Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

Carrera de Computación

Propuesta de un SGSI según la norma ISO/IEC 27001:2013 en la Dirección de Tecnologías de Información de la Universidad Nacional de Loja.

ISMS proposal according to ISO/IEC 27001:2013 in the Information Technology Department of the National University of Loja.

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

AUTOR:

Rubier Andrés Padilla Loaiza

DIRECTOR:

Ing. Cristian Ramiro Narváez Guillen, Mg.Sc.

Loja – Ecuador

2024

Certificación

Loja, 21 de noviembre del 2024

Cristian Ramiro Narváez Guillen, Mg.Sc.
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **Propuesta de un SGSI según la norma ISO/IEC 27001:2013 en la Dirección de Tecnologías de Información de la Universidad Nacional de Loja.**, previo a la obtención del título de **Ingeniero en Ciencias de la Computación**, de la autoría del estudiante **Rubier Andrés Padilla Loaiza**, con cédula de identidad Nro. **1105867079**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo a la presentación del mismo para su respectiva sustentación y defensa.

Firmado electrónicamente por:
CRISTIAN RAMIRO NARVAEZ GUILLEN

Ing. Cristian Ramiro Narváez Guillen, Mg.Sc.
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Rubier Andrés Padilla Loaiza**, declaró ser el autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Integración Curricular en el Repositorio Institucional – Biblioteca Virtual.

Firma: 

Cédula de Identidad: 1105867079

Fecha: 21 de noviembre del 2024

Correo Electrónico: rubier.padilla@unl.edu.ec

Teléfono: +5939665989

Carta de autorización por parte del autor, para consulta, reproducción parcial o total, y/o publicación electrónica del texto completo del Trabajo de Integración Curricular

Yo **Rubier Andrés Padilla Loaiza**, declaró ser el autor del Trabajo de Integración Curricular denominado: **Propuesta de un SGSI según la norma ISO/IEC 27001:2013 en la Dirección de Tecnologías de Información de la Universidad Nacional de Loja.**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con los cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los veintiún días del mes de noviembre de dos mil veinticuatro.

Firma: 

Autor: Rubier Andrés Padilla Loaiza
Cédula: 1105867079
Dirección: Loja (Av. Pío Jaramillo entre Cuba y Chile)
Correo Electrónico: rubier.padilla@unl.edu.ec
Teléfono: +5939665989

DATOS COMPLEMENTARIOS:

Director del Trabajo de Integración Curricular: Ing. Cristian Ramiro Narváez Guillen, Mg.Sc.

Dedicatoria

Dedico este trabajo a mis padres, Natasha Milanova y Rubier Estuardo, quienes han sido mi mayor apoyo y fuente de inspiración en el cumplimiento de mis metas personales y profesionales. A mis hermanas, Carolina y Cristina, por guiarme y aconsejarme en cada nuevo paso que doy en mi vida.

A mis abuelos maternos, Andrés Augusto y María Melva, por el amor y cuidado que me han brindado a lo largo de los años. A mi abuela paterna, Wilma Yolanda, por su constante preocupación y cariño, siempre presente desde que tengo memoria.

A mis amigos, en especial Ana Sofía, Jonathan Josué, Kevin David, Ángel Giovanny, Sandy Dayanna, Denisse Alexandra y Vladimir Abelardo, quienes fueron pilares fundamentales durante mi etapa universitaria. Su amistad, apoyo, alegría y respeto han dejado una huella imborrable, contribuyendo positivamente a mi formación profesional y forjando vínculos que perdurarán para siempre.

Rubier Andrés Padilla Loaiza

Agradecimiento

Expreso mi eterno agradecimiento a la Universidad Nacional de Loja por haberme acogido durante estos cinco años, y a la Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables por su invaluable contribución en mi formación. Agradezco profundamente a los docentes de la Carrera de Computación, quienes, con profesionalismo y dedicación, compartieron sus conocimientos para moldearme como un profesional de calidad.

Mi gratitud también al personal técnico de la Dirección de Tecnologías de Información, por su apoyo en la ejecución de mi Trabajo de Integración Curricular. En especial, al Ingeniero Juan Carlos Riofrío, quien estuvo involucrado activamente en todas las etapas del proyecto, aportando su experiencia para garantizar resultados de calidad que sean útiles para la Dirección.

Al Ingeniero Cristian Narváez, mi Director del Trabajo de Integración Curricular, agradezco su guía, paciencia y respaldo técnico en el ámbito de la seguridad de la información, asegurando que mi trabajo se desarrollará de manera óptima y fuera entregado con éxito a la Dirección de Tecnologías de Información.

Finalmente, agradezco a mi familia y amigos por su amor, apoyo incondicional y motivación constante. ¡Gracias!

Rubier Andrés Padilla Loaiza

Índice de Contenidos

Portada i
Certificación ii
Autoría iii
Carta de autorización iv
Dedicatoria v
Agradecimiento vi
Índice de Contenidos vii
Índice de Tablas ix
Índice de Figuras x
Índice de Anexos xi
1 Título 1
2 Resumen 2
Abstract 3
3 Introducción 4
4 Marco teórico 6
4.1 Antecedentes 6
4.2 Fundamentos Teóricos 7
4.2.1 Seguridad de la información 7
4.2.2 Estándares de Gestión de la Seguridad de la Información 11
4.2.3 Sistema de Gestión de Seguridad de la Información (SGSI) 21
4.2.4 Gestión de riesgos 23
4.2.5 Trabajos relacionados 28
5 Metodología 29
5.1 Área de estudio 29
5.2 Procedimiento 29
5.2.1 Objetivo 1: Implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL) 29
5.2.2 Objetivo 2: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3 32

5.3 Recursos 32
5.3.1 Recursos científicos 32
5.3.2 Recursos técnicos 33
5.3.3 Recursos tecnológicos 34
6 Resultados 35
6.1 Objetivo 1: Implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL) 35
6.1.1 Fase 1: Planificar (P) 35
6.1.2 Fase 2: Hacer (D) 58
6.2 Objetivo 2: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3 63
6.2.1 Fase 3: Verificar (C) 63
6.2.2 Fase 4: Actuar (A) 75
7 Discusión 76
7.1 Objetivo 1: Implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL) 76
7.2 Objetivo 2: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3 77
8 Conclusiones 79
9 Recomendaciones 81
10 Bibliografía 82
11 Anexos 88

Índice de Tablas

Tabla 1. Análisis comparativo. 9
Tabla 2. Familia de la norma ISO 27000. 14
Tabla 3. Trabajos relacionados. 28
Tabla 4. Aplicabilidad de la norma ISO/IEC 27001:2013. 35
Tabla 5. Resumen del grado de aplicabilidad de la norma ISO 27001. 37
Tabla 6. Niveles de madurez. 40
Tabla 7. Roles y Funciones. 44
Tabla 8. Inventario de activos. 47
Tabla 9. Confidencialidad. 48
Tabla 10. Integridad. 48
Tabla 11. Disponibilidad. 49
Tabla 12. Criterios de valoración. 50
Tabla 13. Valoración total del activo. 50
Tabla 14. Amenazas. 51
Tabla 15. Descripción de las amenazas. 52
Tabla 16. Degradación. 52
Tabla 17. Impacto. 52
Tabla 18. Probabilidad. 53
Tabla 19. Nivel de riesgo. 53
Tabla 20. Matriz de riesgos. 55
Tabla 21. Mapa de calor. 57
Tabla 22. Tipos de protección. 63
Tabla 23. Criterios de valoración de salvaguardas contra el impacto. 64
Tabla 24. Criterios de valoración de salvaguardas preventivas. 65
Tabla 25. Descripción de la matriz de casos de prueba. 66
Tabla 26. Matriz de casos de prueba. 67
Tabla 27. Mapa de calor final. 73

Índice de Figuras

Figura 1. Prácticas de gestión más adoptadas por las organizaciones de Latinoamérica en 2023. 7
Figura 2. Seguridad de la información, Seguridad Informática y Ciberseguridad. 9
Figura 3. Tríada de la Seguridad. 10
Figura 4. Origen y Evolución de la norma ISO 27001. 13
Figura 5. Familia de la norma ISO 27000. 13
Figura 6. Estructura de la norma ISO 27001. 17
Figura 7. Estructura de la norma ISO 27002. 19
Figura 8. Modelo PHVA para ISO 27001. 22
Figura 9. Elementos del análisis de riesgos potenciales. 25
Figura 10. Ubicación de la Dirección de Tecnologías de Información – UNL. 29
Figura 11. Organigrama de la DTI. 39
Figura 12. Nivel de Cumplimiento (ISO/IEC 27001:2013). 41
Figura 13. Nivel de Cumplimiento (ISO/IEC 27002:2013). 42
Figura 14. Evaluación de riesgos en la DTI. 57
Figura 15. Mitigación de riesgos en la DTI. 73
Figura 16. Nivel de Cumplimiento posterior al SGSI (ISO/IEC 27001:2013). 74
Figura 17. Nivel de Cumplimiento posterior al SGSI (ISO/IEC 27002:2013). 75

