN DE RIESGO DE LOS DATOS/INFORMACIÓN [D].....	72
TABLA 25 VALORACIÓN DE IMPACTO AMENAZAS DATOS/INFORMACIÓN [D] - APLICANDO NIVELES DE SALVAGUARDAS .....	73
TABLA 26 VALORACIÓN DE RIESGO RESIDUAL DE LOS DATOS/INFORMACIÓN [D] CON APLICACIÓN DE SALVAGUARDA .....	74
TABLA 27 ACTIVOS CRÍTICOS.....	75
TABLA 28 ACTIVOS DATOS / INFORMACIÓN [D] CON ESTADO DE RIESGOS .....	77
TABLA 29 ACTIVOS SERVICIOS [S] CON ESTADO DE RIESGOS.....	77
TABLA 30 ACTIVOS APLICACIONES DE SOFTWARE [SW] CON ESTADO DE RIESGOS..	78
TABLA 31 ACTIVOS EQUIPOS INFORMÁTICOS [HW] CON ESTADO DE RIESGOS .....	78
TABLA 32 ACTIVOS REDES DE COMUNICACIÓN [COM] CON ESTADO DE RIESGOS .....	79
TABLA 33 ACTIVOS INSTALACIONES [L] CON ESTADO DE RIESGOS .....	80
TABLA 34 PREGUNTA ¿CIERRA SU SESIÓN EN LOS SISTEMAS INFORMÁTICOS DESPUÉS DE UTILIZARLOS? .....	85
TABLA 35 ¿COMPARTE SU CONTRASEÑA O CREDENCIALES CON OTROS COLEGAS? .....	86
TABLA 36 ¿VERIFICA LA AUTENTICIDAD DE LOS CORREOS ELECTRÓNICOS ANTES DE ABRIR ARCHIVOS O HACER CLIC EN ENLACES? .....	87
TABLA 37 ¿ES CAUTELOSO(A) AL DESCARGAR ARCHIVOS DE FUENTES NO CONFIABLES EN LOS SISTEMAS DE LA INSTITUCIÓN? .....	89
TABLA 38 ¿TOMA PRECAUCIONES ADICIONALES AL MANEJAR DATOS SENSIBLES DE LOS ESTUDIANTES? .....	91
TABLA 39 ¿HA RECIBIDO CAPACITACIÓN SOBRE LAS MEJORES PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN POR PARTE DEL DEPARTAMENTO DE TIC? ..	93

<b>TABLA 40 ¿HA PARTICIPADO EN SIMULACROS DE SEGURIDAD INFORMÁTICA ORGANIZADOS POR LA INSTITUCIÓN?</b> .....	94
<b>TABLA 41 ¿REPORTA ACTIVIDADES SOSPECHOSAS RELACIONADAS CON LA SEGURIDAD DE LA INFORMACIÓN A LOS DEPARTAMENTOS CORRESPONDIENTES?</b> .....	95
<b>TABLA 42 ¿COOPERA CON LOS PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA ESTABLECIDOS POR LA INSTITUCIÓN EDUCATIVA?</b> .....	96
<b>TABLA 43 ¿HA TENIDO LA OPORTUNIDAD DE REVISAR Y COMPRENDER COMPLETAMENTE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA INSTITUCIÓN?</b> .....	98

## ÍNDICE DE FIGURAS

<b>FIGURA 1</b>	VARIABLES INDEPENDIENTE Y DEPENDIENTE.....	20
<b>FIGURA 2.</b>	TRIADA DE LA SEGURIDAD .....	33
<b>FIGURA 3</b>	ESTRUCTURA DE RED UESDC .....	45
<b>FIGURA 4</b>	INSTRUMENTO DE CONTROL DE SEGURIDAD DE LA INFORMACIÓN.....	48
<b>FIGURA 5</b>	RESULTADO DE EVALUACIÓN DE EFECTIVIDAD.....	49
<b>FIGURA 6</b>	EVALUACIÓN DE CONTROL .....	49
<b>FIGURA 7</b>	NIVEL DE CUMPLIMIENTO.....	50
<b>FIGURA 8</b>	IDENTIFICACIÓN DE ACTIVOS SOBRE MANEJOS DE DATOS PERSONALES .....	58
<b>FIGURA 9</b>	MEDIA DE RIESGO DATOS / INFORMACIÓN [D].....	81
<b>FIGURA 10</b>	MEDIA DE RIESGO SERVICIOS [S] .....	81
<b>FIGURA 11</b>	MEDIA DE RIESGO APLICACIONES DE SOFTWARE [SW] .....	81
<b>FIGURA 12</b>	MEDIA DE RIESGO EQUIPOS INFORMÁTICOS [HW].....	82
<b>FIGURA 13</b>	MEDIA DE RIESGO PERSONAL [P] .....	82
<b>FIGURA 14</b>	MEDIA DE RIESGO REDES DE COMUNICACIÓN [COM].....	82
<b>FIGURA 15</b>	MEDIA DE RIESGO SOPORTE DE INFORMACIÓN [MEDIA].....	83
<b>FIGURA 16</b>	MEDIA DE RIESGO EQUIPAMIENTO AUXILIAR [AUX] .....	83
<b>FIGURA 17</b>	MEDIA DE RIESGO INSTALACIONES [L] .....	83
<b>FIGURA 18</b>	PORTADA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN .....	130
<b>FIGURA 19</b>	ÍNDICE DEL PLAN DE SEGURIDAD .....	131
<b>FIGURA 20</b>	ANTECEDENTES, OBJETIVOS Y ALCANCE DEL PLAN DE SEGURIDAD.....	132
<b>FIGURA 21</b>	POLÍTICA DE USO DE EQUIPOS INFORMÁTICOS .....	133
<b>FIGURA 22</b>	ENCUESTA REALIZADA AL PERSONAL ADMINISTRATIVO Y DOCENTE DE LA UESDC.....	134

# PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCION EN SEGURIDAD INFORMÁTICA

## DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA UNIDADES EDUCATIVAS DEL CANTÓN ESMERALDAS: ENFOQUE EN LA PROTECCIÓN DE DATOS Y RIESGOS.

**Autor:** Campaña Bone Carlos Alberto  
**Director:** Msc. Farinango Endara Henry  
**Año:** 2024

### RESUMEN

Este estudio se centra en los problemas de seguridad de la información que enfrentan las unidades educativas de Esmeraldas, especialmente los ataques de phishing y otras amenazas cibernéticas que comprometen la integridad, confidencialidad y disponibilidad de los datos. El enfoque clave es desarrollar una estrategia de seguridad de la información que utilice un enfoque de gestión de riesgos para minimizar estos riesgos. Para ello, se analizaron metodologías como OCTAVE, ISO 27001, MEHARI y MAGERIT, eligiendo esta última por su adecuación al contexto local. El plan se estructuró en cinco fases: evaluación de la situación actual, preparación del sistema de gestión de seguridad de la información (SGSI), análisis de riesgos, desarrollo del plan de seguridad y resultados. Los principales hallazgos revelan amenazas críticas como la manipulación de registros, abuso de privilegios de acceso, suplantación de identidad y divulgación de información, lo que indica la necesidad de implementar controles como la autenticación multifactor y el cifrado de datos. Además, las vulnerabilidades en el software requieren parches y actualizaciones constantes. Las conclusiones destacan la importancia de la sensibilización y la capacitación en ciberseguridad para todos los miembros de la comunidad educativa. La implementación de un plan de seguridad integral mejorará significativamente la protección de los datos en todos los niveles. Las recomendaciones incluyen aplicar las metodologías propuestas para optimizar los procesos, establecer controles y políticas de seguridad robustas y realizar un seguimiento continuo para evaluar el avance en la mitigación de riesgos. Este trabajo proporciona una base sólida para futuras iniciativas de mejora continua en la seguridad de la información en las unidades educativas de Esmeraldas.

**Palabras clave:** Seguridad de la información, Gestión de riesgos, Unidades educativas.



**PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCION EN  
SEGURIDAD INFORMÁTICA**

**DEVELOPMENT OF AN INFORMATION SECURITY PLAN FOR  
EDUCATIONAL UNITS IN ESMERALDAS CANTON: FOCUS ON DATA  
PROTECTION AND RISKS.**

**Autor:** Campaña Bone Carlos Alberto

**Director:** Msc. Farinango Endara Henry

**Año:** 2024

**ABSTRACT**

This study focuses on information security issues facing educational units in Esmeraldas, particularly phishing attacks and other cyber threats compromising data integrity, confidentiality, and availability. The main objective is to develop an information security plan based on a risk management methodology to mitigate these threats. Methodologies like OCTAVE, ISO 27001, MEHARI, and MAGERIT were analyzed, with the latter chosen for its suitability to the local context. The plan was structured into five phases: assessment of the current situation, preparation of the information security management system (ISMS), risk analysis, development of the security plan, and evaluation of results. Key findings reveal critical threats such as record manipulation, abuse of access privileges, identity spoofing, and information disclosure, emphasizing the need for implementing controls like multifactor authentication and data encryption. Additionally, software vulnerabilities require constant patches and updates. Conclusions underscore the importance of awareness and training in cybersecurity for all members of the educational community. Implementing a comprehensive security plan will significantly enhance data protection at all levels. Recommendations include applying the proposed methodologies to optimize processes, establishing robust security controls and policies, and conducting ongoing monitoring to assess progress in risk mitigation. This work provides a solid foundation for future continuous improvement initiatives in information security in Esmeraldas' educational units.

**Palabras clave:** Information security, Risk management, Educational units.

# CAPITULO I

## 1. EL PROBLEMA

### 1.1. Introducción

En la era digital actual, las unidades educativas se enfrentan a un panorama de amenazas cada vez más complejo. La protección de la información confidencial y sensible de estudiantes, docentes y personal administrativo es una necesidad imperiosa. Las unidades educativas corren el riesgo de enfrentar riesgos importantes como robo de datos, malware y fugas de información debido a la ausencia de un plan de seguridad para la información, lo que puede tener efectos perjudiciales para su reputación y la comunidad educativa.

El principal objetivo de esta tesis es formular una estrategia integral para la protección de la información en las unidades educativas del cantón de Esmeraldas. La atención se centrará en determinar los métodos de gestión y análisis de riesgos más eficaces para estas organizaciones, seleccionar la metodología más adecuada y desarrollar una estrategia de protección de la información basada en la metodología seleccionada.

La protección de la información confidencial y sensible en las unidades educativas del cantón esmeraldas requiere de la investigación y desarrollo de un plan adecuado para protección de la información. La implementación de medidas y estrategias adecuadas puede disminuir el riesgo de pérdida, robo o divulgación no autorizada de información, lo que a su vez ayuda a proteger la privacidad de estudiantes, profesores y personal administrativo, además de salvaguardar la reputación a las instituciones educativas.

Es importante destacar que el tema de la seguridad de la información es cada vez más relevante en el ámbito educativo. El aumento en la utilización de las tecnologías de la información y la comunicación en el proceso de enseñanza-aprendizaje hace que la protección de datos sea un aspecto decisivo. Por lo tanto, la realización de esta tesis es de gran importancia para aportar conocimiento y herramientas valiosas para las unidades educativas del cantón Esmeraldas.

En este estudio, se analizarán diversas metodologías de análisis y gestión de riesgos, como OCTAVE, NIST 800-30, ISO 27001, MEHARI y MAGERIT, para identificar la que mejor se adapta a las necesidades de las unidades educativas de Esmeraldas. El plan de

protección de la información desarrollado se basará en la metodología seleccionada y se estructurará en las siguientes fases:

**Fase 1 Situación Actual (UESDC)**

**Fase 2 Sistema de Gestión Documental / Preparación SGSI**

**Fase 3 Análisis de Riesgo**

**Fase 4 Plan de Seguridad de la Información**

**Fase 5 Resultados**

Se espera que la implementación de este plan contribuya a fortalecer la seguridad de la información en las unidades educativas del cantón Esmeraldas, promoviendo la protección de la información confidencial y el bienestar de la comunidad educativa.

**1.2. Problema de investigación**

Las unidades educativas de la ciudad de Esmeraldas se enfrentan a desafíos significativos relacionados con la seguridad de la información y la infraestructura tecnológica. Estos desafíos incluyen ataques de phishing y otras amenazas cibernéticas que tienen el potencial de comprometer gravemente la integridad, confidencialidad y disponibilidad de los activos digitales de las instituciones. Este problema no solo pone en riesgo la salvaguardia de datos críticos sino también la estabilidad de los sistemas tecnológicos utilizados para las operaciones educativas de la unidad.

Se origina como producto de la sofisticación cada vez mayor de las amenazas cibernéticas y de la deficiencia en las medidas de seguridad de la información en las unidades educativas. Según Microsoft, los ataques cibernéticos a instituciones educativas representan cuatro quintas partes (el 82,6 %) de todo el malware detectado en los últimos 30 días. Pero, además, ocupa los puestos de cabeza de la lista, si no el primero, desde hace años.(Vanessa García, 2022)

El problema es causado por actores externos maliciosos que realizan ataques de phishing y otras amenazas cibernéticas. Estos atacantes pueden ser individuos, grupos organizados o incluso entidades estatales interesadas en acceder a información

confidencial. Estos ataques cibernéticos pueden ocurrir en cualquier momento, pero suelen aumentar durante momentos críticos, como el período de inscripción de estudiantes o la gestión de exámenes, las principales razones por las que las instituciones educativas son el foco de atención de muchos ciberdelincuentes son porque manejan un gran volumen de datos en su día a día.(Blog de Innovación Educativa, 2022)

En la Unidad Educativa Salesiana María Auxiliadora (UESMA) enfrenta desafíos significativos relacionados con la seguridad de su red WiFi, la cual es compartida por estudiantes, docentes y personal administrativo. Este entorno compartido ha resultado en descargas no autorizadas de documentos y programas, lo que plantea un riesgo significativo para la integridad de los datos y la confidencialidad de la información. Además, la UESMA ha experimentado directamente la vulnerabilidad de su red, siendo víctima de un ataque de denegación de servicios. Este ataque se materializó cuando intentaron subir una aplicación y descubrieron que el acceso a la misma estaba bloqueado. Al analizar el tráfico de la red, identificaron un flujo inusual hacia el servidor que alojaba la aplicación, indicando la intrusión de terceros en la red de la institución. A pesar de que tanto el personal docente como administrativo y los estudiantes poseen un conocimiento básico sobre seguridad de la información, falta una comprensión plena del impacto potencial que puede resultar de la pérdida o compromiso de datos sensibles. Estos desafíos evidencian la necesidad apremiante de desarrollar e implementar un plan de protección de la información integral en la UESMA, con un enfoque en la protección de datos y la mitigación de riesgos para salvaguardar la integridad y confidencialidad de la información institucional.

La Unidad Educativa San Daniel Comboni (UESDC), tienen prácticas de seguridad deficientes al dejar sus computadoras sin protección, permitiendo que las sesiones queden iniciadas, incluso con programas sensibles como el de registro de notas y contabilidad, lo que aumenta el riesgo de manipulación y falta de confiabilidad en los datos. Además, enfrentan ataques de phishing frecuentes debido a contraseñas débiles y una excesiva confianza que resulta en una actitud indiferente hacia las recomendaciones del departamento de TIC. La UESDC ha sido víctima previa de un secuestro de información, lo que destaca la vulnerabilidad de la institución. Aunque tomaron medidas al mantener respaldos regulares tanto físicos como en disco duro,

este incidente subraya la necesidad crítica de mejorar las medidas preventivas. A esto, y, la falta de conciencia y preparación por parte de los usuarios es evidente; no están conscientes de la importancia de proteger la información ni de la necesidad de evitar la descarga de archivos desconocidos, lo que aumenta la probabilidad de inconvenientes relacionados con la seguridad. Además, el constante y persistente ataque de phishing es una amenaza cotidiana que la unidad educativa enfrenta. Estos problemas reflejan la urgencia de implementar medidas de seguridad sólidas, reforzar la conciencia de los usuarios y establecer prácticas de seguridad más rigurosas para salvaguardar la integridad y confidencialidad de los datos en la **UESDC**.

Cabe destacar que las amenazas cibernéticas pueden surgir de diversas maneras, dado que en el contexto digital no existen restricciones geográficas. Estos ataques pueden ser ejecutados desde cualquier rincón del mundo, como se ha evidenciado en los desafíos de seguridad que enfrentan tanto la Unidad Educativa Salesiana María Auxiliadora como la Unidad Educativa San Daniel Comboni. Estas instituciones han experimentado intrusiones y ataques, demostrando que la ciberdelincuencia no conoce fronteras físicas y requiere medidas de seguridad robustas y vigilancia constante para protegerse contra tales amenazas globales.

### **1.3. Interrogantes de la investigación**

¿Cuáles son las metodologías de análisis y gestión de riesgos más adecuadas para identificar vulnerabilidades y amenazas en la infraestructura tecnológica de las unidades educativas de la ciudad de Esmeraldas?

¿Cuál de las metodologías identificadas se adapta mejor a las necesidades de protección de la información de las unidades educativas?

¿Cómo se puede desarrollar un plan de seguridad de la información basado en la metodología de análisis de riesgos seleccionada, y cuál será su estructura y contenido específico para abordar las amenazas y vulnerabilidades identificadas en la infraestructura tecnológica de la unidad educativa?

¿Qué resultados se obtienen al implementar el plan de seguridad de la información desarrollado para las unidades educativas?

#### **1.4. Objetivos de la investigación**

##### **1.4.1. Objetivo general**

Proponer un plan de seguridad de la información basada en una metodología de gestión de riesgos para las unidades educativas del cantón Esmeraldas, tendiente a minimizar las amenazas y vulnerabilidades en sus infraestructuras tecnológicas.

##### **1.4.2. Objetivos específicos**

Analizar metodologías de análisis y gestión de riesgos que permitan identificar vulnerabilidades y amenazas en las infraestructuras tecnológicas aplicadas al caso de estudio.

Aplicar la metodología que mejor se adapte a las necesidades de protección de la información de las unidades educativas del cantón Esmeraldas.

Desarrollar un Plan de Seguridad de la Información basado en la metodología de análisis y gestión de riesgos seleccionada para la toma de decisiones en el ámbito de la seguridad.

#### **1.5. Justificación**

La metodología de análisis y gestión de riesgos es un enfoque sistemático que busca identificar, evaluar y mitigar los riesgos asociados a la seguridad de la información. A través de este enfoque, se pueden identificar las posibles amenazas a la información de la Unidad Educativa y evaluar su impacto potencial. Con esta información, se pueden implementar medidas de seguridad adecuadas para reducir o eliminar los riesgos identificados.

Las unidades educativas de la ciudad de Esmeraldas pueden beneficiarse de la implementación de un plan de seguridad de la información que garantice la protección y confidencialidad de los datos y sistemas de la institución. Este plan se basaría en una metodología de análisis y gestión de riesgos que permita identificar y abordar las posibles vulnerabilidades y amenazas a la seguridad de la información.

Esta investigación radica en la importancia crítica de garantizar la seguridad informática de la institución educativa, donde la protección de datos sensibles y la disponibilidad de recursos tecnológicos son fundamentales para el proceso educativo, sin embargo, en la ciudad de Esmeraldas existe un trabajo final de carrera en la Unidad Educativa Salesiana “María Auxiliadora” (UESMA), en el cual se realizó una implementación de un Sistema Gestor de Seguridad de la Información. (Xavier Quiñónez, 2020)

Esta investigación contribuirá a fortalecer la seguridad informática en las unidades educativas del cantón Esmeraldas, generando conocimiento que puede ser aplicado en otros entornos educativos y organizaciones, y ayudando a proteger los activos digitales y la privacidad de la comunidad educativa. Además, se espera que los resultados de esta investigación fomenten una cultura de seguridad informática en la institución y en la comunidad educativa en general.

La inclusión de la ciberseguridad en el sistema educativo es fundamental para garantizar la seguridad de la información y la protección de los ciudadanos en la era digital. La Estrategia Nacional de Ciberseguridad del Ecuador 2022, en su Pilar 5 "Habilidades y Capacidades de Ciberseguridad", establece el objetivo 5.3 de asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades en materia de ciberseguridad. Esta medida es necesaria para preparar a los estudiantes y futuros profesionales en el manejo de las tecnologías de la información y la comunicación, y para que puedan identificar y prevenir posibles amenazas cibernéticas. Además, la inclusión de la ciberseguridad en el sistema educativo puede contribuir a la formación de una cultura de seguridad digital en la sociedad, lo que puede tener un impacto positivo en la prevención de delitos cibernéticos y en la protección de la privacidad de los ciudadanos.

La inserción de la ciberseguridad en el sistema educativo es una medida necesaria y estratégica para garantizar la seguridad de la información y la protección de los ciudadanos en la era digital.

### **1.6. Hipótesis de Trabajo**

La implementación de un plan de seguridad de la información basado en una metodología de gestión de riesgos en las unidades educativas del cantón Esmeraldas disminuirá significativamente las amenazas y vulnerabilidades en sus infraestructuras tecnológicas.

### 1.7. Hipótesis Alternativa

La implementación de un plan de seguridad de la información basado en una metodología de gestión de riesgos en las unidades educativas del cantón Esmeraldas no disminuirá significativamente las amenazas y vulnerabilidades en sus infraestructuras tecnológicas.

### 1.8. Variables Independiente

Plan de seguridad de la información basado en una metodología de gestión de riesgos en la seguridad de la información.

- Metodologías de gestión de Riesgos
- Seguridad de la información
- Implementación de medidas de seguridad

### 1.9. Variables Dependiente

Amenazas y vulnerabilidades en las infraestructuras tecnológicas

- Ciberseguridad
- Tipos de amenazas y vulnerabilidades
- Protección de datos

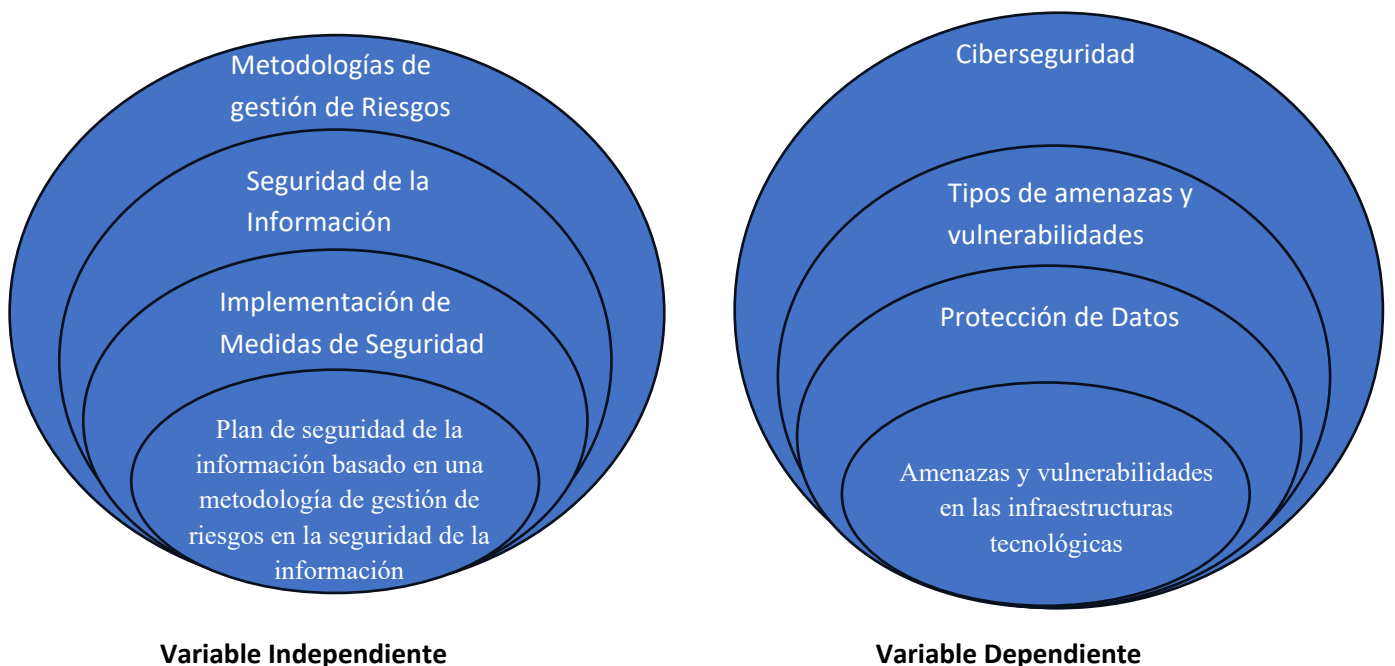


Figura 1 Variables Independiente y Dependiente

Fuente: Autor



## CAPÍTULO II

### 2. MARCO REFERENCIAL

#### 2.1. Antecedentes

Es importante considerar el creciente papel de la tecnología en el ámbito educativo. Con el avance de las herramientas digitales y la integración de la tecnología en el proceso de enseñanza-aprendizaje, las instituciones educativas de Esmeraldas han adoptado diversos sistemas y dispositivos tecnológicos para mejorar la calidad de la educación. Sin embargo, esta dependencia de la tecnología también ha traído consigo nuevos riesgos y desafíos en cuanto a la seguridad de la información.

Es fundamental ser consciente de las amenazas en constante evolución en el entorno actual. Las instituciones educativas se encuentran en la mira de los ciberataques debido a la gran cantidad de información sensible que manejan, como datos de estudiantes y financieros. Además, la infraestructura tecnológica de las escuelas y colegios puede ser vulnerable a diversas amenazas, como programas malignos, ataques de phishing, denegación de servicio (DDoS) y vulnerabilidades de seguridad en software y sistemas.

Es relevante resaltar la importancia de realizar investigaciones previas sobre las metodologías de análisis y gestión de riesgos en el ámbito educativo. Aunque existen varias metodologías disponibles, como MAGERIT, ISO 27001 y OCTAVE, es importante determinar cuáles son las más apropiadas y eficaces para las instituciones educativas de Esmeraldas, considerando sus particularidades y restricciones de recursos.

(Cali & Guadalupe, 2015), proporciona un valioso ejemplo de cómo se puede implementar un plan de seguridad con enfoque a la protección de la información, los autores describen un proceso detallado para el análisis de riesgo, que incluye la identificación de proceso y eventos críticos y la posterior elaboración de un Plan de seguridad de la información con controles adecuados para mitigar los riesgos identificados.

La importancia de adoptar un plan de seguridad con un enfoque a la protección de datos y a los riesgos de los activos de la información y que este basado en estándares que se adapten para la gestión de la seguridad de la información en las instituciones educativas ubicadas en la ciudad de Esmeraldas. Este plan establece un marco sólido para futuras investigaciones en el campo de la seguridad de la información, ofreciendo enseñanzas valiosas sobre cómo abordar los desafíos de seguridad en el entorno organizacional actual.

## **2.2. Marco Teórico**

El marco de investigación se basa en una sólida base teórica que incluye una variedad de fuentes y enfoques especializados en seguridad de la información, proporcionando una base sólida para el diseño y desarrollo de un plan de seguridad de la información adaptado a las peculiaridades y desafíos específicos de las unidades educativas del cantón Esmeraldas.

### **2.2.1. Sistemas de Gestión de Seguridad de la Información**

De acuerdo con (Gómez Fernández et al., 2018, pp 14-15), indica que un Sistema de Gestión de la Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización. Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada.

El objetivo principal de un SGSI es garantizar la confidencialidad, integridad y disponibilidad de la información, así como gestionar los riesgos relacionados con la seguridad de la información de manera efectiva.

(Amaro Pérez Paola, 2023), establece que la norma ISO 27000 tiene los requisitos para la implementación de un SGSI, donde la norma se centra en la gestión de riesgo, controles de seguridad y la mejora continua.

Al implementar un SGSI, las unidades educativas pueden protegerse contra amenazas internas y externas, cumplir con requisitos legales y regulatorios, mejorar la confianza de los padres de familia, proveedores, estudiantes y partes interesadas, y reducir el impacto de incidentes de seguridad de la información. Un SGSI es una parte fundamental de la estrategia de gestión de riesgos de una organización y un componente clave para garantizar la seguridad y protección de la información.

### **2.2.2. Normas/Estándares ISO27001**

De acuerdo con la (*ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*, n.d.), afirma que la ISO/IEC 27001, es la norma más conocida del mundo para sistemas

de gestión de seguridad de la información (SGSI). Además, que la norma proporciona a cualquier tipo de empresa, de todos los sectores para establecer, implantar, mantener y mejorar de manera continua al SGSI.

Para (Estéla et al., n.d.), indica que la norma sirve como una guía práctica para el desarrollo y la implementación de procedimientos y controles de seguridad de la información en una organización.

La serie ISO 27000 abarca una variedad de normas relacionadas con la seguridad de la información, pero la norma principal es la ISO/IEC 27001. Esta norma establece los requisitos para un SGSI y proporciona orientación sobre cómo las organizaciones pueden gestionar de manera efectiva la seguridad de la información, incluyendo la identificación de riesgos, la implementación de controles de seguridad, la capacitación del personal y la mejora continua del sistema.

La ISO/IEC 27001, incluye otras normas que complementan y amplían el alcance de la gestión de la seguridad de la información. A continuación, se presenta un cuadro que resume algunas de las normas de la serie ISO 27000, las cuales son fundamentales en el ámbito de la seguridad de la información. Estas normas proporcionan un marco de referencia y directrices para establecer, implementar y mejorar la seguridad de la información en las organizaciones. Cada norma aborda aspectos específicos de la gestión de la seguridad de la información, desde la definición de requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) hasta la protección de la información personal en la nube. El conocimiento y la aplicación de estas normas son esenciales para garantizar la confidencialidad, integridad y disponibilidad de la información en cualquier entorno organizacional.

**Tabla 1 Resumen de las normas ISO-27000**

<b>Norma ISO 27000</b>	<b>Descripción</b>
----------------------------	--------------------

---

ISO/IEC 27001	Establece las normas para la implementación de un SGSI y brinda un marco para la gestión eficaz de la seguridad de la información.
ISO/IEC 27002	Ofrece lineamientos y prácticas recomendadas para la implementación de controles de seguridad de la información, cubriendo áreas como políticas de seguridad, gestión de activos y otras.
ISO/IEC 27005	Se concentra en la administración de riesgos de seguridad de la información, brindando directrices para el reconocimiento, la evaluación y el tratamiento eficaz de estos riesgos.
ISO/IEC 27017	Presenta directrices específicas para la seguridad de la información en la utilización de servicios en la nube, incluyendo áreas como la gestión de incidentes, el cumplimiento legal y más.
ISO/IEC 27018	Establece directrices para la protección de la información personal en la nube, proporcionando controles y medidas de seguridad específicas para los proveedores de servicios.

---

Fuente: Autor

Es esencial resaltar que estas normas se complementan mutuamente, y si bien algunas pueden ser aplicadas individualmente, se sugiere su uso conjunto para asegurar una gestión integral y efectiva de la seguridad de la información en una organización.

