UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Optimización de la seguridad de la información basada en la norma ISO/IEC 27001"

Trabajo de Integración Curricular previo a la obtención del título de Ingeniero en Ciencias de la Computación

AUTOR: Chicango Rivera Jhojan Alexis
TUTOR: Ing. Del Hierro Mosquera Milton Gabriel, Msc

Tulcán, 2025.

CERTIFICADO DEL TUTOR

Certifico que el estudiante(s) Chicango Rivera Jhojan Alexis con el número de cédula 0401611264 ha desarrollado el Trabajo de Integración Curricular: "Optimización de la seguridad de la información basada en la norma ISO/IEC 27001"

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva

Firmado electrónicamente por:
MILTON GABRIEL DEL HIERRO MOSQUERA

_____

Ing. Del Hierro Mosquera Milton Gabriel, Msc

TUTOR

Tulcán, enero de 2025

AUTORÍA DE TRABAJO

El presente Trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingeniero en la Carrera de computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Chicango Rivera Jhojan Alexis con cédula de identidad número 0401611264 declaro que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

Chicango Rivera Jhojan Alexis
AUTOR

Tulcán, enero de 2025

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo Chicango Rivera Jhojan Alexis declaro ser autor de los criterios emitidos en el Trabajo de Integración Curricular: "Optimización de la seguridad de la información basada en la norma ISO/IEC 27001" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.

Chicango Rivera Jhojan Alexis
AUTOR

Tulcán, enero de 2025

AGRADECIMIENTO

Quiero expresar mi agradecimiento a la Universidad Politécnica Estatal del Carchi y a la Carrera de Computación por proporcionarme los recursos y las facilidades necesarias para llevar a cabo esta investigación. Agradezco al personal administrativo y académico que colaboró de alguna manera en la realización del Trabajo de Integración Curricular.

También quiero agradecer al MSc. Javier Torres Director del Departamento de TIC de la UPEC y a mi tutor MSc. Milton del Hierro por sus valiosos comentarios y sugerencias que han enriquecido y mejorado esta investigación.

Por último, agradezco a mi familia y amigos cercanos por su constante apoyo emocional, motivación y paciencia a lo largo de este desafiante camino.

Chicango Rivera Jhojan Alexis

DEDICATORIA

A mis queridos padres Milton Chicango y Patricia Rivera, que a lo largo de mi vida han sido mi mayor fuente de apoyo y sabiduría. Gracias por creer en mí, por alentarme a seguir mis sueños y por brindarme todas las oportunidades para crecer. Esta tesis es el resultado de su esfuerzo y sacrificio.

A mi querida hermana Grace Chicango, gracias por estar siempre a mi lado, brindándome amor, risas y palabras de aliento.

A mi novia, Alison, por ser mi mayor apoyo y fortaleza en este camino. Gracias por acompañarme en los momentos difíciles y por celebrar cada avance conmigo. La culminación de este trabajo ha sido posible gracias al amor, la paciencia y la comprensión que me has brindado.

A mis compañeros de clase y de vida Yon Montesdeoca y Washington Castro por estar siempre presente con su apoyo a lo largo de esta carrera universitaria.

Dedico este trabajo a ustedes, que son el resultado de su amor y guía incondicional.

Chicango Rivera Jhojan Alexis

ÍNDICE

RESUMEN 14

ABSTRACT 15

INTRODUCCIÓN 16

I. EL PROBLEMA 18

1.1. PLANTEAMIENTO DEL PROBLEMA 18

1.2. FORMULACIÓN DEL PROBLEMA 19

1.3. JUSTIFICACIÓN 19

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN 20

1.4.1. Objetivo General 20

1.4.2. Objetivos Específicos 20

1.4.3. Preguntas de Investigación 21

II. FUNDAMENTACIÓN TEÓRICA 22

2.1. ANTECEDENTES DE LA INVESTIGACIÓN 22

2.2. MARCO TEÓRICO 24

2.2.1. Norma ISO Internacional 24

2.2.2. Norma ISO 27001 25

2.2.2.1. Funcionamiento de la norma ISO 27001 25

2.2.2.2. Beneficios de la norma ISO 27001 26

2.2.2.3. Fases de la norma ISO 27001 27

2.2.2.4. Directrices de la norma ISO 27001 27

2.2.3. Seguridad de la información 28

2.2.3.1. Requerimientos de la seguridad de la información 29

2.2.4. Seguridad Informática 30

2.2.5. Tipos de seguridad informática 31

2.2.5.1. Seguridad en la red 31

2.2.5.2. Seguridad de datos 31

2.2.5.3. Seguridad de aplicaciones. 31
2.2.5.4. Seguridad en la nube 32
2.2.5.5. Seguridad de la identidad 32
2.2.6. Importancia de la seguridad informática 32
2.2.7. Objetivos de la seguridad informática 33
2.2.8. Principios de la seguridad Informática 34
2.2.8.1. Disponibilidad de la información 34
2.2.8.2. Integración de la información 34
2.2.8.3. Confidencialidad de la información 34
2.2.9. Activos de la información 34
2.2.10. Activos de información pura 35
2.2.11. Riesgos informáticos 37
2.2.11.1. Ataques externos 37
2.2.11.2. Errores humanos 37
2.2.11.3. Causas naturales y sociales 38
2.2.12. Análisis de riesgos 38
2.2.13. Riegos de seguridad para la tecnología de la información 38
2.2.14. Vulnerabilidades informáticas. 39
2.2.15. Tipos de vulnerabilidades 40
2.2.15.1. Perdida de autenticación 40
2.2.15.2. Exposición de datos sensibles 40
2.2.15.3. Entidades externas XML (XXE) 40
2.2.15.4. Pérdida de control de acceso 41
2.2.15.5. Configuración de seguridad incorrecta 41
2.2.15.6. Secuencia de comandos en sitios cruzados (XSS) 41
2.2.15.7. Deserialización insegura 41
2.2.15.8. Componentes con vulnerabilidades conocidas. 41
2.2.15.9. Registro y monitoreo insuficientes 41

2.2.16. Delitos informáticos 42
2.2.16.1. Tipos de delitos informáticos 42
2.2.17. Amenazas informáticas 42
2.2.18. Plan de seguridad informática 43
2.2.19. Auditoria Informática 43
2.2.20. Tipos de auditoria informática 44
2.2.21. Auditoria según la funcionalidad a analizar 44
2.2.22. Plan de auditoría 44
2.2.23. Auditoría de cumplimiento normativo 45
2.2.24. Auditoria de politicas y procedimientos 45
2.2.25. Auditoría de seguridad de redes 45
2.2.26. Auditoría de seguridad de aplicaciones. 45
2.2.27. Auditoría de gestión de incidentes 45
2.2.28. Políticas de seguridad 46
2.2.29. Medidas de seguridad 46
2.2.30. Gestión de información 47
III. METODOLOGÍA 48
3.1. ENFOQUE METODOLÓGICO 48
3.1.1. Enfoque 48
3.1.2. Tipo de Investigación 48
3.1.2.1. Investigación de acción 48
3.1.2.2. Investigación bibliográfica documental 49
3.1.2.3. Investigación de campo 49
3.2. IDEA A DEFENDER 50
3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES 50
3.3.1. Definición de variables 50
3.3.2. Operacionalización de variables 51
3.4. MÉTODOS UTILIZADOS 53

3.4.1. Método Inductivo 53
3.4.2. Técnicas e instrumentos 53
3.4.2.1. Entrevista 53
3.4.2.2. Encuesta 54
3.4.3. Población y Muestra 54
3.5. ANÁLISIS ESTADÍSTICO 55
3.5.1. Análisis de la entrevista 55
3.5.1. RECURSOS 61
IV. RESULTADOS Y DISCUSIÓN 63
4.1. RESULTADOS 63
4.1.1. Resultados de las encuestas 63
4.1.1.1. Análisis de los ítems de la encuesta 63
4.2. PROPUESTA 72
4.2.1. Alcance de la propuesta 72
4.2.2. Estudio de factibilidad 73
4.2.3. Análisis de la situación actual 73
4.2.3.1. Análisis de la Intranet 76
4.2.3.2. Análisis de medidas de seguridad 78
4.2.3.3. Análisis de vulnerabilidades de seguridad 79
4.2.4. Diagnóstico FODA 80
4.2.5. Reflexiones y propuestas del presente 81
4.2.6. Plan de seguridad de la información 82
4.2.7. Elaboración del Plan de Seguridad de la información 82
4.2.7.1. Introducción 82
4.2.7.2. Alcance 83
4.2.7.3. Política de Seguridad 83
4.2.8. Enfoque para la Administración del Riesgo 83
4.2.8.1. Cálculo de riesgo 84

4.2.9. Análisis de riesgo 84
4.2.9.1. Identificación de activos 84
4.2.9.2. Metodología MAGERIT 84
4.2.9.3. Tasación de activos 85
4.2.10. Identificación de amenazas y vulnerabilidades 87
4.2.10.1. Clasificación de amenazas 87
4.2.11. Evaluación y análisis del riesgo 90
4.2.11.1. Valoración del Riesgo 95
4.2.12. El manejo del riesgo y el proceso de toma de decisiones 96
4.2.12.1. Toma de decisiones 96
4.2.12.2. Estrategia para reducción de riesgo 96
4.2.12.3. Aceptar el riesgo 96
4.2.12.4. Evitar el riesgo 97
4.2.13. Riesgo residual 97
4.2.14. Seleccionar objetivos de control y controles para los riesgos 97
4.2.15. Declaración de aplicabilidad 98
4.2.15.1. Esquema de Gestión de Riesgo 99
4.2.15.2. Monitoreo del Plan de Seguridad de la Información 100
4.2.15.3. Revisión de los riesgo y evaluación 100
4.3. DISCUSIÓN 101
V. CONCLUSIONES Y RECOMENDACIONES 102
5.1. CONCLUSIONES 102
5.2. RECOMENDACIONES 102
VI. REFERENCIAS BIBLIOGRÁFICAS 104
VII. ANEXOS 109

ÍNDICE DE TABLAS

Tabla 1. Familia ISO/IEC 27000 25
Tabla 2. Operacionalización de la variable independiente 51
Tabla 3. Operacionalización de la variable dependiente 52
Tabla 4. Recursos humanos 61
Tabla 5. Recursos Materiales 61
Tabla 6. Recursos Tecnológicos 62
Tabla 7. Evaluación de red interna 74
Tabla 8. Infraestructura de la Red 74
Tabla 9. Medidas de seguridad 77
Tabla 10. Análisis de Vulnerabilidades 79
Tabla 11. Incidentes de seguridad 79
Tabla 12. Matriz FODA 80
Tabla 13: Tasación de activos 85
Tabla 14: Tasación de activos de información 86
Tabla 15. Activos según MAGERIT 87
Tabla 16: Clasificación de amenazas 88
Tabla 17: Frecuencias de impacto 90
Tabla 18: Análisis del Riesgo 90
Tabla 19. Valoración del Riesgo 95
Tabla 20: Ejemplo de declaración de aplicabilidad 98
Tabla 21. Comparación entre estudios 101

ÍNDICE DE FIGURAS

Figura 1. Fases norma ISO 27001 27
Figura 2. Cambios de ISO 27001 28
Figura 3. Peligros de la seguridad en la tecnología informática 39
Figura 4. Entendimiento de la seguridad informática 63
Figura 5. Comprensión de normativas internas 64
Figura 6. Conocimiento de capacitaciones sobre seguridad 65
Figura 7. Comprensión Integral de la ISO 27001 66
Figura 8. Derechos y deberes en el manejo de datos personales 67
Figura 9. Situación actual de la institución 67
Figura 10. Seguridad de los servidores 68
Figura 11. Resolución de fallos de servicios 69
Figura 12. Salvaguarda de datos y seguridad informática 70
Figura 13. Efectividad de procedimientos manejo de datos 70
Figura 14. Topología red antigua 75
Figura 15. Topología red actual 75
Figura 16. Topología red futura 76
Figura 17: Amenazas según MAGUERIT 121
Figura 18: Certificado de Workshop ISO 27001 122
Figura 19: Certificado Ley Orgánica de Protección de Datos 122

ÍNDICE DE ANEXOS

Anexo 1: Acta de sustentación de Predefensa del TIC……109
Anexo 2: Certificado del abstract por parte de idiomas……110
Anexo 3: Entrevista al Analista de redes……111
Anexo 4: Encuesta dirigida al encargado del manejo de la intranet universitaria…114
Anexo 5: Solicitud de Validación de Instrumentos ……117
Anexo 6: Solicitud para levantamiento de información para Dirección de TIC……118
Anexo 7: Solicitud para adquirir Plan de Contingencia del Data Center……120
Anexo 8: Metodología MAGUERIT ……121
Anexo 9: Certificado de Workshop Norma ISO 27001 ……122
Anexo 10: Certificado Ley Orgánica de Protección de Datos Personales……122
Anexo 11: Plan de Seguridad de la Información para el Departamento de TIC de la UPEC……123
Anexo 12: Acta de entrega del Plan de Seguridad de la información ……124

RESUMEN

Este estudio se enfoca en el diseño de un Plan de Seguridad de la Información que se base en la norma ISO 27001 para el departamento de Tecnologías de la Información y Comunicación (TIC) de la Universidad Politécnica Estatal del Carchi. Resalta la importancia que tiene la institución contar con un documento que mitigue posibles vulnerabilidades fortaleciendo la seguridad de la información y los activos tecnológicos con los que cuenta. Los objetivos específicos incluyen justificar el uso de la norma ISO 27001, evaluar los riesgos de seguridad informática mediante la metodología MAGERIT, proponer controles adecuados y elaborar un plan integral de seguridad informática. Se subraya el valor de la metodología MAGERIT para gestionar riesgos tecnológicos y proteger los activos críticos de la universidad. Se destaca la importancia de aplicar la norma ISO 27001 y utilizar la metodología MAGERIT para garantizar la seguridad de la información en la institución. Las conclusiones destacan la importancia de un enfoque integral hacia la seguridad de la información, la cuidadosa selección de controles y la adopción de estándares internacionales como la norma ISO 27001. Se ofrecen sugerencias prácticas para implementar el Plan de Seguridad de la Información basado en la norma ISO/IEC 27001:2022, actualizar el diagrama de red y concientizar al personal sobre la importancia de la seguridad de la información, con el fin de mejorar la protección de los recursos y cumplir con los estándares de seguridad en la universidad.

Palabras Claves: ISO 27001 – MAGERIT – Plan de seguridad – Seguridad informática

ABSTRACT

This study focuses on the design of an Information Security Plan based on the ISO 27001 standard for the Information and Communication Technologies (ICT) department of the Universidad Politécnica Estatal del Carchi. It highlights the importance for the institution to have a document that mitigates possible vulnerabilities, strengthening the security of information and technological assets. The specific objectives include justifying the use of the ISO 27001 standard, assessing information security risks using the MAGERIT methodology, proposing adequate controls and developing a comprehensive information security plan. The value of the MAGERIT methodology to manage technological risks and protect the university's critical assets is highlighted. The importance of applying the ISO 27001 standard and using the MAGERIT methodology to ensure information security in the institution is highlighted. The conclusions emphasize the importance of a comprehensive approach to information security, the careful selection of controls and the adoption of international standards such as ISO 27001. Practical suggestions are offered to implement the Information Security Plan based on ISO/IEC 27001:2022, update the network diagram and raise staff awareness of the importance of information security, in order to improve the protection of resources and comply with security standards at the university.

Keywords: ISO 27001 - MAGERIT - Security plan - IT security

INTRODUCCIÓN

En la era digital, resguardar la información es una prioridad esencial para las organizaciones. En un entorno tecnológico que se vuelve cada vez más complejo y vulnerable, las empresas enfrentan diversos riesgos y amenazas que pueden poner en peligro la seguridad de sus activos informativos. La implementación de estándares internacionales como la ISO 27001 se ha convertido en una solución eficaz para abordar la gestión integral de la seguridad de la información.

En la Universidad Politécnica Estatal del Carchi (UPEC), se han identificado problemas en la gestión de la seguridad de la información y de los activos, lo que ha llevado a la pérdida de información y al desconocimiento del personal sobre las obligaciones en materia de seguridad.

El diseño de un plan de seguridad informática a medida para la Universidad resulta una herramienta fundamental para identificar, evaluar y mitigar los riesgos que puedan afectar a sus sistemas de información, activos y datos. En este sentido, la metodología MAGERIT se presenta como un marco de referencia robusto para llevar a cabo este proceso de análisis y gestión de riesgos.

El propósito de esta investigación es proponer el diseño de un Plan de Seguridad de la Información basado en la norma ISO 27001, con la finalidad de identificar posibles vulnerabilidades y riesgos en la seguridad de la información en los activos informáticos de la Universidad Politécnica Estatal del Carchi. Este enfoque integral de seguridad, basado en un estándar internacional, contribuirá a mejorar la confidencialidad, integridad y disponibilidad de los datos institucionales, reforzando la protección de los activos informativos y cumpliendo con los requisitos de seguridad necesarios.

De esta manera, se busca contribuir a la mejora de la gestión de la seguridad de la información en la UPEC y servir como referencia para otras instituciones que enfrentan desafíos similares. En pocas palabras, la investigación realizada subraya el valor de

implementar controles y medidas de seguridad bajo un estándar internacional con la finalidad de contribuir a la institución a llevar un mejor control de la información sensible que maneja diariamente.

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Según García (2021) menciona que:

> Las organizaciones utilizan la tecnología como medio para procesar, almacenar y resguardar su información, la tecnología está jugando un rol fundamental dentro del funcionamiento de sus procesos, pero que, a la vez, estos están sometidos a un elevado número de riesgos y amenazas informáticas.

La mayoría de los robos o perdidas de la información en América Latina recae sobre el sector empresarial, por lo que, Pesantes (2023) explica que estos incidentes se deben a las insuficientes medidas de protección, lo que causa pérdidas de productividad, credibilidad y competitividad que comprometen la continuidad de la organización. El uso de políticas basadas en la ISO 27001 mejoran la gestión de la seguridad de la información, pues ayudan a controlar los procesos de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información.

> En Ecuador el organismo gubernamental CNE (Consejo Nacional Electoral), para los comicios electorales del año 2023 encontró puntos críticos de control de información en el proceso de transmisión de datos correspondientes a resultados de actas y parte que se realiza también en el sistema de escrutinio, el problema se ve reflejado al no aplicar ningún plan de seguridad tecnológico que garantice y permita a los ciudadanos tener una transparente integridad de datos, así también tener en cuentas las fases del sufragio. Concejo Nacional Electoral (2023)

Además, el CNE al tener acceso a la información personal de todos los ciudadanos en la base de datos del Registro Civil deben mostrar un plan de protección de datos críticos como es el padrón electoral de acuerdo a técnicas que lo permitan mantener en cadena de custodia, así también mediante fases de control poder identificar inconsistencias y sean depuradas a tiempo evitando problemas en comicios futuros.

En la ciudad de Tulcán – Ecuador la Universidad Politécnica Estatal del Carchi específicamente en el departamento de TIC, se encontró con problemas en la gestión de la seguridad de la información y activos. La falta de políticas adecuadas, procedimientos y controles en los procesos son evidentes, en consecuencia, los usuarios no toman el mínimo cuidado en la pérdida de información, debido a un malware el cual se desconozca su origen. Las políticas de seguridad en la institución no siguen un proceso de verificación, revisión y mejora para que el personal tenga la obligación de cumplirlo dentro del ámbito laborable en el departamento.

1.2. FORMULACIÓN DEL PROBLEMA

La seguridad de la información en los activos de información de la Universidad Politécnica Estatal del Carchi no alcanza los estándares necesarios según la Norma ISO 27001, lo que compromete los datos institucionales en el año 2023.

1.3. JUSTIFICACIÓN

El departamento de TICS es uno de los pilares fundamentales de la Universidad Politécnica Estatal del Carchi, debido a que se involucra en el área tecnológica, sistemas informáticos, equipamiento, adicional se encarga principalmente de las telecomunicaciones y procesamiento de datos, entonces tienden a participar con diferentes procesos, como recursos humanos, obteniendo la mayor fuente de información.

En la institución hay que analizar muchos aspectos en cuanto a seguridad, generalmente dentro del área de TICS y seguridad física ya que no cuentan con una correcta gestión en la seguridad de la información y activos, obteniendo problemas en el incumplimiento de las políticas, perdida de conectividad hacia internet, apagones de energía eléctrica, fallos en el sistema ERP, entre otros.

La universidad debe implementar una norma que integre parámetros de seguridad para proteger los activos de información y evitar inestabilidad laboral ante los riesgos que presenta. La UPEC posee información sensible que debe ser resguardado, para ello la norma ISO 27001 propone un plan de seguridad en el área informática.

Al conocer los procesos que manejan en cada planta dentro de la institución y la importancia de los datos, se estableció el personal que tiene acceso, la cantidad de información que maneja, la integridad que tiene los datos al momento de ser modificada por el personal; lo que contribuyó al objetivo de la investigación. Se

analizó la seguridad del reglamento establecido para autorizar a los usuarios el ingreso a documentos, sea de lectura o edición, actividades que son generadas por el personal y que son resueltos por parte del departamento de TIC.

Con el presente estudio se requiere contribuir al personal del departamento de TIC y el de Redes y Telecomunicaciones en sus labores diarias; con la implementación de un Plan de Seguridad de la Información basado en la Norma ISO 27001 la cual permitirá mejorar la confidencialidad de los activos, considerando las ventajas que tiene la norma, la cual se puede adaptar a la institución al ser una entidad que maneja gran cantidad de información vulnerable.

El principal beneficiario del diseño del plan de seguridad de la información será la Universidad Politécnica Estatal del Carchi, especialmente sus departamentos de TIC y Redes y Telecomunicaciones. Al integrar políticas y normas de seguridad sobre su información y activos informáticos, la comunidad universitaria podrá cumplir con los requerimientos legales y alcanzar un alto nivel de seguridad, diferenciándose así de otras universidades competidoras.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Diseñar un Plan de Seguridad de la Información basado en la norma ISO 27001 en el departamento de TIC de la Universidad Politécnica Estatal del Carchi.

1.4.2. Objetivos Específicos

- Fundamentar bibliográficamente el uso de la norma ISO 27001 y las maneras más comunes de ataques, tecnologías de defensa y control.
- Examinar los riesgos de seguridad informática que existen en los activos de información de la UPEC, empleando la metodología MAGERIT.
- Seleccionar controles de seguridad de la información apropiados y proporcionales a los riesgos identificados, siguiendo las directrices de la norma ISO 27001.
- Proponer acuerdos de confidencialidad y políticas de seguridad tomando como base el plan de seguridad de la información para el proceso de mejora continua y buenas prácticas.

1.4.3. Preguntas de Investigación

- ¿Cómo fundamentan los estudios actuales el uso de la norma ISO 27001 en la protección de la información frente a los ataques más comunes, y cuáles son las tecnologías de defensa y control más efectivas?
- ¿Cuáles son los principales riesgos de seguridad en los activos de red de la Universidad Politécnica Estatal del Carchi, y cómo pueden ser identificados y evaluados con la metodología MAGERIT?
- ¿Cuáles son las medidas de seguridad de la información más apropiadas y proporcionales para mitigar los riesgos identificados en el entorno de la Universidad Politécnica Estatal del Carchi (UPEC), conforme a las directrices establecidas en la norma ISO 27001?
- ¿Cómo se pueden diseñar acuerdos de confidencialidad y políticas de seguridad basados en el plan de seguridad de la información, para promover el proceso de mejora continua y las buenas prácticas en una organización?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Aquí se presentan las referencias bibliográficas que se vinculan estrechamente con el tema propuesto, contribuyendo así a respaldar la investigación actual. Se han recopilado los siguientes antecedentes que fortalecen las variables de estudio, consultados en artículos científicos, revistas científicas y trabajos de titulación anteriores.

Según el estudio de Mayorga y Criollo (2021), se realiza un exhaustivo análisis de la situación actual en cuanto a la seguridad de la información dentro de la institución, tomando en cuenta los riesgos asociados a una amplia gama de amenazas potenciales. El estudio tiene como objetivo reducir estos riesgos mediante la evaluación, planificación e implementación de estrategias basadas en la versión 2013 de la norma ISO 27002.

El enfoque del estudio no solo se centra en la identificación de vulnerabilidades existentes en la infraestructura tecnológica de la institución, sino también en la definición de controles y políticas de seguridad adecuadas. Al incorporar estándares internacionales, se mejora la capacidad para detectar y mitigar vulnerabilidades en la red del GAD del municipio de Salcedo, un factor clave para prevenir tanto ataques internos como externos que puedan comprometer los sistemas de información. Esto incluye la adopción de medidas proactivas y reactivas, con el fin de salvaguardar los activos de información de manera efectiva.

Además, el estudio subraya la importancia de contar con políticas claras que regulen el acceso y manejo de la información, alineadas con las directrices internacionales y aprobadas por la junta directiva de la institución. De esta manera, no solo se asegura una respuesta adecuada ante incidentes de seguridad, sino que también se fortalece el marco de gobernanza de la información, proporcionando beneficios tangibles en términos de protección, cumplimiento normativo y mejora continua de los procesos de seguridad.

La investigación realizada por Castillo y Torres (2022), tiene como objetivo principal la implementación de un modelo preventivo estructurado basado en estándares internacionales, específicamente en la norma ISO, para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa privada Megaprofer S.A. El estudio se enfoca en analizar cómo los elementos clave del SGSI, tales como las políticas de seguridad, los sistemas de control de acceso, la gestión de activos y la seguridad del personal, sirven de base para proponer una política de seguridad actualizada y alineada con las necesidades y requisitos institucionales de la empresa.

El objetivo central de esta propuesta es establecer un marco robusto para el manejo seguro de la información, que permita implementar, mantener y mejorar continuamente el SGSI en la organización. La estructura del modelo está diseñada no solo para cumplir con los requisitos del estándar ISO, sino también para garantizar que todas las medidas de seguridad informática se adapten a los desafíos y riesgos específicos del entorno operativo de Megaprofer S.A. En el marco de este proceso, la empresa busca promover una cultura de seguridad que involucre a todo el personal, asegurando que cada miembro entienda y cumpla con las políticas de seguridad establecidas. La gestión de activos de información, junto con los controles de acceso adecuados y una rigurosa supervisión del cumplimiento, forman los pilares del sistema. Además, el enfoque en la mejora continua asegura que el SGSI evolucione conforme lo hacen las amenazas y necesidades tecnológicas de la organización, permitiendo una mayor resiliencia frente a incidentes de seguridad.

El resultado esperado de la implementación de este modelo es no solo cumplir con los estándares internacionales, sino también crear un entorno de seguridad integral que proteja la confidencialidad, integridad y disponibilidad de la información en Megaprofer S.A., garantizando su sostenibilidad a largo plazo.