Índice de Anexos

Anexo 1: Entrevista inicial al Ing. Juan Carlos Riofrío, Mg. 88
Anexo 2: Actas de reunión con el Ing. Juan Carlos Riofrío, Mg, para determinar el estado de la seguridad de la información en la DTI. 88
Anexo 3: Acta de reunión con el Ing. Juan Carlos Riofrío, Mg, para evaluar la eficacia de las políticas de seguridad de la información. 88
Anexo 4: Acta de reunión con el Ing. Juan Carlos Riofrío, Mg, para evaluar el nivel de madurez de la DTI posterior a la propuesta del SGSI. 88
Anexo 5: Acta de entrega y aceptación de la documentación del SGIS al Ing. Juan Carlos Riofrío, Mg. 88
Anexo 6: Reglamento Orgánico de Gestión Organizacional por Procesos de la Universidad Nacional de Loja. 89
Anexo 7: Manuales de puestos de carrera – LOSEP. 89
Anexo 8: Políticas de Telecomunicaciones, Desarrollo de Software y Redes de la Universidad Nacional de Loja. 89
Anexo 9: Informe sobre el estado de la seguridad de la información en la Dirección de Tecnologías de Información. 89
Anexo 10: Informe sobre las necesidades y expectativas de las partes interesadas en el SGSI 89
Anexo 11: Documento sobre el Alcance del Sistema de Gestión de Seguridad de la Información (SGSI). 89
Anexo 12: Política de seguridad de la información. 90
Anexo 13: Inventario de activos. 90
Anexo 14: Metodología de evaluación y tratamiento de riesgos. 90
Anexo 15: Informe de la situación actual de la DTI. 90
Anexo 16: Declaración de aplicabilidad. 90
Anexo 17: Informe sobre la evaluación y tratamiento de riesgos. 91
Anexo 18: Plan de tratamiento de riesgo. 91
Anexo 19: Política de roles y responsabilidades de seguridad. 91
Anexo 20: Política sobre dispositivos móviles y teletrabajo. 91
Anexo 21: Política trae tu propio dispositivo (BYOD). 91
Anexo 22: Política de uso aceptable 91
Anexo 23: Política de seguridad para proveedores. 91
Anexo 24: Procedimiento para la gestión de incidentes 91
Anexo 25: Política de clasificación de la información. 91
Anexo 26: Política de eliminación y destrucción 92

Anexo 27: Procedimientos operativos para tecnología de la información (TI) y la comunicación. 92
Anexo 28: Política de control de acceso. 92
Anexo 29: Política del uso de controles criptográficos. 92
Anexo 30: Política de seguridad física y ambiental. 92
Anexo 31: Política de pantalla y escritorio limpio. 92
Anexo 32: Política de gestión de cambios. 92
Anexo 33: Política de desarrollo seguro. 93
Anexo 34: Política de creación de copias de seguridad. 93
Anexo 35: Política de gestión de registros y eventos de seguridad. 93
Anexo 36: Política de transferencia de la información. 93
Anexo 37: Política de la continuidad del negocio. 93
Anexo 38: Política de cumplimiento legal, regulatorio y contractual. 93
Anexo 39: Política de revisión y cumplimiento de la seguridad de la información. 93
Anexo 40: Políticas de la DTI. 94
Anexo 41: Informe de casos de pruebas. 94
Anexo 42: Informe sobre la reevaluación del nivel de madurez en la Dirección de Tecnologías de Información. 94
Anexo 43: Certificado de la Dirección de Tecnologías de Información. 94
Anexo 44: Evidencias de la presentación de los resultados del TIC en la Dirección de Tecnologías de Información. 94
Anexo 45: Certificado de traducción del resumen en inglés. 95

1 Título

Propuesta de un SGSI según la norma ISO/IEC 27001:2013 en la Dirección de Tecnologías de Información de la Universidad Nacional de Loja.

ISMS proposal according to ISO/IEC 27001:2013 in the Information Technology Department of the National University of Loja.

2 Resumen

La seguridad de la información es esencial para que las instituciones educativas afronten los riesgos asociados al uso de la tecnología y así cumplan con los objetivos estratégicos que se han planteado, sin embargo, la falta de documentación actualizada y formal que guíe el desempeño de los trabajadores puede provocar perjuicios importantes. Por ello, el presente Trabajo de Integración Curricular tiene como objetivo desarrollar una propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001:2013 para la creación de políticas específicas dirigidas a la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja. El desarrollo del SGSI se estructuró siguiendo el ciclo PDCA y la metodología MAGERIT v.3. En la fase de Planificación (P), se recopiló información relevante del contexto interno y externo de la DTI, se definió el alcance del SGSI, se estableció una política de seguridad de alto nivel y se llevó a cabo una evaluación y tratamiento de riesgos, culminando con la declaración de aplicabilidad de los controles de seguridad. Durante la fase de Ejecución (D), se desarrollaron 27 políticas específicas de seguridad de la información, diseñadas para mitigar los riesgos identificados en la DTI. La fase de Verificación (C) evaluó la efectividad de estas políticas, logrando redistribuir completamente los 114 riesgos con un nivel “Muy Alto” y los 285 con nivel “Alto”, incrementando los riesgos medios y bajos en un 52,53% y 135,09% respectivamente, lo que elevó el nivel de madurez de la DTI de 2 (Ejecutado) a 3 (Definido). Finalmente, en la fase de Actuar (A), se entregó el SGSI a la DTI. Se concluye que las políticas del SGSI apoyan a la reducción de los riesgos relacionados con los activos de información, creando un entorno más seguro y controlado en la DTI.

Palabras clave: Seguridad de la información, Ciclo PDCA, MAGERIT v.3, Mitigación de riesgos

Abstract

Information security is essential for educational institutions to address the risks associated with using technology and thus meet their strategic objectives. However, the absence of up-to-date and formal documentation to direct the performance of employees can result in considerable harm. As a result, the goal of this curricular integration work is to create a proposal for an information security management system (ISMS) based on the ISO/IEC 27001:2013 standard. This proposal will focus on developing specific policies for the Directorate of Information Technology (DTI) at the National University of Loja. The development of the ISMS was structured following the PDCA cycle and the MAGERIT v.3 methodology. In the planning phase (P), we gathered relevant information from both the internal and external contexts of the DTI. We defined the scope of the ISMS, established a high-level security policy, and carried out risk assessment and treatment. This culminated with the declaration of the applicability of security controls. During the implementation phase (D), 27 specific information security policies were developed designed to mitigate the risks identified in the ITD. In the verification phase (C), the effectiveness of these policies was assessed. The 114 risks classified as "very high" and the 285 risks classified as "high" were completely reassessed. This resulted in a 52.53% increase in medium risks and a 135.09% increase in low risks. As a result, the DTI's maturity level improved from 2 (implemented) to 3 (defined). Finally, in the Act (A) phase, the ISMS was handed over to the DTI. It is concluded that the ISMS policies support the reduction of risks related to information assets, creating a more secure and controlled environment in the DTI.

Keywords: Information Security, PDCA Cycle, MAGERIT v.3, Risk Mitigation

3 Introducción

En el ámbito académico, los departamentos responsables de la administración de equipos y sistemas tecnológicos deben implementar medidas de seguridad de la información, debido a los numerosos riesgos asociados al manejo de datos confidenciales a través del uso de la tecnología [1]. Una gestión adecuada de la seguridad de la información es esencial para el desempeño efectivo de las actividades de una institución académica, contribuyendo al cumplimiento de sus objetivos administrativos y académicos [2], generando confianza entre estudiantes y trabajadores, al mismo tiempo que se reducen los riesgos inherentes al uso de sistemas de información [3].

En la Universidad Nacional de Loja (UNL), la Dirección de Tecnologías de Información (DTI) es el departamento encargado del ámbito tecnológico. De acuerdo a una entrevista realizada al encargado del Proceso de Seguridad Informática, se identificó que la DTI cuenta con una política desactualizada e informal que no refleja su situación actual (ver **Anexo 1**). La falta de una política apropiada genera incertidumbre entre los trabajadores, lo que provoca inconsistencias e ineficiencias en la identificación y mitigación de los riesgos de seguridad relacionados con los activos de información, ya sea por su uso indebido o por la falta de controles de seguridad adecuados. Ante esta situación, surge la siguiente pregunta de investigación: "¿En qué medida las políticas de seguridad de un SGSI basado en la ISO/IEC 27001:2013 apoyarán a la reducción de riesgos en la Dirección de Tecnologías de Información?".

El objetivo principal planteado para responder a la pregunta de investigación es desarrollar una propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001:2013 para la creación de políticas específicas dirigidas a la Dirección de Tecnologías de Información de la Universidad Nacional de Loja. Se establecen dos objetivos específicos: el primero consiste en implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información. El segundo objetivo se enfoca en evaluar la eficacia del SGSI por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3.