### **2.2.3. Análisis de metodologías**

Para llevar a cabo esta investigación, se realizó una exhaustiva revisión bibliográfica utilizando repositorios de renombre como la Red de Repositorios de Accesos Abiertos del Ecuador (RRAAE), el Institute of Electrical and Electronics Engineers (IEEE) y Las Publicaciones Científicas de América Latina en Acceso Abierto (LREFERENCIA). Además, se consultaron los repositorios de la Universidad Técnica del Norte (UTN). La búsqueda se enfocó en palabras clave específicas, incluyendo Metodologías de Riesgos, Magerit, Octave, Mehari, Iso3100, Iso27001, Seguridad de la

Información (S.I) y Protección de Datos, con el objetivo de optimizar la eficacia de los resultados obtenidos. Es relevante mencionar que únicamente se consideraron las publicaciones a partir del año 2018, asegurando así la inclusión de información actualizada y pertinente para el caso de estudio.

Las metodologías de análisis y gestión de riesgos son fundamentales para identificar vulnerabilidades y amenazas en las infraestructuras tecnológicas y desarrollar los planos de seguridad de la información. Entre las metodologías más relevantes se encuentran Magerit, Octave y Mehari, entre otros. A continuación, se presenta una comparativa de estas metodologías de acuerdo con otros trabajos de investigación:

**Tabla 2 Resumen de revisión bibliográfica**

Nº	AÑO	TITULO	AUTORES	METODOLOGÍA /NORMA ISO
1	2022	PROPUESTA DE UN MODELO HÍBRIDO BASADO EN LAS METODOLOGÍAS MAGERIT E ISO 27001 PARA CONTROLAR AMENAZAS INTERNAS IDENTIFICADAS EN LA INTRANET DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA	TERESA JACQUELINE CHIRIBOGA MERA	MAGERIT E ISO 27001
2	2018	ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES	CRESPO MARTÍNEZ, ESTEBAN CORDERO TORRES, GEOVANNA	CRAMM Y MAGERIT
3	2018	SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS	ACOSTA ALVARADO, NEXAR JESÚS CARRILLO MORÁN, GUADALUPE FÁTIMA	MAGERIT, OCTAVE, NIST SP800-30, CRAMM, MEHARI

4	2021	<p>GESTIÓN DE RIESGOS  INFORMÁTICOS APLICANDO UNA  METODOLOGÍA DE  ANÁLISIS PARA VERIFICAR LA  SEGURIDAD DE LA INFORMACIÓN  EN UNA  EMPRESA DE AUDITORÍA,  CONSULTORÍA Y CAPACITACIÓN  IMPLEMENTACIÓN DE UNA  METODOLOGÍA PARA GESTIÓN DE  RIESGOS DE</p>	<p>CRISTHIAN ANDRÉS BUITRÓN  GONZAGA</p>	<p>MAGERIT E ISO  27001</p>
5	2019	<p>INFORMACIÓN BASADA EN LAS  NORMAS ISO/IEC 27001 Y 27002 EN EL  INSTITUTO TECNOLÓGICO SUPERIOR  SUCRE</p>	<p>FLAVIO EDUARDO LÓPEZ  VASCO</p>	<p>NIST 800-30 – ISO  27002-ISO27005</p>
6	2020	<p>ANÁLISIS DE METODOLOGÍAS DE LA  GESTIÓN DEL RIESGO  APLICABLES A LA NORMA ISO/IEC  27005:2018</p>	<p>DAVID CHACÓN PRIETO</p>	<p>CRAMM -  MAGERIT Y  OCTAVE</p>
7	2018	<p>REALIZANDO UNA REVISIÓN  SISTEMÁTICA DE METODOLOGÍAS  ISRA ORIENTADAS A LA SEGURIDAD  TIC. PERIODO 2014-2019</p>	<p>L. E. SÁNCHEZ, A. SANTOS-  OLMO, V. FIGUEROA,D.G.  ROSADO, E. FERNANDEZ-  MEDINA</p>	<p>CRAMM, CORAS,  OCTAVE,  MAGERIT,  Microsoft Security  Risk Management  Guide, MEHARI,  ISO27005  OCTAVE,  MAGERIT,</p>
8	2014	<p>METODOLOGÍAS PARA EL ANÁLISIS  DE RIESGOS EN LOS SGSI</p>	<p>HELENA ALEMÁN NOVOA,  CLAUDIA RODRÍGUEZ BARRERA</p>	<p>MEHARI, NIST SP  800:30, CORAS,  CRAMM Y EBIOS</p>
9	2014	<p>EL ANÁLISIS DE RIESGOS  INFORMÁTICOS Y SU INCIDENCIA EN  LA SEGURIDAD E INTEGRIDAD DE  LA INFORMACIÓN EN LA FACULTAD  DE INGENIERÍA CIVIL Y MECÁNICA  DE LA UNIVERSIDAD TÉCNICA DE  AMBATO.</p>	<p>DONALD EDUARDO REYES  BEDOYA</p>	<p>OCTAVE -  MAGERIT</p>

Chiriboga Mera, (2022), propone un modelo híbrido basado en las metodologías MAGERIT e ISO 27001 para controlar amenazas internas identificadas en la intranet de una empresa. El trabajo destaca las características de cada una de las metodologías por etapas de cada una de ellas y muestra las fortalezas y debilidades de cada una de ellas. Además, se destaca que ambas metodologías son muy conocidas para el análisis y tratamiento de riesgos, aunque difieren en que MAGERIT establece la identificación y valoración de activos, amenazas, salvaguardas, el impacto y riesgo por cada activo, y las ISO 27001 está destinada para tratar riesgos identificados a los activos.

Crespo Martínez & Cordero Torres, (2018), explora las similitudes y diferencias entre MAGERIT y CRAMM: dos metodologías para el análisis y gestión de riesgos. El estudio destaca que MAGERIT abarca una gama más amplia de elementos incluidos hardware, software, información electrónica, personas, instalaciones, medio de soporte y comunicación de datos, mientras que CRAMM solo considera a activos de información solo a los datos. Además, se concluye que ambas metodologías son bastante similares y permiten identificar los riesgos y amenazas.

Acosta Alvarado & Carrillo Morán, (2018), realizan una comparación de las metodologías más importantes para el análisis y gestión de riesgos, incluyendo MAGERIT, OCTAVE, NIST 800-30, CRAMM y MEHARI. El estudio compara las metodologías en términos de versiones, objetivos, país de creación y costo, y destaca que MAGERIT es una de las pocas metodologías que se pueden aplicar de manera gratuita.

Buitrón Gonzaga, (2021), realiza una comparación entre las metodologías MAGERIT y ISO 27001 utilizando el método DELPHI. Los resultados de la comparación se basan en criterios en común, y se destaca que MAGERIT tiene documentación, facilidad de aprendizaje, ejemplos de aplicación y automatización fácil, mientras que ISO 27001 se define por su facilidad de aplicación, facilidad de aprendizaje, fácil de entender y fácil de enseñar. Además, se indica que MAGERIT es la metodología más idónea debido a su documentación y ejemplos de aplicación.

López Vasco, (2019), realiza un análisis comparativo entre las normativas ISO 27001, ISO 27002 y NIST SP 800-30 para el análisis y gestión de riesgos. El estudio se enfoca en el control de riesgo de los controles que realiza la norma ISO y en cómo se evalúan los 114 controles que tiene, implementando el plan de tratamiento de riesgos para la Unidad de Titulación del ITSS.

Chacón Prieto, (2020), se efectuó una evaluación de metodologías de gestión de riesgos aplicables a la norma ISO/IEC 27005:2018, se compararon las metodologías CRAMM, MAGERIT y OCTAVE. Se concluyó que las metodologías amplían la cobertura de la seguridad de la información, al hacer visible las relaciones entre los diversos activos de la organización, permitiendo así incrementar su protección. Además, se hizo referencia a que la norma ISO es clara y específica al contar con una guía de implementación, y que es difícil llevar a cabo la gestión de riesgos sin hacer uso de una metodología. De acuerdo con el análisis, se determinó que la metodología que más se adapta al estándar ISO/IEC 27005:2018 es la metodología OCTA

Sánchez et al., (2019), analizan algunas de las principales metodologías de riesgos, como CRAMM, CORAS, OCTAVE, MAGERIT, Microsoft Security Risk Management Guide, MEHARI, ISO27005, entre otras. Se destaca que estas metodologías tienen en común la identificación de activos, amenazas, vulnerabilidades, impactos y medidas de seguridad, pero se diferencian en la forma en que se realizan estas actividades.

En un artículo de la Universidad Nacional Abierta y Distancia (Novoa & Barrera, 2014), presenta una descripción general de las metodologías más relevantes de análisis de riesgos, incluyendo Octave, Magerit, Mehari, NIST SP 800:30 y Coras. Se destaca que estas metodologías tienen en común la identificación de activos, amenazas, vulnerabilidades, impactos y medidas de seguridad, pero se diferencian en la forma en que se realizan estas actividades.

En una tesis de la Universidad Técnica de Ambato (Reyes Bedoya, 2014), se contrastan las metodologías OCTAVE Y MAGERIT para el análisis y gestión de riesgos informáticos. Se destaca que ambas metodologías tienen en común la identificación de activos, amenazas, vulnerabilidades, impactos y medidas de seguridad, pero difieren en la forma en que se realizan estas actividades.

Las tres metodologías más utilizadas para el análisis y gestión de riesgos son:

MAGERIT: La Metodología de Análisis de Riesgos de los Sistemas de Información es una metodología española que se basa en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar).



OCTAVE: La metodología OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) es una metodología estadounidense que se centra en la evaluación de riesgos de las infraestructuras críticas.

MEHARI: La metodología MEHARI (Método de Evaluación de Riesgos de Infraestructuras Tecnológicas) es una metodología francesa que se basa en el análisis de amenazas y vulnerabilidades.

Se presenta a continuación un cuadro comparativo del tratamiento de vulnerabilidades y amenazas con las metodologías más utilizadas para el análisis y gestión de riesgos, de acuerdo con la revisión bibliográfica realizada:

**Tabla 3 Comparación de Metodologías tratamiento de vulnerabilidades.**

METODOLOGÍA	IDENTIFICACIÓN DE VULNERABILIDADES	TRATAMIENTO DE VULNERABILIDADES
<b>MAGERIT</b>	Se realiza mediante una combinación de técnicas, como la revisión de código, la auditoría de seguridad y la evaluación de vulnerabilidades.	<ul style="list-style-type: none"> <li>- Identifica y evalúa vulnerabilidades en los sistemas de información.</li> <li>- Proporciona orientación sobre cómo gestionar y tratar las vulnerabilidades identificadas.</li> <li>- Integra el tratamiento de vulnerabilidades en el contexto general de la gestión de riesgos.</li> </ul>
<b>OCTAVE</b>	Se basa en la identificación de las amenazas y los controles existentes para evaluar las vulnerabilidades.	<ul style="list-style-type: none"> <li>- Se centra en la evaluación y gestión de riesgos organizativos relacionados con la tecnología de la información.</li> <li>- Identifica vulnerabilidades y amenazas específicas para la organización y su contexto.</li> <li>- Proporciona orientación detallada sobre cómo mitigar vulnerabilidades específicas.</li> </ul>

---

**MEHARI**

Se basa en el análisis de las amenazas y las debilidades para identificar las vulnerabilidades.

- Se enfoca en la evaluación de riesgos de seguridad de la información y proporciona un enfoque estructurado para la gestión de riesgos.

- Proporciona indicadores clave de rendimiento (KPIs) para evaluar y gestionar el tratamiento de vulnerabilidades.

- Ofrece orientación sobre cómo priorizar y abordar las vulnerabilidades según su impacto y probabilidad.

---

Fuente: Autor

De esta revisión del tratamiento de las vulnerabilidades podemos determinar que cada metodología tiene muchas fortalezas especiales en su enfoque:

MAGERIT presenta un enfoque técnico que incluye una auditoría de seguridad que evalúa exhaustivamente las vulnerabilidades.

OCTAVE, por otro lado, se centra en la evaluación de riesgos organizacionales, destacando la importancia de mitigar amenazas específicas a la organización y brindando orientación detallada sobre cómo lograrlo.

Finalmente, MEHARI no solo evalúa el riesgo, sino que también proporciona indicadores clave de desempeño para una gestión eficaz de la atención a la fragilidad, priorizando acciones según su impacto y probabilidad.

Este análisis proporciona una valiosa guía para seleccionar la metodología más adecuada en función de la seguridad de la información permitiendo una gestión integral de riesgos y la implementación de medidas específicas para abordar las vulnerabilidades identificadas.

**Tabla 4 Comparación de Metodologías tratamiento de amenazas.**

METODOLOGÍA	IDENTIFICACIÓN DE AMENAZAS	TRATAMIENTO DE AMENAZAS
<b>MAGERIT</b>	Se realiza mediante una combinación de técnicas, como la revisión de documentos, la entrevista a expertos y el análisis de tendencias.	<ul style="list-style-type: none"> <li>- Identificación y análisis exhaustivo de amenazas específicas que podrían afectar los sistemas de información.</li> <li>- Desarrollo de estrategias para prevenir, detectar y responder a estas amenazas.</li> <li>- Evaluación de la efectividad de las contramedidas y ajuste continuo en función de las amenazas emergentes.</li> </ul>
<b>OCTAVE</b>	Se basa en la identificación de los activos y los controles existentes para evaluar las amenazas.	<ul style="list-style-type: none"> <li>- Evaluación profunda de amenazas adaptadas al contexto operativo y de negocio de la organización.</li> <li>- Análisis detallado de las implicaciones de las amenazas para la integridad, confidencialidad y disponibilidad de los activos.</li> <li>- Desarrollo de planes de respuesta específicos para abordar cada categoría de amenazas identificadas.</li> </ul>
<b>MEHARI</b>	Se basa en el análisis de las vulnerabilidades y los controles existentes para identificar las amenazas.	<ul style="list-style-type: none"> <li>- Identificación y clasificación de amenazas basada en la probabilidad de ocurrencia y el impacto potencial.</li> <li>- Desarrollo de contramedidas específicas para cada clase de amenaza identificada.</li> <li>- Integración de la gestión de amenazas en un ciclo de mejora continua para adaptarse a las amenazas en constante evolución.</li> </ul>

Las tres metodologías abordan el tratamiento de las vulnerabilidades y amenazas de forma similar. Sin embargo, existen algunas diferencias en cuanto a las técnicas utilizadas y la forma de evaluar la gravedad de estas.

MAGERIT es la metodología más completa, ya que proporciona una serie de técnicas para la identificación y evaluación de vulnerabilidad y amenazas. OCTAVE es una metodología más sencilla, pero también eficaz. MEHARI es una metodología que se centra en el análisis de las vulnerabilidades y los controles existentes para identificar las vulnerabilidades y amenazas.

En base a la comparativa de estas metodologías, se puede concluir que MAGERIT es una de las metodologías más completas y utilizadas en el ámbito de la seguridad de la información, porque permite identificar y evaluar los riesgos de seguridad de la información, como establecer medidas de seguridad para mitigar los riesgos identificados. Además, MAGERIT es una metodología que se adapta a diferentes contextos y sectores, lo que hace ideal para el desarrollo de un plan de seguridad de la información para unidades educativas del cantón Esmeraldas, con enfoque en la protección de datos y riesgos.

#### **2.2.4. Seguridad De La Información**

Es el proceso de proteger la información de accesos, usos, divulgaciones, alteraciones o destrucciones no autorizadas. Es un aspecto fundamental para cualquier organización, ya que la información es un activo valioso que puede utilizarse para fines maliciosos.

Para (Gimenez Albacete, 2023), busca que los sistemas y equipos de información sean fiables, de acuerdo con lo que indica la norma ISO 27001, la misma que apoya tres aspectos:

**La confidencialidad**, es la garantía de que la información solo sea accesible para las personas autorizadas y que se mantenga alejada de aquellos no autorizados.

**La integridad**, se refiere a la precisión, exactitud y completitud de la información, asegurando que no se haya modificado o alterado de manera no autorizada.

**La disponibilidad**, la información debe estar disponible cuando sea necesaria y accesible para aquellos que están autorizados a utilizarla.

Estos conceptos son fundamentales para la seguridad de la información, es habitual referirse a ellos como la “Triada de la seguridad” o “CIA” (empleando las iniciales de los términos en inglés confidentiality o confidencialidad, integrity o integridad, y availability o disponibilidad).



**Figura 2.** Triada de la seguridad

Fuente: Autor

A las tres propiedades principales de la seguridad de la información MAGERIT las denomina dimensiones, en donde se pueden añadir otras derivadas que acerquen la percepción de los usuarios en los sistemas de información

**Autenticidad;** Es el proceso de verificar la identidad de un usuario o sistema, generalmente a través de contraseñas, biometría o certificados.

**Trazabilidad:** Es la acción de la entidad, son responsabilidad exclusivamente la entidad

Conceptos claves que debemos tomar en cuenta en la seguridad de la información:

**Activo de información:** Cualquier dato o información que tenga valor para una organización.

**Amenaza:** Cualquier evento o acción que pueda causar daño a un activo de información.

**Vulnerabilidad:** Cualquier debilidad o deficiencia en un sistema que puede ser explotada por una amenaza.

**Riesgo:** La posibilidad de que una amenaza se realice y cause daño a los activos de información.

**Control de seguridad:** Cualquier medida que se implemente para mitigar un riesgo.

### **2.2.5. Implementación De Medidas De Seguridad**

MAGERIT es una metodología completa que cubre todos los aspectos del análisis y gestión de riesgos. La metodología se divide en seis fases, que permiten identificar, evaluar y tratar los riesgos de forma sistemática.

Las fases de MAGERIT son las siguientes:

**Planificación:** En esta fase se definen los objetivos del proyecto, se recopila la información necesaria y se seleccionan las herramientas y técnicas que se utilizarán.

**Identificación de activos:** En esta fase se identifican los activos que se deben proteger.

**Identificación de amenazas y vulnerabilidades:** En esta fase se identifican las amenazas y vulnerabilidades que pueden afectar a los activos.

**Evaluación de riesgos:** En esta fase se evalúan los riesgos en función de la probabilidad de ocurrencia y el impacto que podrían tener.

**Planificación de tratamientos:** En esta fase se planifican las medidas de seguridad que se implementarán para tratar los riesgos.

**Seguimiento y control:** En esta fase se realiza un seguimiento de la eficacia de las medidas de seguridad implementadas.

MAGERIT es una metodología que ha sido ampliamente utilizada en el sector público y privado. La metodología es flexible y se puede adaptar a las necesidades específicas de cada organización.

### **2.2.6. Ciberseguridad**

Para (Kaspersky, 2020) Ciberseguridad es la práctica de proteger las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos se conoce como ciberseguridad.

También se conoce como seguridad de datos electrónicos o seguridad de tecnología de la información. El término se usa en una variedad de contextos, desde los negocios hasta la informática móvil, y se puede dividir en varias categorías comunes.

Además, la ciberseguridad también se conoce como seguridad de datos electrónicos o seguridad de tecnología de la información. Este término se utiliza en una variedad de contextos, desde los negocios hasta la informática móvil, y se puede dividir en varias categorías comunes. Algunas de estas categorías incluyen:

**Seguridad de la red:** se refiere a la protección de las redes de computadoras contra intrusiones y ataques maliciosos. Esto incluye la implementación de firewalls, la detección de intrusiones y la prevención de ataques de denegación de servicio (DoS).

**Seguridad de los dispositivos:** se refiere a la protección de los dispositivos móviles y otros dispositivos electrónicos contra ataques maliciosos. Esto incluye la implementación de medidas de seguridad como contraseñas, autenticación de dos factores y encriptación de datos.

**Seguridad de la información:** se refiere a la protección de la información confidencial y los datos personales contra el acceso no autorizado. Esto incluye la implementación de medidas de seguridad como encriptación de datos, gestión de contraseñas y autenticación de usuarios.

### 2.2.7. Tipos De Amenazas y Vulnerabilidades

**Tabla 5 Resumen de Amenazas y vulnerabilidades según MAGERIT**

Amenazas	Descripción	Vulnerabilidad
Natural	Desastres naturales, como terremotos, inundaciones, incendios, etc.	Daños físicos a los sistemas, pérdida de datos, interrupción de los servicios.
Humana	Acciones deliberadas de personas, con o sin intención de causar daño.	Falta de concienciación, errores humanos, fraude, sabotaje, etc.
Técnica	Debilidades en los sistemas, redes o aplicaciones.	Fallos de seguridad, errores de programación, etc.
Operacional	Fallos en los procesos, procedimientos o controles.	Errores humanos, incumplimiento de políticas, etc.

Fuente: Autor

Este cuadro presenta algunas amenazas comunes y las vulnerabilidades asociadas, según el marco MAGERIT (Dirección General de Modernización Administrativa, 2012).

La identificación precisa de amenazas y vulnerabilidades específicas puede variar según el contexto y la naturaleza de los sistemas de información involucrados. MAGERIT propone un enfoque detallado para identificar, analizar y gestionar estas amenazas y vulnerabilidades en el contexto de sistemas de información específicos.

### **2.2.8. Protección De Datos**

La protección de datos se refiere a las medidas y prácticas utilizadas para salvaguardar la información personal y sensible contra accesos no autorizados, pérdida o mal uso.

La protección de datos se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes (*Protección de Los Datos - Gestión de Datos de Investigación - Biblioguias at Biblioteca CEPAL, Naciones Unidas, n.d.*)

(Gil, n.d.), indica que es necesario realizar un análisis de riesgos que puedan derivarse del tratamiento de datos personales en la investigación, para poder adoptar las medidas de seguridad adecuadas que permitan garantizar que personal no autorizado no podrá acceder a dichos datos

En Ecuador existe (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021), que tiene como objetivo principal proteger la privacidad y los datos personales de los ciudadanos ecuatorianos. Esta ley establece los principios y normas que deben seguir las entidades públicas y privadas al recopilar, almacenar, procesar y transferir datos personales.

Algunos aspectos importantes de esta ley son:

**Definición de datos personales:** La ley define qué se considera como datos personales y establece que cualquier información relacionada con una persona identificada o identificable está protegida.



**Consentimiento informado:** La ley establece que el tratamiento de datos personales solo puede llevarse a cabo con el consentimiento informado del titular de los datos. Esto implica que, antes de recolectar y emplear los datos personales de individuos, las entidades deben obtener el consentimiento expreso de dichos mismos.

**Derechos de los titulares de datos:** La ley garantiza una serie de derechos a los titulares de datos, como el derecho de acceso, rectificación, cancelación y oposición. Esto permite a las personas tener control sobre sus datos personales y solicitar su modificación o eliminación si es necesario.

**Seguridad de los datos:** La ley establece que las entidades deben implementar medidas de seguridad adecuadas para proteger los datos personales de accesos no autorizados, pérdidas o alteraciones. Esto incluye la adopción de políticas y procedimientos internos, así como el uso de tecnologías de seguridad.

**Sanciones por incumplimiento:** La ley establece sanciones para las entidades que no cumplan con las disposiciones de protección de datos. Estas sanciones pueden incluir multas y otras medidas correctivas.

Para asegurar la privacidad y la protección de los datos de los ecuatorianos, es esencial la Ley Orgánica de Protección de Datos del Ecuador. Al establecer normas claras y garantizar los derechos de los titulares de datos, esta ley busca fomentar la confianza en el uso de la tecnología y promover un entorno seguro para el intercambio de información personal.

### **2.3. Marco Legal**

Para el caso de esta investigación sobre la seguridad de la información en las unidades educativas nos basamos en la Constitución de la República del Ecuador (CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, 2008) que establece el derecho a la protección de datos personales y la privacidad de las personas. Además, existen leyes y reglamentos específicos que regulan la seguridad de la información, como:

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece que los proveedores de servicios de comercio electrónico deben adoptar medidas de seguridad para proteger la información de sus usuarios. (LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS, 2002)

Reglamento para la Seguridad y Defensa del Ciberespacio: Este reglamento establece las medidas de seguridad cibernética y define las responsabilidades de las instituciones en la prevención y gestión de amenazas cibernéticas. La institución educativa debe cumplir con estas disposiciones para proteger su infraestructura y datos. (LEY ORGÁNICA DE SEGURIDAD DIGITAL, CIBERSEGURIDAD, CIBERDEFENSA Y CIBERINTELIGENCIA, 2021)

Ley Orgánica de Protección de Datos Personales: Esta ley establece los principios, derechos y obligaciones relacionados con la protección de datos personales en Ecuador. La institución debe cumplir con las disposiciones de esta ley para garantizar la adecuada recolección, almacenamiento y procesamiento de datos personales. (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021)

Ley Orgánica de Telecomunicaciones: Esta ley establece las disposiciones generales en materia de telecomunicaciones y tecnologías de la información en Ecuador. La institución educativa debe cumplir con las regulaciones específicas para proteger la seguridad de la información transmitida y almacenada electrónicamente. (LEY ORGANICA DE TELECOMUNICACIONES, 2015)

Ley Orgánica de Educación Intercultural Bilingüe: Esta ley establece que las instituciones educativas tienen la obligación de proteger la información de sus estudiantes, docentes y personal administrativo. (LEY ORGÁNICA DE EDUCACIÓN INTERCULTURAL, 2017)

El Acuerdo Ministerial 006-2021, establece la Política Nacional de Ciberseguridad. La política busca "afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, y a la creación de una confianza digital que favorezca el intercambio de información y de bienes y servicios en línea". (ACUERDO MINISTERIAL 006-2021, 2021)

## CAPÍTULO III

### 3. MARCO METODOLÓGICO

En este capítulo se presenta la estructura de la metodología seguida para llevar a cabo sistemáticamente los objetivos planteados.

La elección de una metodología particular se basa en la necesidad de comprender claramente los riesgos cibernéticos a los que está expuesta la institución y de desarrollar un plan adaptado a las necesidades específicas de la institución.

#### 3.1. Descripción del área de estudio

El proyecto de investigación se realizó en dos unidades educativas, ubicadas en la Ciudad de Esmeraldas, Provincia de Esmeraldas. Las instituciones educativas se especializan en la formación académica de estudiantes y promueve la excelencia educativa mediante enfoques pedagógicos innovadores y programas de desarrollo integral para los alumnos.

La Dirección Distrital de 08D01 Esmeraldas Educación reporta un total de 148 unidades educativas en el cantón Esmeraldas, divididas en Unidades Fiscales, Fiscomisionales y Particulares, para este estudio se ha seleccionado a dos unidades educativas específicas en base a la información previamente analizada: la Unidad Educativa Salesiana María Auxiliadora (UESMA) y la Unidad Educativa San Daniel Comboni (UESDC). Estas unidades educativas han sido elegidas por su relevancia en la comunidad educativa local y por la naturaleza de los desafíos de seguridad de la información que enfrentan, los cuales se han detallan aquí:

**Tabla 6 Unidades Educativas Seleccionadas**

Aspectos de Comparación	UESMA	UESDC
Tamaño y Comunidad Educativa	2415 estudiantes, 146 personal administrativo y docente	4000 estudiantes (matutina y vespertina), 129 personal administrativo y docente
Infraestructura Tecnológica	Aproximadamente 500 dispositivos	Alrededor de 300 dispositivos
Datos Sensibles Manejados	Datos de estudiantes, información alergias y discapacidades, datos de	Datos de estudiantes, registros académicos, datos del personal docente y administrativo,

	representantes legales, información contable	información financiera y contable
Tecnologías de la Información	Sistema de gestión escolar, plataforma educativa en línea, correo electrónico, sistema contable, facturación electrónica	Sistema contable, sistema de gestión académica, correo electrónico, plataforma educativa en línea, servicios de internet
Política de Seguridad de la Información	No cuenta con una política formal, pero sigue mejores prácticas recomendadas	Ausencia de una política formal de seguridad, departamento de TIC's sigue mejores prácticas
Control de Acceso	Roles asignados con pruebas correspondientes	Roles asignados con pruebas correspondientes
Preocupaciones Principales	Conciencia y responsabilidad de usuarios, seguridad de credenciales, cierre de sesiones, evitar compartir estaciones de trabajo	Conciencia de usuarios sobre seguridad informática, cierre de sesiones, evitar compartir estaciones de trabajo

---

Fuente: Autor

La Unidad Educativa Salesiana María Auxiliadora (UESMA), se caracteriza por su considerable tamaño y diversidad de usuarios. La institución alberga a un total de 2415 estudiantes, junto con un equipo administrativo y docente compuesto por 146 personas. En términos de infraestructura tecnológica, la UESMA cuenta con aproximadamente 500 dispositivos, lo que refleja su significativa presencia digital. Respecto a los datos manejados, la UESMA gestiona información personal y sensible, incluyendo detalles como nombres, números de identificación, correos electrónicos, alergias, niveles de discapacidad y datos de los representantes legales de los estudiantes. Además, la institución maneja información contable vital para su funcionamiento diario.

En cuanto a tecnología, la UESMA utiliza diversas herramientas para facilitar su operación educativa. Entre ellas se incluyen un sistema de gestión escolar, una plataforma educativa, correo electrónico y un sistema especializado para contabilidad y facturación electrónica. Aunque actualmente carecen de una política formal de seguridad de la información, el departamento de TIC se esfuerza por implementar prácticas recomendadas y ha proporcionado capacitación básica sobre seguridad a los usuarios.

Además, se han establecido roles específicos en los sistemas de información de la institución para administrar y controlar el acceso, subrayando la importancia de una gestión segura de los datos. La preocupación principal de los directivos de la UESMA radica en la utilización adecuada de los recursos informáticos disponibles, fomentando la conciencia y responsabilidad entre los usuarios respecto a las credenciales de acceso, con el objetivo de garantizar un entorno digital seguro y eficiente para todas las actividades educativas y administrativas.

La Unidad Educativa San Daniel Comboni (UESDC), se distingue por su extensa comunidad educativa y el manejo de datos críticos. La institución alberga aproximadamente 4000 estudiantes en las jornadas vespertina y matutina, junto con 129 miembros del personal administrativo y docente. Además, la infraestructura tecnológica de la UESDC se compone de alrededor de 300 dispositivos, lo que refleja su robusta presencia en el ámbito digital.

En términos de datos manejados, la institución gestiona información personal y educativa esencial. Esto incluye datos de estudiantes, registros académicos detallados, así como información del cuerpo docente y administrativo, junto con datos financieros y contables cruciales para la administración eficaz de la institución. En cuanto a tecnologías de la información, la UESDC emplea una variedad de sistemas, como un sistema contable, gestión académica, servicios de internet, correos electrónicos y una plataforma educativa en línea para facilitar las operaciones educativas y administrativas.

A pesar de su compleja infraestructura y manejo de datos sensibles, la UESDC carece de una política formal de seguridad de la información. Aunque el departamento de Tic sigue las mejores prácticas para la gestión de datos, la ausencia de una política específica es una preocupación destacada. Para mitigar riesgos, se han establecido roles asignados con pruebas correspondientes para controlar el acceso a los sistemas de información. La principal inquietud de los directivos se centra en la conciencia de los usuarios finales y su responsabilidad al utilizar credenciales de acceso. Se enfatiza la necesidad de cerrar sesiones y bloquear computadoras al abandonar los puestos de trabajo, y se advierte sobre compartir estaciones de trabajo con terceras personas. Estas preocupaciones subrayan la urgencia de desarrollar e implementar medidas de seguridad de la información para proteger los datos críticos y promover una cultura de seguridad informática entre los usuarios de la institución.