Para Delgado y Vásquez (2020), en su estudio se identifica la carencia de medidas adecuadas de seguridad de la información, lo que permite desarrollar un modelo conforme a la norma ISO/IEC 27001, enfocado en la protección integral de los activos de la organización. El análisis se orienta hacia la identificación y evaluación de riesgos y amenazas, no solo de carácter económico, sino también en términos de garantizar la confidencialidad, integridad y disponibilidad de la información crítica.

La investigación tiene como objetivo implementar tecnologías especializadas en la seguridad de los sistemas de información, además de llevar a cabo auditorías

exhaustivas para evaluar su eficacia. Estos procesos contribuirán a la optimización del uso de aplicaciones y herramientas con niveles avanzados de protección, fortaleciendo la seguridad general de los sistemas informáticos de la organización.

De acuerdo con la investigación de Mayaquer y Romero (2020), el análisis realizado confirma que la adopción de un enfoque de seguridad de la información alineado con la norma ISO/IEC 27001 generará un impacto positivo en la gestión de la seguridad dentro de la organización. A partir de estos resultados, se ha determinado la necesidad de desarrollar un manual que defina directrices claras para la correcta aplicación de las políticas de seguridad de la información. Este manual estará específicamente orientado a cumplir con los lineamientos de la norma ISO/IEC 27001:2013, con un enfoque particular en la sala de cómputo del programa de Ingeniería en Computación y Redes.

En base a la guía de implementación de normas ISO presentada por NQA Certification Body (2020), da a conocer que en seguridad de la información, el riesgo se gestiona mediante el diseño, implementación y mantenimiento de controles como ventanas bloqueadas, pruebas de software o la ubicación de equipos vulnerables por encima de la planta baja. Un SGSI que cumple con la ISO 27001 tiene un conjunto interrelacionado de procesos de mejores prácticas que facilitan y respaldan el diseño, implementación y mantenimiento de los controles. Los procesos que forman parte del SGSI suelen ser una combinación de procesos comerciales centrales existentes, por ejemplo, reclutamiento, inducción, capacitación, compras, diseño de productos, mantenimiento de equipos, prestación de servicios y aquellos específicos para mantener y mejorar la seguridad de la información.

2.2. MARCO TEÓRICO

2.2.1. Norma ISO Internacional

Las normas ISO representan un conjunto de estándares reconocidos internacionalmente que han sido desarrollados con el objetivo de facilitar la homogeneidad en las prácticas de gestión, prestación de servicios y desarrollo de productos a nivel global. (Normas ISO, 2023).

Tabla 1. Familia ISO/IEC 27000

ISO 27000	Vocabulario estándar para el SGSI.
ISO 27001	Especifica los requisitos para la implantación del SGSI.
ISO 27002	Código de buenas prácticas para la gestión de seguridad de la información.
ISO 27003	Directrices para la implementación del SGSI.

2.2.2. Norma ISO 27001

La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva (Normas ISO, 2023).

La norma ISO 27001 tiene como objetivo primordial resguardar la confidencialidad, integridad y accesibilidad de la información. La norma ofrece una estructura para la seguridad de la información que facilita a las organizaciones la identificación y gestión efectiva de los riesgos relacionados con la seguridad de los datos.

2.2.2.1. Funcionamiento de la norma ISO 27001

ISO 27001 es una norma internacional que garantiza la seguridad, confidencialidad e integridad de los datos y la información y sus sistemas de procesamiento. La norma ISO 27001:2013 para sistemas de gestión de seguridad de la información permite a las organizaciones evaluar los riesgos y aplicar las medidas de control necesarias para mitigarlos o prevenirlos. Según Apia (2022), menciona que "La certificación ISO 27001 es esencial para proteger sus activos más importantes, la información de sus clientes y empleados, la imagen corporativa y otra información privada".

Un enfoque de la ISO 27001 es ayudar a establecer formas de coordinación y comunicación entre todas las secciones de una organización, a generar una cultura de seguridad y a mejorar la responsabilidad de la gestión; impulsa la evaluación y la mejora por medio de auditorías internas, acciones correctivas y preventivas.

La ética de la clasificación ISO 27001 es canalizar la percepción de inseguridad de forma proporcional: entender dónde están los peligros y luego abordarlos con cuidado. Dado que esta parte de la ejecución requerirá la gestión de múltiples

políticas, métodos, usuarios, recursos, etc., ISO 27001 ha determinado cómo bloquear todos estos fondos en un sistema de gestión de documentos.

2.2.2.2. Beneficios de la norma ISO 27001

La norma ISO 27001 es certificable, lo que posibilita que las organizaciones demuestren su compromiso y cumplimiento con los más altos estándares y prácticas en seguridad de la información, generando confianza tanto en clientes como en proveedores. Esta certificación conlleva una serie de beneficios adicionales:

- Comunicar a clientes, proveedores y grupos de interés que la seguridad es una de las prioridades de la empresa.
- Identificar los principales riesgos en materia de seguridad informática y establecer controles para gestionarlos o eliminarlos.
- Clasificar los riesgos en función de su gravedad y posibilidades reales de que se lleguen a producir.
- Adaptar y alinear los controles a todas las áreas de la empresa.
- Crear confianza en los clientes y partes interesadas de que sus datos están debidamente protegidos.
- Cumplir con los requisitos y demostrar conformidad y compromiso con los mismos.
- Cumplimiento de las leyes y reglamentos pertinentes reduciendo así la posibilidad enfrentarse a multas y sanciones.
- Proporcionar el marco más adecuado para la gestión de la seguridad de la información.
- Proteger la reputación de la empresa.
- Ahorrar costes por la reducción de incidentes.
- Implementar procedimientos para permitir la detección oportuna y a tiempo de brechas de seguridad.
- Asegurar que los usuarios que sí están autorizados tengan acceso a la información en el momento en que lo necesitan.
- Se fortalece la organización interna y los procesos de mejora continua.

Es importante saber que esta regulación posibilita la confidencialidad, integridad, disponibilidad y legalidad de la información proporcionada, con el fin de salvaguardar contra posibles riesgos. (Kosutic, 2021).

2.2.2.3. Fases de la norma ISO 27001

Los requisitos establecidos en la norma ISO 27001 sientan las bases para la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y resiliente, capaz de proteger la información de la organización en todo momento y ante cualquier amenaza (Riveros, 2023).

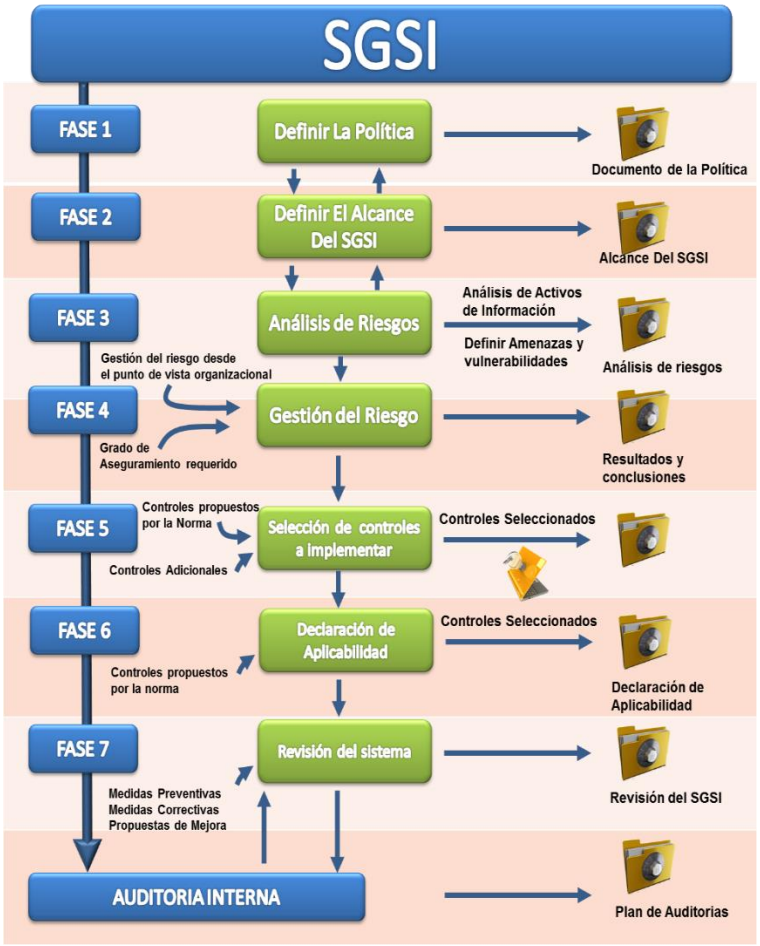

Figura 1. Fases norma ISO 27001
Fuente: (Normas ISO, 2020)

2.2.2.4. Directrices de la norma ISO 27001

Las recomendaciones de seguridad de la información se basan en ISO / IEC 27001.

- Tecnología de la información o también conocida como TI.
- Medidas de seguridad.
- Código de buenas prácticas para la gestión de la seguridad de la información.

Figura 2. Cambios de ISO 27001
Fuente: (Peñafiel, 2022)

2.2.3. Seguridad de la información

La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO / IEC 27000, establece una implementación efectiva de la seguridad de la información empresarial desarrolladas en las normas ISO 27001 / ISO 27002.

De manera detallada podemos encontrar los requerimientos en la norma ISO/IEC 27001 para lograr conservar beneficios específicos que se asocia a su implementación mediante los de controles de seguridad basados en las necesidades que proyecta la institución, brindando un servicio o una acción en específico, dependiendo de los objetivos y los alcances del SGSI que se definan. (Normas ISO, 2020).

En la actualidad, la seguridad de la información se ha convertido en un elemento crucial para el desarrollo de cualquier empresa. Esto es especialmente evidente dada la importancia indiscutible de las nuevas tecnologías de la información y la comunicación. Estas tecnologías desempeñan un papel fundamental en la

promoción de los productos y servicios de una empresa, así como en la comunicación de sus ventajas y beneficios a los consumidores.

Es importante tener en cuenta que el progreso en seguridad de la información ha ido evolucionando de forma gradual, a medida que se ha hecho evidente la necesidad de desarrollar nuevas tecnologías de la información y la comunicación para garantizar el cumplimiento de los objetivos empresariales establecidos. Este avance se fundamenta en la clara ventaja que la informática ofrecía en la manipulación de datos.

2.2.3.1. Requerimientos de la seguridad de la información

Debe tomarse en cuenta que los requisitos demandados para el acceso del cliente a la información de una empresa u organización son varios en dependencia del tipo de herramienta utilizada para el procesamiento de la información, así como el tipo de información que se recepciona. Del mismo modo debe destacarse que los requisitos de seguridad estarán contemplados en el anexo del acuerdo dado por la parte contratante destacándose los riesgos y demandas inherentes a la seguridad, de ahí que el acceso a la información por parte de terceros solamente podrá llevarse a cabo a partir de la autorización expresa de la organización. (Latorre, 2020).

Es importante tener en cuenta que los criterios requeridos para que un cliente obtenga acceso a la información de una empresa u organización difieren según la herramienta empleada para el procesamiento de datos y la naturaleza de la información en cuestión. Igualmente, resulta crucial subrayar que los requisitos de seguridad se especificarán en el anexo del contrato suministrado por la parte contratante, resaltando los riesgos y las exigencias vinculadas a la seguridad.

Los requisitos de seguridad de la información están vinculados con la necesidad urgente de establecer un sistema de gestión de la información que sea ágil y funcional. Este sistema debe implementar medidas de control en el acceso a los datos y, al mismo tiempo, tener la capacidad de realizar investigaciones eficientes ante cualquier incidente relacionado con la información.

Es fundamental resaltar que el fortalecimiento de la seguridad de la información establece pautas exhaustivas para realizar acciones concretas de supervisión y verificación de informes asociados con el uso de la información de la entidad. Estas medidas contribuyen de manera beneficiosa a la gestión y control de dicha

información mediante la implementación de programas y estrategias cibernéticas, facilitando así la resolución efectiva de los desafíos que puedan surgir.

2.2.4. Seguridad Informática

La seguridad informática puede parecer lo mismo. Sobre todo, si se tiene en cuenta que el desarrollo y la evolución de la tecnología tiende hacia el modelo de digitalizar y manejar cualquier tipo de información mediante un sistema informático. (Saeckel, 2021).

Podemos mencionar lo dicho por Triviño (2020):

> Es importante destacar que la seguridad informática se revela como un concepto abarcador que engloba todo el conjunto de acciones y medidas de seguridad dirigidas al espacio cibernético tales como: programas antivirus, firewalls entre otros, así como también el uso de funciones específicas del software, como Java Script, ActiveX que redundan en el uso óptimo de los recursos de la web. (p. 25)

La ciberseguridad adquiere una relevancia crucial al implementar medidas para evitar intentos de robo de información, datos, activos financieros y contraseñas, entre otros elementos ampliamente utilizados en una sociedad moderna que está experimentando un aumento exponencial en el uso de tecnologías de la información y la comunicación.

En el ciberespacio, se presentan diversas amenazas que aumentan considerablemente con la expansión del uso de este en actividades laborales, económicas, culturales, comunicativas, entre otras. Por esta razón, la seguridad informática se percibe como una necesidad fundamental en la actualidad, esencial para asegurar el desarrollo sistemático de la sociedad. (Latorre, 2020).

Con el avance de las tecnologías de la información y la comunicación, ha surgido la figura problemática del "hacker". Este término se refiere a individuos con intenciones delictivas que poseen el conocimiento técnico, la destreza y habilidades necesarias para representar una amenaza a los sistemas informáticos. Estos hackers realizan actividades como la extracción de información y activos financieros, lo que podría comprometer la integridad y el funcionamiento de las empresas y organizaciones que utilizan el ciberespacio.

2.2.5. Tipos de seguridad informática

Dentro de la seguridad informática podemos encontrar algunos tipos como los que da a conocer Coppola (2023):

- Seguridad de red
- Seguridad de datos
- Seguridad de aplicaciones
- Seguridad de la nube
- Seguridad de la identidad

2.2.5.1. Seguridad en la red

La seguridad en la red se enfoca en la protección de la red de una empresa u organización, mediante medidas de protección que identifiquen y repelen amenazas externas, hackers, malware y virus (Chavez, 2024).

Es importante destaca la importancia de implementar y mantener estrategias de seguridad en la red para proteger los sistemas informáticos de empresas u organizaciones de amenazas cibernéticas, como hackers, malware y virus, con un enfoque preventivo y proactivo.

2.2.5.2. Seguridad de datos

Esta categoría de seguridad es esencial, dado que se enfoca en resguardar la información durante su recolección y administración. De esta manera, se salvaguarda la integridad de la información de la empresa, incluyendo los detalles de los clientes, los informes financieros y los registros de los empleados. Sin duda, la prevención de la pérdida de datos es un componente fundamental de la seguridad informática (Delgado, 2022).

La importancia de una categoría de seguridad que se enfoca en proteger la información durante su ciclo de vida, con un énfasis en la prevención de la pérdida de datos. Esta categoría abarca una amplia gama de información crítica para la empresa y es esencial en el campo de la seguridad informática.

2.2.5.3. Seguridad de aplicaciones.

La protección de las aplicaciones empresariales es de gran relevancia para el funcionamiento óptimo de una organización. Esta zona se centra en proteger las

aplicaciones esenciales para una empresa, como el correo electrónico, la mensajería instantánea y el software personalizado que se utiliza (Nillim, 2023).

Proteger las aplicaciones es esencial para garantizar el funcionamiento óptimo de una organización. Se centra en proteger las aplicaciones fundamentales de la empresa, como el correo electrónico, la mensajería instantánea y los programas personalizados, con el objetivo de garantizar la continuidad del negocio y salvaguardar la integridad de las operaciones comerciales.

2.2.5.4. Seguridad en la nube

Esta categoría de seguridad es específica, aunque su alcance se extiende a diversas plataformas y programas que funcionan en entornos de almacenamiento en la nube. Su propósito es resguardar tanto los datos como las aplicaciones que se encuentran alojados en la nube, abarcando la protección de la infraestructura y la integridad de la información almacenada en estos entornos (Chaloupka, 2024).

Se detalla un tipo particular de seguridad dedicado a los entornos de almacenamiento en la nube. Esta área se concentra en proteger la infraestructura, las aplicaciones y la integridad de los datos, siendo crucial para garantizar la seguridad y fiabilidad de estos entornos, siendo una pieza clave en la seguridad informática contemporánea.

2.2.5.5. Seguridad de la identidad

Esta área se relaciona con preservar la identidad en línea tanto de los empleados como de los clientes, abarcando el manejo de acceso y la verificación de usuarios, lo que implica la utilización del SSO (Inicio de sesión único) (Guelmann, 2024).

Nos menciona la importancia de preservar la identidad digital tanto de empleados como de clientes, haciendo hincapié en la gestión de acceso, autenticación de usuarios y la utilización de herramientas como el SSO. Esta área de seguridad es esencial para garantizar la protección de los datos y la privacidad en entornos digitales.

2.2.6. Importancia de la seguridad informática

La seguridad de la información se ha convertido en una agenda prioritaria a lo largo del tiempo, todos sabemos que la seguridad en la calle es importante, pero hoy en día la prioridad también es lo que no puedes ver y lo que te puede dejar vulnerable.

Por lo tanto, Garmendia (2020) plantea que la necesidad de seguridad informática ha surgido como respuesta a los significativos cambios en el sector productivo y al modo en que la sociedad global experimenta la transformación digital. En este contexto, la información se ha convertido en uno de los activos más valiosos tanto para empresas como para individuos. Para preservar la integridad de sus datos, es esencial invertir en seguridad informática. Esta disciplina se dedica a prevenir y detectar el acceso no autorizado a sistemas informáticos, ofreciendo protección contra intrusos que buscan utilizar herramientas o datos empresariales de manera maliciosa o con la intención de obtener beneficios ilegítimos.

2.2.7. Objetivos de la seguridad informática

Tanto las empresas con fines de lucro como aquellas sin ánimo de lucro deben establecer un marco conceptual que se sustente en políticas, reglas, procedimientos y estándares de seguridad de la información, especialmente en lo que respecta a las tecnologías utilizadas para respaldar sus operaciones productivas. Esto no solo proporciona un enfoque estructurado, sino que también ofrece flexibilidad en términos de conformidad y simplificación de las actividades comerciales. (Fernández, 2020).

La seguridad constituye una etapa esencial en cualquier sistema, ya sea computarizado o no, indicando que cierta parte del sistema carece de vulnerabilidades. Sin embargo, enfocarse en alcanzar un sistema completamente seguro no es práctico. Los expertos en seguridad informática subrayan que la sorprendente realidad es la inexistencia de sistemas 100% seguros. Por lo tanto, se vuelve imperativo centrarse en los principios fundamentales de integridad, confidencialidad y disponibilidad de la información. (Sevillano y Beltrán, 2021).

Todas las organizaciones, ya sean con fines lucrativos o sin ánimo de lucro, deben establecer un conjunto de principios esenciales respaldados por políticas, normativas, métodos y criterios de seguridad de la información asociados con las tecnologías utilizadas para respaldar sus operaciones productivas. Esta medida no solo les brinda mayor adaptabilidad, sino que también simplifica las operaciones comerciales, facilitando así el cumplimiento de requisitos y la eficiencia en sus actividades.

2.2.8. Principios de la seguridad Informática

2.2.8.1. Disponibilidad de la información

El principio de accesibilidad de la información o activos de información es fundamental en seguridad informática, garantizando un acceso fiable y oportuno a los datos y recursos por parte de las personas autorizadas.

Conforme a las mejores prácticas y estándares internacionales de seguridad de la información de la serie ISO 27000, el acceso a la información debe regirse por el principio de necesidad. Esto significa que solo aquellos que necesitan conocer la información pertinente deben tener acceso a la misma. (Pérez, 2020).

2.2.8.2. Integración de la información

La integridad es uno de los principios de la seguridad informática. Su aplicación permite mantener intacta la información ante un incidente o intento malicioso interno y/o externo.

El objetivo fundamental de mantener la integridad de un sistema informático es prevenir alteraciones no autorizadas en la información. Así, podemos garantizar que la información es precisa, válida y no ha sido manipulada por terceros. (Haider, 2024).

2.2.8.3. Confidencialidad de la información

La confidencialidad, como principio esencial de la seguridad de la información, asegura el nivel necesario de secreto en el manejo de la información, tanto en su almacenamiento como durante su transmisión, con el fin de prevenir su divulgación no autorizada. (Morales, 2020).

Se destaca la importancia de la confidencialidad como un principio esencial de la seguridad de la información. Se enfoca en garantizar un nivel adecuado de secreto en todas las etapas del manejo de la información, tanto durante su almacenamiento como en su transmisión. La mención de secreto sugiere la necesidad de mantener la información protegida y accesible solo para aquellos autorizados.

2.2.9. Activos de la información

Lo más auténtico en posesión de la empresa u organización, se encuentra distribuido en diversas categorías dentro de medios como papel o plataformas digitales. Cada activo informativo tiene asignado un responsable, comúnmente el titular del proceso,

encargado de implementar las medidas requeridas para preservar dichos activos bajo su responsabilidad. (Arévalo, 2021).

Los recursos informativos representan el activo más preciado para cualquier empresa u organización, manifestándose en variados formatos, ya sea en documentos impresos o en entornos digitales. Cada elemento informativo cuenta con un custodio, generalmente el dueño del proceso, quien asume la responsabilidad de adoptar las medidas esenciales para resguardar y conservar estos activos bajo su tutela.

2.2.10. Activos de información pura

Ya que los activos de información son sujetos a cambios constantes, la situación puede variar significativamente en el futuro, ya sea en semanas, meses o años. Por eso, es aconsejable mantener actualizado el inventario de activos, incluyendo la revisión del Sistema de Gestión de Seguridad de la Información (Grupo ESG, 2020)

Datos digitales

- Personales
- Financieros
- Legales
- Investigación y desarrollo
- Estratégicos
- Comerciales
- Correo electrónico
- Contestadores automáticos
- Bases de datos
- Unidades lógicas
- Copias de seguridad

Activos tangibles

- Personales
- Financieros
- Legales
- Investigación y desarrollo
- Estratégicos y comerciales
- Correo electrónico
- Otros materiales de copia de seguridad

- Llaves de oficinas
- Otros medios de almacenamiento

Activos intangibles

- Conocimiento
- Relaciones
- Secretos comerciales
- Licencias
- Patentes
- Experiencia
- Conocimientos técnicos
- Imagen corporativa
- Marca
- Reputación comercial
- Confianza de los clientes
- Ventaja competitiva
- Ética
- Productividad

Software de aplicación

- Propietario desarrollo por la organización
- Cliente
- Planificación de recursos empresariales
- Gestión de la información
- Utilidades
- Herramientas de bases de datos
- Aplicaciones de comercio electrónico
- Middleware

Sistemas operativos

- Servidores
- Ordenadores de sobremesa
- Ordenadores contrales
- Dispositivos de red
- Dispositivos de mano e incrustados

2.2.11. Riesgos informáticos

Las amenazas cibernéticas pueden surgir en cualquier instante, desencadenando incidentes que potencialmente afectan la información o los recursos informáticos. Es fundamental considerar que los ataques, llevados a cabo por terceros, pueden resultar en perjuicios directos a la información, la infraestructura, o generar considerables inconvenientes en el funcionamiento de la organización.

Para realizar un análisis de riesgos efectivo, el primer paso es identificar todos los activos de la empresa. Estos activos incluyen todos los recursos relacionados con la gestión e intercambio de información comercial, como software, hardware, canales de comunicación, documentos digitales y manuales, e incluso recursos humanos. (Rodriguez, 2020).

2.2.11.1. Ataques externos

Aunque los sistemas informáticos pueden estar altamente protegidos, los ciberdelincuentes suelen aprovechar ciertas vulnerabilidades para llevar a cabo ataques. García (2023) nos muestra los ataques más conocidos tenemos los siguientes:

- **Phishing:** Una técnica para engañar a las personas a través de mensajes fraudulentos para que revelen información confidencial o realicen acciones por voluntad propia)
- **Ransomware:** Implica el secuestro de datos y el bloqueo del dispositivo electrónico.
- **Malware:** Un código malicioso que puede perjudicar los equipos informáticos para robar y borrar datos. Inyección SQL: Un tipo de ataque que consiste en infiltrar un código malicioso para aprovechar errores y vulnerabilidades de una página web.

2.2.11.2. Errores humanos

La intervención de personas en los procesos informáticos siempre implica la posibilidad de cometer errores, ya sea de manera deliberada o accidental. La carencia de conocimientos y formación puede resultar en fallos que pongan en riesgo la integridad de los datos o provoquen problemas en el funcionamiento de los sistemas (Pous, 2022).

La participación de individuos en los procedimientos informáticos siempre acarrea la posibilidad de errores, tanto de forma intencionada como fortuita. La falta de conocimientos y capacitación puede desencadenar fallas que comprometan la integridad de los datos o causen disfunciones en el funcionamiento de los sistemas, lo cual podría desencadenar consecuencias no deseadas y afectar la eficiencia operativa.

2.2.11.3. Causas naturales y sociales

En momentos de emergencia causados por crisis o desastres naturales, a menudo se observa una reducción en la aplicación de protocolos de vigilancia y en las medidas de seguridad. En estas circunstancias, los ciberdelincuentes se valen de esta situación para realizar actividades dañinas que pasan desapercibidas, ya que los recursos y la atención se centran en la urgencia del momento (Lorenzo, 2024).

2.2.12. Análisis de riesgos

El análisis de riesgos no puede prevenir la aparición de problemas, ayuda a abordar adecuadamente los problemas que han surgido en la empresa, de forma que exista una situación real en la que se tengan en cuenta tanto los factores positivos como los negativos (Santos, 2023).

En resumen, el análisis de riesgos aumenta la confianza de los involucrados porque asegura que las decisiones y acciones a tomar sean cuidadosamente evaluadas. Además, el análisis de riesgos le permitirá desarrollar planes de contingencia para cualquier contratiempo que entre en conflicto con su plan, lo que le facilitará responder adecuadamente y tomar los siguientes pasos para superar el problema.

2.2.13. Riegos de seguridad para la tecnología de la información

Los riesgos de seguridad en el campo de la tecnología de la información representan un punto crítico para las instituciones que manejan información privada y personal de manera regular. Una violación a sus sistemas de seguridad informática podría acarrear graves consecuencias, incluida la potencial divulgación de información confidencial, lo que podría resultar en implicaciones legales significativas para la institución. Además, esta vulnerabilidad de seguridad también podría resultar en pérdidas financieras que afectarían la integridad y el funcionamiento de la entidad.