La revisión de trabajos relacionados [4], [5], [6], [7], subraya la importancia de desarrollar un SGSI para proteger la información confidencial de clientes y trabajadores en diversos entornos, como un hospital de especialidades, una cooperativa de ahorro y crédito, y una universidad. Este trabajo aporta un valor adicional al utilizar la metodología MAGERIT v.3 para crear escalas de madurez, que permitirán evaluar la efectividad del SGSI en la reducción de riesgos asociados a los activos de información de la DTI.

El desarrollo de este trabajo ha generado beneficios significativos al proporcionar una documentación formalizada que guía a los trabajadores de la DTI en el desempeño de sus actividades, planteando medidas para proteger la información crítica y sensible. Todo ello se logró diseñando políticas específicas, basadas en los controles de seguridad establecidos en el Anexo A de la norma ISO/IEC 27001:2013. Sumado a esto, se implementó un enfoque estructurado para la evaluación y tratamiento de riesgos, de acuerdo con la metodología MAGERIT v.3, permitiendo identificar los activos de información críticos y los riesgos asociados, descartando métodos poco eficaces, y optimizando el tiempo y los recursos destinados a la seguridad de la información.

El alcance del TIC se limita a la duración de un ciclo académico, lo que impide cumplir en su totalidad las cláusulas de la norma ISO/IEC 27001 en la propuesta del SGSI. Por lo tanto, corresponde a la DTI llevar a cabo auditorías internas para que la alta dirección pueda evaluar el estado de los controles de seguridad y determinar la necesidad de aplicar acciones correctivas.

4 Marco teórico

4.1 Antecedentes

La incorporación de las Tecnologías de la Información y la Comunicación (TIC) en el ámbito académico ha mejorado notablemente el desempeño de estudiantes, docentes y personal administrativo, debido al fácil acceso a la información que requieren y a una comunicación estable entre los diferentes sectores que convergen dentro de las instituciones educativas [8]. Las Instituciones de Educación Superior (IES) han realizado importantes inversiones en la adquisición de software específico para optimizar tanto los procesos de enseñanza-aprendizaje como los administrativos y de gestión [9]. Algunos de los recursos más utilizados en las universidades son páginas web institucionales, plataformas virtuales, sistemas de administración de aprendizaje, foros virtuales, correo electrónico institucional y videoconferencias [10].

La aplicación de las TIC en las universidades ha generado un nuevo panorama que requiere la actualización de normativas y políticas relacionadas con su uso por parte de trabajadores, estudiantes y usuarios en general. Dado que la tecnología es el medio por el cual se ofrece un servicio o producto, la información generada, almacenada y procesada por dichos equipos se convierte en el activo más valioso para una institución educativa. La seguridad de la información representa, por lo tanto, un desafío crucial debido al aumento constante de vulnerabilidades y amenazas, las cuales, con el avance de la tecnología, son cada vez más aptas para causar daños significativos en diversos niveles y a distintos usuarios [11].

Es fundamental un entorno estable que garantice el uso adecuado de las TIC, donde la confianza de los usuarios no se vea comprometida por la difusión de información engañosa o ataques informáticos diseñados para vulnerar aplicaciones o sustraer datos personales. De acuerdo con el informe anual de la Agencia de la Unión Europea de Ciberseguridad (ENISA) y los hallazgos de ESET, en 2023 el 66% de las empresas sufrieron ataques tipo ransomware, afectando la capacidad operativa en el 90% de los casos y causando pérdidas de ingresos en el 86%. Este tipo de amenaza, considerada especialmente preocupante por el 96% de las organizaciones, destaca la importancia de proteger la seguridad de la información [12], [13].

Resulta evidente como el creciente número de amenazas y vulnerabilidades que afectan a los sistemas de información, es un tema preocupante que requiere la atención de todas aquellas personas e instituciones que manejan o generan información crítica. A la hora de establecer controles, se diferencian dos grupos: los basados en tecnología, como soluciones de firewall, y aquellos relacionados con la gestión, enfocados en la concienciación y la generación de procesos para la protección de la información, como las políticas de seguridad [13].

Las encuestas realizadas por ESET en Latinoamérica en 2023, cuyos resultados se presentan en la **Figura 1**, indican que el 81% de las organizaciones cuenta con una política de seguridad, lo que representa un aumento del 10% respecto a 2022. De manera similar, el 42% de las organizaciones dispone de un plan de respuesta a incidentes, reflejando un incremento del 4% en comparación con el año 2022. En cuanto a planes de continuidad de negocio, el 38% de las organizaciones afirma tener uno, el cual es fundamental para restaurar la operatividad tras un ataque informático, por otro lado, el 42% aplica la clasificación de la información como una práctica de gestión [13].

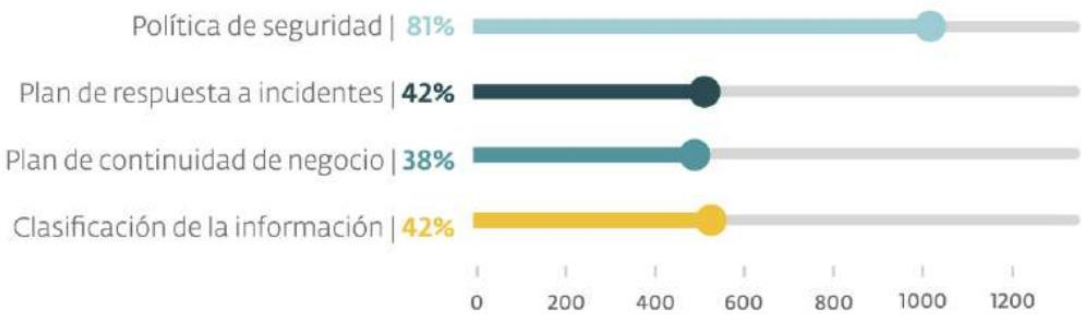

Figura 1. Prácticas de gestión más adoptadas por las organizaciones de Latinoamérica en 2023.
Nota. Recuperado de [13].

Mediante una entrevista con el Ing. Juan Carlos Riofrío, Mg, encargado del Proceso de Seguridad Informática (ver **Anexo 1**), se constató que la DTI posee una política desactualizada que no cumple con los requisitos necesarios para asegurar la integridad de la información frente a ataques informáticos o fallas humanas derivadas de la falta de capacitación o por errores involuntarios.

En vista de lo anterior, el objetivo general del presente Trabajo de Integración Curricular (TIC) es desarrollar una propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) con base en la norma ISO/IEC 27001:2013 para la creación de políticas específicas dirigidas a la Dirección de Tecnologías de Información de la Universidad Nacional de Loja. El sistema incluirá la formulación de una política de seguridad de alto nivel y el diseño de políticas específicas orientadas a la protección de los activos de información, buscando crear un entorno en el que todos los trabajadores se comprometan con la seguridad de la información institucional.

4.2 Fundamentos Teóricos

4.2.1 Seguridad de la información

La adopción de las Tecnologías de la Información y la Comunicación (TIC) ha transformado a la sociedad actual en una red hiperconectada, lo que ha facilitado una amplia variedad de actividades tanto cotidianas como profesionales, tales como la adquisición de productos o servicios en línea, el intercambio de archivos, las transacciones financieras, entre otras; de este modo, la tecnología ha incrementado la

productividad al ofrecer acceso inmediato a una vasta cantidad de información con tan solo un clic [14].

No obstante, el empleo de las TIC conlleva riesgos y amenazas significativas, ya que día a día surgen nuevas vulnerabilidades en los sistemas de información o se desarrollan códigos maliciosos capaces de evadir controles de seguridad. Estos fallos pueden permitir que un atacante acceda a información confidencial, lo que podría derivar en problemas legales y financieros, afectando la reputación de la organización y la confianza de sus clientes [15].

Ante el avance tecnológico y su integración en la vida diaria, la seguridad de la información (InfoSec) emerge como un factor crítico. Este concepto abarca un conjunto de procesos, recursos técnicos y administrativos, así como medidas preventivas y reactivas, destinados a proteger la información crítica y sensible de una organización. Abordando amenazas como el acceso no autorizado, el uso indebido de datos y las interrupciones de servicio, InfoSec proporciona un marco para diseñar salvaguardas que aseguren la integridad y disponibilidad de la información en todo su ciclo de vida [16].

4.2.1.1 Seguridad informática

Se ocupa de proteger la información procesada en infraestructuras tecnológicas y de telecomunicaciones, abarcando dispositivos conectados a internet, como los móviles, que hoy en día almacenan más datos que muchos ordenadores. Esta protección también se extiende a dispositivos IoT y a los almacenes de datos en la nube, impulsada por la creciente adopción del cloud computing [17], [18], [19].

4.2.1.2 Ciberseguridad

El ciberespacio ha difuminado las fronteras internacionales, permitiendo una globalización sin precedentes, convirtiéndose en un campo virtual de conflicto, comercio y comunicación, generando nuevas oportunidades en los ámbitos científico, social y cultural, al igual que graves riesgos para la seguridad de individuos, empresas y naciones. La ciberseguridad busca garantizar la continuidad de las operaciones en este entorno digital frente a amenazas como malware y ataques de secuestro de datos, promoviendo un sistema de defensa robusto que requiere la colaboración entre gobiernos, empresas y la sociedad en general [20], [21].