### **3.2. Enfoque y Tipo de Investigación**

La investigación se centró en el análisis de riesgos y la gestión de la seguridad de la información en las dos unidades educativas ubicadas en la Ciudad de Esmeraldas, Provincia de Esmeraldas, Ecuador. El enfoque de investigación adoptado fue principalmente cualitativo, ya que se enfocó en la comprensión en profundidad de los riesgos que se presenta en las unidades educativas y en la elaboración de un plan de seguridad de la información.

Este estudio utilizó una metodología de investigación de tipo exploratorio-descriptivo. En el contexto de la ciberseguridad, se adoptó un enfoque exploratorio para identificar las amenazas y vulnerabilidades existentes en la infraestructura tecnológica de las instituciones educativas. Luego, se utilizó un enfoque descriptivo para elaborar un plan de seguridad de la información basado en los resultados del análisis de riesgos, describiendo detalladamente las medidas de seguridad recomendadas.

Además, se basó en la revisión de la literatura académica especializada en seguridad de la información y en la selección de una metodología de análisis de riesgos que se adaptara a las necesidades específicas de las unidades educativas.

El objetivo final fue proporcionar a las unidades educativas un plan de seguridad de la información sólido y efectivo, basado en un análisis riguroso de riesgos, que permitiera proteger los activos de información crítica y garantizar la integridad, confidencialidad y disponibilidad de los datos. El estudio proporcionó recomendaciones específicas para la toma de decisiones en el ámbito de la seguridad de la información en el contexto educativo.

### **3.3. Recolección de información**

Con el objetivo de obtener datos relevantes para el desarrollo de un plan de seguridad de la información enfocado en protección de datos y riesgos para unidades educativas del Cantón Esmeraldas. Esta etapa fue fundamental para obtener una comprensión profunda de la situación actual de la seguridad de la información en las instituciones educativas de la zona y para identificar las necesidades y desafíos específicos que enfrentan.

Para la recolección de información, se emplearon varias técnicas de investigación, incluyendo encuestas, entrevistas y revisión de documentos. Se diseñó y distribuyó una encuesta entre directivos, docentes, personal administrativo de la Unidad

Educativa San Daniel Comboni. Esta encuesta se centró en aspectos como prácticas de seguridad, conciencia de riesgos, entrenamiento y concientización, colaboración institucional y conocimientos sobre políticas de seguridad.

Además, se llevaron a cabo entrevistas en profundidad con directivos y responsables de tecnología de la información de algunas instituciones educativas seleccionadas. Las entrevistas proporcionaron información detallada sobre las políticas, procedimientos y prácticas de seguridad de la información de estas instituciones, así como sobre los desafíos y obstáculos que surgieron en el proceso.

### **3.4. Procesamiento de la información**

Después de recopilar la información mediante encuestas, entrevistas y revisión de documentos, se procedió al procesamiento de estos datos para analizarlos y obtener conclusiones significativas, además se utilizaron tablas y referencias de la metodología de riesgo MAGERIT, así como un análisis en relación con la norma ISO 27000 para enriquecer el análisis y comprensión de los datos recopilados.

El procesamiento de la información involucró varias actividades, incluyendo la organización y codificación de los datos recopilados, la tabulación de respuestas de las encuestas y los datos de la entrevista con el personal que está a cargo de la unidad de TIC. Estas actividades se llevaron a cabo de manera sistemática y rigurosa para garantizar la fiabilidad y validez de los resultados.

Se realizaron tablas siguiendo la metodología de riesgo MAGERIT que permitieron organizar y estructurar los datos relacionados con la identificación y evaluación de los riesgos de seguridad de la información de la unidad educativa. Estas tablas proporcionaron una visualización clara de los riesgos identificados, sus causas y consecuencias potenciales, así como las medidas de control propuestas para mitigarlos.

### **3.5. Metodología de investigación**

Para la elaboración del PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA UNIDADES EDUCATIVAS DEL CANTÓN ESMERALDAS, se ha empleado el estándar ISO/IEC 27001 como guía principal. Este estándar establece requisitos fundamentales para establecer, implementar, mantener y mejorar nuestro plan de seguridad, proporcionando un marco sólido y reconocido internacionalmente.

Además, se ha optado por utilizar la metodología MAGERIT para realizar el Análisis de Riesgos de los Sistemas de Información. MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica del Gobierno de España con el objetivo de mitigar los riesgos asociados con el uso y la implementación de tecnologías de la información. La versión más reciente, la versión 3, fue lanzada en 2012 y ofrece un enfoque integral y actualizado para evaluar los riesgos de seguridad de la información.

Es importante destacar que la elaboración del plan se llevará a cabo tomando como referencia los datos obtenidos de la Unidad Educativa San Daniel Comboni. Esta institución se ha seleccionado debido a su relevancia como una de las unidades más extensas y su gran nivel de infraestructura integral, y también por su disposición para colaborar en este estudio. Los datos recopilados de esta unidad educativa proporcionarán una base sólida y representativa para el desarrollo del plan de seguridad de la información

Para la elaboración del plan, se ha determinado una serie de pasos para poder elaborar el mismo los cuales se van a enumerar de la siguiente manera:

### **3.5.1. Fase 1 – Situación Actual (UESDC)**

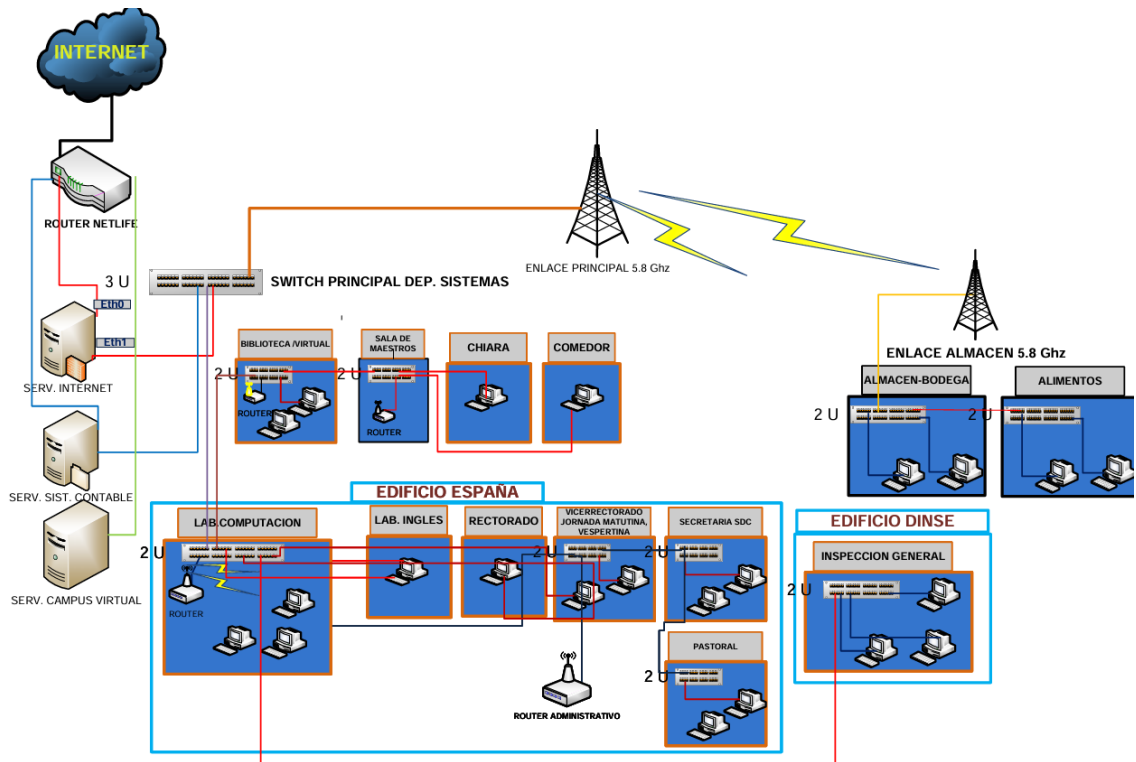
Para el desarrollo del Plan de Seguridad de la Información para las unidades educativas del Cantón Esmeraldas, se llevó a cabo un análisis detallado de la situación actual de la seguridad de la información de la Unidad Educativa San Daniel Comboni. Esta unidad educativa se seleccionó debido a su relevancia como una de las unidades mas grande y completas en la ciudad de Esmeraldas.

- **Infraestructura tecnológica**

La infraestructura tecnológica de la UESDC es altamente completa, abarcando una amplia gama de servicios que incluyen alojamiento web, correos electrónicos institucionales, sistemas contables, sistemas de matrícula y diversos sistemas de información utilizados por el personal docente y administrativo de la institución.

Además, se llevó a cabo un proceso de identificación y clasificación de activos, permitiendo una evaluación exhaustiva de las posibles vulnerabilidades y amenazas que podrían afectarlos.





**Figura 3** Estructura de Red UESDC  
**Autor:** Departamento TIC de la UESDC

La Figura 3, describe la estructura de la red proporcionada por el departamento de TIC de la unidad educativa San Daniel Comboni, con el objetivo de facilitar la conexión a internet, los servicios relacionados con el programa contable y el sistema de gestión de matrículas, así como también en dando la interconectividad con los laboratorios de computación y demás departamentos de la unidad.

- **Política y Procedimientos de Seguridad**

A pesar de su compleja infraestructura y del manejo de datos sensibles, la UESDC no cuenta con una política formal de seguridad de la información. Si bien el departamento de Tic sigue las mejores prácticas para la gestión de datos, la ausencia de una política específica es motivo de preocupación. Para mitigar riesgos, se han establecido roles asignados con pruebas correspondientes para controlar el acceso a los sistemas de información.

En este sentido, se enfatiza la necesidad de cerrar sesiones y bloquear computadoras al abandonar los puestos de trabajo, además de advertir sobre compartir estaciones de trabajo con terceras personas. Estas preocupaciones hacen hincapié en la importancia para desarrollar e implementar medidas de

seguridad para proteger los datos críticos y promover una cultura de seguridad informática entre los usuarios de la unidad.

### 3.5.2. Fase 2 – Sistema de Gestión Documental / Preparación SGSI

De acuerdo con la norma ISO 27001, no es necesario realizar un análisis de la situación inicial antes de implementar un SGI, o en este caso un Plan de Seguridad de la Información, sin embargo, se ha planteado realizar el instrumento para la identificación de la situación actual de la unidad educativa. La ISO 27001, plantea un total de 114 controles que deben ser aplicados en cualquier institución y/o empresa, y da la libertad que se consideren cuáles son los más aptos para la aplicación del plan.

A continuación, se da a conocer la tabla que muestra las métricas que se usó para determinar la identificación del nivel que se encuentra la unidad educativa:

**Tabla 7 Valoración de Controles**

VALORACION DE CONTROLES		
Descripción	Criterio	Calificación
<b>No Aplica</b>	No aplica implementar la salvaguarda	N/A
<b>Inexistente</b>	El control no está implementado, no hay políticas ni medidas para garantizar la seguridad de los equipos.	0
<b>Inicial</b>	1) Hay evidencia de que la Institución reconoce la existencia de un problema y la necesidad de actuar. No existen procedimientos estandarizados. 2) Existen procedimientos documentados, pero no son bien conocidos y/o no se aplican.	20
<b>Repetible</b>	Los procedimientos y controles siguen un patrón consistente. Los procesos han evolucionado hasta el punto de que varias personas se adhieren a diferentes métodos. No existe capacitación o comunicación estructurada sobre los procedimientos y estándares. Existe un nivel importante de confianza en el conocimiento de cada persona, lo que aumenta la probabilidad de cometer errores.	40
<b>Efectivo</b>	Se realiza la documentación y comunicación de procesos y controles. Los controles son muy eficientes y se implementan de manera consistente. Sin embargo, es poco probable que se detecten desviaciones cuando el control no se aplica con prontitud o cuando no se comunica claramente la forma en que se aplica	60
<b>Gestionado</b>	Los controles son monitoreados y medidos constantemente. Es factible rastrear y evaluar el cumplimiento de los procedimientos e implementar medidas correctivas cuando los procesos no funcionan de manera óptima.	80

## VALORACION DE CONTROLES

Descripción	Criterio	Calificación
<b>Optimizado</b>	Se respetan y automatizan las buenas prácticas. Los procesos han sido reevaluados en la medida de las mejores prácticas, teniendo en cuenta los resultados de los esfuerzos de mejora continua	100

Fuente: Autor

La tabla de los 14 requerimientos del Sistema Gestor de Seguridad de la Información provisto por la ISO 27002 se presenta de manera consecutiva para conocer los posibles estados que pueden ser asignados a los diferentes procesos que debería realizar la unidad educativa para poder garantizar la seguridad de los servicios de información.

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD DE LA INFORMACIÓN ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN - ISO 27002					
CONTROL DE SEGURIDAD DE LA INFORMACIÓN					
UNIDAD EDUCATIVA/INSTITUCION			UNIDAD EDUCATIVA FISCOMISIONAL "SAN DANIEL COMBONI"		
FECHA DE EVALUACION DE CONTROL			11 DE MARZO DE 2024		
RESPONSABLE DE LA INSTITUCION			ING. MIGUEL ARMILJO ZULETA		
ELABORADO POR			ING. CARLOS CAMPAÑA BONE		
Ítem	Sección	ITEM	Estado actual del Control	Aplica Si/No	COMENTARIO Justificación de la exclusión (No)
<b>1 Políticas de Seguridad de la Información</b>					
<b>1.1 Dirección de gestión de seguridad de la información</b>					
1	1.1.1	Políticas de Seguridad de la Información	Inexistente	NO	Actualmente, la unidad educativa carece de una política formal de seguridad de la información.
2	1.1.2	Revisión de las políticas para la seguridad de la información	Inexistente	NO	Actualmente, no se lleva a cabo una revisión regular de las políticas de seguridad de la información en la unidad educativa.
<b>2 Organización de la Seguridad de la Información</b>					
<b>2.1 Organización interna</b>					
3	2.1.1	Compromiso de la máxima autoridad de la institución con la seguridad de la información	Inicial	SI	Se ha registrado un compromiso inicial por parte de la máxima autoridad de la institución con respecto a la seguridad de la información
4	2.1.2	Separación de funciones	Inicial	SI	
5	2.1.3	Contacto con las autoridades	Inicial	SI	
6	2.1.4	Contacto con los grupos de interés especial	No Aplica	NO	NO APLICA
7	2.1.5	Seguridad de la Información en la gestión de proyectos	No Aplica	NO	NO APLICA
<b>2.2 Dispositivos móviles y teletrabajo</b>					
9	2.2.1	Política de dispositivos móviles	Inexistente	NO	En la actualidad, no existe una política formal de dispositivos móviles en la unidad educativa.
10	2.2.2	Teletrabajo	Inicial	SI	Videos instructivos de como realizar las video llamadas

**Figura 4** Instrumento de Control de seguridad de la información

Fuente: Autor

Basándonos en el enfoque metodológico de la norma ISO 27002, se realizaron los controles de seguridad de la información en la Unidad Educativa San Daniel Comboni. En el ANEXO A se detalla exhaustivamente la implementación de dichos controles. Este análisis pormenorizado proporciona una comprensión detallada de cómo se encuentra la unidad educativa y lo cual nos va a permitir

implementar controles para salvaguardar la integridad y confidencialidad de la información.

El resultado de la evaluación a los controles de la unidad educativa es el siguiente:

Evaluación de Efectividad de controles				
No.	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	15	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	14	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	2	100	INICIAL
A.9	CONTROL DE ACCESO	11	100	INICIAL
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	28	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	8	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	4	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	0	100	INEXISTENTE
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>8</b>	<b>100</b>	

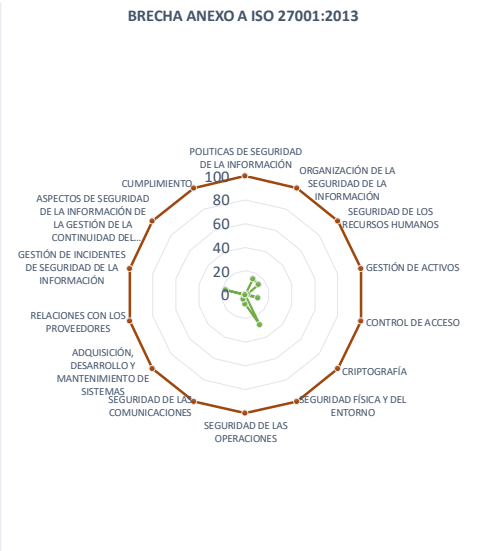


Figura 6 Evaluación de Control

La evaluación de la eficacia de los controles muestra una variedad de circunstancias en varios aspectos de la seguridad de la información de la unidad educativa. Mientras que algunos dominios, como la organización de la seguridad de la información y el control de acceso, muestran una calificación inicial, otros, como las políticas de seguridad de la información y la criptografía, carecen actualmente de controles establecidos. Es positivo observar que ciertos elementos, como la seguridad física y del entorno, continúan presentes, lo que indica que se han llevado a cabo acciones y procedimientos efectivos en esa área específica sin ningún procedimiento aprobado por la máxima autoridad.

Sin embargo, se debe prestar atención especial a los dominios donde la calificación actual es inexistente o inicial, ya que pueden presentar riesgos para la seguridad de la información. Se recomienda priorizar la implementación de controles y políticas en estos dominios para fortalecer la postura de seguridad general de la organización.

A continuación, podemos observar el nivel de cumplimiento por control:

COMPONENTE	DOMINIO	CONTROL DE CUMPLIMIENTO DE NORMA ISO 27002
A.5	POLITICAS DE SEGURIDAD.	NO CUMPLE
A.6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.	NO CUMPLE
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	NO CUMPLE
A.8	GESTIÓN DE ACTIVOS.	NO CUMPLE
A.9	CONTROL DE ACCESOS.	NO CUMPLE
A.10	CIFRADO.	NO CUMPLE
A.11	SEGURIDAD FÍSICA Y AMBIENTAL.	CUMPLE PARCIALMENTE
A.12	SEGURIDAD EN LA OPERATIVA.	NO CUMPLE
A.13	SEGURIDAD EN LAS TELECOMUNICACIONES.	NO CUMPLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	CUMPLE CON LA NORMA
A.15	RELACIONES CON PROVEEDORES.	NO CUMPLE
A.16	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	NO CUMPLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	NO CUMPLE
A.18	CUMPLIMIENTO.	NO CUMPLE

**Figura 7** Nivel de Cumplimiento

La evaluación del cumplimiento de la norma ISO 27002 muestra preocupaciones en varios dominios de la seguridad de la información. La mayoría de los componentes no cumplen con los requisitos establecidos por la norma, incluidas las políticas de seguridad, la gestión de activos, el control de acceso y la seguridad en las operaciones. Esto indica que los controles y las políticas de seguridad en estas áreas importantes no se están aplicando adecuadamente.

Es evidente que se requiere una mejora significativa en la mayoría de los dominios para alcanzar un nivel adecuado de seguridad de la información, aunque hay algunos aspectos, como la seguridad física y ambiental, y la adquisición, desarrollo y mantenimiento de sistemas de información, que cumplen parcial o totalmente con la norma.

### **3.5.3. Fase 3 - Análisis de Riesgo**

Permite identificar y valorar los activos, así como realizar un análisis de las amenazas y vulnerabilidades a las que están expuestos los activos de la Unidad Educativa. Esto le permite estar al tanto de lo que tiene la Unidad Educativa y estar preparado ante cualquier eventualidad ya que podemos establecer medidas

que garanticen la funcionalidad de los activos y establecer las salvaguardas más idóneas para tener nuestros activos muy protegidos.

### 3.5.3.1. Identificación de los Activos

De acuerdo con MAGERIT y la Dirección General de Modernización Administrativa (2012), los activos de la información pueden ser clasificados de la siguiente manera:

**Tabla 8 Tipo de Activo**

TIPO DE ACTIVO	DETALLE
Datos / Información [D]	Es toda la información que se procesa, almacena, comparte dentro y fuera de la unidad educativa
Claves Criptográficas [K]	Permite la protección de la información, a través de claves combinadas
Servicios [S]	Son todos los servicios que permiten el buen funcionamiento de la unidad educativa.
Aplicaciones de Software [SW]	Programas, aplicativos, desarrollos y más, que realizan tareas mejorando el desempeño de la unidad educativa
Equipos Informáticos [HW]	Todo dispositivo electrónico, que procese información para la unidad educativa y que pertenece a la misma.
Personal [P]	Personas que tienen relación de alguna manera con información de la unidad educativa.
Redes de Comunicación [COM]	Dispositivos que permitan la comunicación interna y externa entre los diferentes dispositivos de la unidad educativa
Soporte de Información [MEDIA]	Permite almacenar información y realizar el respaldo por periodos establecidos.
Equipamiento Auxiliar [AUX]	Sirven para soporte al departamento de las TIC

Instalaciones [L]

Lugar donde se encuentran toda la información y comunicación de la unidad educativa

Fuente: Autor

Una vez que tenemos identificados los tipos de activos, se procede a realizar el levantamiento de estos de acuerdo con el cuadro anterior, en la unidad educativa sus activos quedan de la siguiente manera:

**Tabla 9 Inventarios de Activos**

N°	Tipo	Activo	ID	UBICACIÓN	PROPIETARIO
1	Datos / Información [D]	Gestión de Matricula	D01	Unidad Educativa	Secretaría
2		Datos Financieros	D02	Unidad Educativa	Financiera
3		Datos Empleados	D03	Unidad Educativa	RR.HH
4	Servicios [S]	Google Workspace	S01	Virtual	Personal de TICS
5		Página Web	S02	Virtual	Personal de TICS
6	Aplicaciones de Software [SW]	SISTEMA CONTABLE - FENIX	SW01	Centro de Datos de la UE	Personal de TICS
7		SISTEMA NOVASOFT	SW02	Centro de Datos de la UE	Personal de TICS
8	Equipos Informáticos [HW]	Computador de Laboratorio	HW01	Edificio España	Personal de TICS
9		Servidor de Respaldo	HW02	Centro de Datos de la UE	Personal de TICS
10		Firewall	HW03	Centro de Datos de la UE	Personal de TICS
11		Computador de Colecturía	HW04	Edificio Ecuador	Colectora
12		Computador de Biblioteca	HW05	Edificio España	Bibliotecaria
13		Computador DECE	HW06	Edificio España	DECE
14		Computador Bodega	HW07	Edificio España	Bodeguera
15		Computador Alimentos	HW08	Edificio España	Alimentos
16		Computador Rectorado	HW09	Edificio España	Rector
17		Computador Vicerrectorado	HW10	Edificio España	Vicerrector
18		Computador Secretaria	HW11	Edificio España	Secretaria
19		Computador inspección General	HW12	Edificio Dinse	Inspector General
20		Computador Pastoral	HW13	Edificio Dinse	Pastoral
21		Computador Garita	HW14	Acceso Principal	Guardia
22	Personal [P]	Rector	P01	Edificio España	Rector
23		Personal de Sistemas	P02	Edificio España	Personal de TICS
24	Redes de Comunicación [COM]	Router de proveedor Internet	COM01	Centro de Datos de la UE	Personal de TICS



Nº	Tipo	Activo	ID	UBICACIÓN	PROPIETARIO	
25		Pbx Virtual	COM0 2	Centro de Datos de la UE	Personal de TICS	
26		Switch Lan	COM0 3	Centro de Datos de la UE	Personal de TICS	
27		Switch Garita	COM0 4	Acceso Principal	Personal de TICS	
28		Switch Colecturía	COM0 5	Edificio Ecuador	Personal de TICS	
29		Switch Laboratorio	COM0 6	Edificio España	Personal de TICS	
30		Switch Biblioteca Virtual	COM0 7	Edificio España	Personal de TICS	
31		Switch Sala de Maestros	COM0 8	Edificio España	Personal de TICS	
32		Switch DECE	COM0 9	Edificio España	Personal de TICS	
33		Switch Vicerrectorado	COM1 0	Edificio España	Personal de TICS	
34		Switch secretaria	COM1 1	Edificio España	Personal de TICS	
35		Switch inspección General	COM1 2	Edificio Dinse	Personal de TICS	
36		Switch Pastoral	COM1 3	Edificio Dinse	Personal de TICS	
37		Switch Bodega	COM1 4	Edificio España	Personal de TICS	
38		Switch Alimentos	COM1 5	Edificio España	Personal de TICS	
39		Router Administrativo	COM1 6	Edificio España	Personal de TICS	
40		Router Laboratorio	COM1 7	Edificio España	Personal de TICS	
41		Soporte de Información [MEDIA]	Disco de Respaldo	MEDI A01	Centro de Datos de la UE	Personal de TICS
42		Equipamiento Auxiliar [AUX]	Energía eléctrica	AUX01	Edificio España	Personal de TICS
43			CCTV	AUX02	Centro de Datos de la UE	Personal de TICS
44		Instalaciones [L]	CPD Tics	L01	Centro de Datos de la UE	Personal de TICS

Fuente: Autor

Para establecer los valores de las dimensiones, se debe conocer que significa y como se va a evaluar, en base a su disponibilidad, la integridad, la confidencialidad, su autenticidad y la trazabilidad a continuación, se presenta como se los ha clasificado para establecer el valor del impacto de cada activo de la unidad educativa:

**CONFIDENCIALIDAD (C):** La información no debe ser divulgada ni accedida a ella por personas o procesos no autorizados. ¿Cuál sería el daño que sufriría al conocerlo quien no debe?

**INTEGRIDAD (I):** El activo de información no debe haber sido alterado sin autorización. ¿Qué perjuicio causaría que estuviera dañado o corrupto?

**DISPONIBILIDAD (D):** El personal autorizado puede acceder a los recursos según sea necesario. ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

**AUTENTICIDAD (A):** Atributo o característica que indica que una persona de la unidad educativa es lo que dice ser o que garantiza el origen de los datos. ¿Qué daño tendría no tener conocimiento de quien es o ha hecho cada cosa?

**TRAZABILIDAD (D):** Propiedad o característica que consiste en acciones de un objeto que sólo pueden atribuirse a ese objeto. ¿Qué perjuicio tendría no conocer a quien se le brinda este servicio? O sea, ¿Quién esta realizando las tareas y en qué momento?

Estos atributos deben ser evaluados de acuerdo con los posibles daños que pueden ocasionar a los activos de la información, es decir, un análisis de su gravedad y consecuencias en caso de un incidente, de acuerdo con la metodología MAGERIT, establece los siguientes valores:

**Tabla 10 Valores de criticidad**

Escala	Valoración	Criterios
10	Extremo	Daño extremadamente grave.
8-9	Muy Alto	Daño muy grave
6-7	Alto	Daño grave.
4-5	Medio	Daño considerable
2-3	Bajo	Daño menor.
1	Despreciable	Daño irrelevante.

Nota: Tomado de (Dirección General de Modernización Administrativa, 2012)

Después de describir como se realiza las valoraciones, se determina la valoración de acuerdo con las dimensiones establecidas, la identificación de activos y quién es responsable de ellos.