Si se detectan sistemas de seguridades informáticas débiles y poco eficaces frente a la amenaza de ataques cibernéticos, las empresas, organizaciones o instituciones

que los utilizan podrían enfrentar problemas graves debido a la falta de comprensión de los riesgos asociados con las deficiencias en la seguridad informática. Esto resultaría de una insuficiente validación de la información procesada por estos sistemas. Como resultado, los atacantes podrían encontrar vías reales para infiltrarse en los sistemas de seguridad, lo que podría comprometer la funcionalidad del sistema operativo empleado y, como consecuencia, dar lugar a la pérdida de toda la información contenida en él.

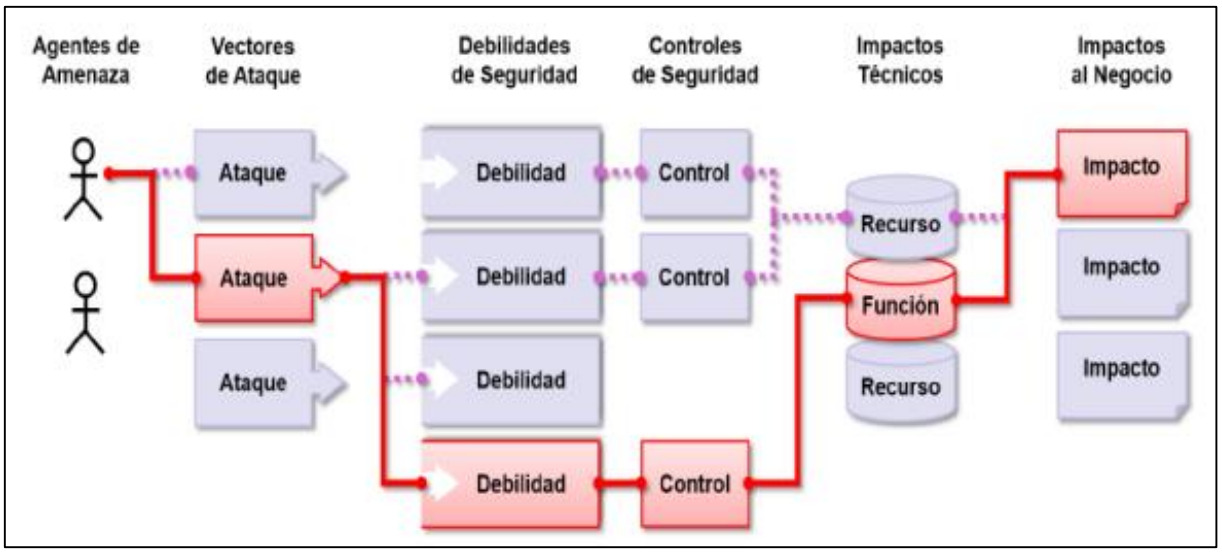

Figura 3. Peligros de la seguridad en la tecnología informática.
Fuente: (OWASP, 2020)

2.2.14. Vulnerabilidades informáticas.

Una vulnerabilidad se define como una fragilidad en un sistema que una persona con intenciones maliciosas puede aprovechar para comprometer su seguridad. Estas debilidades pueden manifestarse en diversos aspectos, ya sea en el hardware, el software, los procedimientos o incluso en las acciones humanas, y están susceptibles a ser explotadas por atacantes con el objetivo de causar daño u obtener acceso no autorizado. (Michali, 2022).

Dentro del campo informático, el término "vulnerabilidad" alude a una fragilidad intrínseca en un sistema que podría ser explotada por individuos con intenciones maliciosas para poner en peligro su seguridad. Estas debilidades pueden materializarse en distintos aspectos, ya sea en relación con el hardware, el software, los procedimientos o incluso errores humanos, y están susceptibles de ser utilizadas por aquellos que buscan llevar a cabo ataques o comprometer la integridad del sistema.

2.2.15. Tipos de vulnerabilidades

Es fundamental señalar que existen múltiples debilidades en las tecnologías de la información y la comunicación, las cuales varían según el servicio que estas tecnologías ofrecen. Siguiendo las directrices del proyecto OWASP (Proyecto de seguridad de aplicaciones web abiertas), se pueden identificar de manera más notoria las siguientes vulnerabilidades (Toapanta, 2024):

- Pérdida de autenticación
- Exposición de datos sensibles
- Entidades externas XML (XXE)
- Pérdida de control de acceso
- Configuración de seguridad incorrecta
- Secuencia de comandos en sitios cruzados (XSS)
- Deserialización insegura
- Componentes con vulnerabilidades conocidas
- Registro y monitoreo insuficientes

2.2.15.1. Perdida de autenticación

Esta vulnerabilidad está vinculada a la autenticación y al manejo de sesiones, con la finalidad de comprometer usuarios, contraseñas, tokens de sesiones u otras deficiencias, permitiendo la asunción temporal o permanente de la identidad de otros usuarios.

2.2.15.2. Exposición de datos sensibles

Algunos desarrollos y API no garantizan una protección adecuada de datos sensibles, como información financiera, de salud o Información Personalmente Identificable (PII). Esto puede posibilitar que personas no autorizadas accedan, roben o modifiquen datos sensibles, dando lugar a la comisión de fraudes, robos de identidad u otros delitos.

2.2.15.3. Entidades externas XML (XXE)

La vulnerabilidad denominada XXE (External Entity XML) hace referencia a ataques de entidad externa que implican la manipulación del procesamiento XML de una aplicación. Esta debilidad posibilita el acceso a archivos del servidor, la exploración de puertos en la red local (LAN), la ejecución de código y la realización de ataques de denegación de servicio (DoS).

2.2.15.4. Pérdida de control de acceso

Esta problemática surge cuando no existen restricciones adecuadas en las funciones disponibles para los usuarios autenticados, resultando en accesos no autorizados a características, datos, archivos, permisos y otros elementos.

2.2.15.5. Configuración de seguridad incorrecta

Esta circunstancia ocurre con regularidad en las aplicaciones debido a la configuración inadecuada de permisos en la nube, la utilización de cuentas predeterminadas o de prueba con contraseñas genéricas, mensajes de error que proporcionan excesivos detalles, la falta de actualización de frameworks, dependencias y componentes, entre otros factores.

2.2.15.6. Secuencia de comandos en sitios cruzados (XSS)

La ejecución de scripts ocurre al enviar información no confiable directamente al navegador web, permitiendo la ejecución de comandos en el navegador del usuario. Este procedimiento puede resultar en la obtención de las credenciales de acceso del usuario, la alteración de sitios web o el redireccionamiento del usuario hacia páginas maliciosas.

2.2.15.7. Deserialización insegura

Se identifica una vulnerabilidad en el proceso de deserialización que se torna riesgosa al utilizar datos no confiables para manipular la lógica de una aplicación. Esta manipulación o eliminación de objetos puede dar lugar a ataques de repetición, inyecciones o ejecución de código remoto en el servidor.

2.2.15.8. Componentes con vulnerabilidades conocidas.

Si alguno de los componentes, ya sea bibliotecas, frameworks o módulos, de una aplicación presenta vulnerabilidades, la propia aplicación puede volverse susceptible a ataques, con el riesgo de pérdida de datos o incluso acceso no autorizado al servidor.

2.2.15.9. Registro y monitoreo insuficientes

La ausencia de una supervisión de registros adecuada, un monitoreo insuficiente y respuestas inadecuadas a diversos incidentes pueden dar lugar a ataques, manipulación o robo de información. Esta vulnerabilidad se encuentra en la responsabilidad del equipo encargado de la administración de la aplicación.

2.2.16. Delitos informáticos

Promover la importancia de los delitos informáticos o ciberdelincuencia que nos preocupan y la gama de riesgos asociados a la navegación por la red utilizando las tecnologías de la información y la comunicación, en adelante denominadas TIC, que son herramientas necesarias y de uso habitual por parte de los ciberdelincuentes. cometer crimenes.

Para los usuarios habituales de este medio, cuando pensamos en delitos informáticos famosos, nos vienen a la mente los espectros de los hackers que delinquen como peligrosos delincuentes navegando por la red; Privacidad de datos, comunicación, propiedad, fe pública, libertad sexual, etc. violaciones necesitamos saber que los ciberdelincuentes están haciendo estas cosas detrás del anonimato. (Derecho Ecuador, 2020).

2.2.16.1. Tipos de delitos informáticos

Esto se considera una debilidad en el sistema que permite que sea atacado y comprometido. Las vulnerabilidades generalmente son causadas por una protección insuficiente contra ataques externos, actualizaciones faltantes, errores de programación y otras razones similares (Pazan, 2022).

Una amenaza representa la probabilidad de que un sistema vulnerable sea objeto de un ataque y comprometido. Las amenazas a los sistemas informáticos generalmente se originan en ataques externos, como malware, denegación de servicio, o inyección SQL, así como en violaciones de políticas de seguridad, como la conexión de dispositivos no autorizados a la red o el uso de contraseñas débiles. Además, eventos fortuitos como incendios o robos físicos también constituyen amenazas potenciales.

El riesgo es la posibilidad de que un sistema esté expuesto a un incidente de seguridad y la amenaza se materialice, causando múltiples daños. Evaluar el riesgo de un sistema informático requiere suponer que existe una vulnerabilidad sin protección. Así, el riesgo es la probabilidad de que una amenaza se materialice al explotar una vulnerabilidad existente. (Acosta, 2020).

2.2.17. Amenazas informáticas

Una amenaza informática es cuando los piratas informáticos intentan obtener acceso a su computadora, dispositivo y/o servidor con intenciones maliciosas. Estos

ataques, dependiendo de lo que sea, se pueden realizar a través de correos electrónicos falsificados, haciendo clic en anuncios maliciosos, etc.

Los motivos principales que impulsan a los piratas informáticos a llevar a cabo amenazas cibernéticas incluyen la obtención de números de tarjetas de crédito y contraseñas de las víctimas, la interrupción de conexiones a Internet, la infección de múltiples computadoras, y la obtención de información bancaria. (López, 2021).

2.2.18. Plan de seguridad informática

Es la cadena de decisiones la que determina los caminos futuros de gestión, así como los medios que se utilizarán para lograrlos. Mientras que Washington (2021), especifica que:

> Los planes de seguridad informática son medidos que puedes tomar para proteger los recursos de tu negocio y minimizar los riesgos informáticos. Pueden incluir acciones sencillas, como cambiar las contraseñas de vez en cuando, o tareas más complicadas, como hacer una copia de seguridad periódica de los recursos.

Las estrategias de seguridad informática son medidas que puedes implementar para resguardar los recursos de tu negocio y reducir los riesgos relacionados con la informática. Estas medidas pueden abarcar desde acciones simples, como cambiar las contraseñas regularmente, hasta tareas más complejas, como realizar copias de seguridad periódicas de los recursos.

2.2.19. Auditoria Informática

La auditoría informática es el procedimiento de examinar los recursos de tecnologías de la información de una empresa con el fin de evaluar su estado y nivel de seguridad actual. Este proceso tiene como objetivo identificar vulnerabilidades y violaciones a las políticas de seguridad, con la finalidad de prevenir posibles incidentes y fortalecer el nivel de protección y seguridad en toda la organización. (Ponce, 2023).

A pesar de que una empresa cuente con sistemas de ciberseguridad, los ataques continúan evolucionando y se esfuerzan por encontrar vulnerabilidades para acceder a sistemas.

En una auditoría de seguridad informática, se examinan principalmente objetivos como la identificación de vulnerabilidades y riesgos en las redes y sistemas de la organización, la evaluación del cumplimiento de las políticas y medidas de seguridad

implementadas, y la determinación de las acciones necesarias para abordar los problemas identificados.

2.2.20. Tipos de auditoria informática

Podemos encontrar dos clasificaciones si hablamos de tipos de auditoría de seguridad informática. Si atendemos a quien la realiza encontramos dos variantes:

- Auditoría externa: la realiza personal ajeno a la organización.
- Auditoría interna: se encargan personas que trabajan directamente para la empresa.

2.2.21. Auditoria según la funcionalidad a analizar

(Vive, 2020) nos plantea las siguientes auditorias:

- Auditoría forense: se realiza tras producirse algún incidente de ciberseguridad con el objetivo de recuperar pruebas que evidencien las causas y a qué le ha afectado.
- Auditoría web: se busca conocer las vulnerabilidades sobre los servicios web y aplicaciones de la organización.
- Auditoría de redes: todos los dispositivos que se conectan a redes son analizados para controlar su seguridad.
- Auditoría de código: este tipo de auditoría de seguridad informática se realiza sobre aplicaciones y programas.
- Hacking ético: consiste en lanzar un test de intrusión tal y como haría un atacante real. Es tarea del hacker ético.
- Auditoría física: tiene como objetivo proteger la zona perimetral para verificar que todo funciona bien (cámaras, medidas de acceso…).
- Auditoría de vulnerabilidades: se buscan agujeros de seguridad informática y en las contraseñas.

2.2.22. Plan de auditoría

Albarrán (2020), afirma que se detalla de manera general el procedimiento con cada una de sus actividades o acciones correspondientes con el tiempos adecuado y sostenible determinando que se realice de manera eficiente las gestiones pertinentes, obteniendo resultados apropiados para establecer controles o normativas.

Se describe de manera amplia el proceso, incluyendo todas sus etapas o actividades junto con los plazos adecuados y sostenibles. Esto asegura que se realicen de manera

efectiva las tareas necesarias, generando resultados adecuados que permiten establecer controles o directrices.

2.2.23. Auditoría de cumplimiento normativo

El propósito de esta revisión es evaluar si una empresa cumple con los requisitos legales y normativos relacionados con la seguridad de la información. Esto implica garantizar el cumplimiento de normativas de protección de datos, regulaciones específicas de sectores particulares, como PCI-DSS para la industria de pagos con tarjeta, o estándares globales como la ISO 27001 (Merinas, 2021).

2.2.24. Auditoria de politicas y procedimientos

Su enfoque se centra en examinar y evaluar las directrices, estándares y procesos de seguridad implementados en una entidad. El propósito es verificar la adecuación, actualización y eficacia de estos procedimientos y directrices, así como su adhesión en la práctica diaria (Martínez, 2021).

2.2.25. Auditoría de seguridad de redes

Indica que su enfoque se centra en analizar los mecanismos y procedimientos utilizados para controlar el acceso a los sistemas y la información dentro de la entidad. Esta evaluación implica examinar la gestión de contraseñas, los niveles de acceso de los usuarios, la implementación de autenticación multifactor y otros mecanismos de control (Gómez, 2024).

2.2.26. Auditoría de seguridad de aplicaciones.

Su enfoque se centra en la evaluación de la seguridad de las aplicaciones y sistemas creados o utilizados por la entidad. Este proceso abarca la revisión del código fuente, la configuración de seguridad de las aplicaciones, la verificación de la identidad y los permisos de los usuarios, además de proteger contra vulnerabilidades comunes de seguridad como inyecciones SQL o scripting entre sitios (XSS) (Garcia, 2021).

2.2.27. Auditoría de gestión de incidentes

Nos informa que su responsabilidad es analizar la forma en que una empresa responde a incidentes de seguridad, evaluando sus métodos y habilidades. Esto incluye desde la preparación y planificación para manejar incidentes hasta la detección y notificación de los mismos, así como la gestión de la respuesta y

recuperación. Además, se centra en aprender de las lecciones extraídas de incidentes anteriores (Forero, 2024).

2.2.28. Políticas de seguridad

Una política de seguridad establece lo que se pretende proteger y las expectativas para los usuarios del sistema. Sirve como fundamento para la planificación de la seguridad al desarrollar nuevas aplicaciones o expandir las redes existentes. Describe las responsabilidades del usuario, como proteger la información confidencial y crear contraseñas seguras.

La política de seguridad también debe describir cómo se monitoreará la efectividad de las medidas de seguridad. Este monitoreo lo ayuda a determinar si alguien podría estar tratando de eludir sus defensas.

En el ámbito político, es esencial mantener una atención constante en todos los componentes que lo conforman. Esto incluye evaluar la susceptibilidad de cada uno de estos elementos ante diversas amenazas y considerar las posibles repercusiones que una vulneración podría tener. Aunque es crucial analizar detenidamente cada uno de estos componentes, es importante recordar que descuidar un área vulnerable específica puede dar lugar a serias vulnerabilidades en términos de seguridad. (Fortra, 2021).

Por otra parte, las políticas consisten en una serie de declaraciones registradas que detallan la manera en que se llevan a cabo determinados procesos dentro del marco de referencia, también indican cómo se debe abordar la complejidad o el contexto limitado. El propósito de una estrategia de ciberseguridad es establecer una secuencia de normativas, reglamentos, criterios y prácticas que aseguren la protección, confidencialidad y disponibilidad de la información. Además, esta estrategia permite que cualquier individuo pueda crear y aplicar estas políticas de manera efectiva.

2.2.29. Medidas de seguridad

Se muestran 3 tipos de medidas de seguridad clasificadas de la siguiente manera:

- Físico, incluidos todos los medios de transmisión como cables, conectores, etc.
- Lógico que controla los programas de almacenamiento, entrada o transmisión.

- Legal va más allá del perfil de la empresa y es creado por la administración o estructuras internacionales.

2.2.30. Gestión de información

Gestión de la Información (GI) es el término convencional que engloba un conjunto de procesos mediante los cuales se controla el ciclo de vida de la información, desde su adquisición (mediante creación o captura) hasta su disposición final (archivado o eliminación). Estos procesos también abarcan la extracción, combinación, depuración y distribución de la información a los interesados. El objetivo de la gestión de la información es asegurar la integridad, disponibilidad y confidencialidad de la información. (De Sousa, 2024).

Estos procedimientos también involucran la extracción, consolidación, depuración y distribución de información a las partes interesadas. El objetivo de la gestión de la información es garantizar la integridad, disponibilidad y confidencialidad de la información.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Para el presente estudio se empleará una combinación de enfoques cuantitativos y cualitativos, debidos a que como lo menciona Vivar (2023) "es un nuevo enfoque o metodología diseñada para superar las limitaciones de los enfoques cuantitativos orientados a variables como las del análisis cualitativo orientado a narrativas de casos".

La estrategia de la investigación implica un enfoque basado en lo cualitativo, enfocado en llevar a cabo una investigación interna fundamental. Es crucial identificar las posibles amenazas mediante métodos de análisis informático para exponer las debilidades presentes en la red interna de la Universidad Politécnica Estatal del Carchi.

En cuanto al enfoque cuantitativo, se recopilan datos numéricos al conocer las vulnerabilidades informáticas y ataques de penetración que ha recibido los activos de información, provenientes de entrevistas estructuradas, cuestionarios y análisis de datos relacionados con la efectividad y el fracaso de los ataques. Esto se presenta mediante porcentajes y gráficos.

3.1.2. Tipo de Investigación

En este proyecto, se examinan diferentes áreas de investigación que se tuvieron en cuenta durante su desarrollo:

3.1.2.1. Investigación de acción

Durante el desarrollo de esta investigación, una vez detectadas las vulnerabilidades en activos de información de la Universidad Politécnica Estatal del Carchi, se utilizaron medidas correctivas para reforzar la seguridad. Estas acciones se realizaron en concordancia con los estándares y controles establecidos por la norma ISO 27001, y se presentaron recomendaciones una vez evaluado los riesgos mediante la metodología MAGUERIT.

Dentro del contexto fundamental de esta investigación, se elaborará un plan de seguridad de la información con el objetivo de proteger tanto los sistemas como los datos institucionales contra posibles amenazas internas. La principal meta es proporcionar información crucial que oriente la toma de decisiones relacionadas con los procedimientos operativos, la tecnología empleada y el personal.

3.1.2.2. Investigación bibliográfica documental

Se empleó una metodología fundamentada en la revisión bibliográfica, que abarcó la consulta de diversas fuentes como libros, tesis y artículos científicos. Esto se realizó con el propósito de elaborar el marco teórico y analizar la implementación de la norma ISO en la documentación empresarial.

Además, esta investigación bibliográfica documental nos permite acceder a la última información disponible sobre el tema de investigación. La norma ISO 27001 y otros estándares relacionados con la seguridad de la información están sujetos a actualizaciones periódicas, por lo que es importante estar al tanto de las versiones más recientes y de las mejores prácticas en el campo de la auditoría informática. La revisión bibliográfica nos ayuda a mantenernos actualizados y a incorporar las últimas tendencias y avances en el trabajo de investigación.

3.1.2.3. Investigación de campo

La elección de centrar esta investigación en el lugar de los acontecimientos se justifica porque permite obtener una comprensión más exhaustiva y detallada del problema.

En el transcurso de la investigación de campo, se pudo interactuar directamente con los participantes del Departamento de TIC y el departamento de Redes y Telecomunicaciones, tales como el personal técnico, los gerentes y los usuarios. Esta interacción proporcionó una perspectiva más completa. Además, se recabaron comentarios sobre los hallazgos preliminares y las recomendaciones, lo cual fue valioso para ajustar y mejorar la investigación.

Al elegir realizar una investigación de campo, se simplificará la identificación de las causas fundamentales del problema. Esto, a su vez, permitirá desarrollar posibles soluciones que contribuyan al logro de los objetivos de la investigación.

3.2. IDEA A DEFENDER

El Plan de Seguridad de la Información del departamento de TIC, basado en la norma ISO 27001, evalúa los riesgos y vulnerabilidades presentes en los activos de información de la Universidad Politécnica Estatal del Carchi y propone recomendaciones para prevenirlas.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

3.3.1. *Definición* de variables

- **Variable independiente**

Seguridad de la información

- **Variable dependiente**

La norma ISO/IEC 27001

3.3.2. Operacionalización de variables

Variable independiente: La norma ISO/IEC 27001

Tabla 2. Operacionalización de la variable independiente

Variable	Definición conceptual	Dimensión	Indicadores	Técnica	Instrumento
Independiente: Seguridad de la información	Protección de los activos de información de una organización contra cualquier amenaza, riesgo o vulnerabilidad que pueda comprometer su confidencialidad, integridad o disponibilidad	• Confidencialidad • Integridad • Disponibilidad • Gestión de accesos • Autenticación	Numero de accesos no autorizados Índices de fuga de datos Revisión de la política de acceso Tasa de errores de datos Porcentaje de datos verificados Efectividad de controles de integridad Retroalimentación del usuario Tiempo de inactividad del sistema Porcentaje de disponibilidad Satisfacción del usuario Evaluación de riesgos Promedio de conceder accesos Índices de cumplimiento con políticas de acceso Auditorias de acceso Tasa de éxito de autenticación Promedio de autenticación Tasa de uso de autenticación Detección de ataques	Auditoría Plan de seguridad Encuesta (prueba de disponibilidad) Documentación	Cuestionario Preguntas predefinidas

Variable Dependiente: Seguridad de la información

Tabla 3. Operacionalización de la variable dependiente

Variable	Definición conceptual	Dimensión	Indicadores	Técnica	Instrumento
Dependiente: La norma ISO/IEC 27001	Se trata de un estándar internacional que establece los requisitos necesarios para implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) en una organización.	• Políticas de seguridad de la información • Activos de información • Gestión de riesgos • Controles de seguridad • Mejora continua	Cumplimiento con políticas Números de incidentes de incumplimiento Claridad de las políticas Análisis de incidentes Inventario de Activos Índice de perdida de activos Evaluación de riesgos de activos Evaluación de la sensibilidad de la información Índice de riesgo residual Frecuencia de evaluación de riesgos Análisis de tendencia de riesgo Documentación de riesgos Controles Críticos Estándares de Controles Efectividad de Controles Usabilidad de Controles Efectividad de Mejoras Revisión de Políticas y Procedimientos Controles de Seguridad	Auditoría Documentación Entrevista Encuesta Auditoría Encuesta	Cuestionario Preguntas Guion de entrevistas Lista de verificación Cuestionario

3.4. MÉTODOS UTILIZADOS

En el transcurso de la investigación, se emplearon diversos enfoques de investigación que facilitaron la recopilación de datos y la adquisición de información significativa en relación con el Departamento de TIC y de Redes y Telecomunicaciones de la Universidad Politécnica Estatal del Carchi.

3.4.1. Método Inductivo

Según Narvaez (2023), el método inductivo es un proceso de razonamiento que se basa en la observación y la experimentación para llegar a una conclusión general a partir de casos específicos.

Mediante la utilización del método inductivo, se logrará reconocer las diversas categorías de incidentes de seguridad informática que han afectado a los activos de información de la Universidad Politécnica Estatal del Carchi. Además, se llevará a cabo un análisis detallado de los modelos y tácticas empleados por los perpetradores para comprometer la integridad de los sistemas.

Asimismo, mediante la aplicación del método inductivo, se posibilitará la evaluación de las causas subyacentes de los ataques informáticos, llevando a cabo un análisis detenido de las posibles deficiencias y vulnerabilidades presentes en la infraestructura de red interna de la UPEC.

3.4.2. Técnicas e instrumentos

3.4.2.1. Entrevista

Para recopilar datos y examinar tanto las variables independientes como dependientes, se empleó una entrevista, la cual se llevó a cabo con el analista de Redes y Telecomunicaciones de la Universidad Politécnica Estatal del Carchi, con el propósito de conocer la situación actual de la intranet y de los activos de información.

Según Atlas (2024):

> Las entrevistas permiten a los investigadores ahondar en las experiencias subjetivas de los individuos, lo que proporciona una perspectiva que puede no ser accesible a través de otros métodos de investigación.

De este modo, las entrevistas nos permitieron obtener información auténtica que contribuirá a identificar aspectos relevantes, considerando los objetivos específicos de este estudio.

3.4.2.2. Encuesta

Con este método de investigación se buscó recopilar información por parte de los encargados del departamento de TIC.

Según Qualtrics (2023):

> Las encuestas son un método de recolección de datos a partir de un muestreo de personas, a menudo con el objetivo de generalizar los resultados para un segmento de población más grande.

3.4.3. Población y Muestra

Para la presente investigación no se necesita una muestra, dado que se trabajará exclusivamente con el personal responsable de la intranet de la Universidad Politécnica Estatal de Carchi, considerándolo como la población relevante para este propósito.

3.5. ANÁLISIS ESTADÍSTICO

3.5.1. Análisis de la entrevista

El 06 de marzo de 2024, se llevó a cabo una entrevista al Ing. Javier Torres, quien ocupa el cargo de Analista de Redes y Comunicaciones de la Universidad Politécnica Estatal del Carchi. Durante la entrevista, hizo las siguientes observaciones con respecto a la seguridad de la información de dicha institución.

ENTREVISTA DIRIGIDA AL ANALISTA DE REDES Y COMUNICACIONES DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

La finalidad de la entrevista es comprender la situación actual de la seguridad de la información en la UPEC. Los datos recabados están vinculados con las medidas de seguridad concebidas para reforzar y proteger la red universitaria ante amenazas cibernéticas.