4.2.1.3 Diferencia entre Seguridad de la Información, Seguridad Informática y Ciberseguridad

Aunque los términos están estrechamente relacionados, es crucial diferenciarlos para evitar confusiones. Como se muestra en la **Figura 2**, la seguridad informática y la ciberseguridad son componentes de la seguridad de la información, cuyo alcance va más allá del ámbito digital e incluye aspectos físicos y organizacionales. Esto implica

fomentar una cultura de seguridad mediante la concienciación, educación y capacitación del personal.

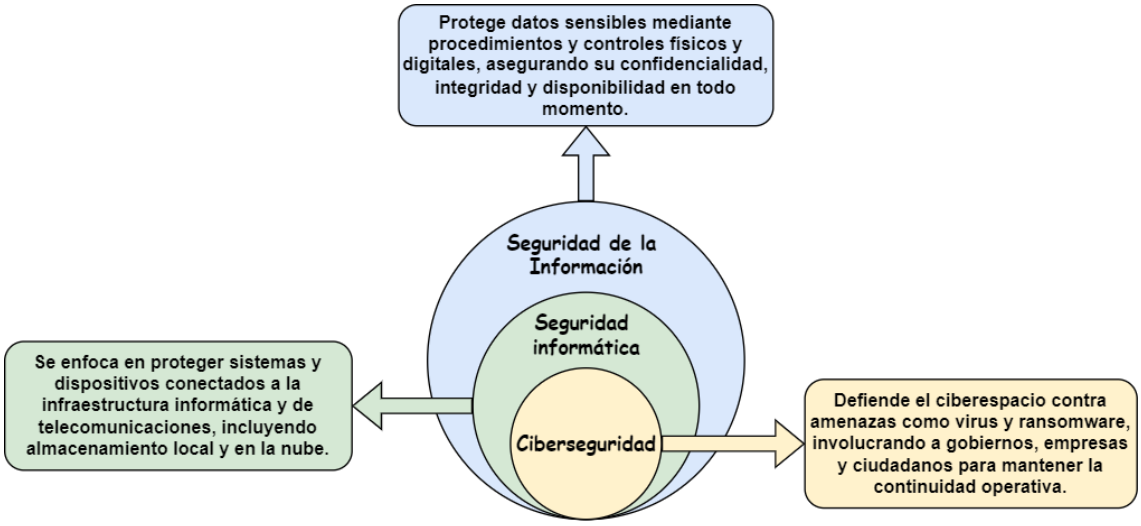

Figura 2. Seguridad de la información, Seguridad Informática y Ciberseguridad.
Nota. Elaboración propia.

En la **Tabla 1** se muestra un análisis comparativo que ilustra las diferencias entre estos tres conceptos en diversos aspectos con base en lo investigado en [22], [23], [24]:

Tabla 1. Análisis comparativo.

Concepto / Característica	Seguridad de la Información	Seguridad Informática	Ciberseguridad
Ámbito de aplicación	Protección de datos e información en cualquier formato contra cualquier riesgo o amenaza.	Aseguramiento de la infraestructura técnica de una organización, incluyendo hardware, software, dispositivos y red.	Defensa exclusiva de datos digitales y sistemas conectados contra amenazas cibernéticas, asegurando la seguridad y gestionando incidentes en el entorno digital.
Medidas de seguridad	Se enfoca en acciones preventivas y de protección para disminuir el riesgo de amenazas que puedan dañar los sistemas interconectados y la información de una empresa.	Engloba una serie de medidas de seguridad destinadas a salvaguardar todos los elementos de la infraestructura tecnológica de una organización, abarcando desde el hardware y el software hasta las redes y los sistemas de información.	Incluye estrategias de protección para prevenir ciberataques y asegurar la integridad, confidencialidad y disponibilidad de la información digital.
Idoneidad	Considera de forma integral a las personas, el cumplimiento de normas y la gestión de la información para proteger los	Se aplica a toda la infraestructura técnica de una organización, incluyendo redes, servidores, infraestructura	Se incluye todo aquello que tenga que ver con redes, servidores, infraestructura crítica, software, hardware, etc.

Concepto / Característica	Seguridad de la Información	Seguridad Informática	Ciberseguridad
	datos y sistemas de una organización.	crítica, software, hardware, etc.	
Funciones	Debe ser aplicada a toda la organización, de manera que todos los departamentos adopten una cultura basada en la seguridad, asegurándose de hacer uso de buenas prácticas para la ejecución de sus labores.	Implica roles especializados que se centran en la seguridad de la infraestructura técnica y de información de una organización.	Se puede agrupar a un departamento que se encargue de monitorizar la seguridad de los datos digitales al ser transportados a través de la red empresarial, no requiere de la participación del personal no especializado.
Procedimientos	El funcionamiento efectivo de la seguridad de la información requiere normas como la ISO 27001, herramientas y tecnologías para proteger los datos, incluyendo el cumplimiento de normativas de retención.	Abarca diversas metodologías como OWASP, COBIT, e ITIL destinadas a proteger todos los aspectos de la infraestructura técnica de una organización.	Emplea métodos, herramientas e innovaciones tecnológicas que se actualizan y renuevan continuamente con el objetivo de mantenerse un paso adelante de los delincuentes informáticos.

Nota. Elaboración propia.

4.2.1.4 Tríada CID

La **Figura 3** muestra las dimensiones clave de la tríada de seguridad: Confidencialidad (C), Integridad (I) y Disponibilidad (D).

Figura 3. Tríada de la Seguridad.
Nota. Recuperado de [25].

Comprender el alcance de estas dimensiones permite evaluar cuál de ellas se ve afectada cuando un riesgo se materializa. A continuación, se detallan:

4.2.1.4.1 Confidencialidad

La información sólo puede ser accedida por las personas autorizadas, de modo que, no sea divulgada ni accedida por terceros. Esto mantiene el secreto de los datos personales, ya sea cuando están almacenados en repositorios o servidores digitales y se transmiten vía internet, o se plasme la información físicamente en documentos en papel y sea entregada de un individuo a otro en el espacio laboral [26], [27], [28].

4.2.1.4.2 Integridad

Se refiere a la preservación de la exactitud y confiabilidad de la información al no ser alterada por error o intencionalmente por personas no autorizadas durante su almacenamiento o transmisión, asegurando su precisión y veracidad en la toma de decisiones estratégicas. Para mantener la integridad, es crucial el control del hardware y software que soportan los datos y de las acciones de los usuarios para que solo accedan a información de la que tienen derechos de configuración [28], [29], [30].

4.2.1.4.3 Disponibilidad

Es la garantía de que la información pueda ser accedida de forma oportuna por las personas autorizadas, por lo que, el conjunto de equipos, dispositivos de comunicación y aplicaciones deben funcionar correctamente y de manera eficiente cuando se les requiera. Además, tienen que ser capaces de recuperarse en el menor tiempo posible después de alguna interrupción provocada por factores ambientales o industriales, y así evitar que la productividad de la organización se vea afectada [19], [28], [31].

4.2.2 Estándares de Gestión de la Seguridad de la Información

La estandarización establece normas y procedimientos para procesos específicos, como los relacionados con la seguridad de la información, que requieren repetición y continuidad. Estas normas, respaldadas por entidades reconocidas a nivel nacional o internacional, otorgan prestigio y reconocimiento a las empresas que las aplican, demostrando madurez en la gestión de datos personales y atrayendo a un público más amplio [32].

Las normas y contenidos de estos estándares son aprobados por organismos reconocidos, conformados por comités técnicos encargados de estudiar, analizar, y definir aspectos clave que se incluirán en los documentos. Los cuales son de ayuda para que las empresas sean competitivas y cumplan con las regulaciones y obligaciones del sector económico en el que se desempeñen. Algunos ejemplos de organismos reconocidos incluyen [33]:

- ISA – International Society of Automation
- ISO – International Organization for Standardization
- IEC – International Electrotechnical Commission

- NIST – National Institute of Standards and Technology

4.2.2.1 La Organización Internacional de Estándares (ISO)

La ISO es una organización internacional, sin fines de lucro ni afiliación gubernamental, fundada en 1947 en Ginebra, Suiza. Se dedica al desarrollo y publicación de normas internacionales a través de comités técnicos compuestos por expertos que comparten sus conocimientos para impulsar la innovación y abordar desafíos globales. Con 172 organismos nacionales y 840 comités técnicos, la ISO ha publicado más de 25.493 normas que abarcan temas técnicos, sociales y laborales, como la responsabilidad social (ISO 26000) y la seguridad en el trabajo (ISO 45001) [34], [35].

4.2.2.2 La Comisión Electrotécnica Internacional (IEC)

Fundada en 1906, la IEC es una organización líder en la publicación de Normas Internacionales para tecnologías eléctricas, electrónicas y afines. Con la participación de 169 países y más de 20.000 expertos, la IEC desarrolla normas que van desde nanotecnología hasta turbinas hidráulicas, promoviendo la cooperación internacional en la normalización electrotécnica para garantizar la seguridad, funcionalidad y fiabilidad de productos y sistemas [36], [37].