**Tabla 11 Valoración de activos según su criticidad**

Nº	Tipo	Activo	ID	UBICACIÓN	PROPIETARIO	C	I	D	A	T	Impacto
1	Datos / Información [D]	Gestión de Matricula	D01	Unidad Educativa	Secretaría	7	8	7	8	6	Alto
2		Datos Financieros	D02	Unidad Educativa	Financiera	8	10	9	10	7	Muy Alto
3		Datos Empleados	D03	Unidad Educativa	Recursos Humanos	7	8	8	9	7	Muy Alto
4	Servicios [S]	Google Workspace	S01	Virtual	Personal de TICS	8	8	7	9	6	Muy Alto
5		Página Web	S02	Virtual	Personal de TICS	7	7	8	8	6	Alto
6	Aplicaciones de Software [SW]	SISTEMA CONTABLE - FENIX	SW01	Centro de Datos de la UE	Personal de TICS	9	10	9	9	8	Muy Alto
7		SISTEMA NOVASOFT	SW02	Centro de Datos de la UE	Personal de TICS	9	10	9	9	8	Muy Alto
8	Equipos Informáticos [HW]	Computador de Laboratorio	HW01	Edificio España	Personal de TICS	5	6	7	5	6	Alto
9		Servidor de Respaldo	HW02	Centro de Datos de la UE	Personal de TICS	10	9	10	9	9	Muy Alto
10		Firewall	HW03	Centro de Datos de la UE	Personal de TICS	8	8	8	9	7	Muy Alto
11		Computador de Colecturía	HW04	Edificio Ecuador	Colectora	8	7	8	8	6	Alto
12		Computador de Biblioteca	HW05	Edificio España	Biblioteca	5	6	3	4	7	Medio
13		Computador DECE	HW06	Edificio España	DECE	6	6	2	4	6	Medio
14		Computador Bodega	HW07	Edificio España	Bodega	5	4	2	3	4	Medio
15		Computador Alimentos	HW08	Edificio España	Alimentos	5	4	2	3	4	Medio
16		Computador Rectorado	HW09	Edificio España	Rector	9	9	9	9	7	Muy Alto
17		Computador Vicerrectorado	HW10	Edificio España	Vicerrector	8	8	9	8	7	Muy Alto
18		Computador secretaria	HW11	Edificio España	Secretaria	8	6	5	5	5	Alto
19		Computador Inspección General	HW12	Edificio Dinse	Inspector General	7	5	5	5	5	Medio
20		Computador Pastoral	HW13	Edificio Dinse	Pastoral	4	5	2	3	4	Medio
21		Computador Garita	HW14	Acceso Principal	Guardia	4	5	2	3	4	Medio
22	Personal [P]	Rector	P01	Edificio España	Rector						
23		Personal de Sistemas	P02	Edificio España	Personal de TICS						
24	Redes de Comunic	Router de proveedor Internet	COM01	Centro de Datos de la UE	Personal de TICS	9	9	9	9	8	Muy Alto

Nº	Tipo	Activo	ID	UBICACIÓN	PROPIETARIO	C	I	D	A	T	Impacto
25	ación [COM]	Pbx Virtual	COM02	Centro de Datos de la UE	Personal de TICS	5	3	8	9	7	Alto
26		Switch Lan	COM03	Centro de Datos de la UE	Personal de TICS	8	8	10	8	6	Muy Alto
27		Switch Garita	COM04	Acceso Principal	Personal de TICS	5	5	7	7	5	Alto
28		Switch Colecturía	COM05	Edificio Ecuador	Personal de TICS	7	7	8	8	6	Alto
29		Switch Laboratorio	COM06	Edificio España	Personal de TICS	7	7	7	8	6	Alto
30		Switch Biblioteca Virtual	COM07	Edificio España	Personal de TICS	6	6	8	7	6	Alto
31		Switch Sala de Maestros	COM08	Edificio España	Personal de TICS	6	6	6	7	6	Alto
32		Switch DECE	COM09	Edificio España	Personal de TICS	6	6	6	7	6	Alto
33		Switch Vicerrectorado	COM10	Edificio España	Personal de TICS	8	8	9	7	6	Muy Alto
34		Switch Secretaria	COM11	Edificio España	Personal de TICS	7	7	9	7	6	Alto
35		Switch Inspección General	COM12	Edificio Dinse	Personal de TICS	4	4	6	3	3	Medio
36		Switch Pastoral	COM13	Edificio Dinse	Personal de TICS	4	4	6	3	3	Medio
37		Switch Bodega	COM14	Edificio España	Personal de TICS	4	4	6	3	3	Medio
38		Switch Alimentos	COM15	Edificio España	Personal de TICS	4	4	6	3	3	Medio
39		Router Administrativo	COM16	Edificio España	Personal de TICS	6	5	7	4	7	Alto
40		Router Laboratorio	COM17	Edificio España	Personal de TICS	7	7	8	4	7	Alto
41		Soporte de Información [MEDIA]	Disco de Respaldo	MEDIA 01	Centro de Datos de la UE	Personal de TICS	6	8	7	7	7
42	Equipamiento Auxiliar [AUX]	Energía Eléctrica	AUX01	Edificio España	Personal de TICS			10			Extremo
43		CCTV	AUX02	Centro de Datos de la UE	Personal de TICS	6	4	6	7	7	Alto
44	Instalaciones [L]	CPD Tics	L01	Centro de Datos de la UE	Personal de TICS	10	9	10	8	7	Muy Alto

Fuente: Autor

Adicional al control que utiliza la metodología MAGERIT, se ha propuesto un instrumento donde se identifica al activo de la información con su proceso macro, subproceso, tipo de activo, categoría del activo, nombre del activo, descripción del activo, intención de uso, tipo de soporte, ubicación, responsable, dimensión del activo en

confidencialidad, integridad y disponibilidad, valor de impacto donde se promedia sus tres valores; Adicionalmente se le adquiere también la información sobre el manejo de los datos personales, según (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021), en el instrumento se registra de la siguiente manera: Contiene datos personales, ¿Contiene datos personales de niños, niñas o adolescentes?, Tipos de datos personales, Finalidad de la recolección de los datos personales, Cual es el tiempo de conservación de los datos?. Por ende, el instrumento valora los activos de la información de la unidad educativa de la siguiente manera:

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD DE LA INFORMACIÓN MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN												LOGO INSTITUCIÓN										
UNIDAD EDUCATIVA / INSTITUCIÓN												UNIDAD EDUCATIVA FISCOMISIONAL "SAN DANIEL COMBONI"										
FECHAS DE EVALUACIÓN CONTROL												31 DE MARZO DE 2024										
RESPONSABLE DE LA INSTITUCIÓN												ING. MIGUEL ARMUJOS ZUETA										
ELABORADO POR												ING. CARLOS CAMPANA BONE										
												VALORACION DE IMPACTO										
												C. Confidencialidad I. Integridad D. Disponibilidad										
												DATOS PERSONALES (LEY DE PORTECCION DE DATOS)										
Activo	Proceso Macro	Subproceso	Tipo de Activo	datos	datos2	Categoría de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación	Responsable	C	I	D	VA	Contiene Datos Personales	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Tipo de consentimiento	Cual es el tiempo de conservación de los datos?
A1	Gestión Sistema Contable	Operaciones del Sistema Contable	Aplicaciones de Software	Aplicaciones de Software	Aplicaciones	Desarrollo a medida (subcontratado)	SYSTEMA CONTABLE- FENIX	El Sistema Contable FENIX es una herramienta informática diseñada para gestionar y registrar todas las transacciones financieras y contables de una organización. Este activo consta de un conjunto de aplicaciones y módulos integrados que permiten realizar funciones como la contabilidad general, gestión de cuentas por pagar y por cobrar, elaboración de estados financieros, entre otras tareas relacionadas con la gestión contable.	El Sistema Contable FENIX es un activo fundamental para la gestión financiera y contable de la organización, proporcionando herramientas y funcionalidades que contribuyen a la eficiencia, precisión y transparencia en el manejo de la información contable.	Digital	Servidor de la UE	Ing. Miguel Armujos	3	3	2	3.00	No	No	No Aplica	No Aplica	No Aplica	5 años
A1.1	Gestión Sistema Contable	Mantenimiento y Actualización del Sistema Contable	Aplicaciones de Software	Aplicaciones de Software	Aplicaciones	Desarrollo a medida (subcontratado)	SYSTEMA CONTABLE- FENIX			Digital			2	2	3	2.00	No	No	No Aplica	No Aplica	No Aplica	
A2	Gestión Académica	Administración de Estudiantes	Aplicaciones de Software	Aplicaciones de Software	Aplicaciones	Desarrollo a medida (subcontratado)	SYSTEMA NOVASOFT	El Sistema Novasoft es una plataforma de gestión académica diseñada para administrar y supervisar todos los aspectos relacionados con la gestión educativa en la UE. Este activo consta de un conjunto de aplicaciones y módulos integrados que permiten gestionar funciones como la matriculación de estudiantes, control de asistencia, calificaciones, gestión de docentes, horarios de clases, entre otras tareas asociadas con la administración académica.	Es un activo fundamental para la gestión eficiente y efectiva de los procesos académicos en una institución educativa, proporcionando herramientas y funcionalidades que contribuyen a la mejora continua de la calidad educativa y el cumplimiento de los objetivos institucionales.	Digital	Servidor de Proveedor	Ing. Miguel Armujos	3	3	2	3.00	SI	SI	Datos de niños, niñas y adolescentes	Para obtener la información de los estudiantes en cada periodo escolar	Inequívoca	5 años
A2.1	Gestión Académica	Gestión de Docentes y Personal	Aplicaciones de Software	Aplicaciones de Software	Aplicaciones	Desarrollo a medida (subcontratado)	SYSTEMA NOVASOFT			Digital	Servidor de Proveedor	Ing. Miguel Armujos	3	3	2	3.00	SI	No	Datos Sensibles	Para obtener la información de la plana de docentes en cada periodo escolar	Inequívoca	5 años
A2.2	Gestión Académica	Gestión Académica y Curricular	Aplicaciones de Software	Aplicaciones de Software	Aplicaciones	Desarrollo a medida (subcontratado)	SYSTEMA NOVASOFT			Digital	Servidor de Proveedor	Ing. Miguel Armujos	3	3	3	3.00	SI	No	Datos Sensibles	Para obtener la información de los estudiantes en cada periodo escolar	Inequívoca	5 años
A2.3	Gestión Académica	Mantenimiento y Soporte del Sistema Novasoft	Aplicaciones de Software	Aplicaciones de Software	Aplicaciones	Desarrollo a medida (subcontratado)	SYSTEMA NOVASOFT			Digital	Servidor de Proveedor	Ing. Miguel Armujos	2	2	3	2.00	SI	No	Datos Sensibles	Para obtener la información de los estudiantes en cada periodo escolar	Inequívoca	5 años

**Figura 8** Identificación de activos sobre manejos de datos personales

Fuente: Autor

### 3.5.3.2. Identificación de Amenazas

Una vez que hemos identificado y evaluado los activos, el siguiente paso es identificar las amenazas que cada activo puede representar. En muchos casos, los activos pueden enfrentar las mismas amenazas, dependiendo de su naturaleza.

Según (Dirección General de Modernización Administrativa, 2012) en su catálogo de elementos, presenta las posibles amenazas sobre los activos de la información de una organización, clasificándolas en las siguientes maneras:

**Desastre Natural [N]:** Los acontecimientos pueden ocurrir sin intervención humana, ya sean causados directa o indirectamente.

**Amenazas de origen industrial [I]:** Los acontecimientos pueden ocurrir por casualidad como resultado de la actividad humana industrial. Estos peligros pueden ocurrir accidental o intencionalmente.

**Errores y fallos no intencionados [E]:** Fallos no intencionado provocados por las personas.

**Ataques intencionados [A]:** Fallos intencionados provocados por las personas.

Después de identificar los activos de la unidad educativa, procedimos a clasificar las amenazas según el tipo de activo, así como a determinar qué amenazas estaban asociadas de acuerdo con esta clasificación.

**Tabla 12 Amenazas Datos [D] – [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	[I] Integridad [C] confidencialidad [D] Disponibilidad
			[E.2] Errores del administrador	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[E.3] Errores de monitorización (log)	[I] Integridad (trazabilidad)
			[E.4] Errores de configuración	[I] Integridad
			[E.15] Alteración accidental de la información	[I] Integridad

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
			[E.18] Destrucción de información	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
		Ataques Intencionados [A]	[A.3] Manipulación de los registros de actividad (log)	[I] Integridad (trazabilidad)
			[A.4] Manipulación de la configuración	[I] Integridad [C] Confidencialidad [A] Disponibilidad
			[A.5] Suplantación de la identidad del usuario	[C] confidencialidad [A] autenticidad [I] Integridad
			[A.6] Abuso de privilegios de acceso	[C] confidencialidad [I] Integridad [D] Disponibilidad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.13] Repudio	[I] Integridad (trazabilidad)
			[A.15] Modificación deliberada de la información	[I] Integridad
			[A.18] Destrucción de información	[D] Disponibilidad
			[A.19] Divulgación de información	[C] Confidencialidad

Fuente: Autor

En esta tabla podemos observar las amenazas relacionadas con los datos/información [D], así como los aspectos que pueden verse afectados por los posibles efectos positivos de las amenazas.

**Tabla 13 Amenazas Servicios [S] – [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Servicios [S]	S01 S02	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	[I] Integridad [C] confidencialidad [D] Disponibilidad
			[E.2] Errores del administrador	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[E.9] Errores de [re-]encaminamiento	[C] Confidencialidad



Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
			[E.10] Errores de secuencia	[I] Integridad
			[E.15] Alteración accidental de la información	[I] Integridad
			[E.18] Destrucción de información	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
			[E.24] Caída del sistema por agotamiento de recursos	[D] Disponibilidad
		Ataques Intencionados [A]	[A.5] Suplantación de la identidad del usuario	[C] confidencialidad [A] autenticidad [I] Integridad
			[A.6] Abuso de privilegios de acceso	[C] confidencialidad [I] Integridad [D] Disponibilidad
			[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.9] [Re-]encaminamiento de mensajes	[C] Confidencialidad
			[A.10] Alteración de secuencia	[I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.13] Repudio	[I] Integridad (trazabilidad)
			[A.15] Modificación deliberada de la información	[I] Integridad
			[A.18] Destrucción de información	[D] Disponibilidad
			[A.19] Divulgación de información	[C] Confidencialidad
			[A.24] Denegación de servicio	[D] Disponibilidad

Fuente: Autor

En esta tabla podemos ver las amenazas relacionadas con el Servicio [S], y la dimensión de la afectación de cuando ocurra una amenaza.

**Tabla 14 Amenazas Aplicaciones de Software [SW] - [I], [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Aplicaciones de Software [SW]	SW01	De Origen Industrial [I]	[I.5] Avería de origen físico o lógico	[D] Disponibilidad
	SW02	Errores y Fallos no Intencio	[E.1] Errores de los usuarios	[I] Integridad [C] confidencialidad [D] Disponibilidad

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
			[E.2] Errores del administrador	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[E.8] Difusión de software dañino	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[E.9] Errores de [re-]encaminamiento	[C] Confidencialidad
			[E.10] Errores de secuencia	[I] Integridad
			[E.15] Alteración accidental de la información	[I] Integridad
			[E.18] Destrucción de información	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
			[E.20] Vulnerabilidades de los programas (software)	[I] Integridad [D] Disponibilidad [C] Confidencialidad
			[E.21] Errores de mantenimiento / actualización de programas (software)	[I] Integridad [D] Disponibilidad
		<b>Ataques Intencionados [A]</b>	[A.5] Suplantación de la identidad del usuario	[C] confidencialidad [A] autenticidad [I] Integridad
			[A.6] Abuso de privilegios de acceso	[C] confidencialidad [I] Integridad [D] Disponibilidad
			[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.8] Difusión de software dañino	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[A.9] [Re-]encaminamiento de mensajes	[C] Confidencialidad
			[A.10] Alteración de secuencia	[I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.15] Modificación deliberada de la información	[I] Integridad
			[A.18] Destrucción de información	[D] Disponibilidad
			[A.19] Divulgación de información	[C] Confidencialidad
			[A.22] Manipulación de programas	[C] confidencialidad [I] Integridad [D] Disponibilidad

A continuación, se detallan las posibles amenazas asociadas con las aplicaciones Software [SW] y el impacto en la dimensión a la que puede ocurrir la amenaza.

**Tabla 15 Amenazas Equipos Informáticos [HW] - [N], [I], [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Equipos Informáticos [HW]	HW01 HW02 HW03 HW04 HW05 HW06 HW07 HW08 HW09 HW10 HW11 HW12 HW13 HW14	Desastre Naturales [N]	[N.1] Fuego	[D] Disponibilidad
			[N.2] Daños por agua	[D] Disponibilidad
			[N.*] Fenómenos meteorológicos	[D] Disponibilidad
		De Origen Industrial [I]	[I.1] Fuego	[D] Disponibilidad
			[I.2] Daños por agua	[D] Disponibilidad
			[I.*] Polvo, Corrosión, congelamiento	[D] Disponibilidad
			[I.3] Contaminación mecánica	[D] Disponibilidad
			[I.4] Contaminación electromagnética	[D] Disponibilidad
			[I.5] Avería de origen físico o lógico	[D] Disponibilidad
			[I.6] Corte del suministro eléctrico	[D] Disponibilidad
			[I.7] Condiciones inadecuadas de temperatura o humedad	[D] Disponibilidad
		[I.11] Emanaciones electromagnéticas	[C] Confidencialidad	
		Errores y Fallos no Intencionados [E]	[E.2] Errores del administrador	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D] Disponibilidad
			[E.24] Caída del sistema por agotamiento de recursos	[D] Disponibilidad
			[E.25] Pérdida de equipos	[D] Disponibilidad [C] confidencialidad
		Ataques Intencionados [A]	[A.6] Abuso de privilegios de acceso	[C] confidencialidad [I] Integridad [D] Disponibilidad
			[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.23] Manipulación de los equipos	[C] Confidencialidad [D] Disponibilidad

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
			[A.24] Denegación de servicio	[D] Disponibilidad
			[A.25] Robo	[D] Disponibilidad [C] confidencialidad
			[A.26] Ataque destructivo	[D] Disponibilidad

Fuente: Autor

Podemos observar las amenazas que están conectadas con los equipos informáticos [HW], y el impacto de su dimensión si ocurriese una amenaza.

**Tabla 16 Amenazas Personal[P] - [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Personal [P]	P01 P02	Errores y Fallos no Intencionados [E]	[E.7] Deficiencias en la organización	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
			[E.28] Indisponibilidad del personal	[D] Disponibilidad
		Ataques Intencionados [A]	[A.28] Indisponibilidad del personal	[D] Disponibilidad
			[A.29] Extorsión	[C] confidencialidad [I] Integridad [D] Disponibilidad
			[A.30] Ingeniería social (picaresca)	[C] confidencialidad [I] Integridad [D] Disponibilidad

Fuente: Autor

Las amenazas relacionadas con el Personal [P], y la dimensión del impacto cuando ocurra una amenaza.

**Tabla 17 Amenazas Redes de Comunicación [COM] - [i], [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Redes de Comunicación [COM]	COM01 COM02	De Origen Industrial [I]	[I.8] Fallo de servicios de comunicaciones	[D] Disponibilidad
	COM03 COM04 COM05	Errores y Fallos no Intencionados	[E.2] Errores del administrador	[D] Disponibilidad [I] Integridad [C] confidencialidad

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
	COM06 COM07 COM08 COM09 COM10 COM11 COM12 COM13 COM14 COM15 COM16 COM17		[E.9] Errores de [re-]encaminamiento	[C] Confidencialidad
			[E.10] Errores de secuencia	[I] Integridad
			[E.15] Alteración accidental de la información	[I] Integridad
			[E.18] Destrucción de información	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
			[E.24] Caída del sistema por agotamiento de recursos	[D] Disponibilidad
		Ataques Intencionados [A]	[A.5] Suplantación de la identidad del usuario	[C] confidencialidad [A] autenticidad [I] Integridad
			[A.6] Abuso de privilegios de acceso	[C] confidencialidad [I] Integridad [D] Disponibilidad
			[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.9] [Re-]encaminamiento de mensajes	[C] Confidencialidad
			[A.10] Alteración de secuencia	[I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.12] Análisis de tráfico	[C] Confidencialidad
			[A.14] Interceptación de información (escucha)	[C] Confidencialidad
			[A.15] Modificación deliberada de la información	[I] Integridad
			[A.19] Divulgación de información	[C] Confidencialidad
			[A.24] Denegación de servicio	[D] Disponibilidad

Fuente: Autor

Las amenazas que están relacionadas con las Redes de Comunicación [COM], están en tabla que antecede, también podemos observar la incidencia en el impacto del nivel si ocurriese una amenaza.

**Tabla 18 Amenazas Soporte de Información [MEDIA] - [N], [I], [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
<b>Soporte de Información [MEDIA]</b>	<b>MEDI A01</b>	<b>Desastre Naturales [N]</b>	[N.1] Fuego	[D] Disponibilidad
			[N.2] Daños por agua	[D] Disponibilidad
			[N.*] Fenómenos meteorológicos	[D] Disponibilidad
		<b>De Origen Industrial [I]</b>	[I.1] Fuego	[D] Disponibilidad
			[I.2] Daños por agua	[D] Disponibilidad
			[I.*] Polvo, Corrosión, congelamiento	[D] Disponibilidad
			[I.3] Contaminación mecánica	[D] Disponibilidad
			[I.4] Contaminación electromagnética	[D] Disponibilidad
			[I.5] Avería de origen físico o lógico	[D] Disponibilidad
			[I.6] Corte del suministro eléctrico	[D] Disponibilidad
			[I.7] Condiciones inadecuadas de temperatura o humedad	[D] Disponibilidad
			[I.10] Degradación de los soportes de almacenamiento de la información	[D] Disponibilidad
			[I.11] Emanaciones electromagnéticas	[C] Confidencialidad
		<b>Errores y Fallos no Intencionados [E]</b>	[E.1] Errores de los usuarios	[I] Integridad [C] confidencialidad [D] Disponibilidad
			[E.2] Errores del administrador	[D] Disponibilidad [I] Integridad [C] confidencialidad
			[E.15] Alteración accidental de la información	[I] Integridad
			[E.18] Destrucción de información	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D] Disponibilidad
			[E.25] Pérdida de equipos	[D] Disponibilidad [C] confidencialidad
		<b>Ataques Intencionados [A]</b>	[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.15] Modificación deliberada de la información	[I] Integridad
			[A.18] Destrucción de información	[D] Disponibilidad
			[A.19] Divulgación de información	[C] Confidencialidad

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
			[A.23] Manipulación de los equipos	[C] Confidencialidad [D] Disponibilidad
			[A.25] Robo	[I] Integridad [D] Disponibilidad
			[A.26] Ataque destructivo	[D] Disponibilidad

Fuente: Autor

Para los activos de Soporte de Información [MEDIA], estas son las amenazas relacionadas, y podemos observar el impacto de la dimensión por la ocurrencia de una amenaza.

**Tabla 19 Equipamiento Auxiliar [AUX] - [N], [I], [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Equipamiento Auxiliar [AUX]	AUX01 AUX02	Desastre Naturales [N]	[N.1] Fuego	[D] Disponibilidad
			[N.2] Daños por agua	[D] Disponibilidad
			[N.*] Fenómenos meteorológicos	[D] Disponibilidad
		De Origen Industrial [I]	[I.1] Fuego	[D] Disponibilidad
			[I.2] Daños por agua	[D] Disponibilidad
			[I.*] Polvo, Corrosión, congelamiento	[D] Disponibilidad
			[I.3] Contaminación mecánica	[D] Disponibilidad
			[I.4] Contaminación electromagnética	[D] Disponibilidad
			[I.5] Avería de origen físico o lógico	[D] Disponibilidad
			[I.6] Corte del suministro eléctrico	[D] Disponibilidad
			[I.7] Condiciones inadecuadas de temperatura o humedad	[D] Disponibilidad
			[I.9] Interrupción de otros servicios y suministros esenciales	[D] Disponibilidad
			[I.11] Emanaciones electromagnéticas	[C] Confidencialidad
		Errores y Fallos no Intencionados [E]	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D] Disponibilidad
			[E.25] Pérdida de equipos	[D] Disponibilidad [C] confidencialidad
		Ataques Intencionados [A]	[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
			[A.23] Manipulación de los equipos	[C] Confidencialidad [D] Disponibilidad
			[A.25] Robo	[D] Disponibilidad [C] confidencialidad
			[A.26] Ataque destructivo	[D] Disponibilidad

Fuente: Autor

Las amenazas relacionadas con el equipamiento Auxiliar [AUX], y su impacto en la dimensión, que ocasionaría si una amenaza pueda ocurrir.

**Tabla 20 Amenazas Instalaciones [L] - [N], [I], [E], [A]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Dimensiones
Instalaciones [L]	L01	Desastre Naturales [N]	[N.1] Fuego	[D] Disponibilidad
			[N.2] Daños por agua	[D] Disponibilidad
			[N.*] Fenómenos meteorológicos	[D] Disponibilidad
		De Origen Industrial [I]	[I.1] Fuego	[D] Disponibilidad
			[I.2] Daños por agua	[D] Disponibilidad
			[I.*] Polvo, Corrosión, congelamiento	[D] Disponibilidad
			[I.11] Emanaciones electromagnéticas	[C] Confidencialidad
		Errores y Fallos no Intencionados [E]	[E.15] Alteración accidental de la información	[I] Integridad
			[E.18] Destrucción de información	[D] Disponibilidad
			[E.19] Fugas de información	[C] Confidencialidad
		Ataques Intencionados [A]	[A.7] Uso no previsto	[D] Disponibilidad [C] confidencialidad [I] Integridad
			[A.11] Acceso no autorizado	[C] confidencialidad [I] Integridad
			[A.15] Modificación deliberada de la información	[I] Integridad
			[A.18] Destrucción de información	[D] Disponibilidad
			[A.19] Divulgación de información	[C] Confidencialidad
			[A.26] Ataque destructivo	[D] Disponibilidad
			[A.27] Ocupación enemiga	[D] Disponibilidad [C] confidencialidad

Fuente: Autor



Y para culminar, observamos las amenazas que están relacionadas con las Instalaciones [L], además podemos observar el impacto de la dimensión si una amenaza ocurra.

### 3.5.3.3. Valoración de amenazas

Una vez que se han identificado las amenazas a los activos, debemos evaluar cuándo el activo es vulnerable. Es importante destacar que la magnitud de la afectación no siempre será uniforme ni será uniforme en todas las dimensiones.

Según MAGERIT, es necesario evaluar su impacto en el valor del activo en dos aspectos:

**La degradación** es la cantidad de daño que sufriría el activo.

**La probabilidad** de que se materialice la amenaza se conoce como probabilidad.

La degradación mide el daño que causa un incidente en el supuesto de que ocurriera.

La determinación y la expresión de la probabilidad de ocurrencia son más complejas. En ocasiones, se puede modelar cualitativamente utilizando una escala nominal:

**Tabla 21 Degradación del valor**

Abreviatura	Nivel	Daño	Materialización
MA	Muy Alta	Casi Seguro	Fácil
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente difícil

Nota: Tomado de (Dirección General de Modernización Administrativa, 2012)

Se determina de la siguiente manera la probabilidad o frecuencia de ocurrencia de una amenaza al activo:

**Tabla 22 Probabilidad de ocurrencia**

Abreviatura	Nivel	Probabilidad	Incidencia
MA	100	Muy Frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año

B	1/10	Poco Frecuente	Cada varios años
MB	1/100	Muy Poco Frecuente	Siglos

Nota: Tomado de (Dirección General de Modernización Administrativa, 2012)

Como ejemplo se muestra las amenazas correspondientes a los Datos/información [D], en la tabla adjunta podemos observar cómo se analizó la frecuencia con la que se puede materializar la amenaza, y el impacto que tiene en las dimensiones de la seguridad, en el ANEXO B de la investigación se encuentra la valoración de todos los activos de información.

**Tabla 23 Valoración de Amenazas Datos/Información [D]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Fre	I D	I I	I C	I A	I T	
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M	4	4	4	5	3	
			[E.2] Errores del administrador	A	5	4	5	5	3	
			[E.3] Errores de monitorización (log)	MB	3	3	3	4	3	
			[E.4] Errores de configuración	A	4	4	5	5	3	
			[E.15] Alteración accidental de la información	A	4	4	5	5	3	
			[E.18] Destrucción de información	MA	5	5	4	5	3	
			[E.19] Fugas de información	MA	5	4	5	4	3	
		<b>Valoración final materialización de amenazas</b>			→ SOON	5	5	5	5	3
Datos / Información [D]	D01 D02 D03	Ataques Intencionados [A]	[A.3] Manipulación de los registros de actividad (log)	A	4	3	2	3	4	
			[A.4] Manipulación de la configuración	MA	4	4	3	4	4	
			[A.5] Suplantación de la identidad del usuario	MA	3	4	4	4	3	
			[A.6] Abuso de privilegios de acceso	MA	4	4	4	4	4	
			[A.11] Acceso no autorizado	MA	5	5	5	5	5	
			[A.13] Repudio	A	4	4	3	4	4	
			[A.15] Modificación deliberada de la información	MA	5	5	5	5	4	
			[A.18] Destrucción de información	MA	4	5	5	5	4	
			[A.19] Divulgación de información	A	5	4	5	4	4	
		<b>Valoración final materialización de amenazas</b>			→ SOON	4	5	5	5	5

Fuente: Autor

Como podemos observar, es importante abordar los errores del administrador, los errores de configuración, la destrucción de información y las fugas de información de manera proactiva mediante la implementación de

controles adecuados, políticas de seguridad robustas y capacitación continua del personal. Los errores de los usuarios y los errores de monitorización también deben ser tenidos en cuenta y abordados mediante la educación y la concienciación sobre seguridad.

Los que tienen un mayor impacto en aspectos de seguridad de la información (ID, II, IC, IA y IT) son más vulnerables a las amenazas de acceso no autorizado, modificación deliberada y destrucción de información. Esto refleja la gravedad potencial de estas amenazas en la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de los datos.

La manipulación de la configuración también presenta un alto impacto, especialmente en la integridad y autenticidad de los datos, lo que indica la importancia de proteger la configuración de sistemas y aplicaciones para garantizar la seguridad de la información.

Amenazas como la manipulación de registros de actividad y el abuso de privilegios de acceso tienen un impacto significativo en la disponibilidad y la integridad de los datos, lo que resalta la necesidad de monitorear y controlar los accesos y actividades dentro del sistema.

La suplantación de la identidad del usuario y la divulgación de información también son amenazas importantes, con un impacto considerable en la confidencialidad y la autenticidad de los datos. Estas amenazas pueden comprometer la seguridad de la información y la identidad de los usuarios, lo que requiere medidas de protección adecuadas, como autenticación multifactor y cifrado de datos sensibles.

#### **3.5.3.4. Estimación del impacto**

El impacto potencial es el daño que un activo sufrirá si se ejecuta una amenaza específica. El cálculo se realiza utilizando la siguiente fórmula:

$$\text{Riesgo} = \text{Frecuencia} * \text{Impacto}$$

Donde frecuencia tiene la siguiente valoración:

---

**Frecuencia**

---

MA Muy frecuente, a diario (x2)

A Frecuente, una vez al mes (x2)

- M Normal, por lo menos al año
- B Poco frecuente, cada varios años
- MB Muy poco frecuente, siglos


Nota: Tomado de (Dirección General de Modernización Administrativa, 2012)

### 3.5.3.5. Riesgo Aceptable

El riesgo aceptable se refiere a la cantidad de incertidumbre sobre la seguridad de los activos que la institución educativa está dispuesta a tolerar. Esta determinación se realiza cuando no es práctico ni rentable reducir la probabilidad de que ocurra una amenaza. En su lugar, se centra en minimizar las consecuencias de tales amenazas a niveles que la unidad educativa considera aceptables, sin causar un daño grave en la información. Este concepto se construye en base a la combinación de la frecuencia con la que se presenta el riesgo y el impacto potencial que podría tener en la unidad educativa.

El siguiente cuadro se toma como ejemplo a los activos Datos/Información [D], el resto de los activos se encuentran en los anexos de la investigación.

**Tabla 24 Valoración de Riesgo de los Datos/Información [D]**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Fre	RD	RI	RC	RA	RT	
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M	4	4	4	5	3	
			[E.2] Errores del administrador	A	10	8	10	10	6	
			[E.3] Errores de monitorización (log)	MB	3	3	3	4	3	
			[E.4] Errores de configuración	A	8	8	10	10	6	
			[E.15] Alteración accidental de la información	A	8	8	10	10	6	
			[E.18] Destrucción de información	MA	10	10	8	10	6	
			[E.19] Fugas de información	MA	10	8	10	8	6	
		<b>Valoración final materialización de amenazas</b>			 <b>SOON</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>6</b>
Datos / Información [D]	D01 D02 D03	Ataques Intencionados [A]	[A.3] Manipulación de los registros de actividad (log)	A	8	6	4	6	8	
			[A.4] Manipulación de la configuración	MA	8	8	6	8	8	
			[A.5] Suplantación de la identidad del usuario	MA	6	8	8	8	6	
			[A.6] Abuso de privilegios de acceso	MA	8	8	8	8	8	
			[A.11] Acceso no autorizado	MA	10	10	10	10	10	

		[A.13] Repudio	A	8	8	6	8	8
		[A.15] Modificación deliberada de la información	MA	10	10	10	10	8
		[A.18] Destrucción de información	MA	8	10	10	10	8
		[A.19] Divulgación de información	A	10	8	10	8	8
<b>Valoración final materialización de amenazas</b>			<b>→ SOON</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>10</b>

Fuente: Autor

Las amenazas se dividen en dos categorías principales Errores y Fallos no Intencionados [E] y Ataques Intencionados [A]; para cada amenaza se detallan la frecuencia de la ocurrencia y el grado de daño que causaría en cada una de las dimensiones de seguridad.

La valoración final del riesgo determina que es crucial para la unidad educativa, para la cual debe determinar las medidas de seguridad adecuadas que deben implementarse para proteger los activos de Datos/Información [D].

### 3.5.3.6. Riesgo Residual

Este concepto se refiere al grado de riesgo que subsiste en la organización después de que se hayan implementado medidas para reducir, mitigar o eliminar los riesgos. Implica la necesidad de tomar precauciones anticipadas para asegurar que, en caso de que estos riesgos se materialicen, su impacto en la institución sea lo más pequeño posible. ANEXO C

**Tabla 25 Valoración de Impacto Amenazas Datos/Información [D] - Aplicando niveles de salvaguardas**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Fr e	I D	I I	I C	I A	I T
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M	1	2	2	2	2
			[E.2] Errores del administrador	A	1	2	2	2	2
			[E.3] Errores de monitorización (log)	MB	1	1	1	1	2
			[E.4] Errores de configuración	A	2	2	2	1	2
			[E.15] Alteración accidental de la información	A	1	2	2	1	2
			[E.18] Destrucción de información	MA	2	1	1	1	2
			[E.19] Fugas de información	MA	1	1	2	1	2
<b>Valoración final materialización de amenazas</b>			<b>→ SOON</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	


Datos / Información [D]	D01 D02 D03	Ataques Intencionados [A]	[A.3] Manipulación de los registros de actividad (log)	A	2	2	2	1	2
			[A.4] Manipulación de la configuración	MA	1	1	2	1	2
			[A.5] Suplantación de la identidad del usuario	MA	2	1	2	1	2
			[A.6] Abuso de privilegios de acceso	MA	1	1	2	1	2
			[A.11] Acceso no autorizado	MA	2	1	2	1	2
			[A.13] Repudio	A	2	1	2	1	2
			[A.15] Modificación deliberada de la información	MA	1	1	2	1	2
			[A.18] Destrucción de información	MA	1	1	2	1	2
			[A.19] Divulgación de información	A	1	1	2	1	2
<b>Valoración final materialización de amenazas</b>				<b>→ SOON</b>	2	2	2	1	2

Fuente: Autor

Podemos observar en el cuadro que la valoración de las amenazas es mínima, ya que se cuenta con aplicación de salvaguardas, de acuerdo con el nivel de madurez, en la unidad educativa.