1. **¿Cuáles han sido los principales incidentes de seguridad informática que ha enfrentado el departamento de TIC de la UPEC?**

Ha habido varios problemas de seguridad informática en la red institucional, Malware, ransomware entre otros. Además de problemas físicos, como servidores obsoletos, dañados o partes internas quemadas.

Análisis

En la respuesta proporcionada se menciona la presencia de varios problemas de seguridad informática en la red institucional, incluyendo malware y ransomware. Estos tipos de amenazas son comunes en entornos informáticos y pueden causar daños significativos al comprometer la integridad, confidencialidad y disponibilidad de los datos y sistemas de la universidad. La presencia de malware y ransomware sugiere posibles deficiencias en las medidas de seguridad implementadas, como firewalls, software antivirus, y prácticas de seguridad informática por parte del personal.

Además de los problemas de seguridad informática, se mencionan problemas físicos en la infraestructura de tecnología de la universidad, como servidores obsoletos, dañados o con partes internas quemadas. Estos problemas indican una falta de mantenimiento adecuado de la infraestructura tecnológica de la universidad. Los servidores obsoletos pueden ser vulnerables a ataques cibernéticos y pueden no ser capaces de soportar las demandas actuales de procesamiento de datos. Los servidores dañados o con partes internas quemadas pueden resultar en

interrupciones en los servicios tecnológicos de la universidad, lo que afecta la productividad y la eficiencia de las operaciones institucionales.

2. **¿Qué medidas ha llevado a cabo el departamento de Redes y Telecomunicaciones en colaboración con el departamento de TIC para elevar la calidad de seguridad de la información?**

Dentro de los proyectos institucionales, se ha previsto la instalación de Antivirus Institucional, implementación de un Next Generation Firewall para la protección perimetral de los equipos y servidores institucionales. Así como varias políticas de acceso a los servicios informáticos que la institución brinda.

Análisis

Las acciones mencionadas reflejan un enfoque global para mejorar la calidad de la seguridad de la información en la organización. La implementación de un antivirus institucional, la puesta en marcha de un firewall de última generación y el establecimiento de políticas de acceso son pasos clave para proteger los sistemas y datos de la institución contra amenazas cibernéticas, y garantizar la integridad y confidencialidad de la información. Estas medidas demuestran un compromiso con las mejores prácticas de seguridad informática y la protección de los activos de información de la institución frente a posibles riesgos y amenazas.

3. **¿La UPEC tiene políticas de seguridad establecidas para proteger la información?**

Si existen políticas de seguridad, entre ellas se encuentran la configuración de puertos en el firewall, donde se permite o bloquea puertos hacia los servidores institucionales para proteger su acceso, doble factor de autenticación en las cuentas de correo, entre otras.

Análisis

Estas políticas de seguridad mencionadas son ejemplos de las medidas proactivas que la UPEC ha implementado para proteger la información. Sin embargo, es importante tener en cuenta que la seguridad de la información es un proceso continuo y en evolución. Las políticas y medidas de seguridad deben revisarse y actualizarse regularmente para abordar las nuevas amenazas y desafíos de seguridad que puedan surgir.

La existencia de políticas de seguridad establecidas, como la configuración de puertos en el firewall y la implementación del doble factor de autenticación, refleja el compromiso de la UPEC con la protección de la información institucional. Estas medidas son componentes importantes de un programa integral de seguridad de la información y ayudan a mitigar riesgos y proteger los activos de datos de la institución contra amenazas cibernéticas y ataques.

4. **¿Cómo es administrada la red interna de la UPEC?**

La red interna está compuesta de varias partes, Red de Datos Cableada, Red de Datos Wi-Fi, Data Center, CCTV, Telefonía IP. Todo se encuentra administrado por el personal de la Unidad de Redes y Telecomunicaciones, cada una de estas partes dispone de su propio software de administración que facilita la gestión de las mismas.

Análisis

La respuesta indica que la red interna de la UPEC está bien estructurada y administrada por personal especializado. La presencia de software de administración dedicado para cada parte de la red y la centralización de la gestión son aspectos positivos que contribuyen a la eficiencia y la seguridad de la infraestructura de red de la institución.

La descripción de la red interna de la UPEC sugiere que se han implementado tecnologías modernas y diversas para satisfacer las necesidades de conectividad y comunicación de la institución. La centralización de la administración de la red bajo la Unidad de Redes y Telecomunicaciones también puede facilitar la coordinación y la implementación de políticas de seguridad y estándares de red en toda la infraestructura.

5. **¿Qué medidas de control de acceso físico se implementan para proteger los servidores de la UPEC?**

El ingreso a los equipos del Data Center no se encuentra óptima debido a que no cumple con las normativas de acceso a Data Centers, pero el personal de la Unidad de Redes y Telecomunicaciones es el único que tiene las llaves de acceso al mismo.

Análisis

La seguridad física de los servidores en un Data Center es crucial para proteger la integridad y la disponibilidad de los datos y sistemas alojados en ellos. La respuesta sugiere que, aunque la situación actual no cumple con todas las normativas de

seguridad, existe un control de acceso limitado a través de la posesión exclusiva de las llaves por parte del personal autorizado.

Sin embargo, es importante señalar que el hecho de que el acceso no cumpla con las normativas óptimas es una preocupación significativa. Las normativas de seguridad para los Data Centers suelen incluir medidas como sistemas de control de acceso biométrico, cámaras de vigilancia, sistemas de alarma, entre otras, para garantizar la protección de los equipos y los datos críticos.

6. **¿Qué criterios se utilizan para determinar qué software y equipos informáticos se asignan a cada miembro del personal del departamento de TIC?**

Cada uno del personal que labora en la Dirección de TIC dispone de su equipo informático con software especializado para poder realizar sus actividades académicas y administrativas, además de que cuentan con acceso a los servidores de desarrollo y producción de cada uno de los servicios informáticos universitarios.

Análisis

En la UPEC, la distribución de software y equipos informáticos para el personal del departamento de TIC se lleva a cabo de manera individualizada y personalizada. Esto garantiza que cada miembro del equipo disponga de las herramientas necesarias para cumplir sus funciones de manera efectiva. Además, el acceso a los servidores de desarrollo y producción permite al personal colaborar y administrar los servicios informáticos de la universidad de manera integral y eficiente.

7. **¿Todo el software utilizado en la UPEC posee licencia?**

La mayoría del software utilizado en la UPEC es bajo software libre, pero en los softwares que se requiera licenciamiento, la UPEC gestiona la adquisición de los mismos.

Análisis

La UPEC adopta una política mixta en cuanto al uso de software, priorizando el software libre siempre que sea posible y adquiriendo licencias para el software propietario cuando sea necesario.

Este enfoque refleja un compromiso con el cumplimiento de las leyes y regulaciones de propiedad intelectual, así como con el uso ético y legal del software en la institución. Al adquirir licencias para el software que así lo requiere, la UPEC asegura

el respeto de los derechos de los desarrolladores y propietarios del software, al mismo tiempo que evita posibles problemas legales derivados del uso de software sin licencia.

8. **¿Qué sistema operativo se emplea en el servidor del centro de datos de la UPEC? ¿Y por qué?**

Los servidores institucionales son bajo el sistema operativo Debian, primero porque es software libre y también por las seguridades y parches de actualización que posee esta distribución, son pocos los servicios que se implementan bajo Windows Server.

Análisis

La elección del sistema operativo Debian para los servidores del centro de datos de la UPEC refleja un compromiso con los principios del software libre, la seguridad y la estabilidad. Debian proporciona una plataforma confiable y versátil para alojar los servicios institucionales, al tiempo que permite a la UPEC mantener un mayor control sobre su infraestructura tecnológica y reducir su dependencia de soluciones propietarias.

9. **¿Qué mecanismos de autenticación se utilizan para controlar el acceso a los servidores de archivos?**

El acceso a los servidores de archivo se lo realiza por medio de los servicios informáticos instalados, ya que se encuentran en una configuración de cluster. Además, cada funcionario está a cargo de sus archivos que pueden almacenarlos en la nube que nos entrega el proveedor de correo electrónico.

Análisis

El manejo del acceso a la información en los servidores de archivos de la UPEC se basa en una combinación de infraestructura de red y sistemas informáticos configurados para la gestión de archivos, así como en la utilización de servicios de almacenamiento en la nube proporcionados por el proveedor de correo electrónico de la institución. Este enfoque proporciona a los usuarios acceso seguro y eficiente a sus archivos, al tiempo que ofrece opciones flexibles para el almacenamiento y la gestión de datos.

10. **Ante la presencia de hosts que estén ejecutando servicios innecesarios o infectados de virus. ¿Cómo se da solución al problema?**

La universidad cuenta con un antivirus y un firewall de última generación que protege, detecta y bloquea este tipo de malware.

Análisis

La implementación de un antivirus y un firewall de última generación en la UPEC evidencia un enfoque proactivo hacia la seguridad de la información y la protección de los sistemas contra amenazas cibernéticas. Estas medidas contribuyen a asegurar la integridad y disponibilidad de los recursos tecnológicos de la universidad, al mismo tiempo que resguardan la confidencialidad de la información institucional.

11. **¿Qué métodos y técnicas se ha empleado para crear los procedimientos de seguridad con el fin de prevenir posibles vulnerabilidades?**

Uno de los métodos empleados es realizar un escaneo a los puertos de cada servidor para determinar su vulnerabilidad, y con ello solamente habilitar los necesarios en cada uno de sus servicios.

Además, se realizan escaneos periódicos en busca de vulnerabilidades de la red para poder mitigarlos.

Análisis

La UPEC emplea métodos proactivos para identificar y mitigar posibles vulnerabilidades en su infraestructura de red y sistemas. Los escaneos a los puertos y los escaneos periódicos en busca de vulnerabilidades son prácticas efectivas que ayudan a fortalecer la seguridad de la universidad y a proteger sus sistemas y datos contra posibles amenazas cibernéticas.

Estos escaneos periódicos son una práctica recomendada en seguridad informática para identificar y mitigar posibles vulnerabilidades y amenazas. Los escaneos pueden incluir la búsqueda de fallos de software, configuraciones inseguras, o cualquier otra vulnerabilidad que pueda ser explotada por los atacantes.

12. **¿Cuál fue el problema interno detectado con respecto a la seguridad de la intranet de la UPEC?**

Dentro de la intranet, el mayor problema son los dispositivos de usuario final que no pertenecen como activos institucionales, es decir computadoras tablets celulares

que pertenecen a estudiantes y docentes los cuales muchas veces no tienen instalados software de protección informática como un antivirus.

Análisis

El problema interno detectado con respecto a la seguridad de la intranet de la UPEC destaca la importancia de abordar los riesgos asociados con la presencia de dispositivos no autorizados y sin protección en la red. Mediante la implementación de políticas y medidas de seguridad adecuadas, la universidad puede mitigar estos riesgos y proteger de manera efectiva su infraestructura de red y sus activos de información.

13. ¿Opina usted que los sistemas informáticos actuales en la UPEC son confiables desde el punto de vista de la seguridad?

Los sistemas si son confiables, aunque existen muchas debilidades que se las deben ir solventando.

Análisis

La opinión expresada sugiere una postura realista y proactiva hacia la seguridad de los sistemas informáticos de la UPEC. Reconoce los logros en términos de confiabilidad, pero también reconoce la necesidad de seguir mejorando y fortaleciendo las medidas de seguridad para hacer frente a los desafíos emergentes en el ámbito de la seguridad cibernética.

3.5.1. RECURSOS

Tabla 4. Recursos humanos

Nombre	Función que desempeña
MSc. Milton del Hierro	Tutor de Trabajo de Integración Curricular
Jhojan Chicango	Investigador
Javier Torres	Encargado del Departamento de Redes y Telecomunicaciones

Tabla 5. Recursos Materiales

Recursos	Características
Hojas	Papel tamaño A4
Ordenadores	Laptop

Tabla 6. Recursos Tecnológicos

Recursos	Características
Laptop	Esta herramienta se utilizó para redactar la documentación de la investigación y para la instalación de herramientas tecnológicas.
Celular Xiaomi Redmi 10	Se usó para el levantamiento de información y para las tutorías.
Internet fijo	Fue necesario para realizar consultas y búsquedas de información necesarias para sustentar la investigación
Software	Para máquinas virtuales y herramientas de auditoria informática
Sistemas Operativos	Debian, Windows 10

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1. Resultados de las encuestas

Se llevaron a cabo encuestas dirigidas a los encargados del manejo de la red universitaria. El propósito primordial es recabar datos sobre la seguridad informática en la Universidad Politécnica Estatal del Carchi. Es fundamental resaltar que, al realizar los sondeos, no se solicitó a los encuestados que suministraran datos personales, con el fin de evitar que factores no pertinentes a la seguridad informática influyeran en los resultados.

4.1.1.1. Análisis de los ítems de la encuesta

Comprensión de la seguridad informática

Objetivo: Medir la comprensión del personal acerca de las regulaciones de seguridad de la información.

Nota: Las preguntas se evalúan en una escala de 1-5 en donde:

1 = 0% 2 = 25% 3 = 50% 4 = 75% 5 = 100%

Pregunta 1: ¿Cuál es su nivel de comprensión en cuanto a la seguridad de la información en la actualidad?

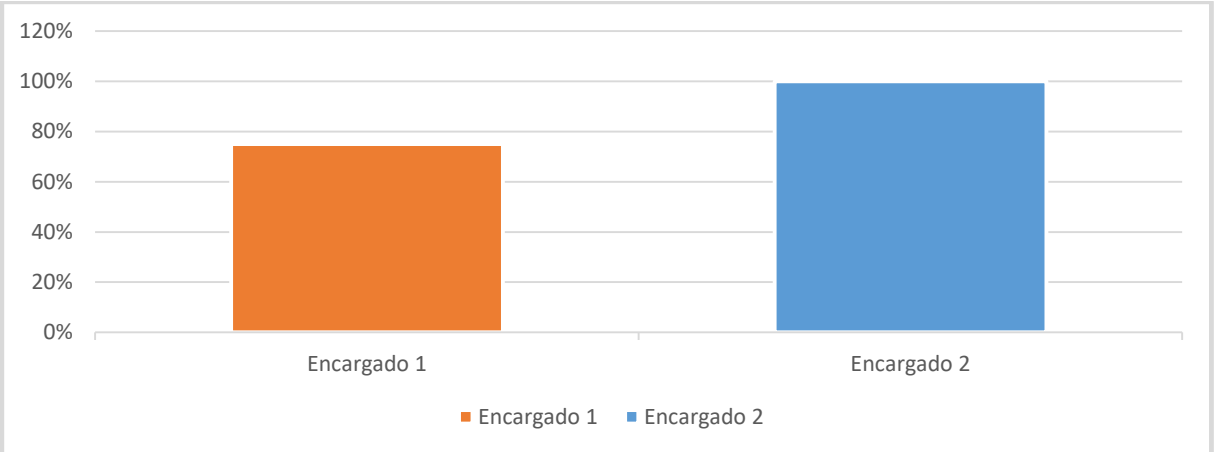

Figura 4. Entendimiento de la seguridad informática

Análisis e interpretación

La pregunta indaga sobre el nivel de comprensión de los encuestados respecto a la seguridad de la información en la red universitaria, con respuestas de 75% y 100%. En donde el encuestado que selecciona 75% probablemente posee un conocimiento sólido de los principios básicos, mientras que el encuestado que opta por 100% probablemente es experto con un entendimiento profundo del tema. La distribución sugiere que los encargados de la red están compuestos por individuos informados sobre seguridad de la información.

Pregunta 2: ¿Cuál es su nivel de comprensión acerca de las normativas internas que rigen la seguridad de la información?

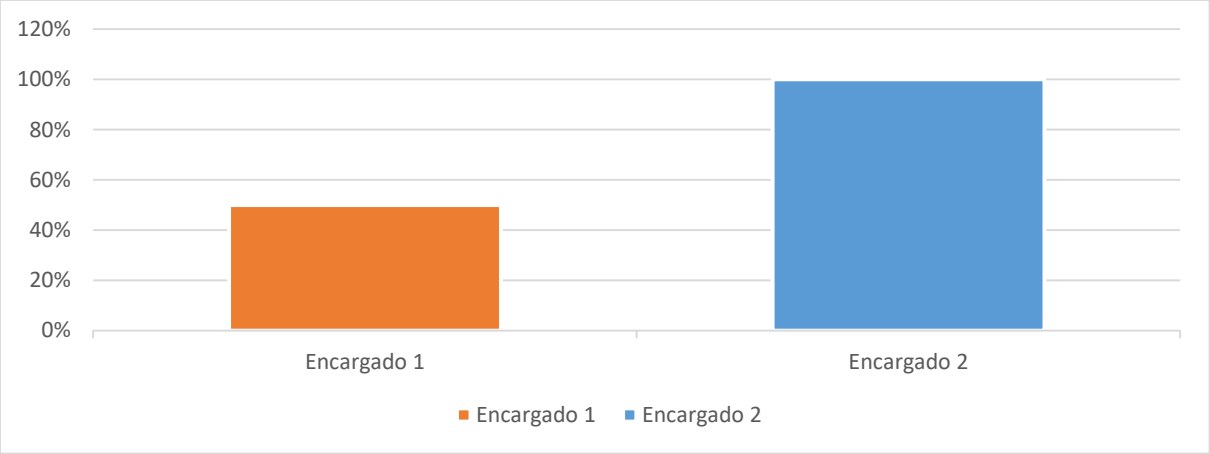

Figura 5. Comprensión de normativas internas

Análisis e interpretación

Tomando en consideración ambas respuestas, se obtiene una visión diversificada del entendimiento que tiene el grupo encuestado sobre las normativas internas que regulan la seguridad de la información.

Mientras que un participante muestra un conocimiento intermedio en el tema, otro revela un dominio avanzado. Esta disparidad sugiere que dentro de la población encuestada hay una amplia gama de niveles de conocimiento y comprensión.

Este hallazgo puede ser de gran utilidad, ya que proporciona información clave para identificar áreas específicas que requieren mejora o refuerzo, así como para adaptar estrategias de capacitación de acuerdo con las necesidades individuales de los participantes.

Pregunta 3: ¿Cuál es el grado de conocimiento que ha adquirido de las capacitaciones sobre seguridad de la información proporcionadas por la UPEC?

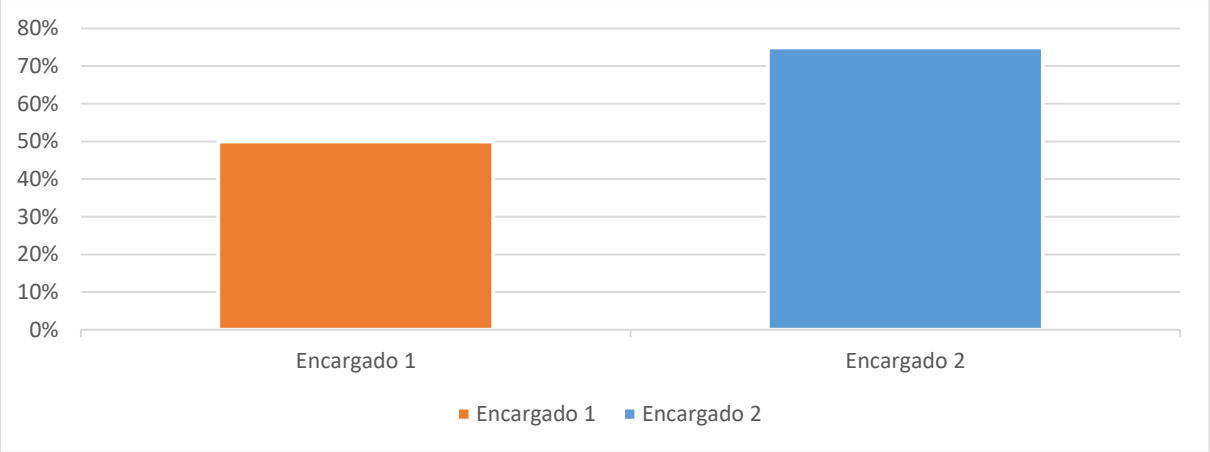

Figura 6. Conocimiento de capacitaciones sobre seguridad

Análisis e interpretación

Las respuestas muestran variabilidad en los niveles de conocimiento, indicando que la efectividad de las capacitaciones puede diferir entre los participantes debido a diferencias en la capacidad de aprendizaje o la calidad de la instrucción.

Este análisis puede ayudar a la UPEC a identificar áreas de mejora en sus programas de capacitación y a reconocer los éxitos en el aprendizaje de seguridad de la información, proporcionando información útil para futuras iniciativas de mejora y personalización de la capacitación.

Conocimiento normativo

Objetivo: Determinar el grado de comprensión respecto a la Norma ISO 27001 y la legislación de protección de datos.

Nota: Las preguntas se evalúan en una escala de 1-5 en donde:

1 = 0% **2 = 25%** **3 = 50%** **4 = 75%** **5 = 100%**

Pregunta 4: ¿Cuál es tu nivel de comprensión actual acerca de la Norma ISO 27001?

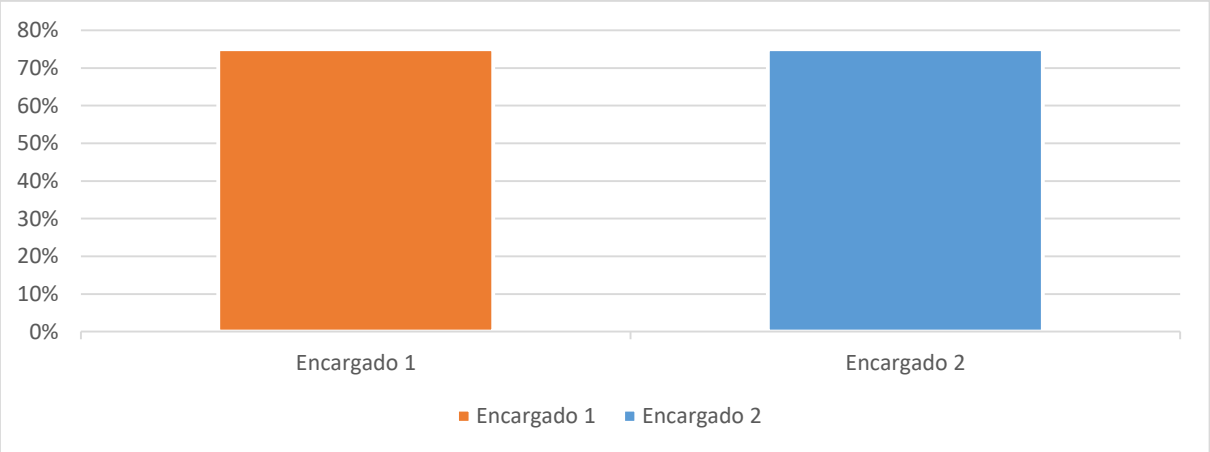

Figura 7. Comprensión Integral de la ISO 27001

Análisis e interpretación

Ambos encuestados han calificado su comprensión de la Norma ISO 27001 con un nivel 4, lo que sugiere un buen entendimiento, pero con margen para mejorar. Esto indica un conocimiento sólido de la norma, aunque aún podría profundizarse.

Este nivel de comprensión puede ser útil si los encuestados están involucrados en la implementación o cumplimiento de la norma en sus organizaciones, pero también podría señalar la necesidad de más formación o recursos para alcanzar una comprensión más completa, especialmente en roles críticos relacionados con la seguridad de la información.

Pregunta 5: ¿Cuál es tu nivel de conocimiento acerca de la ley de protección de datos en el Ecuador?

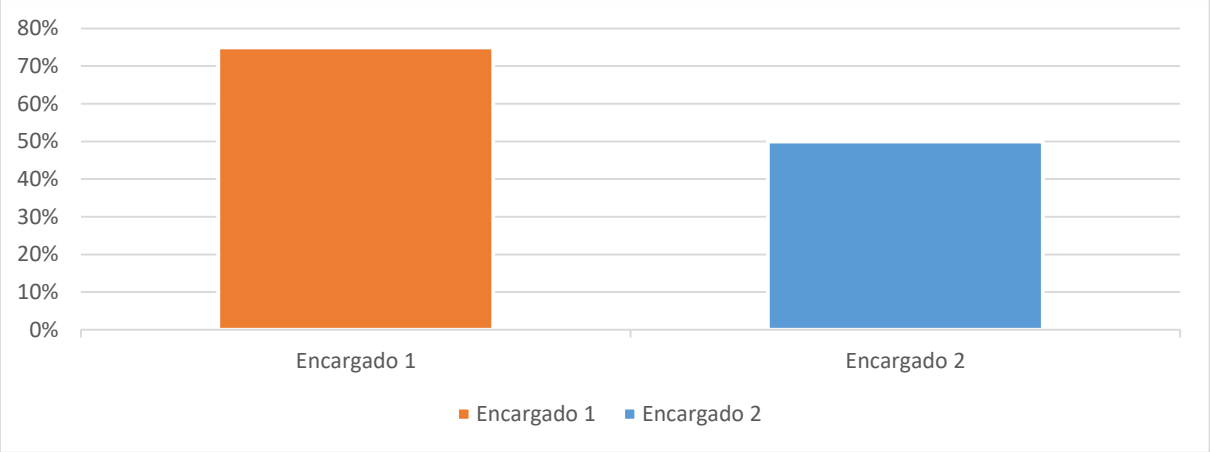

Figura 8. Derechos y deberes en el manejo de datos personales

Análisis e interpretación

Desde una perspectiva interpretativa, la respuesta sugiere que los encuestados tienen un entendimiento que oscila entre lo básico y lo intermedio de la ley de protección de datos en Ecuador. Esto podría resultar beneficioso si están involucrados en la gestión o el cumplimiento de esta ley en sus actividades laborales o personales.

Pregunta 6: ¿Cuál es la situación actual de la Institución en términos de seguridad de la información según las auditorías internas?