4.2.2.3 Origen y evolución de la norma ISO 27000

La serie de normas ISO 27000 se originó en el Instituto Británico de Estándares (BSI), que en 1995 publicó la primera norma técnica de seguridad, la BS 7799-1:1995, la cual proporcionaba directrices recomendadas en seguridad de la información, pero no permitía certificación. En 1998, se publicó la segunda versión, BS 7799-2:1999, estableciendo requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), certificable por una entidad independiente [38].

La norma BS 7799 fue revisada en 1999 y, en 2000, la primera parte fue adoptada por ISO e IEC como ISO/IEC 17799:2000. En 2002, se revisó BS 7799-2 para alinearla con las normas de sistemas de gestión ISO/IEC. En 2005, una revisión más profunda transformó ISO/IEC 17799:2000 en ISO/IEC 17799:2005, mientras que BS 7799-2 se convirtió en ISO/IEC 27001:2005, marcando el inicio de la serie de normas ISO 27000 [39].

En 2007, ISO/IEC 17799:2005 pasó a ser ISO/IEC 27002:2005 y se publicó ISO/IEC 27001:2007. Finalmente, en 2013, ambas normas fueron actualizadas a ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Aunque una nueva versión se publicó en 2022, aún no hay suficiente información bibliográfica disponible para su uso en la propuesta de un SGSI [39].

La **Figura 4** muestra un resumen gráfico del origen y evolución de la serie de normas ISO 27000.

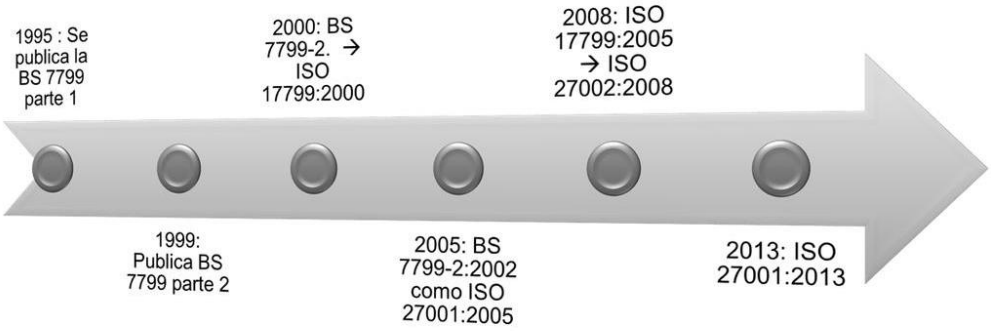

Figura 4. Origen y Evolución de la norma ISO 27001.
Nota. Recuperado de [40].

4.2.2.3.1 Familia de la norma ISO 27000

Después de exponer el origen y evolución de la serie ISO 27000, es relevante destacar el amplio conjunto de normas que conforman un marco de gestión de la seguridad de la información, aplicable a organizaciones de cualquier tipo y tamaño, ya sean públicas o privadas. A este grupo de estándares internacionales, agrupados como una "Familia", lo ha desarrollado la ISO e IEC, dos organismos internacionales mencionados anteriormente [4], [40], [41].

La familia de normas ISO 27000 establece los requisitos para proteger la información y proporciona controles que permiten a las organizaciones cumplir con las leyes y regulaciones vinculadas a la seguridad de la información. Su propósito es facilitar el comercio seguro entre organizaciones, ya sea en el intercambio de información, servicios o productos, fomentando la innovación tecnológica bajo protocolos de seguridad y prevención de riesgos [42], [43].

En la **Figura 5**, se ilustra la organización de las diversas normas que forman parte de la serie 27000.

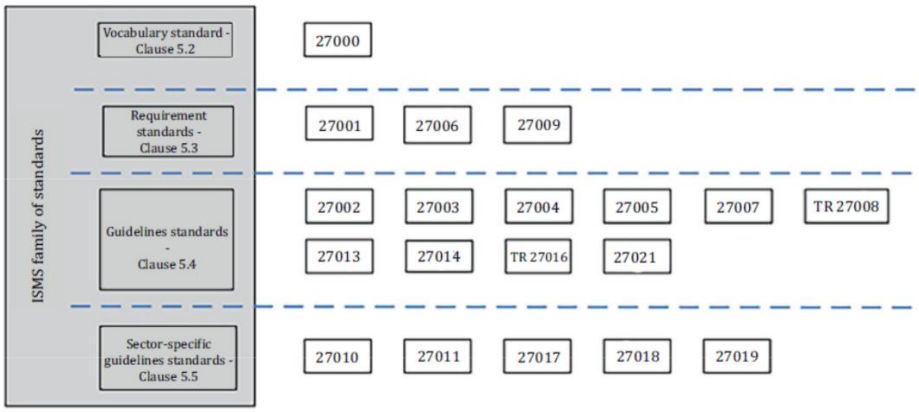

Figura 5. Familia de la norma ISO 27000.
Nota. Recuperado de [44].

La **Tabla 2** describe cada norma según lo mostrado en la **Figura 5**, respaldada por las investigaciones de [4], [40], [41], [42], [43].

Tabla 2. Familia de la norma ISO 27000.

Norma	Alcance	Descripción
	Vocabulario Estándar	
ISO/IEC 27000	Descripción general y vocabulario	Resume los términos y la estructura de las normas ISO 27000, proporcionando definiciones y objetivos.
	Requerimientos Estándar	
ISO/IEC 27001	Especificaciones para un SGSI	Especifica requisitos para implementar y gestionar un SGSI, con un enfoque de gestión de riesgos y mejora continua.
ISO/IEC 27006	Requisitos para los organismos que realizan auditorías y certificaciones de sistemas de gestión de seguridad de la información	Establece los requisitos para la acreditación de organizaciones certificadoras que desean certificar el cumplimiento de la ISO/IEC 27001. Es utilizada junto con la norma ISO/IEC 17021-1 y proporciona un conjunto de requisitos específicos para la certificación de Sistemas de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27009	Aplicación sectorial específica de ISO/IEC 27001	Establece requisitos para crear estándares sectoriales que amplíen y complementen ISO/IEC 27001 y 27002.
	Guías Estándar	
ISO/IEC 27002	Manual de buenas prácticas	Compila buenas prácticas en seguridad de la información con 14 dominios, 35 objetivos y 114 controles.
ISO/IEC 27003	Guía de implementación de un SGSI	Ofrece directrices para implementar un SGSI, apoyando la norma ISO/IEC 27001 con instrucciones detalladas.
ISO/IEC 27004	Sistema de métricas e indicadores	Establece pautas para métricas efectivas en la evaluación del rendimiento de un SGSI.
ISO/IEC 27005	Guía de análisis y gestión de riesgos	Ofrece lineamientos y ejemplos para gestionar riesgos en sistemas de gestión de información, siguiendo ISO/IEC 27001.
ISO/IEC 27007	Guía para auditar un SGSI	Establece criterios para auditorías internas y externas de ISO/IEC 27001, incluyendo planificación y ejecución.
ISO/IEC TR 27008	Guía para auditores sobre controles de seguridad de la información	Ofrece orientación para revisar la implementación y operación de controles de sistemas de información conforme a estándares de seguridad.
ISO/IEC 27013	Orientación sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1	Establece una guía para la integración de las normas ISO/IEC-27001 (SGSI) e ISO/IEC-20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.
ISO/IEC 27014	Gobernanza de la seguridad de la información	Establece principios y proporciona una guía para el gobierno corporativo de la seguridad de la información, ciberseguridad y privacidad.
ISO/IEC TR 27016	Economía organizacional	Ofrece una guía para decisiones económicas en la gestión de la seguridad de la información, apoyando la dirección organizacional.
ISO/IEC 27021	Requisitos de competencia para los profesionales de sistemas de gestión de seguridad de la información	Establece los requisitos de competencia para los profesionales del SGSI que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del SGSI.
	Guías Específicas del Sector Estándar	
ISO / IEC 27010	Gestión de seguridad de la información para las comunicaciones inter-sectoriales e inter-organizacionales	Establece cómo tratar información compartida entre organizaciones, los riesgos y los controles necesarios, especialmente para infraestructuras críticas.
ISO/IEC 27011	Guía de gestión de seguridad de la información específica para telecomunicaciones	Establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando cómo implantar los controles de manera eficiente.

Norma	Alcance	Descripción
ISO/IEC 27017	Controles de Seguridad para Servicios Cloud	Se enfoca en la seguridad de la información en la nube, con controles específicos y guías basadas en ISO/IEC 27002.
ISO/IEC 27018	Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII	Se centra en proteger los datos personales en la nube, estableciendo requisitos para proveedores de servicios en línea. Complementa las normas ISO/IEC-27001 e ISO/IEC-27002 al implementar procedimientos y controles para proteger datos personales en organizaciones que ofrecen servicios en la nube para terceros.
ISO/IEC 27019	Controles de seguridad de la información para la industria de servicios públicos de energía	Facilita una guía basada en la norma ISO/IEC-27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI.

Nota. Elaboración propia.