**Tabla 26 Valoración de Riesgo Residual de los Datos/Información [D] con Aplicación de Salvaguarda**

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	Fre	R D	R I	R C	R A	R T
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M	1	2	2	2	2
			[E.2] Errores del administrador	A	2	4	4	4	4
			[E.3] Errores de monitorización (log)	MB	1	1	1	1	2
			[E.4] Errores de configuración	A	4	4	4	2	4
			[E.15] Alteración accidental de la información	A	2	4	4	2	4
			[E.18] Destrucción de información	MA	4	2	2	2	4
			[E.19] Fugas de información	MA	2	2	4	2	4
<b>Valoración final materialización de amenazas</b>				<b>→ SOON</b>	4	4	4	4	4
Datos / Información [D]	D01 D02 D03	Ataques Intencionados [A]	[A.3] Manipulación de los registros de actividad (log)	A	4	4	4	2	4
			[A.4] Manipulación de la configuración	MA	2	2	4	2	4
			[A.5] Suplantación de la identidad del usuario	MA	4	2	4	2	4
			[A.6] Abuso de privilegios de acceso	MA	2	2	4	2	4
			[A.11] Acceso no autorizado	MA	4	2	4	2	4
			[A.13] Repudio	A	4	2	4	2	4

	[A.15] Modificación deliberada de la información	MA	2	2	4	2	4
	[A.18] Destrucción de información	MA	2	2	4	2	4
	[A.19] Divulgación de información	A	2	2	4	2	4
<b>Valoración final materialización de amenazas</b>		 <b>SOON</b>	4	4	4	2	4

Fuente: Autor

Las amenazas principales Errores y Fallos no Intencionados [E] y Ataques Intencionados [A], indica que se han implementado medidas efectivas para reducir la probabilidad de ocurrencia de estas amenazas y minimizar su impacto en caso de que ocurran. La valoración final del riesgo también es baja en la mayoría de los casos, con un valor máximo de 4, lo que sugiere que el riesgo residual asociado a estas amenazas es mínimo.

La tabla indica que se han implementado medidas efectivas de control para mitigar el riesgo residual asociado con las diferentes amenazas, lo que ha resultado en una valoración final de riesgo baja en la mayoría de los casos. Esto es positivo ya que indica que la institución educativa ha tomado medidas adecuadas para proteger sus activos de datos/información contra posibles amenazas.

### 3.5.3.7. Activos críticos para la unidad Educativa

De acuerdo con el ANEXO B, donde se realiza la valoración de las amenazas de los activos, en este apartado vamos a listar todos los activos en donde al materializarse una amenaza seria perjudicial para la unidad educativa.

Los activos con mayor relevancia de riesgo son:

**Tabla 27 Activos críticos**

ACTIVO	ID
GESTIÓN DE MATRICULA	D01
DATOS FINANCIEROS	D02
DATOS EMPLEADOS	D03
GOOGLE WORKSPACE	S01
PÁGINA WEB	S02
SISTEMA CONTABLE - FENIX	SW01
SISTEMA NOVASOFT	SW02
COMPUTADOR DE LABORATORIO	HW01
SERVIDOR DE RESPALDO	HW02

FIREWALL	HW03
COMPUTADOR DE COLECTURÍA	HW04
COMPUTADOR DE BIBLIOTECA	HW05
COMPUTADOR DECE	HW06
COMPUTADOR BODEGA	HW07
COMPUTADOR ALIMENTOS	HW08
COMPUTADOR RECTORADO	HW09
COMPUTADOR VICERECTORADO	HW10
COMPUTADOR SECRETARIA	HW11
COMPUTADOR INSPECCIÓN GENERAL	HW12
COMPUTADOR PASTORAL	HW13
COMPUTADOR GARITA	HW14
RECTOR	P01
PERSONAL DE SISTEMAS	P02
ROUTER DE PROVEEDOR INTERNET	COM01
PBX VIRTUAL	COM02
SWITCH LAN	COM03
SWITCH GARITA	COM04
SWITCH COLECTURIA	COM05
SWITCH LABORATORIO	COM06
SWITCH BIBLIOTECA VIRTUAL	COM07
SWITCH SALA DE MAESTROS	COM08
SWITCH DECE	COM09
SWITCH VICERECTORADO	COM10
SWITCH SECRETARIA	COM11
SWITCH INSPECCION GENERAL	COM12
SWITCH PASTORAL	COM13
SWITCH BODEGA	COM14
SWITCH ALIMENTOS	COM15
ROUTER ADMINISTRATIVO	COM16
ROUTER LABORATORIO	COM17
DISCO DE RESPALDO	MEDIA01

Fuente: Autor

#### **3.5.4. Fase 4 – Plan de Seguridad de la Información**

Se creó un Plan de Seguridad de la Información para las unidades educativas del Cantón Esmeraldas después de recopilar y analizar los datos de los activos de la Unidad Educativa San Daniel Comboni utilizando la tecnología MAGERIT para evaluar los riesgos. Este plan se ha desarrollado siguiendo los lineamientos de MAGERIT y haciendo uso de estándares de gestión de seguridad, entre ellos



la norma ISO 27000. Los detalles del Plan de Seguridad se presentan en el **Anexo D** de este documento, ofreciendo una visión general de su contenido y alcance.

### 3.5.5. Fase 5 - Resultados

#### 3.5.5.1. De los Riesgos

A continuación, se presentan una tabla con los activos de información que tiene un riesgo de acuerdo con la dimensión de la seguridad en niveles más críticos y los mismos que se deben prestar una mayor atención.

**Tabla 28 Activos Datos / Información [D] con estado de riesgos**

<b>Datos / Información [D]</b>		<b>NIVEL DE RIESGO</b>				
<b>Activos:</b>	<b>Tipos de Amenazas</b>	<b>RD</b>	<b>RI</b>	<b>RC</b>	<b>RA</b>	<b>RT</b>
D01	Ataques Intencionados [A]	10	10	10	10	6
D02						
D03	Errores y Fallos no Intencionados [E]	10	10	10	10	10

Fuente: Autor

Amenazas como la manipulación de registros de actividad y el abuso de privilegios de acceso tienen un impacto significativo en la disponibilidad y la integridad de los datos, lo que resalta la necesidad de monitorear y controlar los accesos y actividades dentro del sistema.

La suplantación de la identidad del usuario y la divulgación de información también son amenazas importantes, con un impacto considerable en la confidencialidad y la autenticidad de los datos. Estas amenazas pueden comprometer la seguridad de la información y la identidad de los usuarios, lo que requiere medidas de protección adecuadas, como autenticación multifactor y cifrado de datos sensibles.

**Tabla 29 Activos Servicios [S] con estado de riesgos**

<b>Servicios [S]</b>		<b>NIVEL DE RIESGO</b>				
<b>Activos:</b>	<b>Tipos de Amenazas</b>	<b>RD</b>	<b>RI</b>	<b>RC</b>	<b>RA</b>	<b>RT</b>
S01	Errores y Fallos no Intencionados [E]	10	10	10	10	10
S02						

Ataques Intencionados [A]      10   10   10   10   10

Fuente: Autor

Todas las amenazas identificadas representan riesgos significativos para la seguridad de la información del servicio y deben ser abordadas con atención y medidas adecuadas de mitigación de riesgos.

Implementar medidas de control para evitar la divulgación de información; así como también medidas de protección contra ataques de denegación de servicio.

**Tabla 30 Activos Aplicaciones de Software [SW] con estado de riesgos**

Aplicaciones de Software [SW]		NIVEL DE RIESGO				
Activos:	Tipos de Amenazas	RD	RI	RC	RA	RT
SW01 SW02	Errores y Fallos no Intencionados [E]]	8	8	8	8	8
	Ataques Intencionados [A]	10	10	10	10	10

Fuente: Autor

Las vulnerabilidades de los programas (software) representan otra amenaza de frecuencia normal, pero de alto impacto. Estas vulnerabilidades pueden ser explotadas por atacantes para comprometer la seguridad de las aplicaciones de software y deben ser abordadas mediante parches de seguridad y actualizaciones regulares.

Implementar medidas de seguridad sólidas y mantenerse al tanto de las amenazas emergentes para proteger las aplicaciones de software de posibles ataques y asegurar la integridad, confidencialidad y disponibilidad de la información que manejan.

**Tabla 31 Activos Equipos informáticos [HW] con estado de riesgos**

Equipos Informáticos [HW]		NIVEL DE RIESGO				
Activos:	Tipos de Amenazas	RD	RI	RC	RA	RT

HW01	Desastre Naturales [N]	10	6	6	8	6
HW02						
HW03						
HW04						
HW05						
HW06	De Origen Industrial [I]	10	6	6	8	6
HW07						
HW08						
HW09						
HW10						
HW11	Errores y Fallos no Intencionados [E]	10	10	10	8	8
HW12						
HW13						
HW14						
HW14		Ataques Intencionados [A]	10	10	10	10

Fuente: Autor

Es importante tomar medidas de precaución, como la instalación de sistemas de extinción de incendios y la protección contra inundaciones, para mitigar los riesgos asociados con estas amenazas. Además, tener planes de continuidad y realizar copias de seguridad regulares son esenciales para garantizar que los datos puedan ser recuperados en caso de desastre.

Además de contar con la implementación de procedimientos de mantenimiento y actualización robustos, así como la adopción de medidas de seguridad física para proteger contra la pérdida o robo de equipos.

**Tabla 32 Activos Redes de Comunicación [COM] con estado de riesgos**

Redes de Comunicación [COM]		NIVEL DE RIESGO				
Activos:	Tipos de Amenazas	RD	RI	RC	RA	RT
COM01	De Origen Industrial [I]					
COM02						
COM03		10	8	8	10	10
COM04						
COM05						
COM06						
COM07						
COM08						
COM09	Errores y Fallos no Intencionados [E]					
COM10		10	8	10	10	10
COM11						
COM12						
COM13						

COM14					
COM15					
COM16					
COM17	Ataques Intencionados [A]	10	10	10	10

Fuente: Autor

Estas amenazas son frecuentes y representan diversos riesgos para la seguridad de las redes de comunicación. Para reducir estos riesgos y garantizar la integridad, confidencialidad, autenticidad y disponibilidad de los datos transmitidos a través de la red, es esencial implementar medidas de seguridad sólidas y mantener una vigilancia constante.

Implementar medidas de control de calidad, monitoreo constante y políticas de seguridad para mitigar los riesgos asociados con estas amenazas y garantizar la disponibilidad, integridad y confidencialidad de las redes de comunicación.

**Tabla 33 Activos Instalaciones [L] con estado de riesgos**

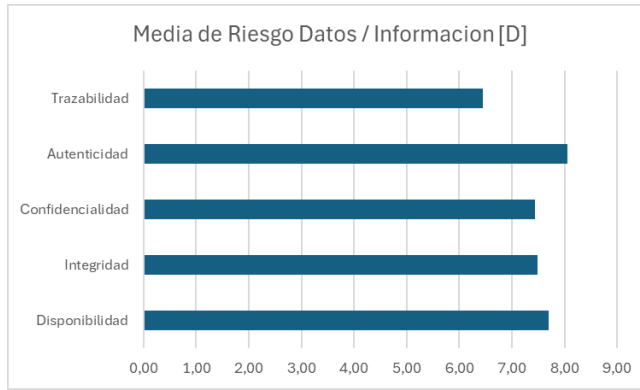
Instalaciones [L]		NIVEL DE RIESGO				
Activos:	Tipos de Amenazas	RD	RI	RC	RA	RT
L01	Desastre Naturales [N]	10	8	8	10	10
	De Origen Industrial [I]	5	4	4	5	5
	Errores y Fallos no Intencionados [E]	8	6	6	8	8
	Ataques Intencionados [A]	8	8	10	8	8

Fuente: Autor

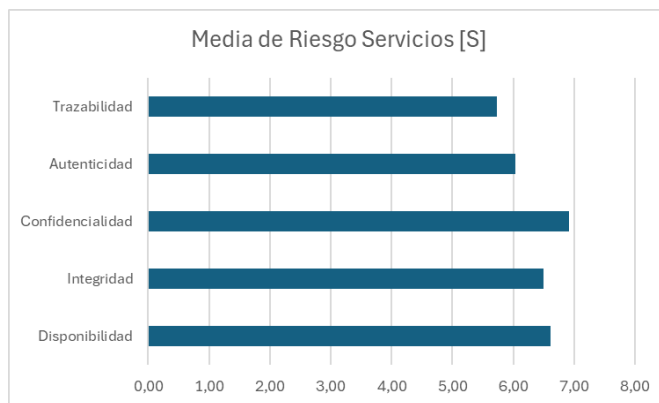
Implementar medidas de protección y mantenimiento preventivo para mitigar el riesgo de daños causados por fuego, agua, polvo, corrosión, congelamiento y emanaciones electromagnéticas en las instalaciones. Esto puede incluir la instalación de sistemas de detección y extinción de incendios, así como la implementación de procedimientos de limpieza y mantenimiento regular para prevenir la acumulación de polvo y corrosión.

### 3.5.5.2. Generales

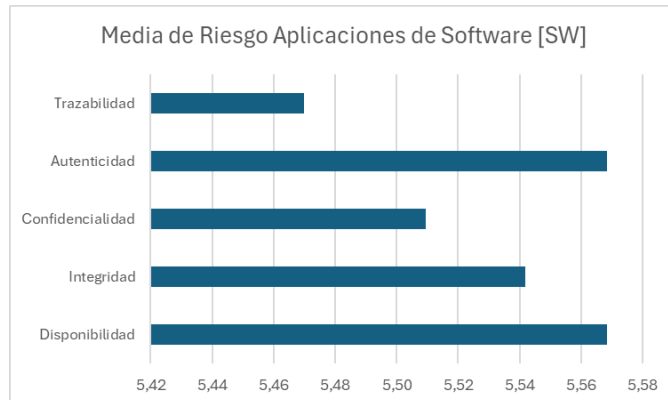
A continuación, se ilustran la media aritmética por cada tipo de activo de la unidad educativa.



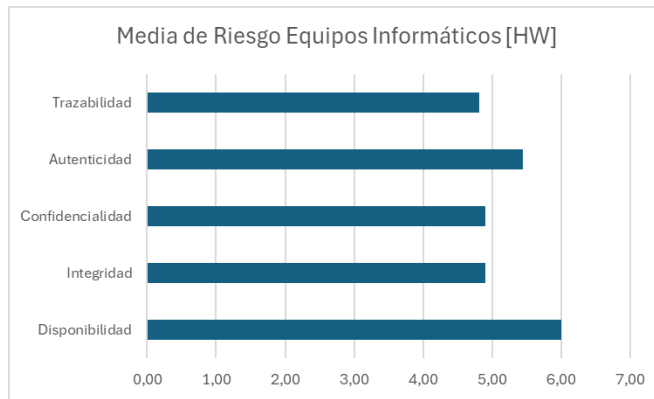
**Figura 9** Media de Riesgo Datos / Información [D]



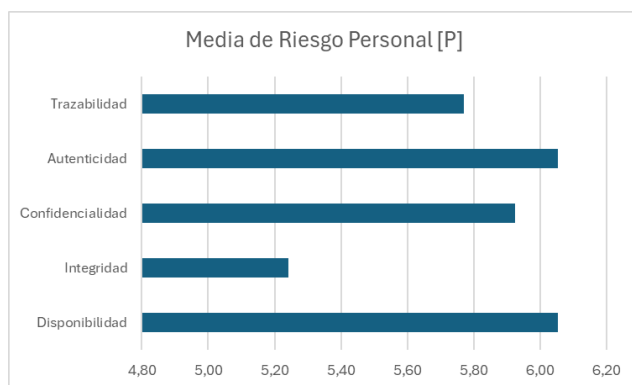
**Figura 10** Media de Riesgo Servicios [S]



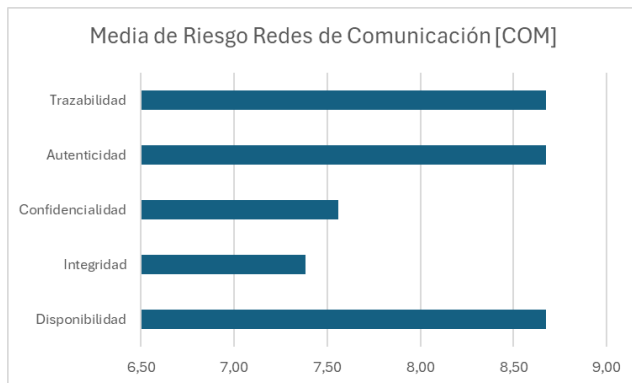
**Figura 11** Media de Riesgo Aplicaciones de Software [SW]



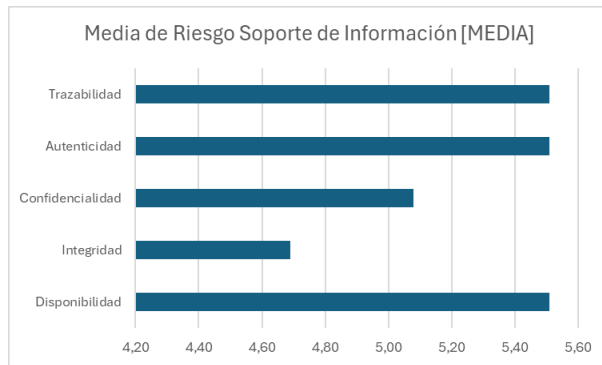
**Figura 12** Media de Riesgo Equipos Informáticos [HW]



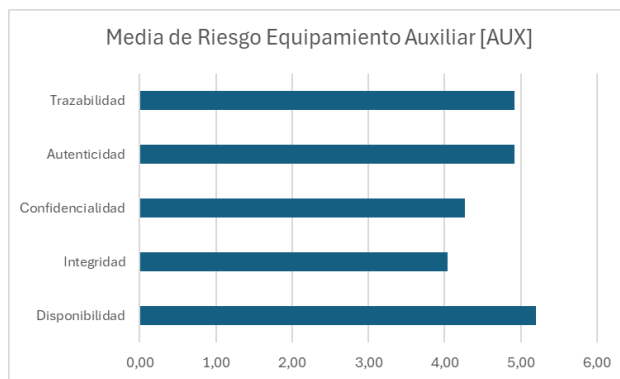
**Figura 13** Media de Riesgo Personal [P]



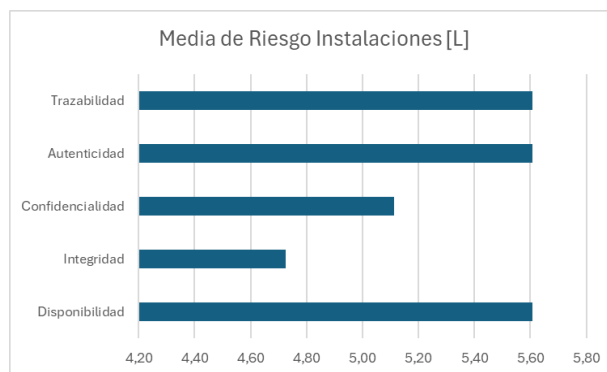
**Figura 14** Media de Riesgo Redes de Comunicación [COM]



**Figura 15** Media de Riesgo Soporte de Información [MEDIA]



**Figura 16** Media de Riesgo Equipamiento Auxiliar [AUX]



**Figura 17** Media de Riesgo Instalaciones [L]

## **4. CAPITULO IV**

### **4.1. RESULTADOS Y DISCUSIÓN**

Se detallarán los resultados derivados del desarrollo del plan de seguridad de la información para las unidades educativas en el Cantón Esmeraldas, se presenta un análisis exhaustivo de los riesgos identificados, su evaluación cuantitativa o cualitativa, y la priorización de medidas de seguridad para mitigar estos riesgos.

Además, se describen las recomendaciones específicas para fortalecer la seguridad de la información, incluyendo detalles sobre la implementación de medidas propuestas, recursos necesarios. Se destaca el cumplimiento normativo, considerando las leyes de protección de datos vigente.

En el Anexo E se muestran el instrumento utilizado para realizar la encuesta entre el personal administrativo y docente de la unidad educativa. El propósito es doble. En primer lugar, evalúa el nivel de conocimiento sobre la seguridad de los datos que manejan en el trabajo diario. En segundo lugar, determina el nivel de participación en las prácticas de protección de la información.

A través de este estudio pretendemos identificar las fortalezas de seguridad TI de las unidades educativas y sus áreas de mejora. Los resultados proporcionan una base sólida para el desarrollo de un plan de seguridad de la información para las unidades educativas y la implementación de estrategias efectivas de capacitación y concientización en ciberseguridad. También servirá como punto de partida para futuras investigaciones y acciones para fortalecer la protección de la información en entornos educativos.

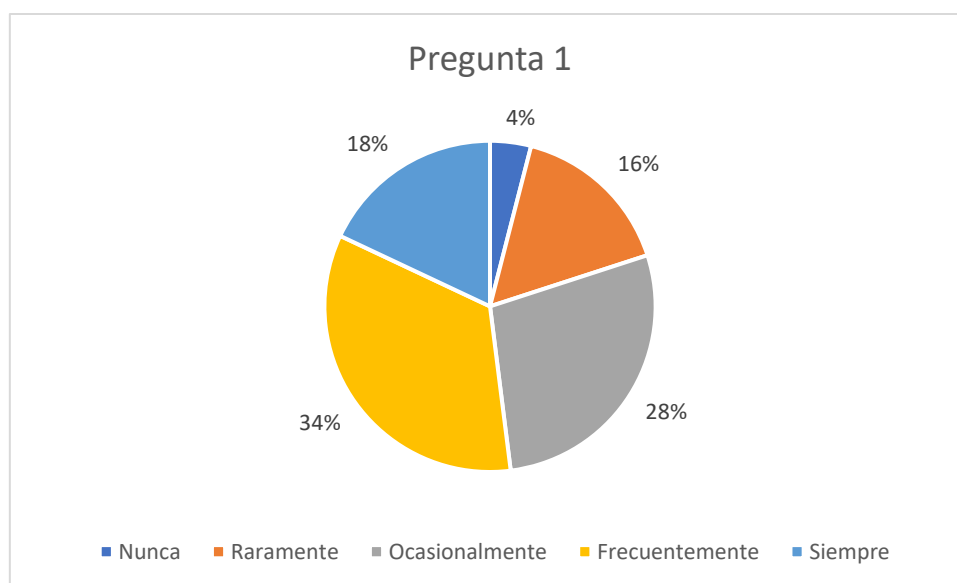
De la siguiente manera queda los resultados de la encuesta que se aplicó en las unidades educativas:



**Tabla 34 Pregunta ¿Cierra su sesión en los sistemas informáticos después de utilizarlos?**

Variable	Frecuencia	Porcentaje
Nunca	2	4%
Raramente	8	16%
Ocasionalmente	14	28%
Frecuentemente	17	34%
Siempre	9	18%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

La mayoría de los encuestados 34% dijeron que cierran sus sesiones con frecuencia al finalizar el uso del sistema informático.

Sin embargo, es importante tener en cuenta que un porcentaje significativo 28% afirma que solo lo hacen ocasionalmente.

Un 18 % afirma que siempre cierran sus sesiones, lo que indica una práctica de seguridad efectiva.

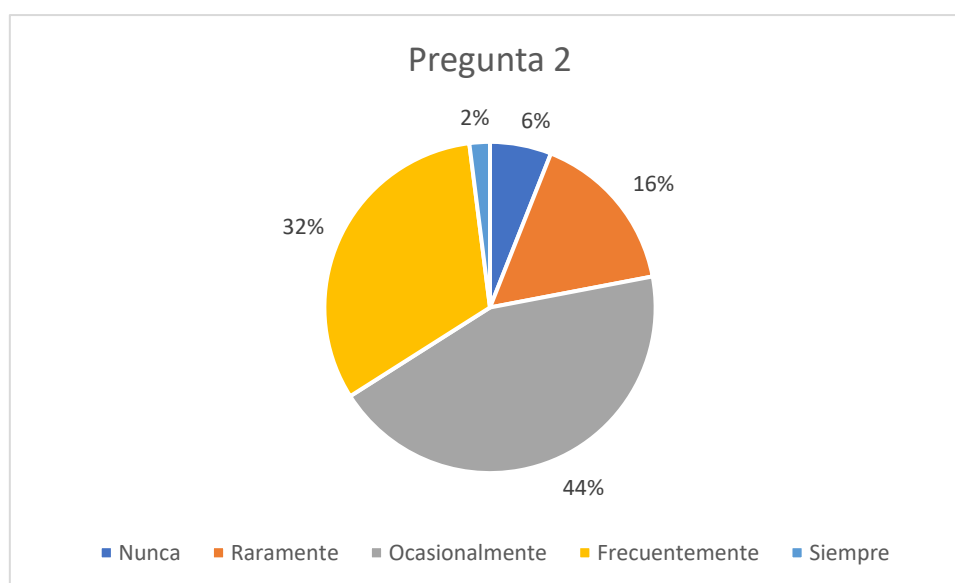
Un pequeño porcentaje 4% expresó que nunca cierran sus sesiones, lo que podría ser una preocupación para la seguridad informática.

Al parecer la mayoría de los encuestados están conscientes de la importancia de cerrar sus sesiones en los sistemas informáticos, aunque todavía se podría mejorar en este aspecto.

**Tabla 35 ¿Comparte su contraseña o credenciales con otros colegas?**

Variable	Frecuencia	Porcentaje
Nunca	3	6%
Raramente	8	16%
Ocasionalmente	22	44%
Frecuentemente	16	32%
Siempre	1	2%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

La mayoría de las personas 44% respondieron, que ocasionalmente comparten sus contraseñas o credenciales con otros colegas.

Un 32% dijo que lo hace frecuentemente, lo que es preocupante para la seguridad de la información.

Sólo un pequeño porcentaje 6% dijo que nunca comparte sus contraseñas o credenciales, lo cual es una buena práctica desde una perspectiva de ciberseguridad.

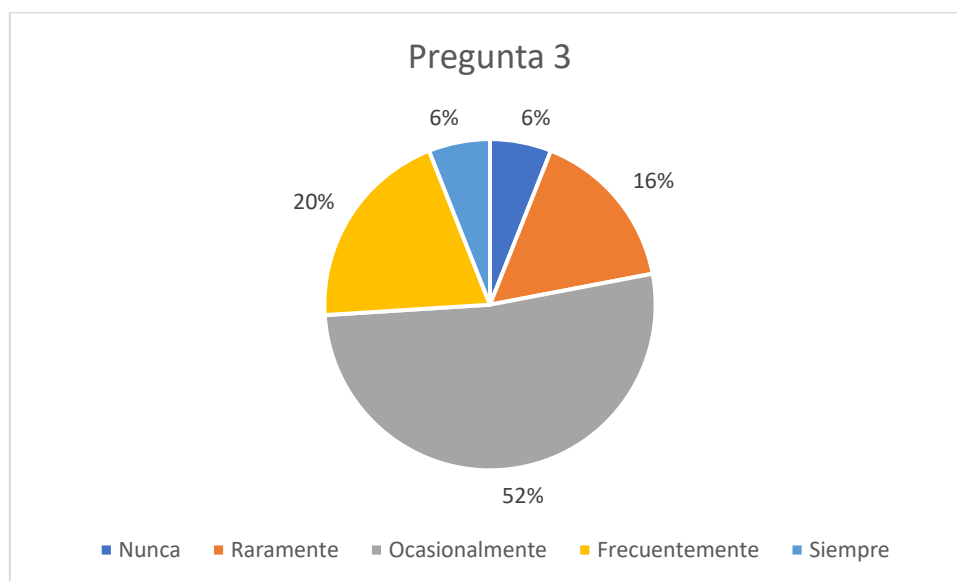
Además, el 2% admitió que siempre comparte sus contraseñas o credenciales, lo que supone un grave riesgo la seguridad de la información.

Los resultados indican que existe un nivel considerable de compartición de contraseñas o credenciales entre colegas, lo que plantea preocupaciones sobre la seguridad de la información y la necesidad de concienciar sobre las buenas prácticas en este ámbito.

**Tabla 36** ¿Verifica la autenticidad de los correos electrónicos antes de abrir archivos o hacer clic en enlaces?

Variable	Frecuencia	Porcentaje
Nunca	3	6%
Raramente	8	16%
Ocasionalmente	26	52%
Frecuentemente	10	20%
Siempre	3	6%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

El 52% de los participantes en la encuesta dijeron que verifican ocasionalmente la autenticidad de los correos electrónicos antes de abrir archivos o hacer clic en enlaces.

El 20% declaró que lo hacen con frecuencia, lo que indica un nivel considerable de conciencia sobre la seguridad de la información.

Un 16% dijo que raramente verificaba la autenticidad de los correos electrónicos, lo que puede indicar una práctica menos común pero todavía presente.

Una práctica recomendable para reducir el riesgo de ataques de phishing y malware es verificar siempre la autenticidad de los correos electrónicos, lo que hizo un pequeño porcentaje del 6%.

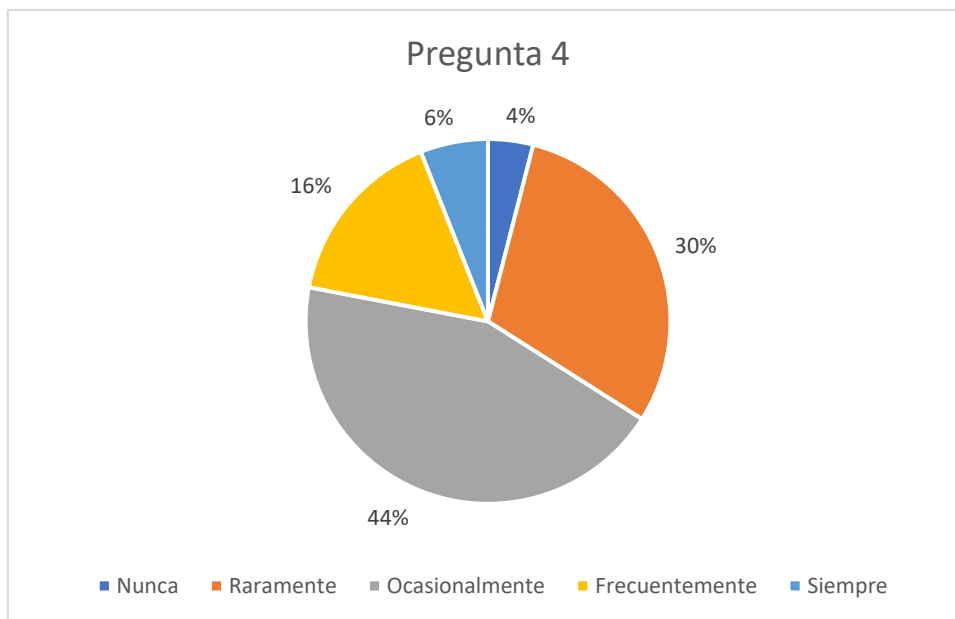
Sorprendentemente, el 6% también declaró que nunca verificaba la autenticidad de los correos electrónicos, lo que podría constituir un riesgo significativo para la seguridad.