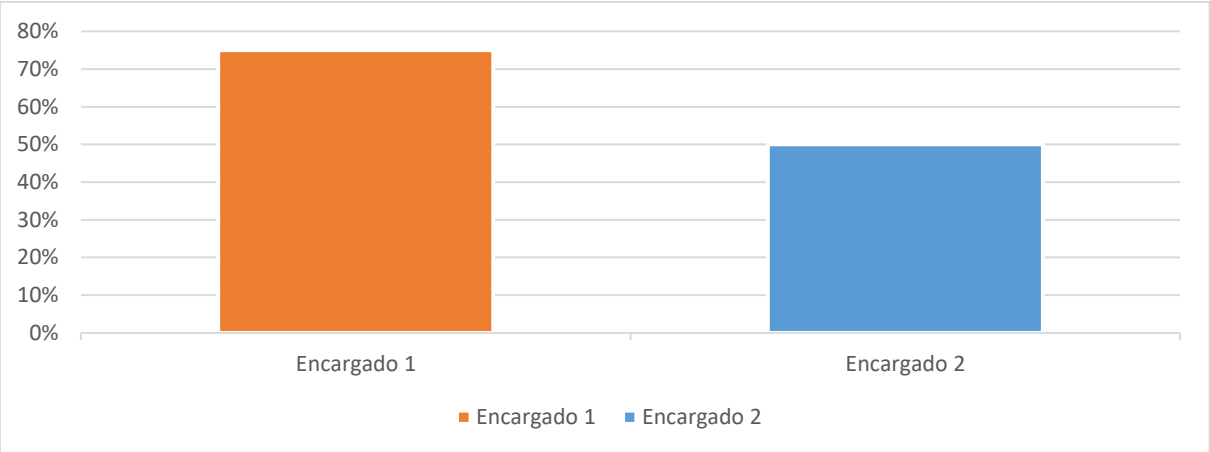

Figura 9. Situación actual de la institución

Análisis e interpretación

Las respuestas por parte de los encuestados sugieren que, de acuerdo con los resultados de las auditorías internas, la institución ha avanzado en la mejora de la seguridad de la información, como se refleja en la calificación 4 otorgada. No

obstante, aún se identifican áreas con potencial de mejora, como se indica con la calificación 3.

Este hallazgo indica que existen aspectos específicos dentro del ámbito de la seguridad de la información que podrían fortalecerse o que requieren atención adicional por parte de la institución. Por lo tanto, aunque se han realizado esfuerzos para mejorar la seguridad de la información, aún queda trabajo por hacer para alcanzar un nivel óptimo de protección y gestión de la información en la organización.

Métodos para salvaguardar datos y garantizar la seguridad de la información.

Objetivo: Obtener información actualizada acerca de la seguridad de los datos mediante la utilización de los servicios proporcionados por el personal.

Nota: Las preguntas se evalúan en una escala de 1-5 en donde:

1 = 0% **2 = 25%** **3 = 50%** **4 = 75%** **5 = 100%**

Pregunta 7: ¿Cuál es el nivel de seguridad de los servidores donde se almacenan los archivos de respaldo?

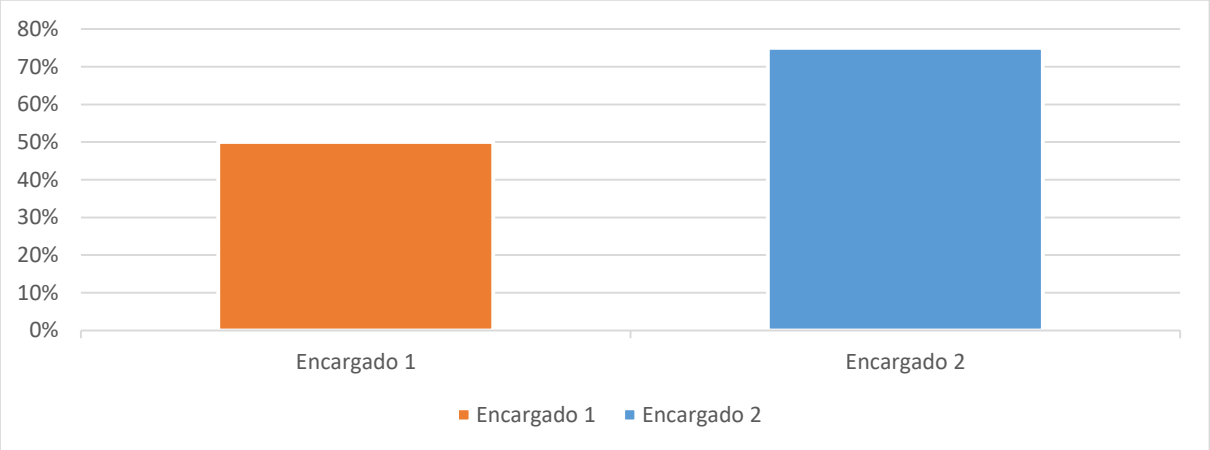

Figura 10. Seguridad de los servidores

Análisis e interpretación

Interpretando la respuesta proporciona una idea de cómo los encuestados perciben la seguridad de los servidores que almacenan los archivos de respaldo. Se sugiere que estos servidores cuentan con ciertos niveles de seguridad implementados, como evidencia la calificación 4 asignada. Sin embargo, también se indica que todavía existe espacio para mejorar la seguridad, ya que se otorga una calificación de 3.

Esto implica que hay aspectos específicos relacionados con la seguridad de los servidores de respaldo que podrían ser fortalecidos o que requieren una mayor atención y medidas de protección adicionales para garantizar la integridad y confidencialidad de los datos almacenados en ellos.

Pregunta 8: Los servicios prestados en caso de tener un fallo ¿Cómo define su accionar en tiempo de respuesta para resolver dichos problemas?

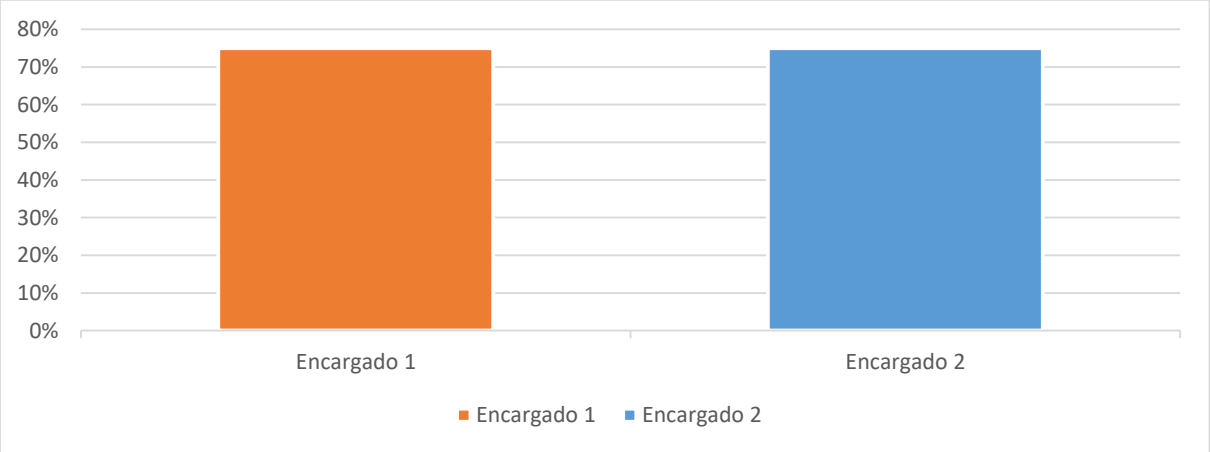

Figura 11. Resolución de fallos de servicios

Análisis e interpretación

Ambos encuestados han calificado con un nivel 4, lo que sugiere que perciben positivamente la capacidad de la organización para responder de manera efectiva y rápida ante fallos en los servicios prestados.

Esto implica que confían en que la organización cuenta con procedimientos y recursos apropiados para abordar los problemas de forma oportuna. La calificación alta indica un compromiso considerable por parte de la organización para reducir al mínimo el tiempo de inactividad y solucionar los problemas de manera eficiente.

Pregunta 9: ¿Cuán importante considera la protección de datos y la seguridad de la información en el entorno universitario?

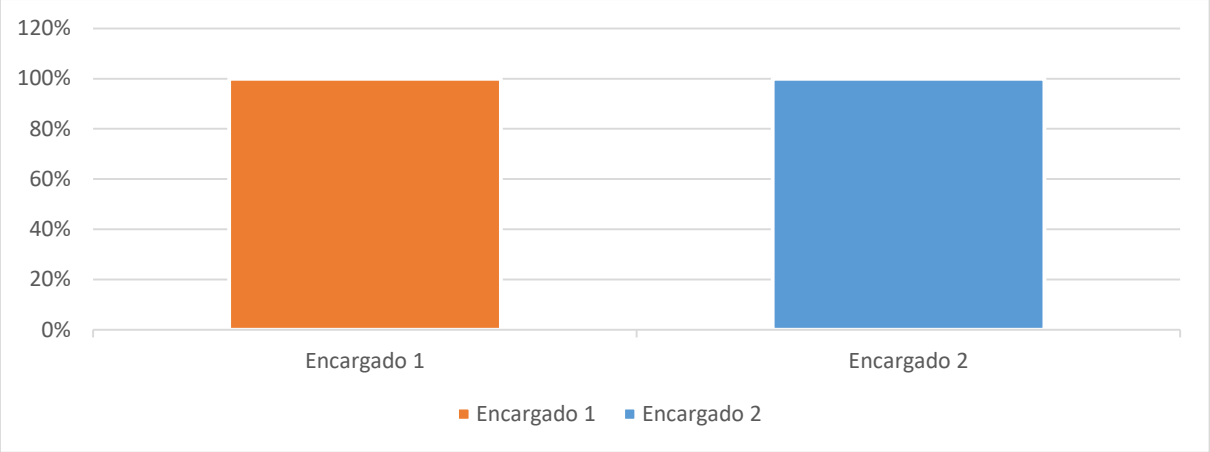

Figura 12. Salvaguarda de datos y seguridad informática

Análisis e interpretación

Ambos encuestados han valorado con un nivel 5, lo que indica que consideran de suma importancia la protección de datos y la seguridad de la información en el ámbito universitario.

Desde una perspectiva interpretativa, esta respuesta indica que los encuestados reconocen la importancia fundamental de proteger los datos y garantizar la seguridad de la información en el ámbito universitario.

Pregunta 10: ¿Cómo califica la efectividad de tus procedimientos para el manejo y almacenamiento seguro de datos sensibles?

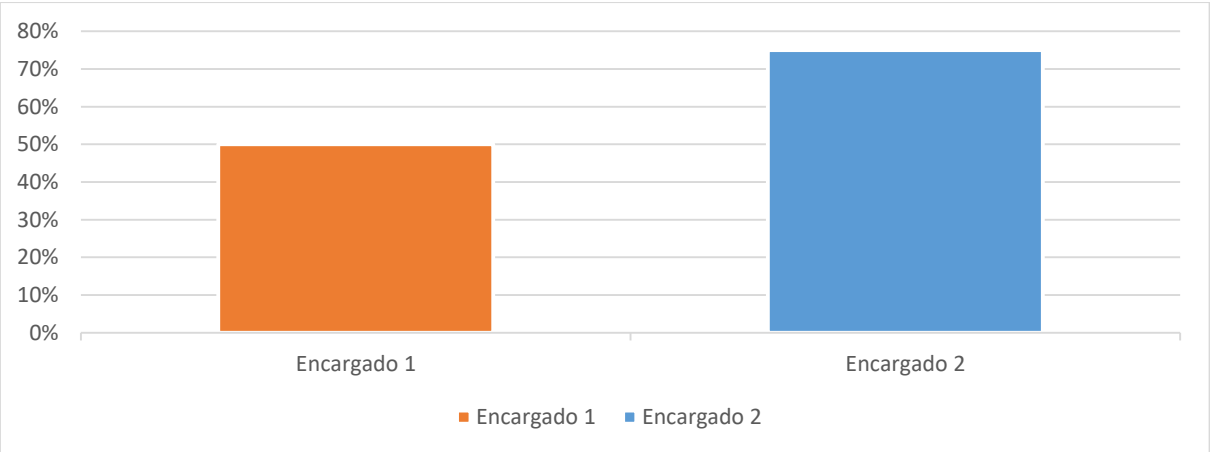

Figura 13. Efectividad de procedimientos manejo de datos

Análisis e interpretación

Los dos encuestados han otorgado calificaciones de 3 y 4 respectivamente. Esto sugiere que tienen percepciones ligeramente divergentes sobre la eficacia de los procedimientos empleados para gestionar y almacenar de forma segura los datos sensibles.

En términos de interpretación, estas respuestas sugieren que los encuestados en su mayoría consideran que los procedimientos implementados son efectivos para proteger la seguridad y confidencialidad de los datos sensibles. La calificación más alta de 4 indica un nivel de satisfacción y confianza superior en comparación con la calificación de 3, aunque ambas indican que aún existe margen para mejorar y optimizar estos procedimientos.

4.2. PROPUESTA

Mi propuesta se enfoca en tratar la seguridad de la información dentro de la Universidad Politécnica Estatal del Carchi, dentro del departamento de TIC, con el propósito de desarrollar un plan de seguridad de la información que cumpla con los estándares definidos por la norma ISO/IEC 27001.

El diseño del plan se enfoca en identificar, evaluar y mitigar los riesgos de seguridad de la información para los activos con mayores riesgos, fortaleciendo la confidencialidad, integridad y disponibilidad de los datos críticos que maneja la institución.

Con el propósito de identificar buenas prácticas que contribuyan a mejorar el proceso de optimización de la seguridad de la información en los activos de información de la UPEC, se analizarán detalladamente las medidas de seguridad implementadas previamente en la institución. Este análisis permitirá evaluar la efectividad de las soluciones aplicadas, identificar áreas de mejora y proponer nuevas estrategias alineadas con los estándares de seguridad, garantizando la protección integral de la información sensible y crítica.

La metodología para esta propuesta implica varios pasos. En primer lugar, se realizará un análisis exhaustivo de la infraestructura de la intranet, activos de información y documentación de la UPEC y de los datos que maneja. El segundo punto consiste en identificar las vulnerabilidades y riesgos potenciales de la red. Basándonos en estos hallazgos, se desarrollará el plan detallado de seguridad de la información que cumpla con los requisitos y controles establecidos en la norma ISO 27001.

Con el diseño del plan de seguridad de la información, se espera que los resultados propuestos no solo contribuyan a fortalecer la seguridad de la intranet de la UPEC, sino que también sirvan como referencia para otras instituciones que busquen mejorar sus prácticas de gestión de la seguridad de la información.

4.2.1. Alcance de la propuesta

El enfoque de este proyecto se dirige a identificar las posibles vulnerabilidades y amenazas en los activos de información de la institución. El aporte previsto al departamento de TIC y al departamento de Redes y Telecomunicaciones es el desarrollo de un plan de seguridad de la información para los activos de la Universidad Politécnica Estatal del Carchi. Esto se llevará a cabo un análisis de

situación actual y conocer sus activos con mayor riesgo de vulnerabilidad, con el objetivo de identificar los controles de seguridad pertinentes para mitigar posibles vulnerabilidades en los activos de información.

4.2.2. Estudio de factibilidad

- **Título: "**Optimización de la seguridad de la información basada en la norma ISO/IEC 27001"
- **Institución Ejecutora:** Universidad Politécnica Estatal del Carchi
- **Beneficiario:** Departamento de Redes y Telecomunicaciones de la UPEC
- **Ubicación:** Carchi – Cantón Tulcán
- **Responsable del Plan:** Jhojan Chicango egresado de la UPEC.

4.2.3. Análisis de la situación actual

La situación actual de la intranet y de los activos de información de la Universidad Politécnica Estatal del Carchi es crucial para garantizar la integridad, confidencialidad y disponibilidad de la red interna, así como para cumplir con políticas de seguridad efectivas.

Sin embargo, existen preocupaciones significativas, como la falta de registros de incidentes de seguridad en el departamento de TIC y Redes y Telecomunicaciones. Esta ausencia dificulta la identificación y abordaje de posibles vulnerabilidades y amenazas en la red interna.

Además, la carencia de registros de incidentes anteriores y medidas correctivas limita la mejora continua de la seguridad. La documentación de la infraestructura de red también es deficiente, ya que carece de detalles completos como marcas y modelos de equipos, y no se registra la configuración de dispositivos.

Es crucial realizar una revisión exhaustiva de la infraestructura de red y de las políticas de seguridad en el departamento de Redes y Telecomunicaciones. También se debe establecer un proceso de registro de incidentes y medidas correctivas para mejorar la respuesta ante posibles brechas de seguridad.

Aunque se dispone de un equipo firewall con características de prevención de intrusiones, la falta de registro de las políticas establecidas en dichas configuraciones dificulta la evaluación y gestión de la seguridad de los activos de información.

Tabla 7. Evaluación de red interna

Documentación de la Red Interna	Descripción	Estado actual	Observaciones
Diagramas de Red física y lógica de la red interna	Diagramas que representan la topología, incluyendo servidores, switches, routers, firewalls, etc.	Se dispone de diagramas de red, tanto de la red de datos antigua, red de datos actual y red de datos a futuro	Se debe realizar la actualización del diagrama de red actual.
Políticas de Seguridad de la información	Documentación oficial de las políticas de la información en la red.	Se dispone de un Documento de Políticas de Seguridad de la Información	El documento se encuentra en los archivos de la Dirección de TIC

Tabla 8. Infraestructura de la Red

Infraestructura de Red	Descripción	Estado actual	Observaciones
Arquitectura de Red de red interna	Descripción detallada de la arquitectura incluyendo equipos, topología, y redundancia.	Se dispone de un diagrama de red, pero no se especifican marcas ni modelos de equipos.	Se recomienda actualizar el diagrama con detalles de marcas y modelos.
Configuración de Dispositivos de Red	Configuración actual de los dispositivos incluyendo switches, routers, firewalls, y servidores	No se dispone de un registro de las configuraciones de los equipos.	Es crucial mantener un registro actualizado de las configuraciones
Segmentación de Redes implementadas	Políticas y medidas de segmentación de la información para mejorar la seguridad y el rendimiento	Si se tiene segmentada la red de datos, pero no se dispone de un documento detallado.	Se sugiere crear un documento que detalle la segmentación actual.
Implementación de Firewalls	Detalles sobre la configuración administración de firewalls en la red	Si se tiene un equipo Firewall configurado, pero no se tiene un registro.	Verificar la efectividad del Firewall y realizar pruebas de seguridad.

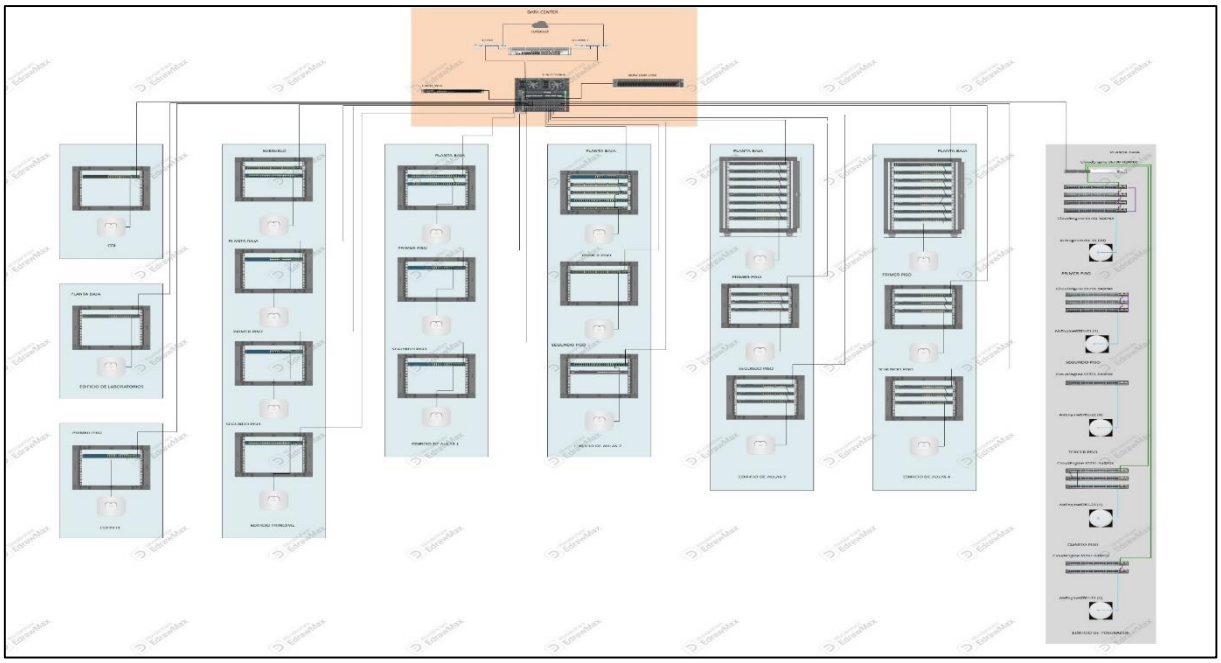

Figura 14. Topología red antigua
Fuente: UPEC

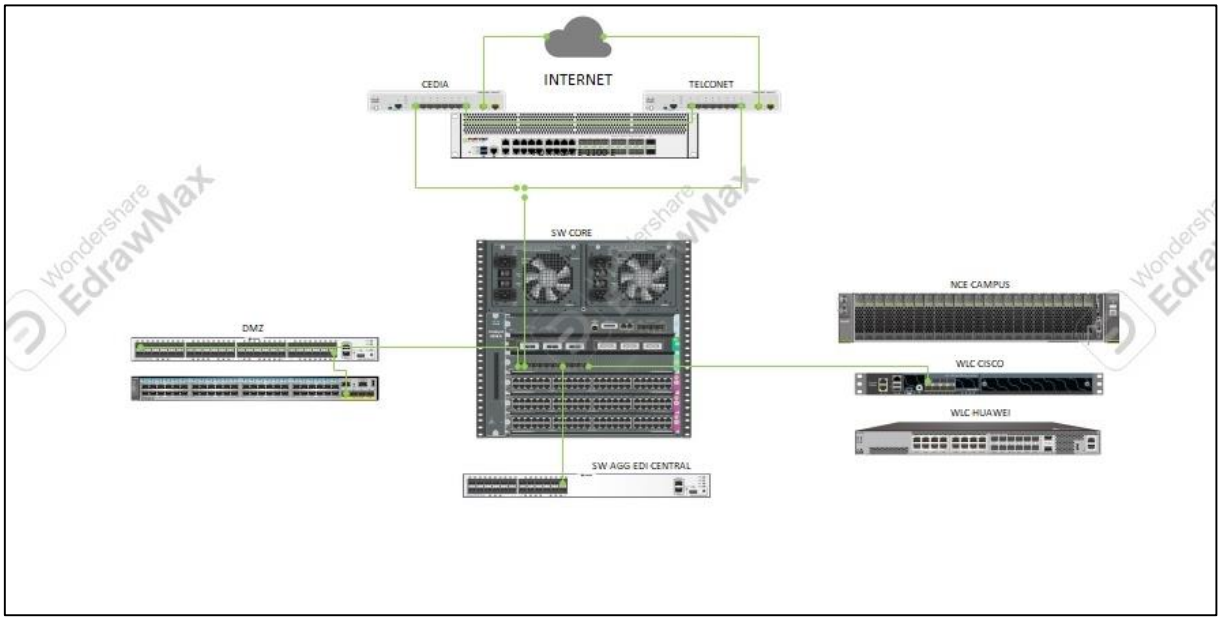

Figura 15. Topología red actual
Fuente: UPEC

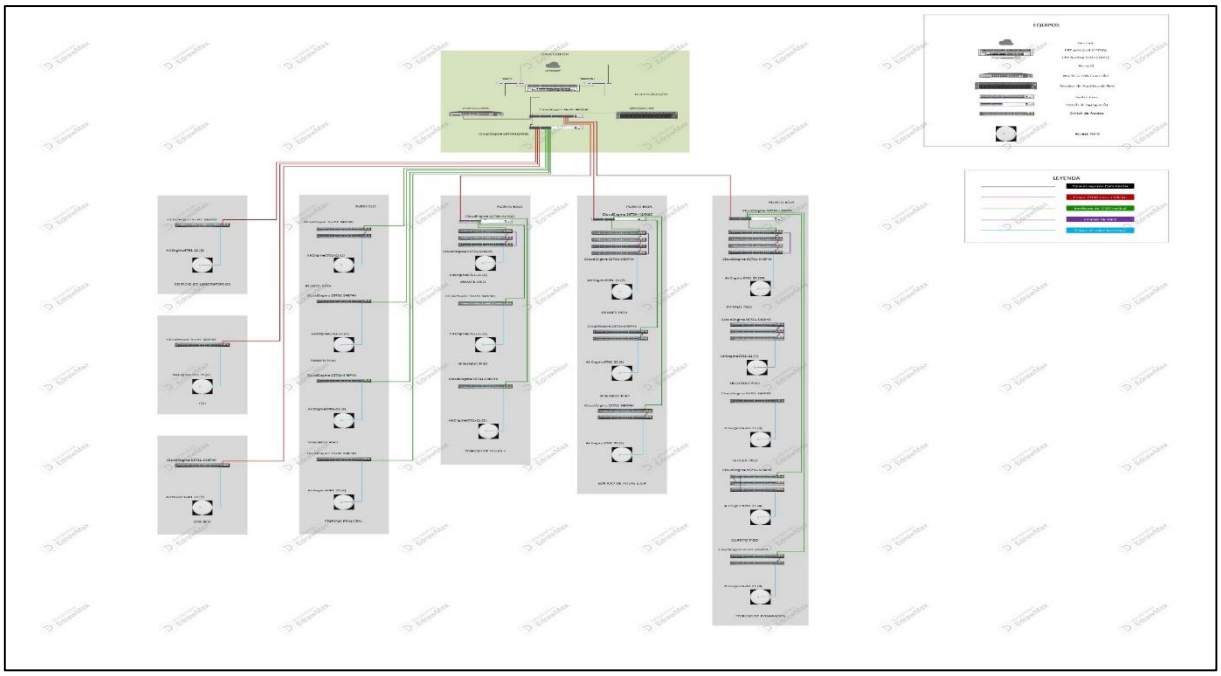

Figura 16. Topología red futura
Fuente: UPEC

4.2.3.1. Análisis de la Intranet

Dentro del departamento de TIC y de Redes y Telecomunicaciones, tener diagramas de red es esencial para comprender la estructura de la red universitaria y anticipar posibles problemas. Aunque es positivo contar con diagramas tanto para la red actual como para la futura, la necesidad de actualizar el diagrama actual sugiere que puede haber discrepancias entre la documentación y la realidad operativa. Esto podría conducir a decisiones erróneas o a una respuesta inadecuada ante incidentes.

Las políticas de seguridad de la información son críticas para proteger los datos de la organización. Aunque es beneficioso tener un documento de políticas, el hecho de que esté archivado en lugar de estar fácilmente accesible puede dificultar su implementación y actualización. Es fundamental que estas políticas estén disponibles y sean conocidas por todo el personal involucrado en la gestión de la red para garantizar una aplicación coherente y efectiva.

La falta de detalles en la arquitectura de red, como marcas y modelos de equipos, dificulta la gestión y el mantenimiento de la red. Sin esta información detallada, es más difícil realizar actualizaciones, identificar posibles puntos de fallo y mantener un inventario preciso de los activos de red. Esto puede llevar a un aumento de los tiempos de inactividad y a una menor eficiencia en la gestión de la red.

La ausencia de registros de configuraciones y políticas de seguridad en los firewalls representa un riesgo significativo para la seguridad de la red. Sin un registro claro de las configuraciones y políticas establecidas en estos dispositivos, es difícil garantizar que se estén aplicando las medidas de seguridad adecuadas. Esto puede dejar a la red vulnerable a ataques y dificultar la identificación y solución de problemas de seguridad.