4.2.2.4 La norma ISO/IEC 27001:2013

En la actualidad, la mayoría de los negocios dispone de información sensible que, si no se protege adecuadamente contra ciberdelincuentes, puede resultar en problemas operativos, financieros y legales, potencialmente llevando a la quiebra al negocio. A pesar de contar con el hardware y software necesarios, muchas empresas no los utilizan apropiadamente debido a factores como la falta de capacitación, mala comunicación y ausencia de documentación formal sobre buenas prácticas de seguridad [45]. Para abordar estos desafíos, la norma ISO/IEC 27001:2013 se ha convertido en la principal opción para asegurar la información, basándose en la gestión de riesgos utilizando la evaluación y mitigación de problemas potenciales que podrían afectar la información [46].

La norma ISO 27001 explica cómo planificar, establecer, implantar, controlar y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema permite una gestión eficaz y la reducción de los riesgos que comprometen la confidencialidad, integridad y disponibilidad de los datos. Además, puede ser implementada para obtener la certificación en cualquier tipo de organización, ya sea con o sin fines de lucro, privada o pública, pequeña o grande. La certificación implica que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización de acuerdo con la norma ISO 27001, lo que representa una ventaja competitiva en el mercado, al demostrar el adecuado manejo de los datos personales de clientes y de la empresa [47].

4.2.2.4.1 Objetivo de la norma

Establecer un entorno basado en la seguridad de la información a partir del análisis y evaluación de los riesgos que podrían materializarse y causar daños, tanto económicos como sociales. Con base en este análisis, se identifican los controles más

adecuados para el contexto institucional, reduciendo los riesgos a niveles aceptables [48].

4.2.2.4.2 Beneficios de la norma

Las empresas recurren a la norma ISO 27001 debido a la creciente cantidad de brechas de seguridad provocadas por el uso inadecuado de los sistemas de información. Esta norma ofrece beneficios generalmente en tres áreas, según [4], [45], [46], [47]:

- **Comercial**

Obtener una certificación internacional mejora la imagen de la empresa ante clientes potenciales, lo que representa una ventaja competitiva. Garantiza un canal de comunicación confiable entre proveedores y clientes para la recepción y entrega de productos y servicios, asegurando el adecuado manejo de datos personales. La implementación de los recursos necesarios para la protección de la información contribuye al incremento de los ingresos comerciales.

- **Operacional**

La ISO 27001 promueve una cultura organizacional que capacita al personal y habilita la tecnología para enfrentar riesgos tecnológicos y otras amenazas. Este enfoque se basa en un marco detallado que abarca procesos clave, incluso aquellos no directamente relacionados con la seguridad, para implementar controles más robustos. Estos controles deben cumplir con las leyes, normas y requisitos contractuales relacionados con la seguridad de la información.

- **Tranquilidad**

Las organizaciones pueden confiar en que su información crítica, como estados financieros, propiedad intelectual, datos de empleados e información de terceros, se mantiene intacta, confidencial y disponible cuando se necesite. La administración centralizada de riesgos con un SGSI robusto y eficiente permite controlar y prevenir los ataques y vulnerabilidades que podrían interrumpir el negocio, afectando así su reputación. Este sistema aplica prácticas de seguridad revisadas por especialistas en el área, lo cual genera confianza entre accionistas, empleados y clientes.

4.2.2.4.3 Estructura de norma

Se han abordado aspectos relacionados con la norma; no obstante, aún no se ha profundizado en su estructura ni en el propósito de cada uno de sus componentes. La norma ISO/IEC 27001:2013 se divide en once apartados principales y un anexo A [45]. Los apartados 0 al 3 constituyen una introducción y, por tanto, no requieren aplicación, por otro lado, los apartados 4 al 10, denominados cláusulas, son de cumplimiento obligatorio para obtener la certificación. La **Figura 6** muestra las cláusulas mencionadas. El anexo A presenta 114 controles de seguridad, cuya aplicabilidad debe evaluarse en el contexto organizacional [49].

Seguidamente, se explican las cláusulas que conforman a la norma ISO 27001, de acuerdo a lo **investigado en [45], [46], [48], [49]:**

Figura 6. Estructura de la norma ISO 27001.
Nota. Recuperado de [50].

- **Cláusula 0:** Introducción

La norma expone de manera resumida su propósito y los requisitos necesarios para establecer y mejorar continuamente un SGSI, destacando su valor estratégico de acuerdo con las necesidades y metas organizacionales. Se enfatiza la integración del sistema con los procesos internos y la gestión de riesgos, para así garantizar la confidencialidad, integridad y disponibilidad de la información, manteniendo compatibilidad con otras normas de gestión.

- **Cláusula 1:** Alcance

Un SGSI puede ser aplicado a cualquier organización, independientemente de su tamaño, sector o madurez en seguridad de la información. Sin embargo, su alcance debe establecerse según la cantidad de activos de información gestionados por empleados y clientes, las actividades involucradas y los recursos dedicados exclusivamente al mantenimiento y mejora continua del sistema.

- **Cláusula 2:** Referencias normativas

Las regulaciones específicas y obligatorias del sector en el que opere la organización han de ser consideradas para el diseño, implementación y mantenimiento del SGSI, de manera que, la empresa no se vea inmiscuida en el incumplimiento de leyes nacionales o internacionales. Asimismo, se debe recordar que se puede hacer uso de otras normas que formen parte de la familia ISO 27000 para promover una cultura basada en la seguridad de la información.

- **Cláusula 3:** Términos y definiciones

La norma ISO/IEC 27000 proporciona términos y definiciones clave, lo cual facilita una comprensión compartida de los requisitos, minimizando interpretaciones subjetivas entre los empleados y reduciendo ambigüedades al emplear controles de seguridad. La versión más reciente de la ISO/IEC incluye 81 términos y definiciones utilizados en la ISO 27001. Al redactar la documentación del SGSI, resulta útil incluir un glosario para quienes no estén familiarizados con la seguridad de la información.

- **Cláusula 4:** Contexto de la organización

La situación interna de la organización y su relación con el entorno externo resultan esenciales para identificar riesgos inherentes a la seguridad de los activos de información. Internamente, deben considerarse aspectos como el nivel de madurez actual en la administración de activos; externamente, es crucial reconocer los organismos reguladores y factores ambientales sobre los que no se tiene control. Esto permite identificar claramente a las partes interesadas que influyen en el SGSI y sus expectativas, lo que define el alcance y focaliza la implementación del sistema en recursos fundamentales para cumplir los procesos organizacionales.

- **Cláusula 5:** Liderazgo

La gerencia desempeña un rol activo en la toma de decisiones para la ejecución y revisión del SGSI, facilitando los recursos necesarios según una política de alto nivel en seguridad de la información alineada con las expectativas de las partes interesadas y los objetivos organizacionales. Respecto al personal, la gerencia asignará roles y responsabilidades en la gestión del SGSI, además de supervisar la presentación de informes sobre su desempeño.

- **Cláusula 6:** Planificación

La evaluación de riesgos aumenta la probabilidad de identificar posibles amenazas, permitiendo tomar decisiones estratégicas basadas en su criticidad. Así se asegura una asignación eficiente de recursos y personal especializado para su tratamiento. Esta tarea se apoya en controles de seguridad que deben analizarse para determinar su idoneidad, la cual queda documentada en la Declaración de aplicabilidad.

- **Cláusula 7:** Soporte

Los recursos, tanto en términos de equipos e infraestructura como del factor humano, son esenciales para ejecutar los procesos empresariales. En el caso del personal, se valora su competencia, es decir, los conocimientos y habilidades que poseen para implementar controles efectivos de seguridad de la información. Además, el recurso humano debe sensibilizarse mediante actividades de comunicación planificadas y bien gestionadas sobre los elementos del SGSI.

- **Cláusula 8:** Operación

Esta cláusula corresponde a la fase de “Hacer (Do)” en el ciclo PDCA y abarca la formalización de procesos relevantes para la seguridad de la información. Dichos procesos deben revisarse con frecuencia, anualmente o según la criticidad y riesgos identificados. Asimismo, el plan de tratamiento de riesgos deberá actualizarse tras evaluaciones técnicas, para luego ser autorizado e implementado nuevamente.

- **Cláusula 9:** Evaluación del desempeño

El monitoreo planificado sobre el proceso del SGSI y de los controles de seguridad es esencial. Las auditorías internas y las revisiones de la dirección permiten evaluar el rendimiento del SGSI; en el caso de las auditorías, se requiere personal capacitado en la documentación y requisitos de la ISO 27001, así como en metodologías de seguridad informática. Las revisiones de la dirección aseguran que el SGSI se mantenga alineado con los objetivos estratégicos de la organización.

- **Cláusula 10:** Mejora

Ningún SGSI es perfecto; sin embargo, estos sistemas de gestión mejoran con el tiempo, incrementando su resistencia ante ataques de seguridad de la información. Esto se logra al tratar las no conformidades como oportunidades de mejora al aplicar acciones correctivas, las cuales pueden identificarse a través de un análisis de la causa raíz del problema.

- **Anexo A:**

Ofrece un conjunto de 114 controles de seguridad, organizados en 14 apartados (de A.5 a A.18).