La mayoría de los encuestados ocasionalmente verifican la autenticidad de los correos electrónicos, igualmente hay un porcentaje no insignificante que no lo hace regularmente. Esto abarca la importancia de la concienciación sobre la seguridad cibernética y la adopción de buenas prácticas en este ámbito.

**Tabla 37 ¿Es cauteloso(a) al descargar archivos de fuentes no confiables en los sistemas de la institución?**

Variable	Frecuencia	Porcentaje
Nunca	2	4%
Raramente	15	30%
Ocasionalmente	22	44%
Frecuentemente	8	16%
Siempre	3	6%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

La mayoría de los encuestados 44% señalaron que ocasionalmente son cautelosos a la hora de la descarga de archivos que tienen fuentes no confiables en los sistemas de la unidad educativa.

Se ha observado que un porcentaje significativo del 30% de los encuestados rara vez toma precauciones al descargar archivos de fuentes no confiables.

Aproximadamente uno de cada seis encuestados 16%, dijo que lo hace con frecuencia, lo que demuestra la importancia de aumentar la conciencia sobre la seguridad informática.

Un 6% de las personas dijeron que siempre son cautelosas, lo que indica una actitud proactiva hacia la seguridad cibernética.

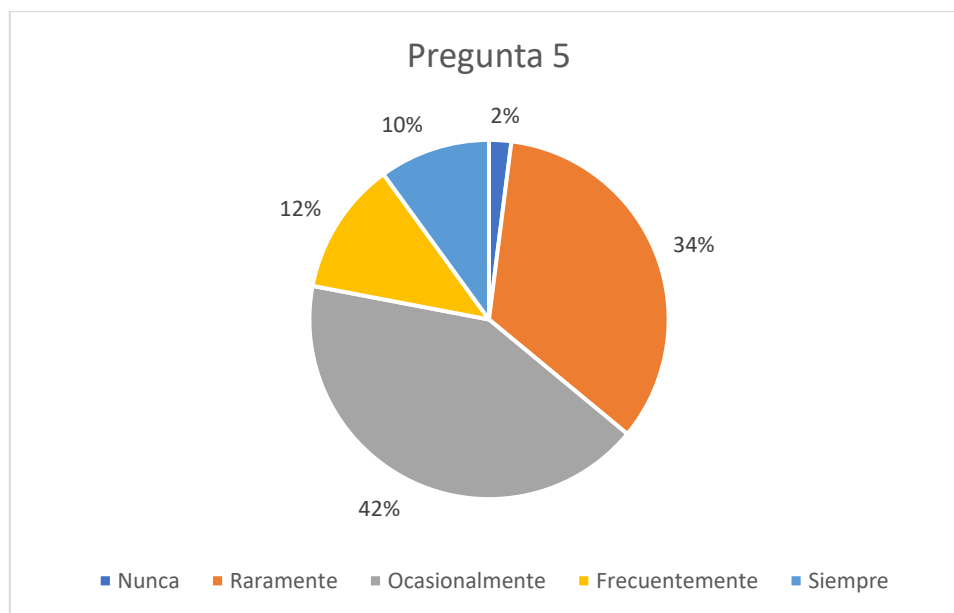
Sin embargo, vale la pena señalar que una proporción significativa 4% dijo que nunca tienen cuidado al descargar archivos de fuentes no confiables, lo que puede representar una amenaza para la seguridad del sistema de la unidad educativa.

Aunque la mayoría de los encuestados muestran cierta cautela al descargar archivos de fuentes no confiables, aún hay un porcentaje considerable que podría mejorar sus prácticas de seguridad informática para proteger los sistemas de la institución.

**Tabla 38 ¿Toma precauciones adicionales al manejar datos sensibles de los estudiantes?**

<b>Variable</b>	<b>Frecuencia</b>	<b>Porcentaje</b>
Nunca	1	2%
Raramente	17	34%
Ocasionalmente	21	42%
Frecuentemente	6	12%
Siempre	5	10%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

La mayoría de los encuestados, el 42 %, expresaron que ocasionalmente toman más precauciones al manejar datos sensibles de los estudiantes.

Se ha observado que un porcentaje significativo 34%, de los encuestados raramente toma precauciones adicionales al manejar estos datos sensibles, lo que podría generar preocupaciones sobre la seguridad de la información.

Un 12% lo hace con frecuencia, lo que indica una conciencia moderada del valor de proteger los datos sensibles de los estudiantes.

El 10% dijo que siempre toma precauciones adicionales, lo cual es alentador en términos de la protección de datos y la seguridad de la información.

Sin embargo, es preocupante que un pequeño porcentaje 2% indicara que nunca toma precauciones adicionales al manejar datos sensibles de los estudiantes, lo que podría representar graves riesgos para la privacidad y la seguridad de los datos.

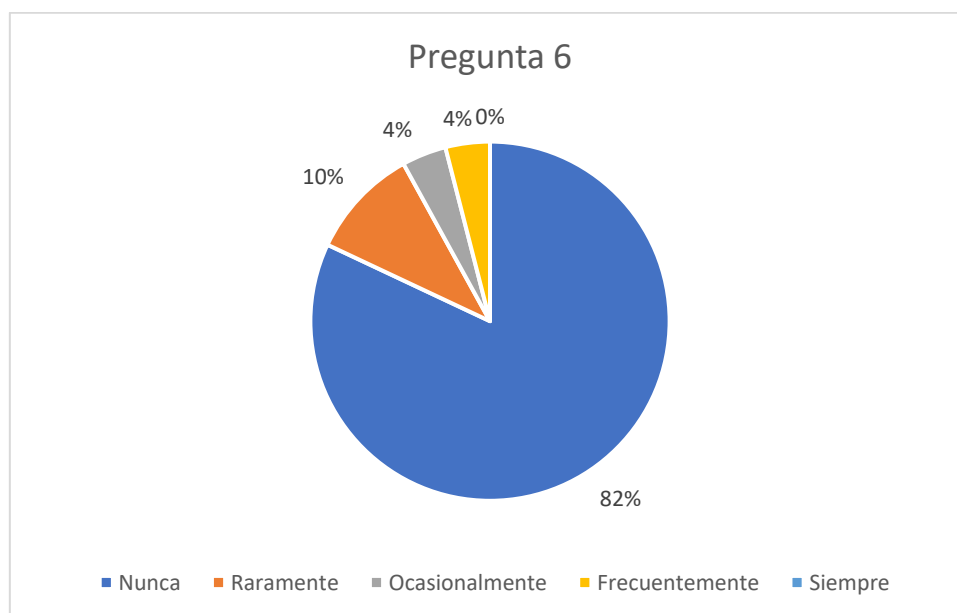
Aunque algunos encuestados manifiestan cierta conciencia y toman precauciones adicionales al manejar datos sensibles de los estudiantes, aún hay margen para mejorar las prácticas de seguridad y protección de la información en este ámbito.



**Tabla 39 ¿Ha recibido capacitación sobre las mejores prácticas de seguridad de la información por parte del departamento de TIC?**

Variable	Frecuencia	Porcentaje
Nunca	41	82%
Raramente	5	10%
Ocasionalmente	2	4%
Frecuentemente	2	4%
Siempre	0	0%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

Se puede observar que un porcentaje significativo 82% de los encuestados dijeron que nunca habían recibido capacitación sobre las mejores prácticas de seguridad de la información por parte del departamento de TIC. Esto indica que la gente generalmente no sabe mucho sobre este aspecto crucial de la seguridad de la información.

Es importante destacar que un porcentaje significativo del 10% indicó que raramente recibe capacitación, lo que deja a muchos empleados sin capacitación adecuada en seguridad de la información.

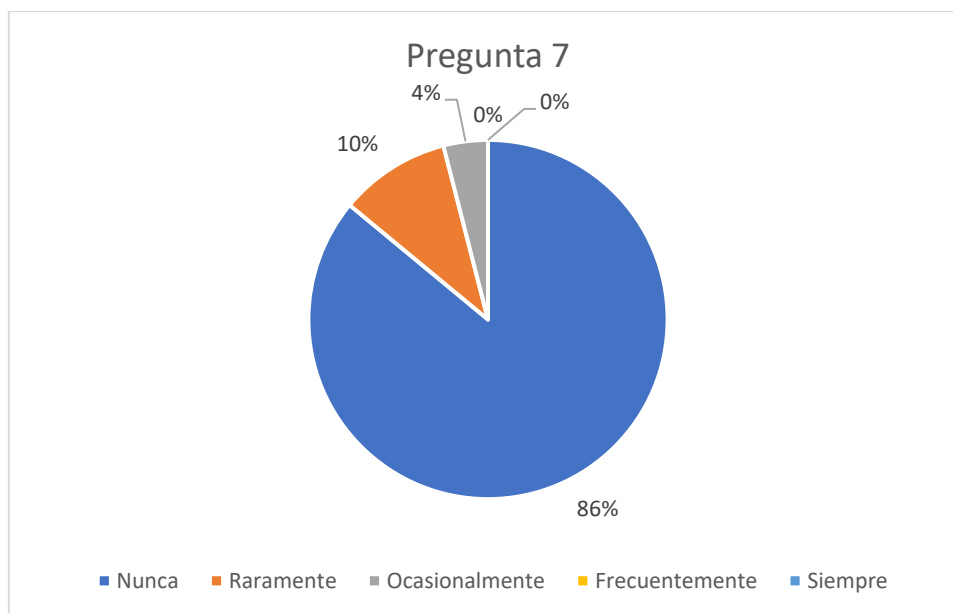
Sin embargo, aunque son solo una minoría de la muestra encuestada, la presencia de personas que reciben capacitación ocasionalmente 4% o con frecuencia 4% se podría decir que es alentadora.

Estos hallazgos destacan la urgencia de mejorar los programas de capacitación en seguridad de la información y aumentar la conciencia de este tema dentro de la unidad educativa.

**Tabla 40 ¿Ha participado en simulacros de seguridad informática organizados por la institución?**

<b>Variable</b>	<b>Frecuencia</b>	<b>Porcentaje</b>
Nunca	43	86%
Raramente	5	10%
Ocasionalmente	2	4%
Frecuentemente	0	0%
Siempre	0	0%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

Debido a un porcentaje muy alto 86% de los encuestados dijeron que nunca habían participado en simulacros de seguridad informática, es evidente que la participación en estas actividades es escasa.

Es importante destacar que un pequeño porcentaje 10% declaró haber participado raramente en estos simulacros, lo que indica que la organización podría estar llevando a cabo estas actividades, pero su alcance o frecuencia podrían ser insuficientes.

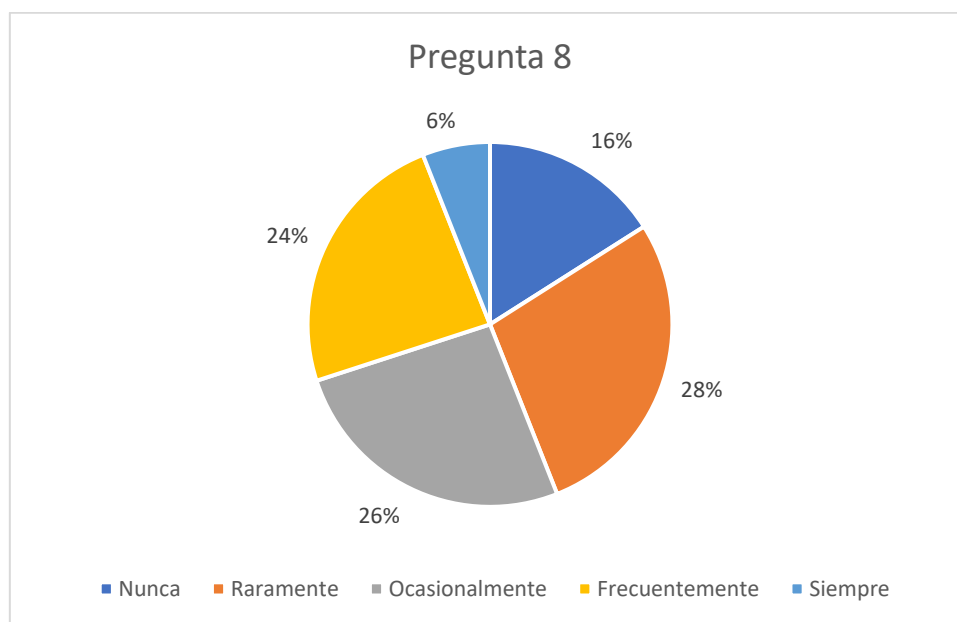
Por otro lado, es positivo observar que un pequeño porcentaje de los encuestados 4% ha participado ocasionalmente en simulacros de seguridad informática, lo que demuestra un cierto nivel de conciencia sobre la importancia de este tipo de ejercicios.

Los resultados indican que la institución educativa debería realizar más y promover simulacros cibernéticos para mejorar la preparación y la conciencia sobre posibles amenazas y ataques cibernéticos.

**Tabla 41 ¿Reporta actividades sospechosas relacionadas con la seguridad de la información a los departamentos correspondientes?**

Variable	Frecuencia	Porcentaje
Nunca	8	16%
Raramente	14	28%
Ocasionalmente	13	26%
Frecuentemente	12	24%
Siempre	3	6%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

La falta de responsabilidad en la actitud hacia la seguridad de la información se puede ver en el hecho de que un porcentaje notable 28% indicó que raramente reporta actividades sospechosas.

Por otro lado, alrededor del 26% y 24% de los encuestados dijeron que reportaban actividades sospechosas ocasional y frecuentemente, lo que indicaba un nivel moderado de conciencia y acción en materia de seguridad de la información.

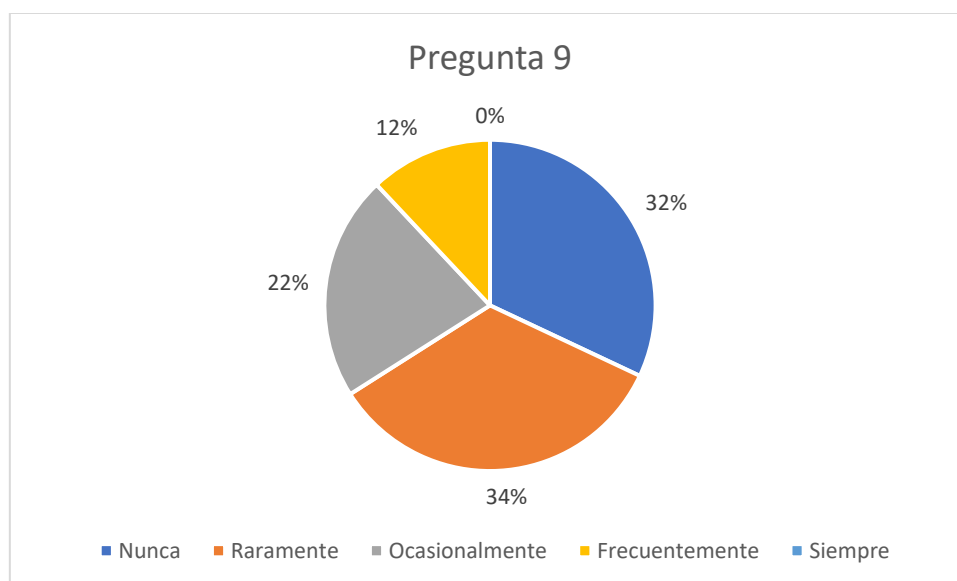
Un porcentaje pequeño pero significativo 6% indicó que reporta estas actividades siempre, lo que demuestra un compromiso claro con la seguridad de la información.

Si bien las respuestas varían según a los encuestado, parece haber una disposición generalizada a informar actividades sospechosas relacionadas con la seguridad de la información, aunque hay margen para mejorar sobre la seguridad de la información.

**Tabla 42 ¿Coopera con los procedimientos de seguridad informática establecidos por la institución educativa?**

Variable	Frecuencia	Porcentaje
Nunca	16	32%
Raramente	17	34%
Ocasionalmente	11	22%
Frecuentemente	6	12%
Siempre	0	0%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

Los datos indican que un porcentaje significativo de los encuestados 32% y 34%, respectivamente optó por las respuestas "Nunca" y "Raramente", lo que indica una falta de colaboración con los procedimientos de seguridad informática establecidos por la institución educativa.

Un porcentaje significativo del 22% indicó que colabora "ocasionalmente", lo que indica que algunos encuestados pueden participar en cierta medida en los procedimientos de seguridad informática, pero no de manera consistente.

Por otro lado, un 12% afirmó colaborar "Frecuentemente", lo que indica que hay un grupo minoritario pero notable que se involucra con frecuencia en los procedimientos de seguridad informática.

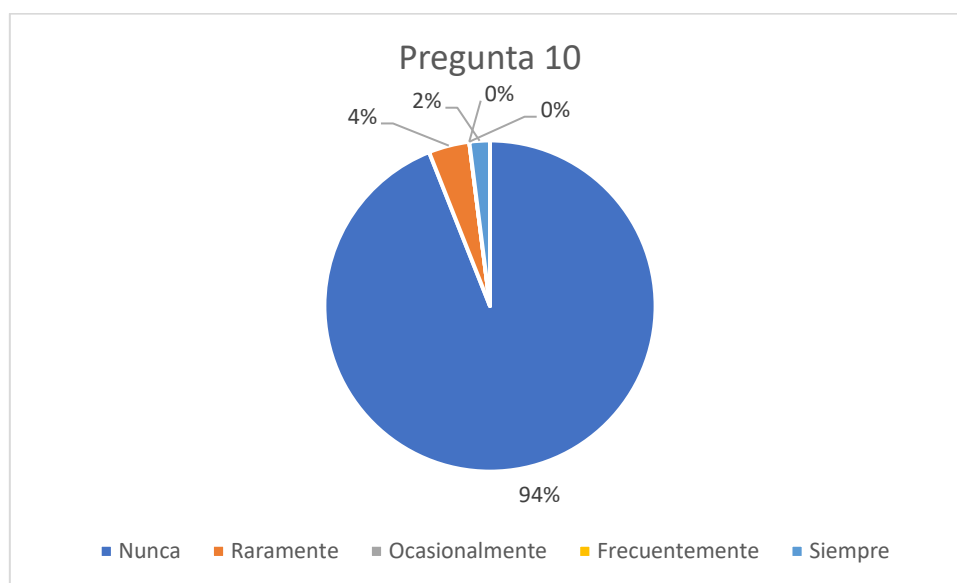
Sorprendentemente, ningún encuestado seleccionó la opción "Siempre", lo que indica que ninguno de los encuestados colaboró plenamente con las medidas de seguridad de la información establecidas por la unidad educativa.

Estos hallazgos indican que existe un margen considerable para mejorar la cooperación en los procedimientos con la seguridad de la información dentro de la institución educativa, ya que la mayoría de los encuestados dijeron que era limitada o inconsistente.

**Tabla 43 ¿Ha tenido la oportunidad de revisar y comprender completamente las políticas de seguridad de la información de la institución?**

Variable	Frecuencia	Porcentaje
Nunca	47	94%
Raramente	2	4%
Ocasionalmente	0	0%
Frecuentemente	0	0%
Siempre	1	2%
<b>Total</b>	<b>50</b>	<b>100%</b>

Fuente: Personal Administrativo y Docente de la UESDC



Fuente: Personal Administrativo y Docente de la UESDC

Según los resultados, la gran mayoría de los encuestados 94%, no ha tenido la oportunidad de revisar o comprender completamente las políticas de seguridad de la información de la institución.

Solo un pequeño porcentaje 4% expresó que raramente ha tenido esta oportunidad, lo que indica que una minoría ha tenido algún tipo de información a estas políticas.

A pesar de que esta cifra es muy baja en comparación con el porcentaje abrumador que nunca ha tenido la oportunidad de revisar y comprender estas políticas, es notable que solo un 2 % lo afirmó.

Dado que la mayoría de los encuestados no han tenido la oportunidad de revisar y comprender completamente las políticas de seguridad de la información de la institución educativa, estos resultados resaltan la importancia de mejorar la comunicación y la disponibilidad de estas políticas.

## **CONCLUSIONES Y RECOMENDACIONES**

### **CONCLUSIONES**

El proyecto ha implementado diversas metodologías para la recopilación de datos, el análisis de riesgos y la creación de un plan de seguridad de la información para las unidades educativas. Dichas metodologías se sustentan en estándares nacionales e internacionales, como se ha descrito en el documento.

A través del proyecto, se han identificado puntos críticos que se puede traducir en amenazas reales y potenciales riesgos para la seguridad de la información de la unidad educativa.

El proyecto ha proporcionado información valiosa para mejorar la postura de seguridad de la información para la unidad educativa.

La sensibilización sobre las amenazas cibernéticas es fundamental para que los miembros de las unidades educativas puedan identificar y reportar situaciones sospechosas.

Los hallazgos presentados en este análisis resaltan la imperiosa necesidad de fortalecer los programas de capacitación en seguridad de la información y elevar el nivel de conciencia sobre este tema crucial dentro de la unidad educativa.

La implementación de controles dentro de un plan de seguridad bien estructurada permite fortalecer la seguridad en todos los niveles, incluyendo la seguridad física, estructural, tecnológica y documental. Esta estrategia facilita la identificación de amenazas y vulnerabilidades, lo que la convierte en un tema de estudio relevante para las unidades educativas del cantón Esmeraldas. A través de este estudio, se pueden identificar mecanismos de solución y proponer la aplicación de controles y políticas de seguridad adecuadas para las unidades.

### **RECOMENDACIONES**

Se recomienda aplicar las metodologías propuestas en este estudio para optimizar los procesos de las unidades educativas y, en consecuencia, fortalecer la protección de la información crítica.

Se recomienda implementar los controles y políticas sugeridos en este plan de seguridad para garantizar la protección de la información y prevenir incidentes relacionados con las vulnerabilidades que se puedan presentar en el desarrollo de las actividades de las unidades educativas.

La implementación de este plan de seguridad descrito en este documento permitirá reducir significativamente los riesgos actualmente presentes en los procesos de activos, recursos humanos y continuidad de servicios de seguridad. Además, este documento servirá como base sólida para futuras iniciativas de mejora continua.

Se recomienda realizar un seguimiento a la UESDC, para evaluar el avance en la implementación de las medidas y recomendaciones identificadas en este estudio.



## BIBLIOGRAFÍA

Acosta Alvarado, N. J., & Carrillo Morán, G. F. (2018). SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS.

ACUERDO MINISTERIAL 006-2021 (2021).

Amaro Pérez Paola. (2023). Desarrollo de un SGSI para un ecommerce. Universidad de Alicante.

Blog de Innovacion Educativa. (2022). Ciberseguridad en la educación | Universidad Europea. <https://innovacion-educativa.universidadeuropea.com/noticias/ciberseguridad-educacion/>

Buitrón Gonzaga, C. A. (2021). GESTIÓN DE RIESGOS INFORMÁTICOS APLICANDO UNA METODOLOGÍA DE ANÁLISIS PARA VERIFICAR LA SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA DE AUDITORÍA, CONSULTORÍA Y CAPACITACIÓN.

Cali, S., & Guadalupe, F. (2015). PLAN DE SEGURIDAD INFORMÁTICA DE LA ESPE SEDE SANTO DOMINGO.

Chacón Prieto, D. (2020). ANÁLISIS DE METODOLOGÍAS DE LA GESTIÓN DEL RIESGO.

Chiriboga Mera, T. (2022). PROPUESTA DE UN MODELO HÍBRIDO BASADO EN LAS METODOLOGÍAS MAGERIT E ISO 27001 PARA CONTROLAR AMENAZAS INTERNAS IDENTIFICADAS EN LA INTRANET DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA.

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, 449 Registro Oficial 25 (2008). [www.lexis.com.ec](http://www.lexis.com.ec)

Crespo Martínez, E., & Cordero Torres, G. (2018). ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES. 38–47.

Dirección General de Modernización Administrativa. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. <http://administracionelectronica.gob.es/>

Estévia, F., Coelho Luiz, S., Segadas, G., & Kowask Bezerra, A. E. (n.d.). Gestión de la seguridad de la información.

- Gil, E. (n.d.). Big data, privacidad y protección de datos.
- Gimenez Albacete, J. F. (2023). Seguridad en equipos informaticos. IFCT0510 (2a. ed.). IC Editorial. <https://elibro.net/es/lc/utnorte/titulos/232696>
- Gómez Fernández, Luis., Fernández Rivero, P. Pablo., & ProQuest. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.
- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. (n.d.). Retrieved May 10, 2024, from <https://www.iso.org/es/contents/data/standard/08/28/82875.html>
- Kaspersky. (2020). ¿Qué es la ciberseguridad? <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS (2002). [www.lexis.com.ec](http://www.lexis.com.ec)
- LEY ORGÁNICA DE EDUCACIÓN INTERCULTURAL (2017). [www.educacion.gob.ec](http://www.educacion.gob.ec)
- LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (2021). [www.lexis.com.ec](http://www.lexis.com.ec)
- LEY ORGÁNICA DE SEGURIDAD DIGITAL, CIBERSEGURIDAD, CIBERDEFENSA Y CIBERINTELIGENCIA (2021).
- LEY ORGANICA DE TELECOMUNICACIONES (2015).
- López Vasco, F. E. (2019). IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA GESTIÓN DE RIESGOS DE INFORMACIÓN BASADA EN LAS NORMAS ISO/IEC 27001 Y 27002 EN EL INSTITUTO TECNOLÓGICO SUPERIOR SUCRE.
- Novoa, H. A., & Barrera, C. R. (2014). METODOLOGÍAS PARA EL ANÁLISIS DE RIESGOS EN LOS SGSI - METHODOLOGIES FOR ANALYSIS OF RISK IN THE ISMS.
- Protección de los datos - Gestión de datos de investigación - Biblioguias at Biblioteca CEPAL, Naciones Unidas. (n.d.). Retrieved October 24, 2023, from <https://biblioguias.cepal.org/c.php?g=495473&p=4398118>
- Reyes Bedoya, Do. E. (2014). EL ANÁLISIS DE RIESGOS INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

Sánchez, L. E., Santos-Olmo, A., Figueroa, V., Rosado, D. G., & Fernandez-Medina, E. (2019). GESTIÓN DE LA SEGURIDAD Y ANÁLISIS DE RIESGOS. <https://doi.org/10.12804/si9789587844337.11>

Vanessa Garcia. (2022). Ciberseguridad en el sector educativo: una asignatura pendiente. <https://revistabyte.es/tendencias-tic/educativo-seguridad/>

Xavier Quiñónez, F. (2020). PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN UESMA.

## ANEXOS

### ANEXO A: CONTROL DE SEGURIDAD DE LA INFORMACIÓN

#### INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD DE LA INFORMACION

#### ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN - ISO 27002

#### CONTROL DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD EDUCATIVA/INSTITUCION	UNIDAD EDUCATIVA FISCOMISIONAL "SAN DANIEL COMBONI"
FECHA DE EVALUACION DE CONTROL	11 DE MARZO DE 2024
RESPONSABLE DE LA INSTITUCION	ING. MIGUEL ARMIJO ZULETA
ELABORADO POR	ING. CARLOS CAMPAÑA BONE

Ítem	Sección	ITEM	Estado actual del Control	Aplicación Si/No	COMENTARIO Justificación de la exclusión (No)
	<b>1</b>	<b>Políticas de Seguridad de la Información</b>			
	1.1	<b>Dirección de gestión de seguridad de la información</b>			
1	1.1.1	Políticas de Seguridad de la Información	Inexistente	NO	Actualmente, la unidad educativa carece de una política formal de seguridad de la información.
2	1.1.2	Revisión de las políticas para la seguridad de la información	Inexistente	NO	Actualmente, no se lleva a cabo una revisión regular de las políticas de seguridad de la información en la unidad educativa.
	<b>2</b>	<b>Organización de la Seguridad de la Información</b>			
	2.1	<b>Organización interna</b>			
3	2.1.1	Compromiso de la máxima autoridad de la institución con la seguridad de la información	Inicial	SI	Se ha registrado un compromiso inicial por parte de la máxima autoridad de la institución con respecto a la seguridad de la información
4	2.1.2	Separación de funciones	Inicial	SI	
5	2.1.3	Contacto con las autoridades	Inicial	SI	

6	2.1.4	Contacto con los grupos de interés especial	No Aplica	NO	NO APLICA
7	2.1.5	Seguridad de la Información en la gestión de proyectos	No Aplica	NO	NO APLICA
	2.2	<b>Dispositivos móviles y teletrabajo</b>			
9	2.2.1	Política de dispositivos móviles	Inexistente	NO	En la actualidad, no existe una política formal de dispositivos móviles en la unidad educativa.
10	2.2.2	Teletrabajo	Inicial	SI	Videos instructivos de como realizar las video llamadas
	3	<b>Seguridad de los recursos humanos</b>			
	3.1	<b>Antes del empleo</b>			
11	3.1.1	Investigación de antecedentes	Inicial	SI	Talento Humano se fia a lo que esta expuesto en las hojas de vidas de los candidatos
12	3.1.2	Términos y condiciones laborales	Inexistente	NO	No se cuenta con términos y condiciones laborales establecidos en la unidad educativa.
	3.2	<b>Durante el empleo</b>			
13	3.2.1	Responsabilidades de la Máxima Autoridad o su delegado	Inicial	SI	La unidad educativa cuenta con videos explicativos, los mismo que han se comparten con el personal, docente y administrativos del uso de la información
14	3.2.2	Concienciación, educación y formación en seguridad de la información	Inicial	SI	La unidad educativa cuenta con TIC, quien realiza charlas por periodos para que tomen la seguridad de su información, como respaldos en

					la nube y medios físicos
15	3.2.3	Proceso disciplinario	Inexistente	NO	No se ha establecido un proceso disciplinario en la unidad educativa. Esto puede deberse a la cultura organizacional que prioriza enfoques más colaborativos y conciliatorios sobre medidas disciplinarias formales.
	3.3	<b>Finalización o cambio de empleo</b>			
16	3.3.1	Responsabilidades ante la finalización o cambio de empleo	Inicial	SI	Realizan el comunicado verbalmente, al área de TIC
	4	<b>Gestión de activos</b>			
	4.1	<b>Responsabilidad de los activos</b>			
17	4.1.1	Inventario de activos	Inexistente	NO	La unidad educativa no cuenta con un inventario de activos. Esto puede deberse a una falta de recursos o conocimiento sobre la importancia de mantener un registro detallado de los activos de información.
18	4.1.2	Propiedad de los activos	Inexistente	NO	No se ha establecido una política de propiedad de activos. Esto puede deberse a una falta de claridad sobre cómo definir y gestionar la propiedad de los activos de información.
19	4.1.3	Uso aceptable de los activos	No Aplica	NO	NO APLICA

20	4.1.4	Devolución de activos	Inicial	SI	Cumplen parcialmente, ya que el responsable de bodega emite acta de entrega recepción y el responsable de TIC, revisa la información de los equipos
	4.2	<b>Clasificación de la información</b>			
21	4.2.1	Directrices de Clasificación de la información	Inexistente	NO	No hay políticas sobre la clasificación de datos.
22	4.2.2	Etiquetado de la información	Inexistente	NO	
23	4.2.3	Manejo de los activos de la información	Inexistente	NO	
	4.3	<b>Manejo de los Soportes de almacenamiento - medios</b>			
24	4.3.1	Gestión de medios extraíbles	Inexistente	NO	La gestión de medios extraíbles no sigue un procedimiento establecido; a veces se basa en su uso empírico.
25	4.3.2	Eliminación de los medios	Inexistente	NO	
26	4.3.3	Transferencia de medios físicos	No Aplica		NO APLICA
	5	<b>Control de acceso</b>			
	5.1	<b>Requisitos institucionales para el control de acceso</b>			
27	5.1.1	Política de control de acceso	Inicial	SI	Aunque no hay una política clara, el control se lleva a cabo en ciertos roles.
28	5.1.2	Acceso a redes y servicios de red	Inicial	SI	Aunque se comunican de manera verbal, no hay controles para detectar el mal uso de los servicios de red.
	5.2	<b>Gestión de acceso de los usuarios</b>			
29	5.2.1	Registro y retiro de usuarios	Inexistente	SI	Aunque no hay una política definida, el departamento de TIC realiza la baja de usuarios cuando se separan de la institución.
30	5.2.2	Provisión de accesos a usuarios	Inexistente	SI	No hay registro de solicitudes o aprobaciones de acceso; se hace verbalmente.