Además, la falta de documentación detallada sobre la segmentación de redes hace difícil comprender cómo se ha implementado y gestionado esta medida de seguridad. La segmentación de redes es crucial para limitar el alcance de posibles ataques y proteger los datos sensibles, pero sin una documentación adecuada, es difícil garantizar su efectividad y mantenerla adecuadamente en el tiempo.

Tabla 9. Medidas de seguridad

Medidas de Seguridad	Descripción	Estado actual	Observaciones
Encriptación de Datos	Métodos de encriptación de datos utilizados para proteger la confidencialidad de la información en tránsito y en reposo.	No se dispone de encriptación de datos.	Se recomienda implementar métodos de encriptación tanto en tránsito como en reposo para proteger los datos sensibles.
Protocolos de Acceso y Autenticación	Protocolos y métodos utilizados para autenticar y gestionar el acceso a la red interna	Se dispone de varios métodos de autenticación dependiendo los servicios, correo institucional, portafolio institucional, aulas virtuales, servicios federados, etc.	Es importante asegurar que estos métodos sean robustos y estén actualizados para prevenir accesos no autorizados.
Herramientas de Monitoreo y Detección de Intrusiones	Herramientas utilizadas para monitorear y detectar intrusiones y actividades sospechosas en la red interna	Se dispone de un equipo firewall que presenta características de IPS e IDS	Es fundamental realizar revisiones periódicas y actualizaciones de estas herramientas para garantizar su efectividad en la detección y prevención de intrusiones y amenazas.

4.2.3.2. Análisis de medidas de seguridad

En el análisis de las medidas de seguridad, se observa la importancia crítica de tres aspectos fundamentales en la protección de la red interna de la UPEC: la encriptación de datos, los protocolos de acceso y autenticación, y las herramientas de monitoreo y detección de intrusiones.

La ausencia de encriptación de datos constituye un riesgo significativo para la confidencialidad de la información. Sin este mecanismo de protección, los datos quedan expuestos a posibles accesos no autorizados, lo que podría comprometer tanto su integridad como su privacidad. Implementar una sólida encriptación de datos es crucial para garantizar que la información sensible esté protegida adecuadamente contra posibles amenazas.

Además, aunque existan múltiples métodos de autenticación para diversos servicios, la falta de aplicación de protocolos de acceso y autenticación incrementa la vulnerabilidad de la red interna. Esta situación puede propiciar accesos no autorizados a los sistemas y datos de la institución, comprometiendo la seguridad de la información. Resulta fundamental implementar y mantener protocolos robustos de autenticación para proteger de manera adecuada los recursos de la red.

Por último, a pesar de contar con un Firewall que incluye capacidades de detección de intrusiones, la ausencia de herramientas adicionales de monitoreo y detección limita la capacidad del departamento de Redes y Telecomunicaciones para identificar y responder de manera proactiva a posibles amenazas de seguridad. La implementación de herramientas de monitoreo y detección de intrusiones proporcionaría una capa adicional de seguridad, permitiendo una detección temprana de actividades sospechosas y una respuesta rápida ante posibles incidentes de seguridad.

Tabla 10. Análisis de Vulnerabilidades

Evaluación de vulnerabilidades	Descripción	Estado actual	Observaciones
Resultados de Escaneo de Vulnerabilidades	Resultados de escaneos de vulnerabilidades en la red interna, incluyendo detalles sobre las vulnerabilidades identificadas	Se obtienen resultados periódicos de los escaneos a vulnerabilidades de nuestros servidores institucionales configurados con IP pública.	Se recomienda mantener un registro de los hallazgos y realizar seguimiento a las vulnerabilidades para garantizar su remediación.
Pruebas de Penetración Autorizadas	Resultados y hallazgos de pruebas de penetración autorizadas realizadas en la red interna	No se han realizado pruebas de penetración autorizadas en la red interna.	Se recomienda mantener un registro de los hallazgos y realizar seguimiento a las vulnerabilidades para garantizar su remediación.

Tabla 11. Incidentes de seguridad

Incidentes de seguridad anteriores	Descripción	Estado actual	Observaciones
Descripción de Incidentes Anteriores	Descripción de incidentes de seguridad anteriores registrados en la red interna, incluyendo impacto y medidas tomadas	No se dispone de una Descripción de Incidentes Anteriores de seguridad.	Establecer un registro detallado de todos los incidentes de seguridad, incluyendo el impacto y las medidas tomadas para mitigar futuros riesgos.
Medidas Correctivas Implementadas	Detalles sobre las medidas correctivas implementadas después de incidentes de seguridad	No se dispone de un documento donde se detalle las medidas correctivas implementadas después de los incidentes de seguridad	Establecer un registro detallado de todos los incidentes de seguridad, incluyendo el impacto y las medidas tomadas para mitigar futuros riesgos.

4.2.3.3. Análisis de vulnerabilidades de seguridad

Se destacan una serie de deficiencias en la gestión de la seguridad de la red interna que demandan una atención inmediata. En primer lugar, los resultados de los escaneos de vulnerabilidades muestran deficiencias alarmantes. A pesar de que se realizan escaneos periódicos, la falta de seguimiento y mitigación de las vulnerabilidades identificadas sugiere una brecha significativa en el proceso de gestión de la seguridad de la red interna. Esta omisión expone a la organización a un riesgo considerable de ataques cibernéticos y potenciales violaciones de seguridad.

Del mismo modo, la ausencia de pruebas de penetración autorizadas es preocupante desde el punto de vista de la seguridad cibernética. Estas pruebas son esenciales para identificar las debilidades y los vectores de ataque potenciales en la red interna.

La falta de estas evaluaciones rigurosas deja a la red vulnerable a posibles explotaciones por parte de usuarios malintencionados, lo que podría resultar en la pérdida de datos sensibles, interrupción de servicios críticos o incluso daños a la reputación de la organización.

Además, la carencia de documentación detallada sobre incidentes de seguridad anteriores y las medidas correctivas implementadas después de dichos incidentes refleja una falta crítica de seguimiento y aprendizaje en la organización.

Sin un registro exhaustivo de incidentes pasados y las acciones tomadas para mitigarlos, la institución pierde valiosas oportunidades de aprendizaje y mejora continua en materia de seguridad. Esto no solo pone en riesgo la seguridad de la red interna, sino que también compromete la capacidad de la organización para cumplir con las regulaciones de seguridad y proteger la confidencialidad, integridad y disponibilidad de los datos críticos.

4.2.4. Diagnóstico FODA

Se lleva a cabo el análisis de la matriz FODA para presentar las fortalezas, oportunidades, debilidades y amenazas que se encuentran dentro del departamento de TIC y de Redes y Telecomunicaciones de la Universidad Politécnica Estatal del Carchi, utilizando los datos recopilados durante la investigación de campo.

Tabla 12. Matriz FODA

FORTALEZAS	OPORTUNIDADES
• Software empleado en la UPEC es bajo software libre. • Cada uno del personal de TIC dispone de equipo informático y software especializado. • Personal capacitado para realizar sus actividades académicas y administrativas • La institución reconoce el valor de los datos sensibles. • Contraseñas para el uso de los equipos de la institución.	• Instalación de un Next Generation Firewall para la protección perimetral. • Estandarización de la institución con la norma ISO 27001. • Capacitar a usuarios de manera periódica sobre la seguridad de la información. • Implementación de nuevas herramientas tecnológicas para la seguridad de la información. • Instalación de Antivirus Institucional.
DEBILIDADES	**AMENAZAS**

• Políticas de seguridad de la información definidas, pero no aplicadas completamente • El acceso al área de servidores no se encuentra bien protegido. • Recursos económicos no suficientes para implementar tecnología nueva. • Servidores obsoletos, dañados o con partes quemadas.	• Usuarios finales que no tienen software de protección informática instalada. • Perdida de información por no verificar las copias de seguridad una vez que se ejecuten. • Afectación a la integridad de los datos por accesos permitidos no controlados. • No se tiene un Antivirus Institucional para los equipos informáticos.

4.2.5. Reflexiones y propuestas del presente

Reflexiones

- La falta de encriptación de datos, protocolos de acceso y autenticación débiles, y la ausencia de herramientas de monitoreo y detección de intrusiones representan graves riesgos para la seguridad de la red interna.
- La carencia de registros de incidentes y medidas correctivas anteriores indica una falta de seguimiento y aprendizaje de las vulnerabilidades pasadas.
- La gestión efectiva y el mantenimiento de la red se ven obstaculizados por la falta de documentación precisa en la arquitectura de red, políticas de seguridad, registros de configuraciones y segmentación de redes.
- La implementación efectiva de las políticas de seguridad de la información se ve obstaculizada por la falta de accesibilidad y conocimiento de las mismas por parte del personal.

Propuestas

- Elaborar un plan de seguridad que englobe todos los activos de información de la empresa, siguiendo estándares reconocidos como la ISO 27001. Esta norma ofrece un enfoque sistemático para implementar controles apropiados a los activos, garantizando la protección y el valor añadido de la información de la organización.
- Actualizar y completar la documentación de la infraestructura de red, detallando las marcas y modelos de los equipos, las configuraciones de los dispositivos y la segmentación de redes.
- Crear un procedimiento oficial para registrar incidentes y tomar medidas correctivas con el fin de mejorar la respuesta ante posibles brechas de seguridad. Esto facilitará el aprendizaje de vulnerabilidades pasadas.
- Crear una gestión de riesgos efectiva utilizando una metodología apropiada permitirá identificar amenazas en los activos de información de manera

eficiente. Esto facilitará el establecimiento de medidas de seguridad adecuadas para responder eficazmente ante cualquier incidente.

4.2.6. Plan de seguridad de la información

El plan de seguridad de la información desarrollado en el departamento de TIC de la Universidad Politécnica Estatal del Carchi tiene como objetivo servir de guía para futuras investigaciones para instituciones que manejan activos de información con un alto nivel de riesgo o vulnerabilidad dentro de sus actividades académicas, proporcionándoles las directrices necesarias para la gestión de su seguridad informática y permitiendo conocer cómo se gestiona actualmente.

El plan se basa en la Norma ISO/IEC 27001:2022, considerando las 4 partes de este estándar como las directrices que fundamentarán su desarrollo, teniendo en cuenta las versiones actuales de las partes de este estándar y los estándares que reemplazaron algunas de ellas.

El plan se aplicará y validará tomando en consideración si es o no oportuno aplicarlo, y esto lo realizara el director de TIC una vez el plan sea acogido por parte del departamento. El objetivo es que este plan ayude al manejo de la seguridad de la información y a su vez aportar a la seguridad que debería tener su infraestructura, de manera que puedan brindar seguridad, continuidad, confiabilidad y servicio de calidad.

4.2.7. Elaboración del Plan de Seguridad de la información

Según las consideraciones previamente mencionadas, se establecerán una introducción, el alcance y los objetivos, para luego proceder con la elaboración del plan de seguridad informática.

4.2.7.1. Introducción

El crecimiento acelerado en el uso de tecnologías de la información dentro de la UPEC hace indispensable la implementación de Sistemas Informáticos robustos, así como la definición de planes de Seguridad Informática para proteger los activos más valiosos de la universidad, su información. Por ello, es fundamental aplicar estándares reconocidos a nivel mundial como la norma ISO 27001, la cual proporciona un marco adecuado para la gestión de la seguridad de la información.

El objetivo de desarrollar un plan de seguridad informática basado en la ISO 27001 es proporcionar una guía clara para gestionar eficazmente los riesgos relacionados con

la seguridad de la información, estableciendo prioridades en su tratamiento. Este plan debe ser adaptable a la estructura organizacional de la UPEC, su tamaño, misión y la naturaleza de la información que maneja.

Es importante destacar que la implementación de un plan de seguridad informática requiere una inversión considerable de recursos, tanto humanos como financieros. Por ello, la universidad debe tener plenamente documentados los costos y beneficios asociados, garantizando que la adopción de este plan responda a una necesidad estratégica justificada.

4.2.7.2. Alcance

El alcance del plan dependerá totalmente de la Universidad Politécnica Estatal del Carchi, abarcando el departamento de TIC. Luego de determinar el alcance, se deben identificar los activos de información que serán la parte esencial del plan, ya que en base a estos se seleccionarán y definirán las políticas de seguridad.

4.2.7.3. Política de Seguridad

Una vez que se ha delimitado claramente el alcance del plan, la universidad procede a definir las políticas de seguridad necesarias para iniciar la implementación del plan de seguridad de la información. Estas políticas constituyen la base para garantizar la protección de los activos informáticos y deben alinearse con los objetivos estratégicos de la institución, así como con las normativas vigentes.

De acuerdo con el alcance definido, será responsabilidad del director del departamento de TIC, revisar y aprobar las políticas de seguridad, asegurando su coherencia con los lineamientos corporativos. Además, es esencial garantizar que estas políticas sean debidamente comunicadas a todos los actores involucrados en el proceso, que comprendan el impacto y las responsabilidades que conllevan, y que se asegure su correcta implementación y cumplimiento en toda la comunidad universitaria de la UPEC.

4.2.8. Enfoque para la Administración del Riesgo

Es esencial establecer un equilibrio adecuado entre los tres pilares fundamentales de la seguridad de la información: confidencialidad, disponibilidad e integridad. La confidencialidad garantiza que el acceso a la información esté restringido solo a personas autorizadas, mientras que la disponibilidad asegura que la información esté

accesible en el momento y lugar requeridos por quienes la necesiten. La integridad, por su parte, protege la exactitud y fiabilidad de los datos.

Por ello, es crucial diseñar e implementar políticas de seguridad que encuentren un punto de equilibrio entre la protección frente a accesos no autorizados y la facilidad de acceso por parte de quienes requieren la información para cumplir con sus funciones, minimizando de este modo los riesgos asociados a cada uno de estos factores.

4.2.8.1. Cálculo de riesgo

Para llevar a cabo el análisis de riesgos, es necesario realizar las siguientes actividades:

- Identificar los activos clave.
- Valorar los activos, tomando en cuenta los posibles impactos derivados de la pérdida de confidencialidad, integridad y disponibilidad.
- Detectar las amenazas y vulnerabilidades asociadas a cada activo.
- Estimar la probabilidad de que las amenazas y vulnerabilidades identificadas se materialicen.

4.2.9. Análisis de riesgo

4.2.9.1. Identificación de activos

La identificación de los activos de información del departamento de TIC de la Universidad Politécnica Estatal del Carchi es fundamental para implementar un plan de seguridad de información efectivo, ya que en base a estos se definirán las políticas de seguridad. Comprender claramente qué se considera un activo de información es crucial para realizar un análisis y evaluación de riesgos adecuados, dado que los activos de información abarcan un amplio rango.

4.2.9.2. Metodología MAGERIT

La metodología se centra en el análisis y manejo de riesgos mediante un enfoque sistemático que toma en cuenta las tecnologías de la información y comunicación. Su meta es implementar controles efectivos para minimizar los riesgos a los que se enfrentan los activos de información.

Según PAE (2021):

> MAGERIT es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad

(ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización.

La eficacia de esta metodología radica en su enfoque en los activos más críticos de la empresa, específicamente aquellos relacionados con la información.

MAGERIT persigue los siguientes Objetivos Directos:

- Sensibilizar a los responsables de las organizaciones sobre la existencia de riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a identificar y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La eficacia de esta metodología radica en su enfoque en los activos más críticos de la empresa, específicamente aquellos relacionados con la información.

4.2.9.3. Tasación de activos

Para detectar los posibles riesgos en los activos de información, se realiza una evaluación de cada uno de ellos considerando su grado de Confidencialidad, Disponibilidad e Integridad.

Esta evaluación se lleva a cabo en una escala del 1 al 5, y es coordinada por el departamento de Redes y Telecomunicaciones bajo la supervisión del Ingeniero Javier Torres.

Tabla 13: Tasación de activos

Niveles	Valor
Extrema	5
Alta	4
Media	3
Regular	2
Deficiente	1

Tomando los niveles de confidencialidad, disponibilidad y la integridad vamos a identificar los riesgos de los activos más importantes para la institución.

Tabla 14: Tasación de activos de información

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Data Center	3	5	4	4
Instalaciones administrativas	4	4	4	4
Instalaciones gerenciales	3	3	2	2,67
Seguridad Física	4	4	4	4
Servidor DMZ-11	4	4	4	4
Servidor DMZ-12	4	4	4	4
Servidor DMZ-13	4	4	4	4
Servidor DMX-15	4	4	4	4
Servidor INT-105	4	4	4	4
Servidor INT-120	4	4	4	4
Servidor INT-140	4	4	4	4
Computadores de escritorio	4	4	4	4
Computadores portátiles	4	4	4	4
Impresoras	4	3	2	3
Switches	3	4	3	3,33
Routers	4	4	3	3,67
Access Point	4	4	3	3,67
Windows Server 2012	3	4	4	3,67
Sistema operativo Windows	4	3	4	3,67
Distribución de Linux	4	4	4	4
Microsoft Office	3	4	3	3,33
Oracle Apex	4	4	4	4
Sistemas de gestión académica	5	5	5	5
Software de investigación	5	5	5	5
Software de seguridad	5	5	4	4,67
Software de gestión de recursos	4	4	3	3,67
Bases de datos de empleados	5	5	5	5
Bases de datos de administrativos	5	5	5	5
Bases de datos estudiantes de carrera	5	5	5	5
Bases de datos de estudiantes egresados	5	5	5	5
Bases de datos de estudiantes posgrados	4	5	5	4,67
Bases de datos Pago de aranceles	5	5	5	5
Bases de datos proveedores	4	4	5	4,33
Backups generadas de bases de datos	3	3	3	3
Bases de datos Correos Institucionales	3	2	3	2,67
Centro de Procesos de datos	4	3	4	3,67
Acceso a internet	5	5	3	4,33
Líneas telefónicas	4	3	3	3,33
Fax	3	2	2	2,33
Red de acceso inalámbrico	3	4	4	3,67
Red cableada	4	4	4	4
Correo institucional	5	5	5	5
Portafolio institucional	4	4	5	4,33
Backups de usuarios	2	2	3	2,33
Internet	4	4	3	3,67
Aulas virtuales	3	2	2	2,33
Servicios federados	3	3	4	3,33
Aire acondicionado (Data Center)	3	5	4	4
Cableado LAN	4	4	4	4

Cableado eléctrico	4	4	3	3,67
Racks	4	4	4	4
Personal académico	3	2	2	2,33
Personal administrativo	3	3	2	2,67
Personal Investigación	2	2	2	2
Servicios estudiantiles	2	2	2	2
Personal biblioteca	3	1	2	2
Discos Duros Backups	3	4	4	3,67
USB	2	3	3	2,67
Equipos de respaldo	4	3	4	3,67
Servicio en la nube	4	3	4	3,67

A continuación, es necesario llevar a cabo la identificación de los activos. En este caso, se empleará la metodología MAGUERIT, que permite estructurar esta identificación en siete categorías, facilitando así la clasificación de los activos de información previamente mencionados.

Tabla 15. Activos según MAGERIT

Activos	Descripción
Instalaciones	Ubicaciones donde se alojan los sistemas de información y comunicaciones.
Hardware	Los recursos materiales y físicos, destinados a sustentar directa o indirectamente los servicios que proporciona la organización.
Software	Tareas que han sido automatizadas para su ejecución por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos, permitiendo la explotación de la información para la prestación de servicios.
Datos	La información que permite a la organización brindar sus servicios.
Redes y comunicaciones	Son los medios de transporte que trasladan datos de un lugar a otro. Se incluyen tanto las instalaciones dedicadas como los servicios de comunicaciones contratados a terceros.
Equipamiento Auxiliar	Otros equipos que sirven de apoyo a los sistemas de información, sin estar directamente relacionados con ellos.
Personal	Personas vinculadas con los sistemas de información.
Soportes de información	Dispositivos físicos que permiten almacenar información de manera permanente o, al menos, durante largos períodos de tiempo.

4.2.10. Identificación de amenazas y vulnerabilidades

Todos los activos identificados en una organización están expuestos a amenazas, las cuales pueden clasificarse de diversas maneras según su origen, naturaleza, entre otros aspectos.

4.2.10.1. Clasificación de amenazas

La metodología MAGERIT categoriza las amenazas asignándoles un código específico, teniendo en cuenta su relación directa con los activos de información y el impacto potencial que estas amenazas pueden generar en los principios fundamentales de seguridad de la información: confidencialidad, integridad y disponibilidad. Este enfoque permite una evaluación estructurada de los riesgos asociados. En el Anexo 8, se puede observar el desglose detallado de dichas

amenazas. Además, la Tabla 16 ofrece una clasificación exhaustiva de estas amenazas, proporcionando una visión clara de su jerarquización y relevancia en el contexto de la seguridad de los sistemas de información.

Tabla 16: Clasificación de amenazas

ID	Amenaza	Descripción
N1	Fuego	Desastres Naturales (N)
N2	Daños por agua	
N3	Rayos	
N4	Tormenta Eléctrica	
N5	Terremoto	
I1	Fuego	De origen Industrial (I)
I2	Daños por agua	
I3	Explosiones	
I4	Derrumbes	
I5	Contaminación química	
I6	Sobrecarga Eléctrica	
I7	Fluctuaciones Eléctricas	
I8	Accidentes de tráfico	
I9	Contaminación mecánica	
I10	Contaminación Electromagnética	
I11	Avería de origen físico o lógico	
I12	Corte de suministro eléctrico	
I13	Condiciones inadecuadas de temperatura o humedad	
I14	Fallo de servicios de comunicaciones	
I15	Irrupción de otros servicios y suministros esenciales	
I16	Degradación de los soportes de almacenamiento de la información	
I17	Emanaciones electromagnéticas	
E1	Errores de usuarios	Errores y fallos no intencionados (E)
E2	Errores de administrador	
E3	Errores de monitorización	
E4	Errores de configuración	
E7	Deficiencias en la organización	
E8	Difusión de software dañino	
E9	Errores de Re-encaminamiento	
E10	Errores de secuencia	
E14	Escapes de información	
E15	Alteración accidental de la información	
E18	Destrucción de información	
E19	Fugas de información	
E20	Vulnerabilidades de los programas	
E21	Errores de mantenimiento / Actualización de programas	
E23	Errores de mantenimiento / Actualización de equipos	
E24	Caída del sistema por agotamiento de recursos	

E25	Perdida de equipos	
E28	Indisponibilidad del personal	
A3	Manipulación de los registros de actividad	Ataques intencionados (A)
A4	Manipulación de la configuración	
A5	Suplantación de la identidad del usuario	
A6	Abuso de privilegios de acceso	
A7	Uso no previsto	
A8	Difusión de software dañino	
A9	Re-encaminamiento de mensajes	
A10	Alteración de secuencia	
A11	Acceso no autorizado	
A12	Análisis de tráfico	
A13	Repudio	
A14	Intercepción de información	
A15	Modificación deliberada de la información	
A18	Destrucción de la información	
A19	Divulgación de la información	
A22	Manipulación de ´programas	
A23	Manipulación de los equipos	
A24	Denegación de servicio	
A25	Robo	
A26	Ataque destructivo	
A27	Ocupación enemiga	
A28	Indisponibilidad del personal	
A29	Extorsión	
A30	Ingeniería social	

Fuente: (Ministerio de Hacienda y Administraciones Publicas, 2023)

Como se muestra en la Tabla 16, las amenazas pueden tener su origen tanto en desastres naturales como en ataques intencionados, y para que estas puedan ocasionar un impacto en los activos de información, deben explotar una o más vulnerabilidades identificadas.

Una vez que las amenazas han sido determinadas, se procedió con la evaluación de la probabilidad de ocurrencia. Esta medición se realizó de manera conjunta con el director del departamento de TIC y se basó en estudios previos sobre las amenazas. La evaluación se llevó a cabo con un enfoque colaborativo, integrando las perspectivas y conocimientos del director y del equipo de TIC.

Además, la evaluación fue respaldada mediante el análisis de estadísticas pertinentes, lo que permitió una comprensión más profunda de la naturaleza de las amenazas y su probabilidad de ocurrencia.

Por lo que como se muestra en la tabla 17 se dan los parámetros para evaluar el impacto que tiene estas amenazas a la confidencialidad, integridad y disponibilidad de los activos de información.

Tabla 17: Frecuencias de impacto

Frecuencias	ID	Rango	Valor
Frecuencia Extrema	MA	1 vez al día	Valor > 95%
Frecuencia Alta	A	1 vez cada 2 semanas	75% < Valor > 95%
Frecuencia Media	M	1 vez cada 2 meses	50% < Valor > 75%
Frecuencia Baja	B	1 vez cada 6 meses	30% < Valor > 50%
Frecuencia Muy Baja	MB	1 vez al año	10% < Valor > 30%

En esta etapa, la universidad debe tomar decisiones estratégicas respecto al análisis de las amenazas. Es crucial revisar con especial atención la decisión sobre cuáles amenazas serán descartadas debido a su baja probabilidad de ocurrencia. Existe la posibilidad de que una amenaza con baja probabilidad de materializarse pueda generar las consecuencias más graves para el departamento de TIC. Por lo tanto, es indispensable considerar tanto la probabilidad como el impacto antes de tomar decisiones definitivas sobre la mitigación o eliminación de riesgos.

4.2.11. Evaluación y análisis del riesgo

El análisis del riesgo permite identificar, cuantificar y evaluar los riesgos asociados a los activos de información, basándose en un proceso exhaustivo de identificación de activos y en el cálculo detallado de las amenazas que podrían comprometer su seguridad. Este proceso incluye la estimación de la frecuencia con la que cada amenaza podría materializarse, así como la evaluación del impacto que tendría en los distintos pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.

El análisis proporciona una visión integral de las amenazas que enfrenta la Universidad Politécnica Estatal del Carchi y el Departamento de TIC, facilitando la toma de decisiones informadas sobre las medidas de mitigación y protección necesarias para salvaguardar sus activos.