4.2.2.5 La norma ISO/IEC 27002:2013

Al seleccionar los controles del Anexo A de la ISO/IEC 27001:2013, es fundamental consultar la ISO/IEC 27002:2013, ya que proporciona pautas útiles para una adopción adecuada en el SGSI. Esta norma está estructurada en 14 dominios, 35 objetivos de seguridad y 114 controles de seguridad, tal como se observa en la **Figura 7**. A continuación, se describen los dominios de seguridad conforme a lo investigado en [7], [40], [42], [51], [52]:

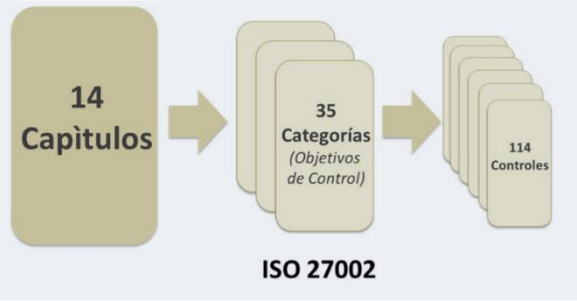

Figura 7. Estructura de la norma ISO 27002.
Nota. Recuperado de [40].

1. **Políticas de seguridad de la información:** Ofrece orientación y apoyo a la gerencia en el ámbito de la seguridad de la información, conforme a los objetivos de la organización y las regulaciones aplicables.
2. **Organización de la seguridad de la información:** Consiste en la implementación de un modelo de gestión interno que permita a los involucrados comprender sus roles y responsabilidades, manteniendo contacto con los grupos de interés pertinentes.
3. **Seguridad relativa a los recursos humanos:** Contratar nuevos empleados requiere una investigación previa para verificar su idoneidad para el puesto y la capacidad de manejar los activos de información. Una vez contratados, será responsabilidad de la organización proporcionarles capacitación en seguridad de la información.
4. **Gestión de activos:** Los activos de información deben identificarse y recibir el nivel adecuado de protección según su importancia dentro de la organización. Se asignarán propietarios responsables de asegurar un uso adecuado de los sistemas de información y equipos.
5. **Control de accesos:** El acceso a la información y a las instalaciones de procesamiento de datos se limitará a personas autorizadas, quienes deben mantener sus credenciales en secreto. Las actividades realizadas deberán registrarse para detectar cualquier intento de vulnerar los sistemas de información.
6. **Criptografía:** El uso de la criptografía es una estrategia eficaz para garantizar la confidencialidad e integridad de la información, aunque requiere una gestión cuidadosa de las claves para controlar quiénes pueden acceder a ciertos datos.
7. **Seguridad física y del entorno:** Los equipos deben ubicarse en áreas donde no sean accesibles para personas ajenas a la organización y deben contar con medidas de protección contra riesgos ambientales o externos. El acceso a las instalaciones será controlado empleando mecanismos de autenticación, como identificaciones.
8. **Seguridad de las operaciones:** Se documentarán los procedimientos operativos de TI, que deberán estar disponibles para el personal involucrado. Es crucial prevenir la infección por código malicioso en las instalaciones de procesamiento de información y mantener un registro de eventos para presentar evidencia en caso de ser necesario.
9. **Seguridad de las comunicaciones:** El intercambio de información se realizará aplicando controles tanto en las redes internas de la organización como a nivel

externo con otras entidades, asegurando un acuerdo que garantice la integridad de la información.

10. **Adquisición, desarrollo y mantenimiento de los sistemas de información:** La seguridad debe incorporarse en cada fase del ciclo de desarrollo de sistemas de información, empleando metodologías y recomendaciones de entidades internacionales en el ámbito del software. Antes de poner una aplicación en producción, deben realizarse pruebas para validar su correcto funcionamiento.
11. **Relación con proveedores:** Los proveedores con acceso a los activos de información de la organización deberán aceptar acuerdos que establezcan su protección y limitaciones de uso. Además, los servicios que provean deben cumplir con los requisitos de seguridad necesarios para asegurar la calidad y satisfacer las necesidades de la entidad.
12. **Gestión de incidentes de seguridad de la información:** Contar con un procedimiento formal para identificar y resolver incidentes es crucial para brindar un servicio estable a los usuarios. La recolección de evidencias y el aprendizaje de cada incidente permiten mejorar la detección y recuperación ante posibles incidentes futuros.
13. **Aspectos de seguridad de la información para la gestión de la continuidad del negocio:** En caso de desastre, la recuperación de recursos y servicios puede lograrse mediante un plan de continuidad del negocio, en el cual se asignen responsabilidades y actividades orientadas a reanudar la operatividad.
14. **Cumplimiento:** La organización debe considerar los requisitos legales y contractuales al implementar el SGSI, de modo que este aporte valor y aumente la resiliencia frente a posibles amenazas.

4.2.3 Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI es una herramienta de gestión compuesta por procedimientos destinados a identificar riesgos y definir controles para su mitigación. Las políticas aplicadas para administrar la información contribuyen a las organizaciones asegurar un tratamiento adecuado de los activos de información, garantizando la confidencialidad, integridad y disponibilidad [4], [53].

4.2.3.1 ¿Para qué necesitamos un SGSI?

Los factores internos y externos de una organización influyen en la decisión de la gerencia para implementar un SGSI. Dado el uso generalizado de la tecnología en el ámbito corporativo y el surgimiento constante de amenazas y vulnerabilidades en las aplicaciones, se requiere una gestión efectiva. Un SGSI permite establecer procedimientos alineados con los objetivos organizacionales y los requisitos

regulatorios, optimizando la relación costo/beneficio al evitar interrupciones y pérdida de recursos en procesos informales [54].

4.2.3.2 Metodología PDCA

El ciclo Planificar-Hacer-Verificar-Actuar (PHVA o PDCA, por sus siglas en inglés), también conocido como ciclo Deming o ciclo de mejora continua, provee un marco sistemático para implementar un sistema de garantía de calidad desde una planificación inicial. Esta metodología, originada en los cambios posteriores a la Segunda Guerra Mundial, fue impulsada por Walter A. Shewhart y luego por W. Edwards Deming, entre otros. El PDCA se ha utilizado ampliamente en diversas organizaciones, desde la industria productiva hasta la educación, para la mejora de procesos.

Este ciclo, que se compone de cuatro fases: Planificar, Hacer, Verificar y Actuar, es fundamental en la implementación y gestión de Sistemas de Gestión de Seguridad de la Información (SGSI). Propicia un enfoque de mejora continua en cada uno de los elementos, incluyendo indicadores y métricas para cuantificar el progreso de la organización. La estructura cíclica del modelo PDCA habilita evaluar periódicamente las actividades y procesos, incorporando nuevos avances, y su aplicación es amplia, abarcando cualquier proceso o actividad institucional (revisar **Figura 8**) [4], [55], [56], [57].

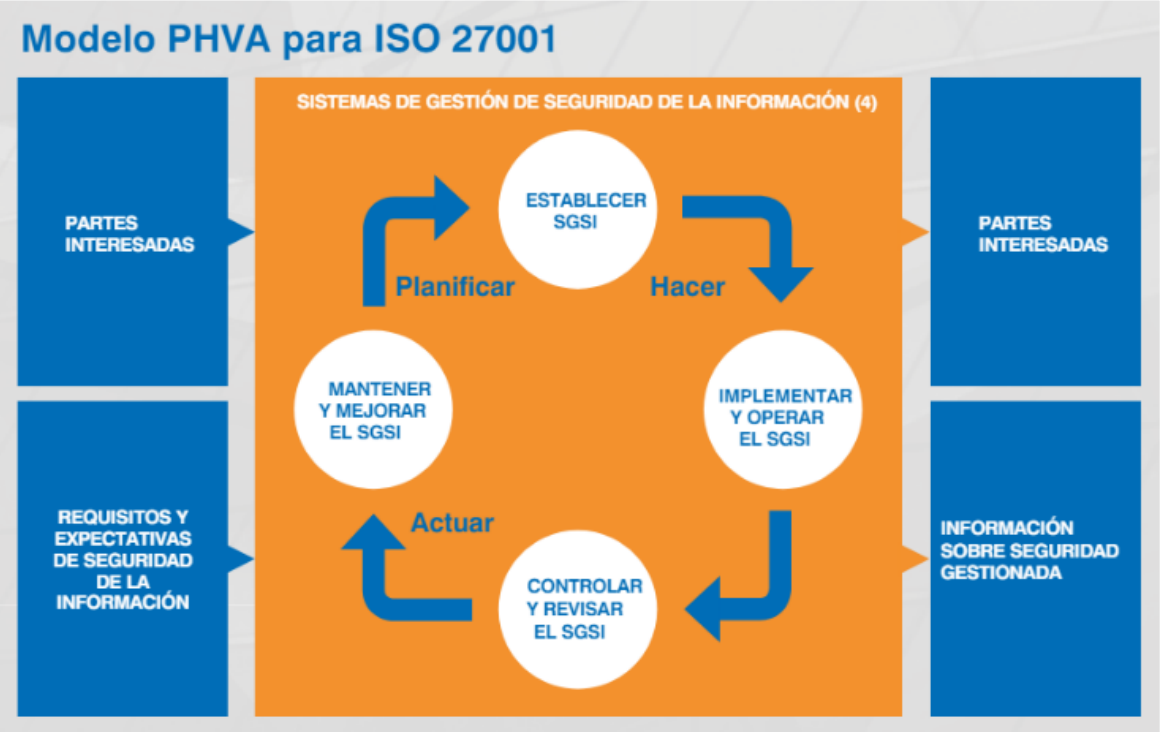

Figura 8. Modelo PHVA para ISO 27001.
Nota. Recuperado de [45].