31	5.2.3	Gestión de los derechos de acceso con privilegios especiales	Inexistente	SI	Solo se aplica a los usuarios por roles en los diversos sistemas de información de la unidad educativa.
32	5.2.4	Gestión de la información confidencial de autenticación de los usuarios	Inicial	SI	Por medio de memorandum de la maxima autoridad
33	5.2.5	Revisión de los derechos de acceso de usuario	Inicial	SI	Nivel educativo
34	5.2.6	Retiro o reasignación de los derechos de acceso	Inicial	SI	De manera verbal informan a Tic del personal que sale
	5.3	<b>Responsabilidades del usuario</b>			
35	5.3.1	Uso de la información confidencial para la autenticación	Inexistente	NO	No existe un procedimiento para asegurar estos tipos de datos.
	5.4	<b>Control de acceso a sistemas y aplicaciones</b>			
36	5.4.1	Restricción del acceso a la información	Inicial	SI	Aunque no es un proceso definido, ocurre ocasionalmente.
37	5.4.2	Procedimientos seguros de inicio de sesión	Inicial	SI	Control interno
38	5.4.3	Sistema de gestión de contraseñas	Inexistente	SI	Aunque se les pide que creen contraseñas seguras a los usuarios, no hay un proceso o control para hacerlo.
39	5.4.4	Uso de herramientas de administración de sistemas	Inicial	SI	El departamento de TIC está a cargo de la administración, pero no se tiene control sobre estos
40	5.4.5	Control de acceso al código fuente de los programas	No Aplica	NO	NO APLICA
	6	<b>Criptografía</b>			
	6.1	<b>Controles criptográficos</b>			
41	6.1.1	Política de uso de los controles criptográficos	Inexistente	NO	La unidad educativa no tiene una política de control de criptograficos.
42	6.1.2	Gestión de Claves	Inexistente	NO	
	7	<b>Seguridad física y del entorno</b>			
	7.1	<b>Áreas seguras</b>			
43	7.1.1	Perímetro de seguridad física	Inicial	SI	La infraestructura física es uno de los puntos importantes



44	7.1.2	Controles físicos de entrada	Inicial	SI	en cuanto a la seguridad de los equipos y sistemas de TI debido a los diversos estándares que deben cumplir como institución educativa.
45	7.1.3	Seguridad de oficinas, despachos e instalaciones	Inicial	SI	
46	7.1.4	Protección contra las amenazas externas y ambientales	Inicial	SI	
47	7.1.5	Trabajo en áreas seguras	Inexistente	NO	
48	7.1.6	Áreas de carga y entrega	No Aplica	NO	NO APLICA
	7.2	<b>Seguridad de los Equipos</b>			
49	7.2.1	Ubicación y protección de equipos	Efectivo	SI	El lugar está protegido de las amenazas del entorno, pero solo se necesita de una llave para tener una entrada fácil.
50	7.2.2	Instalaciones de suministro	Efectivo	SI	Todos los equipos tienen baterías de energía eléctrica instaladas en cada puesto de trabajo.
51	7.2.3	Seguridad del cableado	Efectivo	SI	A excepción de nuevos puntos en lugares no previstos, las instalaciones se han llevado a cabo con parámetros de cableado estructurado.
52	7.2.4	Mantenimiento de los equipos	Efectivo	SI	Aunque hay fechas y responsables calificados para el mantenimiento de los equipos, no se lleva un control o informes de los procesos.
53	7.2.5	Salida de los activos fuera de las instalaciones de la institución	Efectivo	SI	Aunque no hay una política que determine la responsabilidad, siempre hay una firma de autorización de la máxima autoridad para que los equipos salgan.
54	7.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Inexistente	NO	No hay una política que determine la responsabilidad

55	7.2.7	Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento	Inexistente	SI	No existe una política, pero cuando se asigna un equipo de computo a un nuevo usuario y/o responsable, se hace un formateo, lo que deja el equipo listo para usar y se respalda la información que reposaba allí.
56	7.2.8	Equipo informático de usuario desatendido	Inexistente	SI	Se deja a la voluntad de los usuarios,
57	7.2.9	Política de puesto de trabajo despejado y pantalla limpia	Efectivo	SI	ocasionalmente por las configuraciones de fabrica de los sistemas operativos, y a veces de manera verbal se da a conocer la importancia sobre la limpieza de su puesto de trabajo.
<b>8 Seguridad de las operaciones</b>					
<b>8.1 Procedimientos y responsabilidades operacionales</b>					
58	8.1.1	Documentación de procedimientos de operación	Inicial	SI	No hay reglas claras para estos procesos, que ocasionalmente se realizan por voluntad del responsable de TI.
59	8.1.2	Gestión de cambios	No Aplica	NO	
60	8.1.3	Gestión de capacidades	No Aplica	NO	
61	8.1.4	Separación de ambientes de desarrollo, pruebas y producción	No Aplica	NO	NO APLICA
<b>8.2 Protección contra un malware</b>					
62	8.2.1	Controles contra malware	Inexistente	SI	El antivirus solo se mantiene actualizado en computadoras con el sistema operativo propio, mientras que el resto se actualiza de manera improvisada en caso de problemas.
<b>8.3 Copias de seguridad</b>					

63	8.3.1	Copias de seguridad de la información	Inicial	SI	En ciertas fechas, se realizan respaldos de información de varios sistemas, pero a veces no se completan.
<b>8.4 Registro y monitoreo</b>					
64	8.4.1	Registro de eventos	Inexistente	NO	No hay procedimientos para este tipo de eventos, ni tampoco se llevan a cabo controles.
65	8.4.2	Protección de los registros de información	Inexistente	NO	
66	8.4.3	Registros de administración y operación	Inexistente	NO	
67	8.4.4	Sincronización de relojes	Inicial	SI	Están sincronizados con una misma zona horaria los diferentes equipos de la institución
<b>8.5 Control del software en producción</b>					
68	8.5.1	Instalación del software en sistemas en producción	No Aplica	NO	NO APLICA
<b>8.6 Gestión de la vulnerabilidad técnica</b>					
69	8.6.1	Gestión de las vulnerabilidades técnicas	Inexistente	NO	Cuando hay inconsistencia en la unidad, no se registran las acciones tomadas.
70	8.6.2	Restricciones en la instalación de software	Inexistente	NO	Solo en los laboratorios de Informática, existe la restricción para instalar de software no autorizados
<b>8.7 Consideraciones sobre la auditoría de sistemas de información</b>					
71	8.7.1	Controles de auditoría de sistemas de información	Inexistente	NO	No se realizan auditorías
<b>9 Seguridad en las comunicaciones</b>					
<b>9.1 Gestión de la seguridad de redes</b>					
72	9.1.1	Controles de red	Inexistente	NO	Se han realizado algunas configuraciones que no han sido documentadas y solo se han solucionado parcialmente algunos problemas presentados. Algunos elementos
73	9.1.2	Seguridad de los servicios de red	Inexistente	NO	
74	9.1.3	Separación en las redes	Inicial	SI	

					están disponibles pero no se utilizan. La división de la red se ha realizado de manera eficiente y eficaz, aunque todavía hay algunas medidas de seguridad que tomar.
	9.2	<b>Transferencia de información</b>			
75	9.2.1	Políticas y procedimientos de transferencia de información	Inexistente	NO	No hay procedimientos establecidos para enviar y recibir información; se utilizan controles de manera empíricos.
76	9.2.2	Acuerdos de transferencia de información	Inexistente	NO	
77	9.2.3	Mensajería electrónica	Inexistente	NO	
78	9.2.4	Acuerdos de confidencialidad o no revelación	Inexistente	NO	
	10	<b>Adquisición, desarrollo y mantenimiento de los sistemas</b>			
	10.1	<b>Requisitos de seguridad de los sistemas de información</b>			
79	10.1.1	Análisis de requisitos y especificaciones de seguridad de la información	No Aplica	NO	NO APLICA
80	10.1.2	Asegurar los servicios de aplicaciones en redes públicas	No Aplica	NO	
81	10.1.3	Controles de transacciones en línea	No Aplica	NO	
	10.2	<b>Seguridad en el desarrollo y en los procesos de soporte</b>			
82	10.2.1	Política de desarrollo seguro	No Aplica	NO	NO APLICA
83	10.2.2	Procedimientos de control de cambios en sistemas	No Aplica	NO	
84	10.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No Aplica	NO	
85	10.2.4	Restricciones a los cambios en los paquetes de software	No Aplica	NO	

86	10.2.5	Principios de ingeniería de sistemas seguros	No Aplica	NO	
87	10.2.6	Ambiente de desarrollo seguro	No Aplica	NO	
88	10.2.7	Desarrollo externalizado	No Aplica	NO	
89	10.2.8	Pruebas de seguridad del sistema	No Aplica	NO	
90	10.2.9	Pruebas de aceptación de sistemas	No Aplica	NO	
	10.3	<b>Datos de prueba</b>			
91	10.3.1	Protección de los datos de prueba	No Aplica	NO	NO APLICA
	11	<b>Relaciones con proveedores</b>			
	11.1	<b>Seguridad de la información en relación con los proveedores</b>			
92	11.1.1	Política de seguridad de la información en las relaciones con los proveedores	Inexistente	NO	Se han firmado contratos con empresas externas para desarrollar software, los cuales describen las funciones y el alcance de los sistemas adquiridos, pero no hay una política que regule los términos y condiciones sobre la protección de los datos y la información de la institución.
93	11.1.2	Requisitos de seguridad en contratos con terceros	Inexistente	NO	
94	11.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones	Inexistente	NO	
	11.2	<b>Gestión de la provisión de servicios del proveedor</b>			
95	11.2.1	Monitoreo y revisión de los servicios de proveedores	Inexistente	NO	No se elaboran estadísticas ni métricas relacionadas con las reuniones con los proveedores de sistemas, pero existe una comunicación fluida y no formal con ellos.
96	11.2.2	Gestión de cambios en los servicios de proveedores	Inexistente	NO	
	12	<b>Gestión de incidentes de seguridad de la información</b>			
	12.1	<b>Gestión de los incidentes de seguridad de la información y mejoras</b>			

97	12.1.1	Responsabilidades y procedimientos	Inicial	SI	La gestión de la seguridad se lleva a cabo de manera improvisada y sin experiencia en la protección de datos. A veces solucionan problemas, pero no toman las medidas para evitarlos en el futuro. Tampoco llevan un control o documento del incidente, de cómo lo resolvieron y cual fue la causa o factor que lo provocó.
98	12.1.2	Reporte de los eventos de seguridad de la información	Inicial	SI	
99	12.1.3	Reporte de debilidades de seguridad de la información	Inicial	SI	
100	12.1.4	Apreciación y decisión sobre los eventos de seguridad de la información	Inicial	SI	
101	12.1.5	Respuesta a incidentes de seguridad de la información	Inicial	SI	
102	12.1.6	Aprendizaje de los incidentes de seguridad de la información	Inicial	NO	
103	12.1.7	Recopilación de evidencias	Inexistente	NO	
<b>13</b>	<b>Aspectos de seguridad de la información para la gestión de la continuidad del negocio</b>				
	13.1	<b>Continuidad de seguridad de la información</b>			
104	13.1.1	Planificación de la continuidad de seguridad de la información	Inexistente	NO	No toman medidas para garantizar la continuidad de la seguridad de la información, ni tampoco tienen planes para implementar ninguna estrategia de prueba de continuidad.
105	13.1.2	Implementación de la continuidad de seguridad de la información	Inexistente	NO	
106	13.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información	Inexistente	NO	
	13.2	<b>Redundancias</b>			
107	13.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Inexistente	NO	Solo el servidor ERp está respaldado en caso de un desastre en la unidad educativa.
<b>14</b>	<b>Cumplimiento</b>				
	14.1	<b>Cumplimiento de los requisitos legales y contractuales</b>			
108	14.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Inexistente	NO	No existe política
109	14.1.2	Derechos de propiedad intelectual	No Aplica	NO	No hay reglas o procedimientos para proteger los registros, la privacidad de los datos personales y
110	14.1.3	Protección de los registros	No Aplica	NO	

111	14.1.4	Protección y privacidad de la información de carácter personal	No Aplica	NO	los controles criptográficos, pero los usuarios utilizan métodos prácticos para proteger sus datos.
112	14.1.5	Reglamentos de controles criptográficos	Inexistente	NO	
14.2 <b>Revisiones de seguridad de la información</b>					
113	14.2.1	Revisión independiente de seguridad de la información	Inexistente	NO	No hay pruebas de cumplimiento técnico, por lo que no se realiza ninguna revisión de seguridad de la información ni se cumplen las políticas y normas de seguridad.
114	14.2.2	Cumplimiento de las políticas y normas de seguridad	Inexistente	NO	
115	14.2.3	Comprobación del cumplimiento técnico	Inexistente	NO	

## ANEXO B: VALORACION DE LAS AMENZAS DE LOS ACTIVOS DE LA UESDC

Tip o de Act ivo	Activ o	Tipo de Amena za	Amenaza	F r e	I D	I C	I C	I A	I T	R D	R I	R C	R A	R T
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M	4	4	4	5	3	4	4	4	5	3
			[E.2] Errores del administrador	A	5	4	5	5	3	0	8	0	0	6
			[E.3] Errores de monitorización (log)	M B	3	3	3	4	3	3	3	3	4	3
			[E.4] Errores de configuración	A	4	4	5	5	3	8	8	0	0	6
			[E.15] Alteración accidental de la información	A	4	4	5	5	3	8	8	0	0	6
			[E.18] Destrucción de información	M A	5	5	4	5	3	0	0	8	0	6
			[E.19] Fugas de información	M A	5	4	5	4	3	0	8	0	8	6
			<b>Valoración final materialización de amenazas</b>				→ soon	5	5	5	5	3	1	1
Datos / Información [D]	D01 D02 D03	Ataques Intencionados [A]	[A.3] Manipulación de los registros de actividad (log)	A	4	3	2	3	4	8	6	4	6	8
			[A.4] Manipulación de la configuración	M A	4	4	3	4	4	8	8	6	8	8
			[A.5] Suplantación de la identidad del usuario	M A	3	4	4	4	3	6	8	8	8	6
			[A.6] Abuso de privilegios de acceso	M A	4	4	4	4	4	8	8	8	8	8
			[A.11] Acceso no autorizado	M A	5	5	5	5	5	0	0	0	0	0

			[A.13] Repudio	A	4	4	3	4	4	8	8	6	8	8		
			[A.15] Modificación deliberada de la información	M						1	1	1	1			
				A	5	5	5	5	4	0	0	0	0	8		
			[A.18] Destrucción de información	M						1	1	1				
				A	4	5	5	5	4	8	0	0	0	8		
			[A.19] Divulgación de información	A						1	1					
				A	5	4	5	4	4	0	8	0	8	8		
		<b>Valoración final materialización de amenazas</b>			→	4	5	5	5	5	1	1	1	1	1	
				SOON	4	5	5	5	5	0	0	0	0	0		
Servicios [S]	S01 S02	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M												
				A	3	4	3	2	2	6	8	6	4	4		
			[E.2] Errores del administrador	A	4	4	4	3	3	8	8	8	6	6		
			[E.9] Errores de [re-]encaminamiento	M	3	2	3	2	2	3	2	3	2	2		
			[E.10] Errores de secuencia	A	3	2	3	2	2	6	4	6	4	4		
			[E.15] Alteración accidental de la información	A	3	3	4	3	2	6	6	8	6	4		
			[E.18] Destrucción de información	A	4	4	5	4	2	8	8	0	8	4		
			[E.19] Fugas de información	M								1				
				A	4	4	5	4	3	8	8	0	8	6		
		[E.24] Caída del sistema por agotamiento de recursos	A								1	1	1	1	1	
			A	5	5	5	5	5	0	0	0	0	0	0		
			<b>Valoración final materialización de amenazas</b>			→	5	5	5	5	5	1	1	1	1	1
						SOON	5	5	5	5	5	0	0	0	0	0
				Ataques Intencionados [A]	[A.5] Suplantación de la identidad del usuario	M						1		1		
						A	5	4	4	5	4	0	8	8	0	8
					[A.6] Abuso de privilegios de acceso	M						1	1	1	1	1
						A	5	5	5	5	5	0	0	0	0	0
					[A.7] Uso no previsto	M										
						B	2	3	3	2	3	2	3	3	2	3
					[A.9] [Re-]encaminamiento de mensajes	B	3	3	3	3	3	3	3	3	3	3
					[A.10] Alteración de secuencia	M	3	4	3	3	3	3	4	3	3	3
					[A.11] Acceso no autorizado	A						1	1	1	1	1
						A	5	5	5	5	5	0	0	0	0	0
					[A.13] Repudio	A	4	3	3	4	4	8	6	6	8	8
		[A.15] Modificación deliberada de la información	M							1	1	1	1	1		
			A		5	5	5	5	5	0	0	0	0	0		
		[A.18] Destrucción de información	A							1	1	1	1	1		
			A	5	5	5	5	5	0	0	0	0	0			
		[A.19] Divulgación de información	A							1						
			A	4	4	5	4	4	8	8	0	8	8			
		[A.24] Denegación de servicio	A						1	1	1	1	1			
			A	5	5	5	4	5	0	0	0	8	0			
		<b>Valoración final materialización de amenazas</b>			→	5	5	5	5	5	1	1	1	1	1	
				SOON	5	5	5	5	5	0	0	0	0	0		
Aplicación	SW01 SW02	De Origen	[I.5] Avería de origen físico o lógico	M	4	3	3	4	3	4	3	3	4	3		



		Industrial [I]																
		<b>Valoración final materialización de amenazas</b>			→ SOON	4	3	3	4	3	4	3	3	4	3			
		<b>Errores y Fallos no Intencionados [E]</b>	[E.1] Errores de los usuarios	M	4	3	3	4	3	8	6	6	8	6				
			[E.2] Errores del administrador	M	4	4	4	4	4	8	8	8	8	8				
			[E.8] Difusión de software dañino	M	5	5	5	5	5	5	5	5	5	5				
			[E.9] Errores de [re-]encaminamiento	B	3	3	3	3	3	3	3	3	3	3				
			[E.10] Errores de secuencia	M	3	4	3	3	3	3	4	3	3	3				
			[E.15] Alteración accidental de la información	A	3	3	3	3	3	6	6	6	6	6				
			[E.18] Destrucción de información	A	4	4	4	4	4	8	8	8	8	8				
			[E.19] Fugas de información	A	4	4	4	4	4	8	8	8	8	8				
			[E.20] Vulnerabilidades de los programas (software)	M	5	5	5	5	5	5	5	5	5	5				
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	4	3	3	4	4	4	3	3	4	4				
			<b>Valoración final materialización de amenazas</b>			→ SOON	5	5	5	5	5	8	8	8	8			
			<b>Ataques Intencionados [A]</b>	[A.5] Suplantación de la identidad del usuario	A	5	4	5	5	4	1	1	1	0	8	0	0	8
		[A.6] Abuso de privilegios de acceso		A	5	5	5	5	5	1	1	1	1	1	0	0	0	0
		[A.7] Uso no previsto		M	2	3	3	2	3	2	3	3	2	3				
		[A.8] Difusión de software dañino		M	5	5	5	5	5	5	5	5	5	5				
		[A.9] [Re-]encaminamiento de mensajes		B	3	3	3	3	3	3	3	3	3	3				
		[A.10] Alteración de secuencia		M	3	4	3	3	3	3	4	3	3	3				
		[A.11] Acceso no autorizado		A	5	5	5	5	5	1	1	1	1	1	0	0	0	0
		[A.15] Modificación deliberada de la información		M	5	5	5	5	5	1	1	1	1	1	0	0	0	0
		[A.18] Destrucción de información		A	5	5	5	5	5	1	1	1	1	1	0	0	0	0
		[A.19] Divulgación de información		A	4	4	5	4	4	8	8	0	8	8	1			
		[A.22] Manipulación de programas		M	4	4	4	4	4	4	4	4	4	4				
		<b>Valoración final materialización de amenazas</b>			→ SOON	5	5	5	5	5	1	1	1	1	1			
<b>Equipos Informáticos</b>	<b>HW0 1 HW0 2 HW0 3</b>	<b>Desastre Naturales [N]</b>	[N.1] Fuego	A	5	3	3	4	3	1	0	6	6	8	6			
			[N.2] Daños por agua	M	5	3	3	4	3	5	3	3	4	3				
			[N.*] Fenómenos meteorológicos	M	4	3	3	4	3	4	3	3	3	4	3			

	HW0 4	<b>Valoración final materialización de amenazas</b>		→ SOON	5	3	3	4	3	1	0	6	6	8	6	
	HW0 5	De Origen Industrial [I]	[I.1] Fuego	B	5	3	3	4	3		5	3	3	4	3	
	HW0 6		[I.2] Daños por agua	B	5	3	3	4	3		5	3	3	4	3	
	HW0 7		[I.*] Polvo, Corrosión, congelamiento	B	3	3	3	3	3		3	3	3	3	3	
	HW0 8		[I.3] Contaminación mecánica	B	3	3	3	3	3		3	3	3	3	3	
	HW0 9		[I.4] Contaminación electromagnética	B	3	3	3	3	3		3	3	3	3	3	
	HW1 0		[I.5] Avería de origen físico o lógico	M A	4	3	3	4	3		8	6	6	8	6	
	HW1 1		[I.6] Corte del suministro eléctrico	A	5	3	3	4	3		1	0	6	6	8	6
	HW1 2		[I.7] Condiciones inadecuadas de temperatura o humedad	M B	3	3	3	3	3		3	3	3	3	3	
	HW1 3		[I.11] Emanaciones electromagnéticas	B	3	3	3	3	3		3	3	3	3	3	
	HW1 4	<b>Valoración final materialización de amenazas</b>		→ SOON	5	3	3	4	3	1	0	6	6	8	6	
		Errores y Fallos no Intencionados [E]	[E.2] Errores del administrador	M A	5	5	5	4	4		1	1	1			
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	5	5	5	4	4		1	1	1			
			[E.24] Caída del sistema por agotamiento de recursos	A	5	5	5	4	4		1	1	1			
			[E.25] Pérdida de equipos	M B	4	3	3	4	3		4	3	3	4	3	
		<b>Valoración final materialización de amenazas</b>		→ SOON	5	5	5	4	4	1	1	1				
		Ataques Intencionados [A]	[A.6] Abuso de privilegios de acceso	M A	5	4	4	5	4		1			1		
			[A.7] Uso no previsto	A	5	3	3	4	4		1	0	6	6	8	8
			[A.11] Acceso no autorizado	M A	5	5	5	5	5		1	1	1	1	1	
			[A.23] Manipulación de los equipos	A	5	5	5	4	4		1	1	1			
			[A.24] Denegación de servicio	A	5	4	4	5	5		1			1	1	
			[A.25] Robo	B	4	3	3	4	3		4	3	3	4	3	
			[A.26] Ataque destructivo	B	5	5	5	5	5		5	5	5	5	5	
		<b>Valoración final materialización de amenazas</b>		→ SOON	5	5	5	5	5	1	1	1	1	1		
Personal [P]	P01 P02	Errores y Fallos no Intencionados	[E.7] Deficiencias en la organización	M	3	3	3	3	3		3	3	3	3	3	
			[E.19] Fugas de información	A	4	4	5	4	4		1	8	8	0	8	8
			[E.28] Indisponibilidad del personal	M	4	3	3	4	4		4	3	3	4	4	

		<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	5	4	4	8	8	0	8	8
		<b>Ataques Intencionados [A]</b>	[A.28] Indisponibilidad del personal	A	4	3	3	4	4	8	6	6	8	8
			[A.29] Extorsión	M	4	3	4	4	3	8	6	8	8	6
			[A.30] Ingeniería social (picaresca)	A	4	4	5	4	4	8	8	0	8	8
		<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	5	4	4	8	8	0	8	8
		<b>De Origen Industrial [I]</b>	[I.8] Fallo de servicios de comunicaciones	A	5	4	4	5	5	1		1	1	
		<b>Valoración final materialización de amenazas</b>		→ SOON	5	4	4	5	5	1		1	1	
		<b>Errores y Fallos no Intencionados [E]</b>	[E.2] Errores del administrador	M	4	3	3	4	4	8	6	6	8	8
			[E.9] Errores de [re-]encaminamiento	A	4	3	3	4	4	8	6	6	8	8
			[E.10] Errores de secuencia	A	4	3	3	4	4	8	6	6	8	8
			[E.15] Alteración accidental de la información	A	4	4	4	4	4	8	8	8	8	8
			[E.18] Destrucción de información	B	4	4	5	4	4	4	4	5	4	4
			[E.19] Fugas de información	A	4	4	5	4	4	8	8	0	8	8
			[E.24] Caída del sistema por agotamiento de recursos	A	5	4	4	5	5	1		1	1	
			<b>Valoración final materialización de amenazas</b>		→ SOON	5	4	5	5	5	1		1	1
		<b>Ataques Intencionados [A]</b>	[A.5] Suplantación de la identidad del usuario	A	5	4	4	5	5	0	8	8	0	0
			[A.6] Abuso de privilegios de acceso	A	5	4	4	5	5	0	8	8	0	0
			[A.7] Uso no previsto	A	4	3	3	4	4	8	6	6	8	8
			[A.9] [Re-]encaminamiento de mensajes	A	5	4	4	5	5	0	8	8	0	0
			[A.10] Alteración de secuencia	A	4	3	3	4	4	8	6	6	8	8
			[A.11] Acceso no autorizado	A	5	5	5	5	5	0	0	0	0	0
			[A.12] Análisis de tráfico	A	4	3	3	4	4	8	6	6	8	8
			[A.14] Interceptación de información (escucha)	A	5	4	4	5	5	1		1	1	
			[A.15] Modificación deliberada de la información	A	5	5	5	5	5	0	0	0	0	0
			[A.19] Divulgación de información	A	5	5	5	5	5	1	1	1	1	1
		[A.24] Denegación de servicio	A	5	5	5	5	5	0	0	0	0	0	

		<b>Valoración final materialización de amenazas</b>		→	5	5	5	5	5	0	0	0	0	0	1	1	1	1	1		
Soporte de Información [MEDIA]	MED IA01	Desastre Naturales [N]	[N.1] Fuego	A	5	4	4	5	5	0	8	8	0	0	1		1	1			
			[N.2] Daños por agua	B	5	4	4	5	5	5	4	4	5	5							
			[N.*] Fenómenos meteorológicos	M	4	3	3	4	4	4	3	3	4	4							
				<b>Valoración final materialización de amenazas</b>		→	5	4	4	5	5	0	8	8	0	0	1		1	1	
		De Origen Industrial [I]	[I.1] Fuego	B	5	4	4	5	5	5	4	4	5	5							
			[I.2] Daños por agua	B	5	4	4	5	5	5	4	4	5	5							
			[I.*] Polvo, Corrosión, congelamiento	M	4	3	3	4	4	4	3	3	4	4							
			[I.3] Contaminación mecánica	M	4	3	3	4	4	4	3	3	4	4							
			[I.4] Contaminación electromagnética	M	4	3	3	4	4	4	3	3	4	4							
			[I.5] Avería de origen físico o lógico	M	5	4	4	5	5	5	4	4	5	5							
			[I.6] Corte del suministro eléctrico	B	5	4	4	5	5	5	4	4	5	5							
			[I.7] Condiciones inadecuadas de temperatura o humedad	M	4	3	3	4	4	4	3	3	4	4							
			[I.10] Degradación de los soportes de almacenamiento de la información	M	4	3	3	4	4	4	3	3	4	4							
			[I.11] Emanaciones electromagnéticas	M	4	3	3	4	4	4	3	3	4	4							
				<b>Valoración final materialización de amenazas</b>		→	5	4	4	5	5	5	4	4	5	5					
		Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	A	4	3	3	4	4	8	6	6	8	8							
			[E.2] Errores del administrador	A	4	3	3	4	4	8	6	6	8	8							
			[E.15] Alteración accidental de la información	A	4	4	4	4	4	8	8	8	8	8							
			[E.18] Destrucción de información	B	4	4	5	4	4	4	4	5	4	4							
[E.19] Fugas de información	A		4	4	5	4	4	8	8	0	8	8			1						
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A		4	3	3	4	4	8	6	6	8	8									
[E.25] Pérdida de equipos	B		4	4	5	4	4	4	4	5	4	4									
		<b>Valoración final materialización de amenazas</b>		→	4	4	5	4	4	8	8	0	8	8		1					
Ataques Intencionados [A]	[A.7] Uso no previsto	A	4	3	3	4	4	8	6	6	8	8									
	[A.11] Acceso no autorizado	A	4	4	5	4	4	8	8	0	8	8			1						
	[A.15] Modificación deliberada de la información	A	4	4	5	4	4	8	8	0	8	8			1						
	[A.18] Destrucción de información	B	4	4	5	4	4	4	4	5	4	4									
	[A.19] Divulgación de información	A	4	4	5	4	4	8	8	0	8	8			1						