Tabla 18: Análisis del Riesgo

Definición	Amenaza	Activo afectado	Frecuencia	% Impacto C	D	I
Desastres naturales (N)	Fuego N1	Instalaciones (L)	MB		100	
		Hardware (HW)	MB		100	
		Red de comunicaciones (COM)	MB		100	

		Equipamiento Auxiliar (AUX)	MB	75
	Daños por agua (N2)	Instalaciones (L)	MB	75
		Hardware (HW)	MB	75
		Red de comunicaciones (COM)	MB	100
		Equipamiento auxiliar (AUX)	MB	75
	Rayos (N3)	Instalaciones (L)	MB	50
		Hardware (HW)	MB	75
		Red de comunicaciones (COM)	MB	60
		Equipamiento auxiliar (AUX)	MB	75
	Tormenta Eléctrica (N4)	Hardware (HW)	MB	75
		Red de comunicaciones (COM)	MB	100
		Equipamiento auxiliar (AUX)	MB	75
	Terremoto (N5)	Instalaciones (L)	MB	75
		Hardware (HW)	MB	75
		Equipamiento auxiliar (AUX)	MB	75
De origen industrial (I)	Fuego (I1)	Instalaciones (L)	MB	100
		Hardware (HW)	MB	100
		Red de comunicaciones(COM)	MB	100
		Equipamiento Auxiliar (AUX)	MB	100
	Daños por agua (I2)	Instalaciones (L)	MB	75
		Hardware (HW)	MB	100
		Red de comunicaciones(COM)	MB	100
		Equipamiento Auxiliar (AUX)	MB	75
	Explosiones (I3)	Instalaciones (L)	MB	100
		Hardware (HW)	MB	100
		Red de comunicaciones(COM)	MB	100
		Equipamiento Auxiliar (AUX)	MB	100
	Derrumbes (I4)	Instalaciones (L)	MB	100
		Hardware (HW)	MB	80
		Red de comunicaciones(COM)	MB	60
		Equipamiento Auxiliar (AUX)	MB	60
	Contaminación química (I5)	Instalaciones (L)	MB	50
		Hardware (HW)	MB	50
		Red de comunicaciones(COM)	MB	75
		Equipamiento Auxiliar (AUX)	MB	60
	Sobrecarga eléctrica (I6)	Instalaciones (L)	MB	50
		Hardware (HW)	B	75
		Red de comunicaciones(COM)	B	60
		Equipamiento Auxiliar (AUX)	B	60
		Instalaciones (L)	MB	50

	Fluctuaciones eléctricas (I7)	Hardware (HW)	B		60	
		Red de comunicaciones(COM)	MB		60	
		Equipamiento Auxiliar (AUX)	MB		50	
	Accidentes de tráfico (I8)	Instalaciones (L)	MB		60	
		Hardware (HW)	MB		30	
		Red de comunicaciones(COM)	MB		30	
		Equipamiento Auxiliar (AUX)	MB		30	
	Contaminación mecánica (I9)	Instalaciones (L)	MB		30	
		Hardware (HW)	MB		50	
		Red de comunicaciones(COM)	MB		50	
		Equipamiento Auxiliar (AUX)	MB		50	
	Contaminación electromagnética (I10)	Instalaciones (L)	MB		50	
		Hardware (HW)	MB		75	
		Red de comunicaciones(COM)	MB		75	
		Equipamiento Auxiliar (AUX)	MB		75	
	Avería de origen físico o lógico (I11)	Instalaciones (L)	B		20	
		Hardware (HW)	M		75	
		Red de comunicaciones(COM)	M		75	
		Equipamiento Auxiliar (AUX)	M		40	
		Software (SW)	M		75	
		Servicios (S)	M		80	
		Datos (D)	B		25	
	Corte de suministro eléctrico (I12)	Hardware (HW)	B		100	
		Red de comunicaciones(COM)	B		100	
		Equipamiento Auxiliar (AUX)	B		100	
	Condiciones inadecuadas de temperatura o humedad (I13)	Red de comunicaciones(COM)	B		60	
		Red de comunicaciones(COM)	B		60	
		Equipamiento Auxiliar (AUX)	B		60	
	Fallo de servicios de comunicaciones (I14)	Acceso a Internet Principal (COM)	M		100	
		Acceso a Internet Edificios (COM)	M		100	
		Líneas móviles (COM)	M		100	
		Servicios (S)	M		100	
	Irrupción de otros servicios y suministros esenciales (I15)	Equipamiento Auxiliar (AUX)	B		60	
	Degradación de los soportes de almacenamiento de la información (I16)	Hardware (HW)	MB		100	
		Hardware (HW)				
	Emanaciones electromagnéticas (I17)	Instalaciones (L)	MB		20	20
		Hardware(HW)	MB		50	50
		Equipamiento Auxiliar (AUX)	MB		20	20
Errores y fallos no	Errores de usuarios (E1)	PCs (HW)	M	20	60	20
		Móviles (HW)	M	25	60	20
		Datos (D)	M	75	75	30

intencionados (E)		Instalaciones (L)	M	25	20	60
	Errores de administrador (E2)	Instalaciones (L)	B	20	50	20
		Hardware (HW)	M	20	75	20
		Software(SW)	M	20	75	20
		Datos (D)	M	20	75	20
		Equipamiento Auxiliar (AUX)	M		75	
		Servicios (S)	M		80	
		Datos (D)	M		75	
		Software (SW)	B		75	
	Errores de configuración (E4)	Datos (D)	B		50	
		Equipamiento Auxiliar (AUX)	B		50	
		Personal (P)	M	50	75	30
	Deficiencias en la organización (E7)	Datos (D)	M	75	75	30
		Servicios (S)	M	50	75	30
	Difusión de software dañino (E8)	Software (SW)	B	75	75	75
	Errores de re-encaminamiento (E9)	Red de Comunicaciones (COM)	MB	40	75	
		Servicios (S)	MB	60	75	
		Software (SW)	B		100	
	Errores de secuencia (E10)	Servicios (S)	MB	50	75	
		Red de Comunicaciones (COM)	MB	50	75	
		Software (SW)	B	50	75	
	Escapes de información (E14)	Servicios (S)	MB	50		
		Software (SW)	B	50		
		Datos (D)	B	100		
	Alteración accidental de la información (E15)	Datos (D)	M			75
		Servicios (S)	MB			50
	Destrucción de información (E18)	Datos (D)	MB		100	
	Fugas de información (E19)	Software (SW)	B	65		
		Servicios (S)	MB	30		
		Datos (D)	MB	100		
	Vulnerabilidades de los programas (E20)	Datos (D)	M	75	75	25
		Software (SW)	M	75	75	25
	Errores de mantenimiento / Actualización de programas (E21)	Software (SW)	B		75	60
	Errores de mantenimiento / Actualización de equipos (E23)	Hardware (HW)	B		75	
	Caída del sistema por agotamiento de recursos	Equipos informáticos (HW)	MB		100	
		Servicios (S)	MB		100	
		Redes de comunicaciones (COM)	MB		100	
	Perdida de equipos (E25)	Equipos informáticos - Hardware (HW)	B	50	100	
	Indisponibilidad del personal (E28)	Personal (P)	A		100	
	Manipulación de los registros de actividad (A3)	Servicios (S)	MB			

	Manipulación de la configuración (A4)	Servicios (S)	MB	75		75
		Datos	MB	75		75
	Suplantación de la identidad del usuario (A5)	Software (SW)	B	100		80
		Datos (D)	B	100		80
		Red de comunicaciones (COM)	B	75		75
		Servicios (S)	B	75		75
	Abuso de privilegios de acceso (A6)	Instalaciones (L)	B	75		75
		Software (SW)	B	75	50	50
		Red de comunicaciones (COM)	B	75	50	50
		Servicios (S)	B	75	50	50
	Uso no previsto (A7)	Instalaciones (L)	MB	25	25	25
		Software (SW)	MB	25	25	25
		Red de comunicaciones (COM)	MB	25	25	25
		Servicios (S)	MB	25	25	25
		Hardware (HW)	MB	25	25	25
	Difusión de software dañino (A8)	Software (SW)	B	75	75	20
		Datos (D)	B	75	75	20
Ataques intencionados (A)	Re-encaminamiento de mensajes (A9)	Servicios (S)	MB	50	75	
		Redes de comunicaciones (COM)	MB	50	75	
		Software (SW)	MB	50	75	
	Alteración de secuencia (A10)	Software (SW)	B	50	75	
		Servicios (S)	MB	50	75	
		Red de comunicaciones (COM)	MB	50		
	Acceso no autorizado (A11)	Instalaciones (L)	B	20	20	20
		Hardware (HW)	MB		50	
		Software (SW)	B	75	75	75
		Datos (D)	B	100	100	100
		Red de comunicaciones (COM)	B	30	75	30
		Equipamiento Auxiliar (AUX)	B		50	
		Servicios (S)	B	75	75	50
	Análisis de tráfico (A12)	Datos (D)	MB	50		
	Repudio (A13)	Servicios (S)	MB			
	Interpretación de información (A14)	Redes de comunicaciones (COM)	B	100		
	Modificación deliberada de la información (A15)	Datos (D)	B			100
		Software (SW)	B			100
	Destrucción de la información (A18)	Datos (D)	B		100	
		Software (SW)	B		100	

	Divulgación de la información (A19)	Datos (D)	B	100		
		Software (SW)	B	100		
	Manipulación de programas (A22)	Software (SW)	B		100	
	Manipulación de los equipos (A23)	Hardware (HW)	B		100	
	Denegación de servicio (A24)	Servicios (S)	B		100	
		Red de comunicaciones (COM)	B		100	
	Robo (A25)	Hardware (HW)	B		75	
		Equipo auxiliar (AUX)	MB		75	
	Ataque destructivo (A26)	Datos (D)	MB	100	100	
		Instalaciones (L)	MB		100	
		Hardware (HW)	MB		100	
		Equipamiento Auxiliar (AUX)	MB		100	
		Red de comunicaciones (COM)	MB		100	
		Servicios (S)	MB		100	
		Datos (D)	MB		100	
	Ocupación enemiga (A27)	Instalaciones (L)	MB	20	100	
		Hardware (HW)	MB	20	100	
		Software (SW)	MB	75	100	
		Equipamiento Auxiliar (AUX)	MB	20	100	
		Red de comunicaciones (COM)	MB	30	100	
		Servicios (S)	MB	80	100	
		Datos (D)	MB	100	100	
	Indisponibilidad del personal (A28)	Personal (P)	M		100	
	Extorsión (A29)	Personal (P)	B	25	25	20
	Ingeniería social (A30)	Personal (P)	B	20	20	20

4.2.11.1. Valoración del Riesgo

Para evaluar el riesgo, es necesario identificar las amenazas más relevantes, para lo cual se utiliza los siguientes criterios:

- Consecuencias económicas del riesgo.
- Duración estimada para la recuperación de la Universidad.
- Probabilidad efectiva de que el riesgo se materialice.
- Potencial de interrupción de las operaciones de la Universidad.

Tabla 19. Valoración del Riesgo

Riesgo		**Criterios para evaluar la importancia del riesgo**				
Activos	Amenazas	Consecuencias económicas del riesgo	Duración estimada para la recuperación de la Universidad	Probabilidad efectiva de que el riesgo se materialice	Potencial de interrupción de las operaciones de la Universidad	Total

4.2.12. El manejo del riesgo y el proceso de toma de decisiones

Después de completar el análisis y la evaluación del riesgo, es necesario determinar las medidas que se implementarán en relación con los activos involucrados. Esto implica tomar decisiones sobre cómo gestionar los riesgos identificados, ya sea mediante la mitigación, transferencia, aceptación o eliminación de los mismos, con el objetivo de proteger y optimizar el uso de dichos activos dentro de la organización.

4.2.12.1. Toma de decisiones

Una vez evaluado el riesgo, se debe proceder con la toma de decisiones para determinar su tratamiento. Esta decisión está principalmente condicionada por los objetivos estratégicos de la organización y suele estar vinculada a dos factores clave:

- El impacto potencial en caso de materialización del riesgo.
- La probabilidad de ocurrencia del riesgo.

4.2.12.2. Estrategia para reducción de riesgo

Si se opta por la reducción del riesgo, es crucial definir con precisión los controles que permitirán implementar dicha decisión. Los controles reducen el riesgo de dos maneras:

- Disminuyendo la probabilidad de que una vulnerabilidad sea explotada por una amenaza.
- Mitigando el impacto potencial en caso de materialización del riesgo, mediante la detección de eventos no deseados, así como la respuesta y recuperación ante los mismos.

No existe un enfoque universal para seleccionar objetivos de control y controles específicos. Este proceso implica múltiples decisiones y consultas, generalmente mediante discusiones con diversas partes de la institución y con personal clave.

En última instancia, la selección de controles debe generar un resultado que se ajuste de manera óptima a los requisitos específicos de la Universidad y el departamento de TIC.

4.2.12.3. Aceptar el riesgo

En ocasiones, el departamento no identifica controles efectivos para mitigar un riesgo, y en la mayoría de estos casos, la implementación de los controles resulta más

costosa que las consecuencias asociadas al riesgo. En este contexto, la opción más apropiada es aceptar el riesgo.

Esta aceptación debe ser documentada, estableciendo claramente los criterios de aceptación. La aprobación final de la aceptación del riesgo debe ser autorizada y firmada por la alta gerencia.

4.2.12.4. Evitar el riesgo

La evitación del riesgo implica cualquier acción dirigida a modificar las actividades o la forma de llevar a cabo una operación comercial específica. El riesgo puede evitarse mediante:

- La suspensión de ciertas actividades comerciales (como la no utilización de Internet).
- El traslado de activos fuera de una zona de riesgo.
- La decisión de no procesar información crítica.

4.2.13. Riesgo residual

El riesgo residual es el riesgo que permanece tras la implementación de las decisiones de tratamiento del riesgo. Aunque su cálculo puede ser complejo, es necesario realizar al menos una evaluación para asegurar que se alcanza un nivel de protección adecuado. Si el riesgo residual es inaceptable, se deben tomar medidas adicionales, como aplicar controles adicionales o establecer acuerdos con aseguradoras para reducir el riesgo a niveles aceptables.

En algunos casos, reducir el riesgo a niveles aceptables puede no ser viable o puede implicar costos excesivamente altos. En tales situaciones, se adopta la estrategia de aceptación del riesgo.

La dirección del departamento de TIC debe aprobar los riesgos residuales propuestos, realizar evaluaciones periódicas y revisar tanto el nivel de riesgo residual como el nivel de riesgo aceptable previamente identificado.

4.2.14. Seleccionar objetivos de control y controles para los riesgos

Una vez que se han identificado y evaluado los procesos de gestión del riesgo, es necesario determinar los objetivos de control y las medidas de control a implementar. La selección de estos objetivos y medidas debe realizarse considerando los criterios

establecidos para la aceptación del riesgo, así como los requisitos legales, regulatorios y contractuales aplicables.

4.2.15. Declaración de aplicabilidad

La declaración de aplicabilidad constituye un apartado fundamental dentro del marco del Plan de Seguridad de la Información. Este apartado debe detallar de manera exhaustiva los objetivos de control que serán implementados, así como aquellos controles que se decidirá excluir del ámbito de aplicación.

La declaración de aplicabilidad permite al departamento de TIC verificar de forma sistemática que no se ha pasado por alto ningún control necesario, garantizando así la integridad y efectividad de la gestión de seguridad de la información. Además, este marco de referencia facilita la evaluación continua de los controles en relación con los riesgos identificados, asegurando el cumplimiento de las normativas y estándares pertinentes.

Tabla 20: Ejemplo de declaración de aplicabilidad

ISO/IEC 27001	Aplicable	No aplicable	Justificación
5. CONTROLES ORGANIZACIONALES			
5.1 Políticas de seguridad de la información	X		Este proceso abarca desde la definición y aprobación por parte de la gerencia, hasta la comunicación, reconocimiento por parte del personal y partes interesadas, así como la revisión periódica y adaptación a cambios significativos.
5.2 Roles y responsabilidades de seguridad de la información	X		Esto facilita la coordinación, la toma de decisiones y el cumplimiento de los objetivos de seguridad de la organización.
6. CONTROLES DE PERSONAS			
6.1 Poner en pantalla	X		Es importante realizar los controles de verificación de los antecedentes de los candidatos antes de unirse a la institución y de manera continua a lo largo de su empleo
6.2 Términos y condiciones de empleo	X		Estos acuerdos pueden abarcar normas para garantizar la seguridad de los datos, proteger las contraseñas, mantener la confidencialidad de la información y seguir las políticas y procedimientos de seguridad.
7. CONTROLES FISICOS			

7.1 Perímetros físicos de seguridad	X		La institución puede identificar áreas específicas que necesitan un nivel específico de protección.
7.2 Entrada física	X		Es importante contar con este control para limitar el acceso no autorizado a áreas críticas y salvaguardar los activos de la institución.
8. CONTROLES TECNOLOGICOS			
8.1 Dispositivos de punto final de usuario	X		La relevancia de salvaguardar la información almacenada, procesada o accesible mediante los dispositivos finales del usuario.
8.2 Derechos de acceso privilegiado		X	Debido a que estos privilegios conceden a los usuarios un alto grado de acceso a sistemas, datos y recursos esenciales de la organización, lo cual puede incrementar considerablemente el riesgo de abuso o uso indebido si no se administran de manera apropiada.

4.2.15.1. Esquema de Gestión de Riesgo

Una vez definido el tratamiento del riesgo, es necesario identificar y planificar las actividades correspondientes. Cada actividad de implementación debe ser claramente delineada y desglosada en subactividades, lo que permitirá una adecuada asignación de responsabilidades entre el personal involucrado. Las actividades que se consideran esenciales para la formulación del plan de tratamiento del riesgo incluyen:

- Identificar de manera precisa los factores limitantes del proyecto y desarrollar estrategias para mitigarlos.
- Establecer las prioridades del proyecto de forma clara.
- Definir con exactitud las fechas de entrega, así como los hitos clave del proyecto.
- Estimar los requerimientos de recursos necesarios e identificar los recursos disponibles.
- Delimitar la ruta crítica del proyecto para asegurar el cumplimiento de los plazos establecidos.

4.2.15.2. Monitoreo del Plan de Seguridad de la Información

Todo proyecto debe someterse a revisiones periódicas, lo cual también aplica a los objetivos de control y controles implementados. Dado que con el tiempo los servicios y mecanismos tienden a deteriorarse, el monitoreo tiene como objetivo identificar dicho deterioro y activar las acciones correctivas necesarias.

Las actividades de monitoreo del plan incluyen:

- Identificación de eventos de seguridad, previniendo incidentes mediante el uso de indicadores clave.
- Evaluación de la efectividad de las acciones implementadas para mitigar violaciones de seguridad.
- Definición de criterios para medir la eficiencia de los controles y asegurar el cumplimiento de los requisitos de seguridad.
- Revisión periódica de las evaluaciones de riesgos, con análisis del riesgo residual y aceptable previamente identificados.
- Realización de revisiones por parte del director de TIC del plan para verificar que su alcance sigue siendo adecuado.

Este enfoque asegura la capacidad continua del Plan de seguridad para responder a amenazas y mantener la conformidad con los estándares definidos.

4.2.15.3. Revisión de los riesgo y evaluación

Es necesario llevar a cabo una revisión exhaustiva de los resultados obtenidos del análisis y la evaluación de riesgos con el fin de identificar cualquier modificación necesaria. La continua evolución del Departamento de TIC y de la tecnología puede dar lugar a la aparición de nuevos activos de información o a la modificación de los existentes.

Las revisiones de la efectividad de los controles, así como la identificación de nuevas amenazas y vulnerabilidades, pueden impactar significativamente el panorama de riesgos. Existen múltiples fuentes que pueden contribuir a la aparición de nuevos riesgos; al detectar un riesgo emergente, es fundamental recalcular e identificar las variaciones en las opciones de tratamiento correspondientes, así como realizar las modificaciones necesarias en los objetivos de control y en los controles previamente establecidos y documentados.

4.3. DISCUSIÓN

La discusión se enfoca en diseñar un Plan de Seguridad de la Información para los activos de información para el Departamento de TIC de la Universidad Politécnica Estatal del Carchi. Se utiliza la Norma ISO 27001: 2022 como marco de referencia y la Metodología MAGERIT para identificar los activos vulnerables. La Norma ISO 27001:2022 establece requisitos para que el Sistema de Gestión de la Seguridad de la Información, enfocándose en la evaluación y tratamiento de los riesgos de la seguridad, además la metodología MAGERIT nos ayudó a identificar, analizar y valorar los activos críticos, amenazas y vulnerabilidades dentro del institución. El Plan Seguridad de la Información tiene como objetivos identificar y clasificar los activos críticos, evaluar riesgos, establecer controles de seguridad y monitorear continuamente el plan para garantizar su eficacia.

En comparación con estudios anteriores, esta investigación se centra en utilizar controles de seguridad de la información con el estándar de la Norma ISO/IEC 27001:2022 para aplicar un control de riesgos con sus cláusulas 5 a 8, en lugar de utilizar el estándar de la versión anterior, además, la investigación cuenta dentro de la propuesta con un análisis de la situación actual de los activos de información de la institución, con el fin de identificar las amenazas, evaluar su impacto y determinar la frecuencia con la que ocurren.

El manual de políticas de seguridad de la UPEC fue fundamental para realizar una evaluación comparativa sobre la gestión de la seguridad y verificar si se están aplicando estrictamente todos los controles detallados. En conclusión, la investigación propone una serie de medidas y sugerencias para fortalecer la seguridad de la información de los activos de información, con el fin de disminuir las vulnerabilidades existentes y prevenir posibles daños o ataques cibernéticos.

Tabla 21. Comparación entre estudios

Investigación ISO 27001:2022	Antecedentes ISO 27001:2013
Dentro del enfoque normativo se centra más en la información	Su enfoque enfatiza en la organización o empresa
En la investigación las directrices hacen un análisis de riesgos más flexible	En estudios anteriores el manejo del análisis de riesgos es más detallado
Se integra una metodología que nos ayuda a gestionar los activos vulnerables debido a su mayor énfasis en integración.	En las investigaciones integran sistemas de gestión pero debido a las directrices tiene un menor énfasis.
Se utiliza la versión más reciente del estándar debido a su flexibilidad en sus requisitos de documentación por lo que se puede adaptar a cualquier organización.	La versión que se emplea en estudios anteriores integra requisitos de documentación más específicos dependiendo de la organización

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La fundamentación bibliográfica fue crucial para respaldar la importancia de la norma ISO 27001 y las estrategias de defensa contra vulnerabilidades informáticas adecuadas. Esto permitió seleccionar una metodología para gestionar los riesgos de seguridad de la información.
- El uso de la metodología MAGERIT para analizar los riesgos de seguridad informática en los activos de red de la UPEC ha brindado una visión clara y estructurada de las posibles amenazas y vulnerabilidades, lo que ha permitido identificar áreas de riesgo y establecer medidas preventivas y correctivas para proteger la integridad y confidencialidad de la información.
- La selección de controles de seguridad de la información conforme a la norma ISO 27001 facilitó la descripción de medidas proporcionales a los riesgos identificados, optimizando la protección de los activos de información.
- La propuesta de políticas de seguridad respaldadas por un plan de seguridad de la información no solo simplifica el proceso de mejora continua y la incorporación de prácticas óptimas, sino que también robustece la salvaguarda de los activos de información dentro de un entorno digital cada vez más complejo y desafiante.

5.2. RECOMENDACIONES

- Implementar un proceso constante de identificación, evaluación y gestión de riesgos de acuerdo con los principios establecidos en la norma ISO 27001. De esta manera, se logrará una comprensión más profunda de las amenazas y vulnerabilidades, lo que permitirá tomar medidas preventivas y correctivas adecuadas.
- Es importante brindar capacitación periódica y detallada sobre las políticas y procedimientos de seguridad de la información a todo el personal encargado de la red universitaria. Esto asegurará que todos estén conscientes de su

responsabilidad en la protección de la información y estén preparados para detectar y manejar adecuadamente cualquier amenaza.

- Implementar un sistema de monitoreo y revisión continua que permita supervisar de forma proactiva el cumplimiento de los controles de seguridad establecidos. Asimismo, llevar a cabo revisiones periódicas del sistema de gestión de seguridad de la información con el fin de identificar áreas de mejora y oportunidades de optimización.
- Mantener actualizado al personal sobre los progresos en el ámbito de la seguridad digital y las regulaciones asociadas, ajustando de manera constante las políticas y procedimientos de seguridad en función de estos cambios.

VI. REFERENCIAS BIBLIOGRÁFICAS

Saeckel, A. (11 de marzo de 2021). Blog especializado en seguridad de la información. Obtenido de https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Acosta, M. (2020). Ambit. Obtenido de Diferencias entre amenaza, vulnerabilidad y riesgo: https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo

Apliint Software Development. (17 de agosto de 2021). Obtenido de Vulnerabilidades de las aplicaciones web: https://apliint.com/2021/08/17/vulnerabilidades-de-las-aplicaciones-web/

Arévalo, M. (27 de agosto de 2021). Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/08/clasificacion-de-la-informacion-segun-iso-27001/

ATLAS.ti. (16 de enero de 2024). Obtenido de La entrevista como poderoso método de investigación: https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/entrevistas

Chaloupka, P. (10 de marzo de 2024). Seguridad de datos en la nube. Obtenido de https://www.safetica.com/es/blog/seguridad-de-datos-en-la-nube-definiciones-riesgos-y-7-mejores-practicas-para-la-proteccion-de-datos-en-la-nube

Chavez. (8 de mayo de 2024). Obtenido de Seguridad de la red: ¿Qué es, cómo funciona y qué tipos existen?: https://www.deltaprotect.com/blog/seguridad-de-la-red

Chicaiza Castillo, D. V., & Torres Chango, C. D. (enero de 2020). Universidad Técnica de Ambato. Obtenido de Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.: https://repositorio.uta.edu.ec/jspui/handle/123456789/30690

Concejo Nacional Electoral. (5 de Febrero de 2023). Concejo Nacional Electoral. Obtenido de RESULTADOS PRELIMINARES: https://app01.cne.gob.ec/resultados2023

Coppola, M. (23 de mayo de 2023). HubSpot. Obtenido de Auditoria de seguridad: https://blog.hubspot.es/website/auditoria-de-seguridad

De Sousa, B. (17 de abril de 2024). Gestión de la Información. Obtenido de https://www.ipnet.cloud/blog/es/datos/gestion-de-la-informacion-importancia-y-como-hacer/

Delgado Saavedra, M. M., & Vásquez Zevallos, J. L. (2020). Alicia Concytec. Obtenido de MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L.: https://alicia.concytec.gob.pe/vufind/Record/RUDL_3f7ca7654f0dc394f66767d97c9394e3

Delgado, L. (31 de julio de 2022). Riesgos de seguridad de los datos en la web. Obtenido de https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/18

Derecho Ecuador. (2020). Obtenido de Delitos Informaticos o ciberdelitos: https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/

Escuela Europea de Excelencia. (21 de noviembre de 2020). Obtenido de ¿Cómo funciona la seguridad de la información en ISO 27001?: https://www.escuelaeuropeaexcelencia.com/2019/11/como-funciona-la-seguridad-de-la-informacion-en-iso-27001/

Forero, T. (3 de octubre de 2024). Programa de Auditoría de gestión de incidentes. Obtenido de https://www.auditool.org/tecnologia-de-informacion/ciberseguridad/programa-de-auditoria-de-gestion-de-incidentes-y-violaciones-de-datos

Fortra. (2021). Obtenido de Monitoreo de Seguridad e integridad: https://www.fortra.com/es/soluciones/seguridad-informatica/infraestructura/monitoreo-de-seguridad-e-integridad

García, A. (junio de 2023). worldsys. Obtenido de 3 Tipos de riesgos informaticos a los que se exponen las empresas: https://www.worldsys.co/3-tipos-de-riesgos-informaticos-a-los-que-se-exponen-las-empresas/

García, C. R. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. Obtenido de https://ingenieria.ute.edu.ec/enfoqueute/public/journals/1/html_v12n2/art005.html

Garcia, V. (4 de junio de 2021). Auditoría de seguridad de aplicaciones móviles. Obtenido de https://openaccess.uoc.edu/handle/10609/95927?locale=es

Gómez, J. (20 de agosto de 2024). Auditoría de seguridad informática. Obtenido de https://www.deltaprotect.com/blog/auditoria-de-seguridad-informatica

Grupo ESG. (2020). Obtenido de Blog especializado eb seguridad de la información: https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/

Guelmann, A. (5 de junio de 2024). Protección de Identidad. Obtenido de https://www.silverfort.com/es/glossary/identity-protection/

Haider, K. (28 de febrero de 2024). Obtenido de What is Data Integration: https://www.astera.com/es/type/blog/data-integration/

Innovate Consultores. (27 de marzo de 2022). Obtenido de ISO 27001 : https://qinnovateconsultores.com/iso-27001/

Kosutic, D. (4 de septiembre de 2021). Obtenido de Beneficios de aplicar la norma ISO 27001: https://www.isotools.us/2015/09/08/beneficios-de-aplicar-la-norma-iso-27001/

López, X. (2021). Arroba System. Obtenido de ¿Qué son las amenazas informáticas y cómo protegerte de ellas?: https://arrobasystem.com/blogs/blog/que-son-las-amenazas-informaticas-y-como-protegerte-de-ellas

Lorenzo. (6 de Febrero de 2024). SMOWL Proctoring. Obtenido de https://smowl.net/es/blog/vulnerabilidad-en-la-seguridad-informatica/

Martínez, V. (15 de junio de 2021). La Auditoría interna. Obtenido de https://www.auditool.org/blog/auditoria-interna/auditoria-interna-debe-redactar-las-politicas-y-procedimientos

Mayaquer Andino, J. A., & Romero Castro, M. I. (5 de noviembre de 2020). Universidad Estatal del Sur de Manabí. Obtenido de ANÁLISIS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001, PARA IDENTIFICAR VULNERABILIDADES EN LA SALA DE COMPUTO DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES: http://repositorio.unesum.edu.ec/handle/53000/2581

Mayorga Mayorga, F. O., & Criollo Tasinchana, S. M. (2020). Universidad Técnica de Ambato. Obtenido de Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo: https://repositorio.uta.edu.ec/jspui/handle/123456789/26537

Merinas, A. (9 de octubre de 2021). Auditoría de cumplimiento normativo. Obtenido de https://www.compliance-antisoborno.com/auditoria-de-cumplimiento-normativo-como-prepararse-para-superarla-con-exito/

Michali. (20 de Julio de 2022). Check Point Software. Obtenido de https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

Ministerio de Hacienda y Administraciones Publicas. (2023). Cni.es. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Morales, O. (2020). Confidencialidad. Obtenido de Banco Santander: https://www.bancosantander.es/glosario/confidencialidad-informacion

Narvaez, M. (26 de junio de 2023). QuestionPro. Obtenido de Método inductivo: qué es, características y ejemplos: https://www.questionpro.com/blog/es/metodo-inductivo/

Nillim. (26 de septiembre de 2023). Die Bedeutung der Sicherheit mobiler Apps. Obtenido de https://www.appleute.de/es/app-entwickler-bibliothek/importancia-seguridad-aplicaciones-moviles/

Normas ISO. (2020). Normas ISO. Obtenido de ISO 27001 - Seguridad de la información: Norma ISO IEC 27001/27002: https://www.normas-iso.com/iso-27001/

Normas ISO. (22 de septiembre de 2023). Obtenido de ¿Qué es la norma ISO 27001 y para qué sirve?: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,y%20disponibilidad%20de%20la%20informaci%C3%B3n.

Normas ISO. (28 de septiembre de 2023). GlobalSuite Solutions. Obtenido de https://www.globalsuitesolutions.com/es/que-son-normas-iso/

NQA Certification Body. (2020). Obtenido de Guía para la implementación de la norma ISO 27001: https://www.nqa.com/es-es/certification/standards/iso-27001/implementation

PAE. (2021). MAGERIT v.3. Obtenido de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Pazan, C. (25 de julio de 2022). El Comercio. Obtenido de https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Pérez, D. (2020). Seguridad y Alta Disponibilidad. Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/

Pesantes, K. (18 de octubre de 2023). Pimicias. Obtenido de Ciberataques: ¿Cuánto le cuesta a las empresas el robo de datos?: https://www.primicias.ec/noticias/tecnologia/ciberataques-costo-robo-datos-empresas/

Ponce, J. (9 de agosto de 2023). Auditoría informática. Obtenido de https://www.ikusi.com/mx/blog/auditoria-informatica/

Pous, H. (2022). The Conversation. Obtenido de https://theconversation.com/el-mayor-peligro-para-la-ciberseguridad-son-los-fallos-humanos-asi-podemos-evitarlos-223477

Qualtrics. (28 de noviembre de 2023). Obtenido de Cómo diseñar una encuesta eficaz: https://www.qualtrics.com/es-la/gestion-de-la-experiencia/investigacion/que-es-una-encuesta/

Riveros, A. (5 de octubre de 2023). EALDE Business School. Obtenido de https://www.ealde.es/fases-implementar-iso-27001-seguridad-informacion/

Rodriguez, P. (2020). Obtenido de Análisis de riesgos informáticos y ciberseguridad: https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Santos, D. (20 de enero de 2023). Hubspot. Obtenido de ¿Qué es y cómo hacer un análisis de riesgos?: https://blog.hubspot.es/marketing/analisis-de-riesgos

Sevillano, F., & Beltrán, M. (2021). Dirección de seguridad y gestión del ciberriesgo. Madrid: Ediciones de la U.

Toapanta, K. (10 de mayo de 2024). ITSQMET. Obtenido de https://itsqmet.edu.ec/descubre-los-riesgos-informaticos-protege-tu-empresa/

Triviño Mosquera, I. (2020). Seguridad Informatica. En I. Triviño Mosquera, Seguridad Informatica (pág. 25). Madrid: Sintesis.

Vive, U. (2020). UNIR FP. Obtenido de Auditoría de seguridad informática: definición, tipos y fases: https://unirfp.unir.net/revista/ingenieria-y-tecnologia/auditoria-seguridad-informatica/#:~:text=Podemos%20encontrar%20dos%20clasificaciones%20si,trabajan%20directamente%20para%20la%20empresa.

Washington, M. (diciembre de 2021). Plan de seguridad informática para la red . Obtenido de https://dspace.uniandes.edu.ec/handle/123456789/8394

VII. ANEXOS

Anexo 1: Acta de sustentación de Predefensa del TIC

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

ACTA

DE LA SUSTENTACIÓN ORAL DE LA PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR CON ENFOQUE EN INVESTIGACIÓN

ESTUDIANTE:	Chicaiza Rivera Jhajan Alexis	**CÉDULA DE IDENTIDAD:**	0401611264
PERIODO ACADÉMICO:	2023B		
PRESIDENTE TRIBUNAL	MSC. MARCO ANTONIO YANDUN VELASTEGUI	**DOCENTE TUTOR:**	MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
DOCENTE:	MSC. GEORGINA GUADALUPE ARCOS PONCE		
TEMA DEL TIC:	"Optimización de la seguridad de la información basada en la norma ISO/IEC 27001"		

No.	CATEGORÍA	Evaluación cuantitativa	OBSERVACIONES Y RECOMENDACIONES
1	PROBLEMA - OBJETIVOS	7,67	Reformular la formulación del problema
2	FUNDAMENTACIÓN TEÓRICA	7,67	Revisar que máximo una cita por autor, diversificar en fuentes
3	METODOLOGÍA	7,67	
4	RESULTADOS	7,67	Revisar los resultados de investigación
5	DISCUSIÓN	7,67	
6	CONCLUSIONES Y RECOMENDACIONES	7,67	Debe existir el Plan de mejoras en la propuesta presentada.
7	DEFENSA, ARGUMENTACIÓN Y VOCABULARIO PROFESIONAL	7,67	
8	FORMATO, ORGANIZACIÓN Y CALIDAD DE LA INFORMACIÓN	7,67	Revisar los errores informados en la predefensa

Obteniendo una nota de: **7,67** Por lo tanto, **APRUEBA** : debiendo el o los investigadores acatar el siguiente artículo:

Art. 66.- De la aprobación de la pre defensa del informe final de TIC.- El estudiante deberá obtener una nota mínima de 7/10; al finalizar el proceso de pre-defensa se procederá a levantar el acta correspondiente. En el caso de aprobar con observaciones el estudiante deberá adjuntar el informe final de cumplimiento de observaciones y recomendaciones emitido por el Tribunal previo a la defensa final en un término maximo de 10 días.

Para constancia del presente, firman en la ciudad de Tulcán el martes, 9 de julio de 2024

MSC. MARCO ANTONIO YANDUN VELASTEGUI
PRESIDENTE TRIBUNAL

MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
DOCENTE TUTOR

MSC. GEORGINA GUADALUPE ARCOS PONCE
DOCENTE

Anexo 2: Certificado del abstract por parte de idiomas

ABSTRACT- EVALUATION SHEET

NAME: Chicango Rivera Jhojan Alexis
DATE: 14 de noviembre de 2024
Topic: "Optimización de la seguridad de la información basada en la norma ISO/IEC 27001"

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐

TOTAL/AVERAGE

9 - 10: EXCELLENT
7 - 8,9: GOOD
5 - 6,9: AVERAGE
0 - 4,9: LIMITED

TOTAL 9

Anexo 1: Entrevista al Analista de redes

ENTREVISTA DIRIGIDA AL ANALISTA DE REDES Y COMUNICACIONES DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

La entrevista tiene como propósito entender la situación actual de la seguridad de la información en la UPEC. Los datos recopilados están relacionados con medidas de seguridad diseñadas para fortalecer y proteger la red universitaria frente a amenazas cibernéticas.

1. **¿Qué problemas de seguridad informática ha tenido el departamento de TIC de la UPEC?**

Ha habido varios problemas de seguridad informática en la red institucional, Malware, rasonware entre otros. Además de problemas físicos, como servidores obsoletos, dañados o partes internas quemadas.

2. **¿Qué medidas ha llevado a cabo el departamento de Redes y Telecomunicaciones en colaboración con el departamento de TIC para elevar la calidad de seguridad de la información?**

Dentro de los proyectos institucionales, se ha previsto la instalación de Antivirus Institucional, implementación de un Next Generation Firewall para la protección perimetral de los equipos y servidores institucionales. Así como varias políticas de acceso a los servicios informáticos que la institución brinda.

3. **¿La UPEC tiene políticas de seguridad establecidas para proteger la información?**

Si existen políticas de seguridad, entre ellas se encuentran la configuración de puertos en el firewall, donde se permite o bloquea puertos hacia los servidores institucionales para proteger su acceso, doble factor de autenticación en las cuentas de correo, entre otras.

4. **¿Cómo es administrada la red interna de la UPEC?**

La red interna está compuesta de varias partes, Red de Datos Cableada, Red de Datos Wi-Fi, Data Center, CCTV, Telefonía IP. Todo se encuentra administrado por el

personal de la Unidad de Redes y Telecomunicaciones, cada una de estas partes dispone de su propio software de administración que facilita la gestión de las mismas.

5. **¿Cómo se encuentra la seguridad física para acceso a los servidores en la UPEC?**

El ingreso a los equipos del Data Center no se encuentra óptima debido a que no cumple con las normativas de acceso a Data Centers, pero el personal de la Unidad de Redes y Telecomunicaciones es el único que tiene las llaves de acceso al mismo.

6. **¿Cómo es la distribución de software y equipos informáticos para el personal del departamento de TIC?**

Cada uno del personal que labora en la Dirección de TIC dispone de su equipo informático con software especializado para poder realizar sus actividades académicas y administrativas, además de que cuentan con acceso a los servidores de desarrollo y producción de cada uno de los servicios informáticos universitarios.

7. **¿Todo el software utilizado en la UPEC posee licencia?**

La mayoría del software utilizado en la UPEC es bajo software libre, pero en los softwares que se requiera licenciamiento, la UPEC gestiona la adquisición de los mismos.

8. **¿Qué sistema operativo se emplea en el servidor del centro de datos de la UPEC? ¿Y por qué?**

Los servidores institucionales son bajo el sistema operativo Debian, primero porque es software libre y también por las seguridades y parches de actualización que posee esta distribución, son pocos los servicios que se implementan bajo Windows Server.

9. **¿Cómo se maneja el acceso a la información de los servidores de archivos?**

El acceso a los servidores de archivo se lo realiza por medio de los servicios informáticos instalados, ya que se encuentran en una configuración de cluster. Además, cada funcionario está a cargo de sus archivos que pueden almacenarlos en la nube que nos entrega el proveedor de correo electrónico.

10. **Ante la presencia de hosts que estén ejecutando servicios innecesarios o infectados de virus. ¿Cómo se da solución al problema?**

La universidad cuenta con un antivirus y un firewall de última generación que protege, detecta y bloquea este tipo de malware.

11. ¿Qué métodos y técnicas se ha empleado para crear los procedimientos de seguridad con el fin de prevenir posibles vulnerabilidades?

Uno de los métodos empleados es realizar un escaneo a los puertos de cada servidor para determinar su vulnerabilidad, y con ello solamente habilitar los necesarios en cada uno de sus servicios.

Además, se realizan escaneos periódicos en busca de vulnerabilidades de la red para poder mitigarlos.

12. ¿Cuál fue el problema interno detectado con respecto a la seguridad de la intranet de la UPEC?

Dentro de la intranet, el mayor problema son los dispositivos de usuario final que no pertenecen como activos institucionales, es decir computadoras tablets celulares que pertenecen a estudiantes y docentes los cuales muchas veces no tienen instalados software de protección informática como un antivirus.

13. ¿Opina usted que los sistemas informáticos actuales en la UPEC son confiables desde el punto de vista de la seguridad?

Los sistemas si son confiables, aunque existen muchas debilidades que se las deben ir solventando.

Anexo 2: Encuesta dirigida al encargado del manejo de la intranet universitaria

ENCUESTA DIRIGIDA AL ENCARGADO DEL MANEJO DE LA INTRANET UNIVERSITARIA

Conocimiento de seguridad de la información

Objetivo: Evaluar el grado de comprensión que tiene el personal sobre las regulaciones de seguridad de la información.

Nota: Las preguntas se evalúan en una escala de 1-5 en donde:

1 = 0% 2 = 25% 3 = 50% 4 = 75% 5 = 100%

1. ¿Cuál es su nivel de comprensión en cuanto a la seguridad de la información en la actualidad?

- 1
- 2
- 3
- 4
- 5

2. ¿Cuál es su nivel de comprensión acerca de las normativas internas que rigen la seguridad de la información?

- 1
- 2
- 3
- 4
- 5

3. ¿Cuál es el grado de conocimiento que ha adquirido de las capacitaciones sobre seguridad de la información proporcionadas por la UPEC?

- 1
- 2
- 3
- 4
- 5

Conocimiento normativo

Objetivo: Determinar el grado de comprensión respecto a la Norma ISO 27001 y la legislación de protección de datos.

Nota: Las preguntas se evalúan en una escala de 1-5 en donde:

1 = 0% 2 = 25% 3 = 50% 4 = 75% 5 = 100%

4. ¿Cuál es tu nivel de comprensión actual acerca de la Norma ISO 27001?

- 1
- 2
- 3
- 4
- 5

5. ¿Cuál es tu nivel de conocimiento acerca de la ley de protección de datos en el Ecuador?

- 1
- 2
- 3
- 4
- 5

6. ¿Cuál es la situación actual de la Institución en términos de seguridad de la información según las auditorías internas?

- 1
- 2
- 3
- 4
- 5

Técnicas para la protección de datos y seguridad de la información

Objetivo: Obtener información actualizada acerca de la seguridad de los datos mediante la utilización de los servicios proporcionados por el personal.
Nota: Las preguntas se evalúan en una escala de 1-5 en donde:
1 = 0% 2 = 25% 3 = 50% 4 = 75% 5 = 100%

7. ¿Cuál es el nivel de seguridad de los servidores donde se almacenan los archivos de respaldo?

- 1
- 2
- 3
- 4
- 5

8.Los servicios prestados en caso de tener un fallo ¿Cómo define su accionar en tiempo de respuesta para resolver dichos problemas?

- 1
- 2
- 3
- 4

- 5

9. ¿Cuán importante considera la protección de datos y la seguridad de la información en el entorno universitario?

- 1
- 2
- 3
- 4
- 5

10. ¿Cómo califica la efectividad de tus procedimientos para el manejo y almacenamiento seguro de datos sensibles?

- 1
- 2
- 3
- 4
- 5

Anexo 3: Solicitud de Validación de Instrumentos

Solicitud de Validación de Instrumentos de Entrevista y Encuesta

Tulcán, 30 de enero de 2024

MSc. Jairo Hidalgo G
DOCENTE DE LA CARRERA DE COMPUTACIÓN - UPEC

De mi consideración:

Me dirijo a usted en calidad de estudiante de la Carrera de Computación, con el fin de solicitar su valiosa colaboración en el proceso de validación de los instrumentos de entrevista y encuesta que han sido desarrollados para la investigación relacionada con el Trabajo de Integración Curricular de tema: **"OPTIMIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001"**, dirigida por **JHOJAN ALEXIS CHICANGO RIVERA** en la **UNIVERSIDA POLITÉCNICA ESTATAL DEL CARCHI (UPEC)**.

El objetivo es asegurar la confiabilidad y validez del instrumento diseñado para la recolección de datos, el cual será fundamental para el éxito de este importante proyecto de investigación. Reconozco su experiencia y conocimientos en el área de seguridad de la información y considero que su retroalimentación será invaluable para el perfeccionamiento del instrumento.

Adjunto a este oficio, encontrará una copia del instrumento de entrevista y encuesta. Agradecería sinceramente si pudiera revisar detenidamente el instrumento y proporcionarme sus comentarios y sugerencias con respecto a la claridad, pertinencia y validez de las preguntas planteadas.

Estoy abierto a cualquier ajuste o modificación que considere necesario para mejorar la calidad del instrumento y garantizar la robustez de los datos recopilados.

Quedo a su disposición para cualquier consulta o aclaración que pueda necesitar, y le agradezco de antemano su tiempo y colaboración en este importante proceso.

Atentamente,

Jhojan Alexis Chicango Rivera
ESTUDIANTE DE LA CARRERA DE COMPUTACIÓN

Anexo 4: Solicitud para levantamiento de información para Dirección de TIC

Tulcán, 20 de marzo de 2024

Señor:

MSc. Carlitos Guano

DIRECTOR DE LA CARRERA DE COMPUTACIÓN

De mi consideración.-

Yo, Chicango Rivera Jhojan Alexis con CI: 0401611264, me dirijo a usted en calidad de estudiante de Carrera de Computación en la Universidad Politécnica Estatal del Carchi, con el propósito de solicitar su colaboración para llevar a cabo un levantamiento de información relacionado con el manejo de la intranet en la red institucional, para el Trabajo de Integración Curricular con enfoque en Investigación con el tema: **Optimización de la seguridad de la Información basada en la norma ISO/IEC 27001** con asesoramiento del tutor: Milton Gabriel Del Hierro Mosquera con CI: 0603483405.

El alcance de mi investigación es evaluar y mejorar la seguridad de la información en la intranet de nuestra institución. Para lograr este objetivo, es crucial realizar un levantamiento de información detallado sobre el manejo actual de la intranet, abarcando aspectos relacionados con las políticas de seguridad, medidas técnicas implementadas, protocolos de acceso, entre otros.

En este sentido, solicito su colaboración para que, en su calidad de Director de la Carrera de Computación, pueda facilitar la comunicación y el apoyo necesario para enviar una solicitud formal a la **Dirección de Tecnologías de la Información y Comunicación (TIC)** de nuestra Universidad. Esta solicitud contendrá la autorización y respaldo necesario para que pueda llevar a cabo el levantamiento de información requerido para mi investigación.

A continuación, detallo algunos de los aspectos que me gustaría abordar durante este levantamiento de información:

- Políticas y procedimientos de seguridad de la información relacionados con la intranet.
- Medidas de seguridad implementadas en la infraestructura de la intranet.
- Protocolos de acceso y autenticación utilizados para gestionar el acceso a la intranet.
- Posibles brechas de seguridad o incidentes registrados en la intranet.
- Planes de contingencia y procedimientos de recuperación ante incidentes de seguridad.

La información obtenida será utilizada únicamente con fines académicos y será tratada con absoluta confidencialidad. Agradezco de antemano su apoyo en este proceso y quedo a su disposición para cualquier consulta o aclaración adicional que pueda surgir.

Quedo a la espera de su pronta respuesta y agradecido por su atención a esta solicitud.

Atentamente:

Jhojan Alexis Chicango Rivera

ESTUDIANTE

040161126-4

Anexo 5: Solicitud para adquirir Plan de Contingencia del Data Center

UPEC

POLITÉCNICA DEL CARCHI

Memorando Nro. UPEC-CACO-2024-088-MA
Tulcán, 20 de agosto del 2024

Para: MSc. Javier Torres
DIRECTOR DE TIC - UPEC

De mi consideración. -

Por medio de la presente, me permito solicitar de la manera más cordial el acceso al "Plan de Contingencia para el Data Center de la Universidad Politécnica Estatal del Carchi", al estudiante egresado de la Carrera de Computación Jhojan Alexis Chicango Rivera con CI: 040161126-4, esta solicitud tiene como propósito que dicho documento sea utilizado exclusivamente para fines académicos en la elaboración de su propuesta del Trabajo de Integración Curricular titulada "Optimización de la seguridad de la Información basada en la norma ISO/IEC 27001" con el asesoramiento del MSc. Milton Gabriel del Hierro Mosquera.

El estudiante se encuentra actualmente realizando las debidas correcciones dadas en su sustentación de pre defensa y considera que el acceso a este plan de contingencia será de gran valor para su investigación. El documento le permitirá contar con un modelo práctico y contextualizado que enriquecerá su análisis y propuestas sobre la seguridad de la información.

Agradezco de antemano su apoyo en este proceso y quedo a su disposición para cualquier consulta o aclaración adicional que pueda surgir.

Particular que pongo en su conocimiento que la información obtenida será tratada con absoluta confidencialidad y únicamente para fines académicos pertinentes.

Atentamente,

Firmado digitalmente por 1710015171 CARLITOS ALBERTO GUANO CARDENAS

UNIVERSIDAD POLITECNICA ESTATAL - CARCHI
UPEC COMPUTACIÓN
TULCAN

MSc. Carlitos Guano Cárdenas.
DIRECTOR DE LA CARRERA DE COMPUTACIÓN

CG/jc

Calle Antisana y Av. Universitaria
Telf: (06) 2980837 - 2984435
info@upec.edu.ec
www.upec.edu.ec
Tulcán - Ecuador

Anexo 6: Metodología MAGUERIT

5. Amenazas

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

5.1. [N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen:
Natural (accidental)

5.1.1. [N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

Figura 17: Amenazas según MAGUERIT

Anexo 7: Certificado de Workshop Norma ISO 27001

Figura 18: Certificado de Workshop ISO 27001

Anexo 8: Certificado Ley Orgánica de Protección de Datos Personales

Figura 19: Certificado Ley Orgánica de Protección de Datos

Anexo 9: Plan de Seguridad de la Información para el Departamento de TIC de la UPEC

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Plan de Seguridad de la Información para el departamento de TIC de la Universidad Politécnica Estatal del Carchi

POLITÉCNICA DEL CARCHI

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Anexo 10: Acta de entrega del Plan de Seguridad de la información

ACTA DE ENTREGA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

Fecha: 8 de octubre de 2024

Lugar: Tulcán – Carchi

Departamento: Dirección de Tecnologías de la Información y Comunicaciones (DTIC)

Responsable de Entrega: Jhojan Alexis Chicango Rivera

Docente Tutor: MSc. Milton Gabriel Del Hierro Mosquera

Responsable de Recepción: MSc. Javier Torres Director de TIC.

Objetivo:

El presente documento tiene como finalidad formalizar la entrega del Plan de Seguridad de la Información para la Dirección de Tecnologías de la Información y Comunicaciones (DTIC), el cual ha sido desarrollado conforme a las normativas vigentes y mejores prácticas en seguridad de la información, incluyendo los lineamientos establecidos en la norma ISO 27001. Esto como propuesta del Trabajo de Integración Curricular que lleva por título "Optimización de la seguridad de la Información basada en la norma ISO 27001"

Descripción del Plan Entregado:

El Plan de Seguridad de la Información tiene como objetivo principal la protección de los activos de información del departamento de TIC, abarcando las siguientes áreas clave:

- Gestión de riesgos: Identificación, análisis, y tratamiento de los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información.
- Políticas de seguridad: Definición de políticas internas de seguridad alineadas con las necesidades del departamento y la normativa ISO 27001.
- Controles de acceso: Implementación de controles que limiten el acceso a la información únicamente a personal autorizado.
- Protección de datos sensibles: Medidas para garantizar la seguridad de los datos críticos y personales almacenados, procesados y transmitidos.
- Evaluación y monitoreo continuo: Mecanismos para evaluar la efectividad de los controles implementados y asegurar la mejora continua del plan.

Responsabilidades de la Dirección de TIC:

- Asegurar la implementación efectiva de los controles establecidos en el plan.
- Realizar un seguimiento periódico de los riesgos y adaptar el plan según sea necesario.

- Garantizar que todo el personal tenga conocimiento y cumpla con las políticas de seguridad.

Documentación Adjunta:

Plan de Seguridad de la Información que contiene:

- Análisis de riesgos y matriz de controles.
- Procedimientos y políticas de seguridad aplicables.
- Anexos de acta de confidencialidad y Documento de actualización de Políticas.

Conclusión:

Con esta acta se deja constancia de la entrega del Plan de Seguridad de la Información a la Dirección de TIC. La gerencia del departamento se compromete a implementar, supervisar y actualizar el plan conforme a los procedimientos internos y las normativas vigentes.

Firma de Entrega:

Nombre: Jhojan Chicango

Cargo: Estudiante egresado

Firma: _____

Nombre: MSc. Milton Del Hierro

Cargo: Docente Tutor

Firma: _____

Firma de Recepción:

Nombre: MSc. Javier Torres

Cargo: Director de TIC

Firma: _____