			[A.23] Manipulación de los equipos	A	4	4	5	4	4	8	8	0	8	8	1		
			[A.25] Robo	B	4	4	5	4	4	4	4	5	4	4			
			[A.26] Ataque destructivo	B	4	4	5	4	4	4	4	5	4	4			
			<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	5	4	4	8	8	0	8	8	1		
		Desastre Naturales [N]	[N.1] Fuego	B	5	4	4	5	5	5	4	4	5	5			
			[N.2] Daños por agua	B	5	4	4	5	5	5	4	4	5	5			
			[N.*] Fenómenos meteorológicos	M	4	3	3	4	4	4	3	3	4	4			
			<b>Valoración final materialización de amenazas</b>	→ SOON	5	4	4	5	5	5	4	4	5	5			
		De Origen Industrial [I]	[I.1] Fuego	B	5	4	4	5	5	5	4	4	5	5			
			[I.2] Daños por agua	B	5	4	4	5	5	5	4	4	5	5			
			[I.*] Polvo, Corrosión, congelamiento	M	4	3	3	4	4	4	3	3	4	4			
			[I.3] Contaminación mecánica	M	4	3	3	4	4	4	3	3	4	4			
			[I.4] Contaminación electromagnética	M	4	3	3	4	4	4	3	3	4	4			
			[I.5] Avería de origen físico o lógico	M	5	4	4	5	5	5	4	4	5	5			
			[I.6] Corte del suministro eléctrico	B	5	4	4	5	5	5	4	4	5	5			
			[I.7] Condiciones inadecuadas de temperatura o humedad	M	4	3	3	4	4	4	3	3	4	4			
			[I.9] Interrupción de otros servicios y suministros esenciales	M	4	3	3	4	4	4	3	3	4	4			
			[I.11] Emanaciones electromagnéticas	M	4	3	3	4	4	4	3	3	4	4			
				<b>Valoración final materialización de amenazas</b>	→ SOON	5	4	4	5	5	5	4	4	5	5		
		Errores y Fallos no Intencionados [E]	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	5	3	3	4	4	1	0	6	6	8	8		
			[E.25] Pérdida de equipos	B	4	4	5	4	4	4	4	4	5	4	4		
			<b>Valoración final materialización de amenazas</b>	→ SOON	5	4	5	4	4	1	0	6	6	8	8		
		Ataques Intencionados [A]	[A.7] Uso no previsto	A	4	3	3	4	4	8	6	6	8	8			
			[A.11] Acceso no autorizado	A	5	4	5	4	4	4	1	1	0	8	0	8	8
			[A.23] Manipulación de los equipos	A	5	4	5	4	4	4	1	1	0	8	0	8	8
			[A.25] Robo	B	5	4	5	4	4	4	5	4	5	4	4		
			[A.26] Ataque destructivo	B	5	4	5	4	4	4	5	4	5	4	4		
			<b>Valoración final materialización de amenazas</b>	→ SOON	5	4	5	4	4	1	0	8	0	8	8		
Instalación	L01	Desastre Natural	[N.1] Fuego	A	5	4	4	5	5	1	0	8	8	0	0		

		[N.2] Daños por agua	B	5	4	4	5	5	5	4	4	5	5
		[N.*] Fenómenos meteorológicos	M	4	3	3	4	4	4	3	3	4	4
	<b>Valoración final materialización de amenazas</b>												
			→ SOON	5	4	4	5	5	1	8	8	1	1
	<b>De Origen Industrial [I]</b>	[I.1] Fuego	B	5	4	4	5	5	5	4	4	5	5
		[I.2] Daños por agua	B	5	4	4	5	5	5	4	4	5	5
		[I.*] Polvo, Corrosión, congelamiento	M	4	3	3	4	4	4	3	3	4	4
		[I.11] Emanaciones electromagnéticas	M	4	3	3	4	4	4	3	3	4	4
	<b>Valoración final materialización de amenazas</b>												
			→ SOON	5	4	4	5	5	5	4	4	5	5
	<b>Errores y Fallos no Intencionados</b>	[E.15] Alteración accidental de la información	A	4	3	3	4	4	8	6	6	8	8
		[E.18] Destrucción de información	B	4	4	5	4	4	4	4	5	4	4
		[E.19] Fugas de información	A	4	3	3	4	4	8	6	6	8	8
	<b>Valoración final materialización de amenazas</b>												
			→ SOON	4	4	5	4	4	8	6	6	8	8
	<b>Ataques Intencionados [A]</b>	[A.7] Uso no previsto	A	4	3	3	4	4	8	6	6	8	8
		[A.11] Acceso no autorizado	A	4	4	5	4	4	8	8	0	8	8
		[A.15] Modificación deliberada de la información	A	4	4	5	4	4	8	8	0	8	8
		[A.18] Destrucción de información	B	4	4	5	4	4	4	4	5	4	4
		[A.19] Divulgación de información	A	4	3	3	4	4	8	6	6	8	8
		[A.26] Ataque destructivo	B	4	4	5	4	4	4	4	5	4	4
		[A.27] Ocupación enemiga	B	4	4	5	4	4	4	4	5	4	4
	<b>Valoración final materialización de amenazas</b>												
			→ SOON	4	4	5	4	4	8	8	0	8	8

### ANEXO C: VALORACION DE LAS AMENAZAS DE LOS ACTIVOS DE LA UESDC APLICADOS SALVAGUARDA

Tipo de Activo	Activo	Tipo de Amenaza	Amenaza	F	R	I	I	I	I	R	R	R	R	R	
				e	D	I	C	A	T	D	I	C	A	T	
Datos / Información [D]	D01 D02 D03	Errores y Fallos no Intencionados [E]	[E.1] Errores de los usuarios	M	1	2	2	2	2	1	2	2	2	2	
			[E.2] Errores del administrador	A	1	2	2	2	2	2	4	4	4	4	
			[E.3] Errores de monitorización (log)	M											
			[E.4] Errores de configuración	B	1	1	1	1	2	1	1	1	1	1	2
			[E.15] Alteración accidental de la información	A	2	2	2	1	2	4	4	4	2	4	
				A	1	2	2	1	2	2	4	4	2	4	

			[E.18] Destrucción de información	M	2	1	1	1	2	4	2	2	2	4				
			[E.19] Fugas de información	M	1	1	2	1	2	2	2	4	2	4				
		<b>Valoración final materialización de amenazas</b>			→ SOON	2	2	2	2	2	4	4	4	4				
<b>Datos / Información [D]</b>	<b>D01 D02 D03</b>	<b>Ataques Intencionados [A]</b>	[A.3] Manipulación de los registros de actividad (log)	A	2	2	2	1	2	4	4	4	2	4				
			[A.4] Manipulación de la configuración	M	1	1	2	1	2	2	2	4	2	4				
			[A.5] Suplantación de la identidad del usuario	M	2	1	2	1	2	4	2	4	2	4				
			[A.6] Abuso de privilegios de acceso	M	1	1	2	1	2	2	2	4	2	4				
			[A.11] Acceso no autorizado	M	2	1	2	1	2	4	2	4	2	4				
			[A.13] Repudio	A	2	1	2	1	2	4	2	4	2	4				
			[A.15] Modificación deliberada de la información	M	1	1	2	1	2	2	2	4	2	4				
			[A.18] Destrucción de información	M	1	1	2	1	2	2	2	4	2	4				
			[A.19] Divulgación de información	A	1	1	2	1	2	2	2	4	2	4				
					<b>Valoración final materialización de amenazas</b>			→ SOON	2	2	2	1	2	4	4	4	2	4
<b>Servicios [S]</b>	<b>S01 S02</b>	<b>Errores y Fallos no Intencionados [E]</b>	[E.1] Errores de los usuarios	M	2	3	2	1	1	4	6	4	2	2				
			[E.2] Errores del administrador	A	3	2	2	2	2	6	4	4	4	4				
			[E.9] Errores de [re-]encaminamiento	M	2	1	2	1	1	2	1	2	1	1				
			[E.10] Errores de secuencia	A	2	1	2	1	1	4	2	4	2	2				
			[E.15] Alteración accidental de la información	A	2	2	3	2	1	4	4	6	4	2				
			[E.18] Destrucción de información	A	3	2	3	2	1	6	4	6	4	2				
			[E.19] Fugas de información	M	3	3	3	2	2	6	6	6	4	4				
			[E.24] Caída del sistema por agotamiento de recursos	A	3	3	3	3	3	6	6	6	6	6				
					<b>Valoración final materialización de amenazas</b>			→ SOON	2	2	2	2	2	6	6	6	6	6
					<b>Ataques Intencionados [A]</b>	[A.5] Suplantación de la identidad del usuario	M	3	2	2	3	2	6	4	4	6	4	
	[A.6] Abuso de privilegios de acceso	M	3	3		3	3	3	6	6	6	6	6					
	[A.7] Uso no previsto	M	1	2		2	1	2	1	2	2	1	2					
	[A.9] [Re-]encaminamiento de mensajes	B	2	2		2	2	2	2	2	2	2	2					
	[A.10] Alteración de secuencia	M	2	4		2	2	2	2	4	2	2	2					
	[A.11] Acceso no autorizado	A	3	3		3	3	3	6	6	6	6	6					

		[A.13] Repudio	A	4	2	2	4	4	8	4	4	8	8		
		[A.15] Modificación deliberada de la información	M												
		[A.18] Destrucción de información	A	3	3	3	3	3	6	6	6	6	6		
		[A.19] Divulgación de información	A	4	4	3	4	4	8	8	6	8	8		
		[A.24] Denegación de servicio	A	3	3	3	4	3	6	6	6	8	6		
		<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	3	4	4	8	8	6	8	8		
Aplicaciones de Software [SW]	SW01 SW02	<b>De Origen Industrial [I]</b>													
		[I.5] Avería de origen físico o lógico	M	4	2	2	4	2	4	2	2	4	2		
			<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	3	4	4	4	2	2	4	2	
		<b>Errores y Fallos no Intencionados [E]</b>	[E.1] Errores de los usuarios	M	4	2	2	4	2	8	4	4	8	4	
			[E.2] Errores del administrador	M	4	4	4	4	4	8	8	8	8	8	
			[E.8] Difusión de software dañino	M	3	3	3	3	3	3	3	3	3	3	
			[E.9] Errores de [re-]encaminamiento	B	2	2	2	2	2	2	2	2	2	2	
			[E.10] Errores de secuencia	M	2	4	2	2	2	2	4	2	2	2	
			[E.15] Alteración accidental de la información	A	2	2	2	2	2	4	4	4	4	4	
			[E.18] Destrucción de información	A	4	4	4	4	4	8	8	8	8	8	
			[E.19] Fugas de información	A	4	4	4	4	4	8	8	8	8	8	
			[E.20] Vulnerabilidades de los programas (software)	M	3	3	3	3	3	3	3	3	3	3	
			[E.21] Errores de mantenimiento / actualización de programas (software)	M	4	2	2	4	4	4	2	2	4	4	
				<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	3	4	4	8	8	8	8	8
			<b>Ataques Intencionados [A]</b>	[A.5] Suplantación de la identidad del usuario	A	3	4	3	3	4	6	8	6	6	8
		[A.6] Abuso de privilegios de acceso		A	3	3	3	3	3	6	6	6	6	6	
		[A.7] Uso no previsto		M	1	2	2	1	2	1	2	2	1	2	
		[A.8] Difusión de software dañino		M	3	3	3	3	3	3	3	3	3	3	
		[A.9] [Re-]encaminamiento de mensajes		B	2	2	2	2	2	2	2	2	2	2	
		[A.10] Alteración de secuencia		M	2	4	2	2	2	2	4	2	2	2	
		[A.11] Acceso no autorizado		A	3	3	3	3	3	6	6	6	6	6	
		[A.15] Modificación deliberada de la información		M	3	3	3	3	3	6	6	6	6	6	
		[A.18] Destrucción de información		A	3	3	3	3	3	6	6	6	6	6	
		[A.19] Divulgación de información		A	4	4	3	4	4	8	8	6	8	8	





			[E.19] Fugas de información	A	4	4	3	4	4	8	8	6	8	8	
			[E.28] Indisponibilidad del personal	M	4	2	2	4	4	4	2	2	4	4	
			<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	4	4	4	8	8	6	8	8
	P01 P02	Ataques Intencionados [A]	[A.28] Indisponibilidad del personal	A	4	2	2	4	4	8	4	4	8	8	
			[A.29] Extorsión	M	4	2	4	4	2	8	4	8	8	4	
			[A.30] Ingeniería social (picaresca)	A	4	4	3	4	4	8	8	6	8	8	
			<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	4	4	4	8	8	8	8	8
		De Origen Industrial [I]	[I.8] Fallo de servicios de comunicaciones	A	3	4	4	3	3	6	8	8	6	6	
			<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	4	4	4	6	8	8	6	6
	COM 01	Errores y Fallos no Intencionados [E]	[E.2] Errores del administrador	M	4	2	2	4	4	8	4	4	8	8	
	COM 02		[E.9] Errores de [re-]encaminamiento	A	4	2	2	4	4	8	4	4	8	8	
	COM 03		[E.10] Errores de secuencia	A	4	2	2	4	4	8	4	4	8	8	
	COM 04		[E.15] Alteración accidental de la información	A	4	4	4	4	4	8	8	8	8	8	
	COM 05		[E.18] Destrucción de información	B	4	4	3	4	4	4	4	3	4	4	
	COM 06		[E.19] Fugas de información	A	4	4	3	4	4	8	8	6	8	8	
	COM 07		[E.24] Caída del sistema por agotamiento de recursos	A	3	4	4	3	3	6	8	8	6	6	
	COM 08		<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	4	4	4	8	8	8	8	8
	COM 09		Ataques Intencionados [A]	[A.5] Suplantación de la identidad del usuario	A	3	4	4	3	3	6	8	8	6	6
	COM 10	[A.6] Abuso de privilegios de acceso		A	3	4	4	3	3	6	8	8	6	6	
	COM 11	[A.7] Uso no previsto		A	4	2	2	4	4	8	4	4	8	8	
	COM 12	[A.9] [Re-]encaminamiento de mensajes		A	3	4	4	3	3	6	8	8	6	6	
	COM 13	[A.10] Alteración de secuencia		A	4	2	2	4	4	8	4	4	8	8	
	COM 14	[A.11] Acceso no autorizado		A	3	3	3	3	3	6	6	6	6	6	
	COM 15	[A.12] Análisis de tráfico		A	4	2	2	4	4	8	4	4	8	8	
	COM 16	[A.14] Interceptación de información (escucha)		A	3	4	4	3	3	6	8	8	6	6	
	COM 17	[A.15] Modificación deliberada de la información		A	3	3	3	3	3	6	6	6	6	6	
			[A.19] Divulgación de información	A	3	3	3	3	3	6	6	6	6	6	
			[A.24] Denegación de servicio	A	3	3	3	3	3	6	6	6	6	6	
			<b>Valoración final materialización de amenazas</b>		→ SOON	4	4	4	4	4	8	8	8	8	8
Sop ORTE		Des astr e	[N.1] Fuego	A	3	4	4	3	3	6	8	8	6	6	

			[N.2] Daños por agua	M																		
			[N.*] Fenómenos meteorológicos	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4		
			<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	4	4	4	6	8	8	6	6	6	6	6	6	6	6		
		<b>De Origen Industrial [I]</b>	[I.1] Fuego	B	3	4	4	3	3	3	4	4	3	3	3	4	4	3	3	3		
			[I.2] Daños por agua	B	3	4	4	3	3	3	4	4	3	3	3	4	4	3	3	3	3	
			[I.*] Polvo, Corrosión, congelamiento	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4	4	
			[I.3] Contaminación mecánica	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4	4	
			[I.4] Contaminación electromagnética	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4	4	
			[I.5] Avería de origen físico o lógico	M	3	4	4	3	3	3	4	4	3	3	3	4	4	3	3	3	3	
			[I.6] Corte del suministro eléctrico	B	3	4	4	3	3	3	4	4	3	3	3	4	4	3	3	3	3	
			[I.7] Condiciones inadecuadas de temperatura o humedad	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4	4	
			[I.10] Degradación de los soportes de almacenamiento de la información	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4	4	
			[I.11] Emanaciones electromagnéticas	M	4	2	2	4	4	4	2	2	4	4	4	2	2	4	4	4	4	
			<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4		
	<b>MED IA01</b>	<b>Errores y Fallos no Intencionados [E]</b>	[E.1] Errores de los usuarios	A	4	2	2	4	4	8	4	4	8	8	8	4	4	8	8	8	8	
			[E.2] Errores del administrador	A	4	2	2	4	4	8	4	4	8	8	8	4	4	8	8	8	8	8
			[E.15] Alteración accidental de la información	A	4	4	4	4	4	8	8	8	8	8	8	8	8	8	8	8	8	8
			[E.18] Destrucción de información	B	4	4	3	4	4	4	4	4	3	4	4	4	4	3	4	4	4	4
			[E.19] Fugas de información	A	4	4	3	4	4	8	8	6	8	8	8	8	6	8	8	8	8	8
			[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	4	2	2	4	4	8	4	4	8	8	8	4	4	8	8	8	8	8
			[E.25] Pérdida de equipos	B	4	4	3	4	4	4	4	4	3	4	4	4	4	3	4	4	4	4
					<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	4	4	4	8	8	8	8	8	8	8	8	8	8	8
		<b>Ataques Intencionados [A]</b>	[A.7] Uso no previsto	A	4	2	2	4	4	8	4	4	8	8	8	4	4	8	8	8	8	
			[A.11] Acceso no autorizado	A	4	4	3	4	4	8	8	6	8	8	8	8	6	8	8	8	8	
			[A.15] Modificación deliberada de la información	A	4	4	3	4	4	8	8	6	8	8	8	8	6	8	8	8	8	
			[A.18] Destrucción de información	B	4	4	3	4	4	4	4	3	4	4	4	4	3	4	4	4	4	
			[A.19] Divulgación de información	A	4	4	3	4	4	8	8	6	8	8	8	8	6	8	8	8	8	
			[A.23] Manipulación de los equipos	A	4	4	3	4	4	8	8	6	8	8	8	8	6	8	8	8	8	
			[A.25] Robo	B	4	4	3	4	4	4	4	3	4	4	4	4	3	4	4	4	4	
			[A.26] Ataque destructivo	B	4	4	3	4	4	4	4	3	4	4	4	4	3	4	4	4	4	
			<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	4	4	4	8	8	6	8	8	8	6	8	8	8	8		
<b>Equipo</b>		<b>Descripción</b>	[N.1] Fuego	B	3	4	4	3	3	3	4	4	3	3	3	4	4	3	3	3		

Instalaciones [L]	AUX 01 AUX 02		[N.2] Daños por agua	B	3	4	4	3	3	3	4	4	3	3		
			[N.*] Fenómenos meteorológicos	M	4	2	2	4	4	4	2	2	4	4		
		<b>Valoración final materialización de amenazas</b>			→ SOON	4	4	4	4	4	4	4	4	4	4	4
		De Origen Industrial [I]	[I.1] Fuego	B	3	4	4	3	3	3	4	4	3	3		
			[I.2] Daños por agua	B	3	4	4	3	3	3	4	4	3	3		
			[I.*] Polvo, Corrosión, congelamiento	M	4	2	2	4	4	4	2	2	4	4		
			[I.3] Contaminación mecánica	M	4	2	2	4	4	4	2	2	4	4		
			[I.4] Contaminación electromagnética	M	4	2	2	4	4	4	2	2	4	4		
			[I.5] Avería de origen físico o lógico	M	3	4	4	3	3	3	4	4	3	3		
			[I.6] Corte del suministro eléctrico	B	3	4	4	3	3	3	4	4	3	3		
			[I.7] Condiciones inadecuadas de temperatura o humedad	M	4	2	2	4	4	4	2	2	4	4		
	[I.9] Interrupción de otros servicios y suministros esenciales		M	4	2	2	4	4	4	2	2	4	4			
	[I.11] Emanaciones electromagnéticas		M	4	2	2	4	4	4	2	2	4	4			
	<b>Valoración final materialización de amenazas</b>			→ SOON	4	4	4	4	4	4	4	4	4	4	4	
	Errores y Fallos no Intencionados [E]	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	3	2	2	4	4	6	4	4	8	8			
		[E.25] Pérdida de equipos	B	4	4	3	4	4	4	4	3	4	4			
	<b>Valoración final materialización de amenazas</b>			→ SOON	4	4	4	4	4	6	4	4	8	8		
	Ataques Intencionados [A]	[A.7] Uso no previsto	A	4	2	2	4	4	8	4	4	8	8			
		[A.11] Acceso no autorizado	A	3	4	3	4	4	6	8	6	8	8			
		[A.23] Manipulación de los equipos	A	3	4	3	4	4	6	8	6	8	8			
		[A.25] Robo	B	3	4	3	4	4	3	4	3	4	4			
		[A.26] Ataque destructivo	B	3	4	3	4	4	3	4	3	4	4			
	<b>Valoración final materialización de amenazas</b>			→ SOON	4	4	4	4	4	8	8	6	8	8		
	L01	Desastre Naturales [N]	[N.1] Fuego	A	3	4	4	3	3	6	8	8	6	6		
			[N.2] Daños por agua	B	3	4	4	3	3	3	4	4	3	3		
			[N.*] Fenómenos meteorológicos	M	4	2	2	4	4	4	2	2	4	4		
		<b>Valoración final materialización de amenazas</b>			→ SOON	3	4	4	3	3	6	8	8	6	6	
De Origen Industrial [I]		[I.1] Fuego	B	3	4	4	3	3	3	4	4	3	3			
		[I.2] Daños por agua	B	3	4	4	3	3	3	4	4	3	3			
		[I.*] Polvo, Corrosión, congelamiento	M	4	2	2	4	4	4	2	2	4	4			
		[I.11] Emanaciones electromagnéticas	M	4	2	2	4	4	4	2	2	4	4			

		<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	4	4	4	4	4	4	4	4
<b>Errores y Fallos no Intencionados</b>		[E.15] Alteración accidental de la información	A	4	2	2	4	4	8	4	4	8	8
		[E.18] Destrucción de información	B	4	4	3	4	4	4	4	3	4	4
		[E.19] Fugas de información	A	4	2	2	4	4	8	4	4	8	8
		<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	3	4	4	8	4	4	8	8
<b>Ataques Intencionados [A]</b>		[A.7] Uso no previsto	A	4	2	2	4	4	8	4	4	8	8
		[A.11] Acceso no autorizado	A	4	4	3	4	4	8	8	6	8	8
		[A.15] Modificación deliberada de la información	A	4	4	3	4	4	8	8	6	8	8
		[A.18] Destrucción de información	B	4	4	3	4	4	4	4	3	4	4
		[A.19] Divulgación de información	A	4	2	2	4	4	8	4	4	8	8
		[A.26] Ataque destructivo	B	4	4	3	4	4	4	4	3	4	4
		[A.27] Ocupación enemiga	B	4	4	3	4	4	4	4	3	4	4
		<b>Valoración final materialización de amenazas</b>	→ SOON	4	4	4	4	4	8	8	6	8	8

## ANEXO D: PLAN DE SEGURIDAD DE INFORMACION

---

	Plan de Seguridad de la Información para unidades educativas del Cantón Esmeraldas	Elaborado por: Ing. Carlos Campaña
		Versión Documento: 1.0
		Pag:0 de 22

# PLAN DE SEGURIDAD DE LA INFORMACIÓN

PARA UNIDADES EDUCATIVAS DEL CANTON ESMERALDAS

### Resumen

Este plan aborda la protección de datos y riesgos en el entorno educativo, estableciendo directrices claras y procedimientos efectivos para garantizar la confidencialidad, integridad y disponibilidad de la información. Basado en estándares internacionales como ISO/IEC 27001 y metodologías de análisis de riesgos, este plan se adapta específicamente a las necesidades de las unidades educativas del Cantón Esmeraldas, brindando un enfoque integral y proactivo para mitigar amenazas y garantizar un entorno seguro para estudiantes, personal y los datos institucionales.

Ing. Carlos Campaña Bone  
Maestrante Computación – Seguridad informática

**Figura 18** Portada del Plan de Seguridad de la Información

	Plan de Seguridad de la Información para unidades educativas del Cantón Esmeraldas	Elaborado por: Ing. Carlos Campaña
		Versión Documento: 1.0
		Pag:1 de 22

#### TABLA DE CONTENIDO

1.1	ANTECEDENTES.....	2
1.2	OBJETIVOS.....	2
2.	LIDERAZGO.....	2
2.1	ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	2
2.2	ALCANCES Y USUARIOS.....	2
3.	POLÍTICAS.....	3
3.1	Políticas de Uso de Equipos Informáticos móviles y fijos.....	3
3.2	Políticas de seguridad de los recursos humanos.....	4
3.3	Políticas gestión de activos.....	5
3.4	Políticas gestión de medios de almacenamiento.....	6
3.5	Políticas control de acceso.....	7
3.6	Políticas seguridad física y del entorno.....	9
3.7	Política de Acceso a Redes y Servicios de Red.....	10
3.8	Política de Uso de la Información Confidencial para la Autenticación.....	11
3.9	Política de Seguridad de los Activos Fuera de las Instalaciones.....	12
3.10	Políticas puesto de trabajo despejado y pantalla limpia.....	13
3.11	Políticas uso de software no autorizados.....	14
3.12	Política de Uso de Correo Electrónico y Mensajería Electrónica.....	15
3.13	Política de Seguridad de la Información en las Relaciones con los Proveedores.....	16
4.	APOYO O SOPORTE.....	18
4.1	TOMA DE CONCIENCIA.....	18
4.2	COMUNICACIÓN.....	18
5.	EVALUACIÓN DEL DESEMPEÑO.....	19
5.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.....	19
5.2	REVISIÓN POR LA DIRECCIÓN.....	19

**Figura 19** Índice del Plan de Seguridad

	Plan de Seguridad de la	Elaborado por: Ing. Carlos Campaña
	Información para unidades	Versión Documento: 1.0
	educativas del Cantón Esmeraldas	Pag:2 de 22

## PLAN DE SEGURIDAD DE LA INFORMACION

### 1.1 ANTECEDENTES

La creación de un Plan de Seguridad de la Información para las unidades educativas del Cantón Esmeraldas surge como respuesta a la necesidad imperante de proteger los datos sensibles y mitigar los riesgos asociados a la seguridad de la información en el entorno educativo. La importancia de contar con una política de seguridad de la información radica en salvaguardar la integridad, confidencialidad y disponibilidad de los datos, así como en prevenir posibles incidentes de seguridad que podrían tener consecuencias adversas para la unidad educativa.

### 1.2 OBJETIVOS

- Establecer un marco de seguridad de la información que garantice la protección adecuada de los datos en las unidades educativas del Cantón Esmeraldas.
- Promover una cultura de seguridad informática entre el personal, estudiantes y demás miembros de la comunidad educativa.
- Mitigar los riesgos asociados a la seguridad de la información mediante la implementación de medidas preventivas y correctivas.

## 2. LIDERAZGO

### 2.1 ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

**Responsable de TIC:** Encargado de coordinar y ejecutar todas las actividades relacionadas con la seguridad de la información en la unidad educativa. Esto incluye la implementación de controles de seguridad, la supervisión de la infraestructura tecnológica y la respuesta a incidentes de seguridad.

**Máxima Autoridad de la Unidad Educativa:** Responsable de garantizar el cumplimiento de las políticas de seguridad de la información y de brindar el apoyo necesario para su implementación. Asimismo, tiene la responsabilidad de aprobar los recursos y presupuestos necesarios para mantener un adecuado sistema de gestión de seguridad de la información en la institución.

**Talento Humano:** Responsable de sensibilizar y capacitar al personal en materia de seguridad de la información y de garantizar el cumplimiento de las políticas establecidas.

### 2.2 ALCANCES Y USUARIOS

El plan se aplica en todas las unidades educativas del Cantón Esmeraldas y su alcance abarca a todo el personal, estudiantes y cualquier otra persona que tenga acceso a los recursos de información de la institución.

**Figura 20** Antecedentes, Objetivos y Alcance del Plan de Seguridad



	Plan de Seguridad de la Información para unidades educativas del Cantón Esmeraldas	Elaborado por: Ing. Carlos Campaña
		Versión Documento: 1.0
		Pág:3 de 22

### 3. POLÍTICAS

#### 3.1 Políticas de Uso de Equipos Informáticos móviles y fijos

##### Objetivo:

Garantizar el uso seguro y adecuado de los equipos informáticos móviles y fijos dentro de las unidades educativas del Cantón Esmeraldas, con el fin de proteger la integridad, confidencialidad y disponibilidad de la información.

##### Alcance:

Esta política se aplica a todo el personal, estudiantes y colaboradores que utilicen equipos informáticos móviles y fijos propiedad de la institución o que accedan a recursos tecnológicos dentro del ambiente educativo.

##### Gestión de Equipos:

Se mantendrá un inventario actualizado de todos los equipos informáticos móviles y fijos utilizados en la institución, incluyendo detalles como el número de serie, ubicación y responsable asignado.

Los equipos informáticos móviles y fijos serán utilizados únicamente para fines educativos y administrativos autorizados por la institución.

##### Seguridad de los Equipos:

Todos los equipos informáticos móviles y fijos deberán contar con medidas de seguridad adecuadas, como contraseñas seguras, actualizaciones regulares de software y software antivirus actualizado.


Se establecerán políticas de acceso basadas en roles para garantizar que cada usuario tenga acceso solo a los recursos y datos necesarios para llevar a cabo sus funciones.

##### Uso Adecuado:

Los usuarios serán responsables de utilizar los equipos informáticos móviles y fijos de manera adecuada y responsable, evitando acciones que puedan comprometer la seguridad de la información o afectar el rendimiento de los equipos.


**Figura 21** Política de Uso de Equipos Informáticos

## ANEXO E: ENCUESTA REALIZADA AL PERSONAL ADMINISTRATIVO Y DOCENTE DE LA UESDC



REPUBLICA DEL ECUADOR

**UNIVERSIDAD TÉCNICA DEL NORTE**  
 Acreditada Resolución Nro. 173-SE-33-CACES-2020  
**FACULTAD DE POSGRADO**



Cuestionario para el Trabajo de Titulación previo a la obtención del Título de Magister en Computación del tema “**DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA UNIDADES EDUCATIVAS DEL CANTÓN ESMERALDAS: ENFOQUE EN LA PROTECCIÓN DE DATOS Y RIESGOS.**”, elaborado por el Ing. Carlos Alberto Campaña Bone - Maestrante.

**Instrucciones:** Por favor, responda a las siguientes preguntas, marcando la respuesta de acuerdo con su experiencia y conocimiento en relación con la seguridad de la información en la institución educativa en la que usted trabaja.

PREGUNTAS	Nunca	Raramente	Ocasionalmente	Frecuentemente	Siempre
	5	4	3	2	1
<b>Prácticas de Seguridad</b>					
¿Cierra su sesión en los sistemas informáticos después de utilizarlos?					✓
¿Comparte su contraseña o credenciales con otros colegas?	✓				
¿Verifica la autenticidad de los correos electrónicos antes de abrir archivos o hacer clic en enlaces?		✓			
<b>Conciencia de Riesgos:</b>					
¿Es cauteloso(a) al descargar archivos de fuentes no confiables en los sistemas de la institución?			✓		
¿Toma precauciones adicionales al manejar datos sensibles de los estudiantes?			✓		
<b>Entrenamiento y Concientización:</b>					
¿Ha recibido capacitación sobre las mejores prácticas de seguridad de la información por parte del departamento de TIC?	✓				
¿Ha participado en simulacros de seguridad informática organizados por la institución?			✓		
<b>Colaboración Institucional:</b>					
¿Reporta actividades sospechosas relacionadas con la seguridad de la información a los departamentos correspondientes?				✓	
¿Coopera con los procedimientos de seguridad informática establecidos por la institución educativa?		✓			
<b>Conocimiento sobre Políticas de Seguridad:</b>					
¿Ha tenido la oportunidad de revisar y comprender completamente las políticas de seguridad de la información de la institución?	✓				

Ciudadela Universitaria Barrio El Olivo  
 Av.17 de Julio 5-21 y Gral. José María Córdova  
 Ibarra-Ecuador

**Figura 22** Encuesta realizada al personal administrativo y docente de la UESDC