A continuación, según [4], [56], [57], se especifica las cuatro etapas que conforman esta metodología:

4.2.3.2.1 Establecer y manejar el SGSI (Fase – Planificar (P))

Se diseña el Sistema de Gestión de Seguridad de la Información (SGSI). Se define el alcance del SGSI y se elabora su política de seguridad. También se identifican problemas y recursos necesarios para el sistema, se definen los requisitos de las partes interesadas y condiciones de ejecución, se establecen objetivos, estrategias, planes de acción y políticas organizativas dentro del SGSI, junto con la identificación de riesgos y oportunidades.

4.2.3.2.2 Implementar y operar el SGSI (Fase – Hacer (D))

Se llevan a cabo actividades como la ejecución de la política de seguridad, la metodología de análisis de riesgos y el plan de comunicación. Se registran problemas durante la implementación, en fases de prueba y ejecución real. Además, se asignan responsabilidades y tareas para ejecutar estrategias y controles en el Sistema de Gestión de Seguridad de la Información (SGSI).

4.2.3.2.3 Monitorear y revisar el SGSI (Fase – Verificar (C))

Se revisan los resultados obtenidos durante la implementación para asegurar su alineación con los objetivos de la administración. Se evalúan procesos de gestión y controles de seguridad al aplicar auditorías internas y análisis de riesgos planificados. Durante esta fase, se comparan los resultados con las expectativas planteadas y se toman medidas para corregir desviaciones. Se enfoca en identificar áreas problemáticas y mejorar continuamente el sistema de gestión de seguridad de la información.

4.2.3.2.4 Mantener y mejorar el SGSI (Fase – Actuar (A))

Se implementan mejoras en el SGSI en caso de desalineación con los objetivos establecidos. Se aplican acciones correctivas y, ocasionalmente, de mejora, las cuales pueden extenderse a toda la organización. Si los resultados son satisfactorios, se mantiene el curso original, pero generalmente se requiere ajustes. Con base en las evaluaciones efectuadas se realizan acciones preventivas y correctivas para mejorar el rendimiento del sistema de gestión de seguridad de la información.

4.2.4 Gestión de riesgos

La información es vulnerable a diversas amenazas digitales y físicas que pueden comprometer su integridad, afectando tanto a la organización como a los propietarios de los datos personales almacenados. Las organizaciones deben mejorar continuamente su seguridad mediante políticas, hardware, software y protocolos que mantengan niveles aceptables de riesgo. La gestión de riesgos, parte del SGSI, incluye procesos y actividades para prevenir filtraciones, ataques y manipulación indebida de información en todos sus estados y formas. Se identifican y evalúan amenazas internas y externas, se diseñan estrategias para mitigarlas y, si no es posible, se evita la actividad generadora del riesgo o se transfiere a otra organización [58], [59].

4.2.4.1 Análisis de Riesgos

La evaluación, gestión y tratamiento de riesgos forman parte del análisis de riesgos, un proceso sistemático y analítico para evaluar que todos los aspectos de la empresa estén protegidos de posibles amenazas. Lo cual conlleva comprender la naturaleza de las posibles consecuencias negativas de las amenazas sobre la vida humana, la salud, los activos de información y el medio ambiente [60].

4.2.4.2 Términos clave para el análisis de riesgos

4.2.4.2.1 Activo de información

Es todo aquello que tiene algún valor para la organización y, por ende, debe protegerse, pueden ser tangibles o intangibles. Ejemplos de activos incluyen la infraestructura informática, los equipos auxiliares, las redes de comunicaciones, las instalaciones y las personas, especialmente aquellas que tienen acceso a información crítica y sensible [19].

4.2.4.2.2 Ataque

Un ataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital. Son efectuados por todo tipo de razones, desde hurtos menores hasta actos de guerra. Se utilizan diversas tácticas, como ataques de malware, estafas de ingeniería social y robo de contraseñas, para obtener acceso no autorizado a sus sistemas objetivo [19].

4.2.4.2.3 Amenaza

Las amenazas representan cualquier factor que pueda comprometer la seguridad de un sistema de información. Pueden ser diversas y abarcar desde fallos en la infraestructura auxiliar y fraudes asistidos por computadora, hasta el desconocimiento o mal uso de la información por parte de los empleados, robo de equipos, espionaje o vandalismo, entre otros [19], [61].

4.2.4.2.4 Vulnerabilidad

Es cualquier debilidad o fallo en un sistema de información que compromete su seguridad, varían según la naturaleza de los sistemas y son inherentes a los activos, pudiendo estar relacionadas con el hardware, software, redes, personal, infraestructura u organización. Entre las vulnerabilidades se incluyen fallas en el diseño, errores de configuración, falta de procedimientos y controles, falta de formación adecuada y ausencia o supervisión del personal [19], [61].

4.2.4.2.5 Degradación

Evalúa el nivel de daño causado por un incidente, generalmente definido como una fracción del valor total del activo. Así, es posible concluir que ha sido “parcialmente degradado” o “totalmente degradado” [61].

4.2.4.2.6 Impacto

Medida del daño causado a un activo debido a la materialización de una amenaza. Al comprender el valor de los activos en distintas dimensiones y la degradación que provocan las amenazas, es posible calcular directamente el impacto que éstas tendrían sobre el sistema [19], [54].

4.2.4.2.7 Probabilidad de ocurrencia

Se refiere a la posibilidad de que ocurra un evento, la cual puede ser definida, medida o determinada de manera objetiva o subjetiva, tanto cualitativa como cuantitativamente. Esta medida puede describirse utilizando términos generales o mediante fórmulas matemáticas, como una probabilidad o una frecuencia durante un período de tiempo específico [61].

Todos estos conceptos se relacionan entre sí de la siguiente manera:

AMENAZA explota VULNERABILIDAD afecta ACTIVO provoca IMPACTO

4.2.4.2.8 Riesgo

El riesgo es el resultado de la estimación de la probabilidad de que una amenaza se materialice y el impacto que tendría para la organización, es posible estimarla de forma cuantitativa aplicando la siguiente fórmula mencionada en [61]:

RIESGO = IMPACTO x PROBABILIDAD

En la **Figura 9** se presenta la relación que tienen todos estos términos.

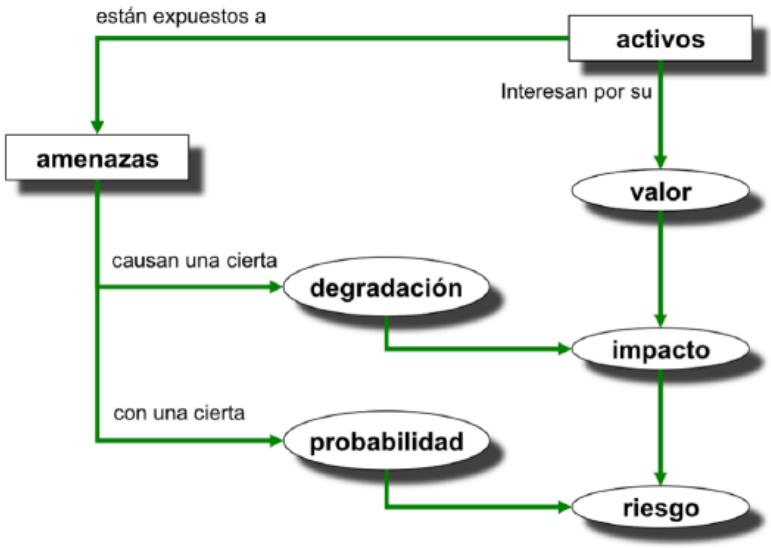

Figura 9. Elementos del análisis de riesgos potenciales.
Nota. Recuperado de [61].

4.2.4.3 Tratamiento de riesgos

Una vez realizado el análisis y la evaluación de los riesgos, considerando el impacto y la probabilidad de su materialización, el siguiente paso es tratarlos. Aquí surge un nuevo concepto denominado “apetito por el riesgo”, que se refiere a la disposición de

una organización para aceptar riesgos en función de los servicios y/o productos que ofrece a sus clientes. Según el nivel de riesgo que una organización está dispuesta a aceptar, existen cuatro estrategias efectivas de tratamiento de riesgos, y estas son [62]:

4.2.4.3.1 Reducir el riesgo

La norma menciona dos enfoques distintos. El primero se refiere al cambio de probabilidad, lo que implica la implementación de un control para reducir las oportunidades, ya sea completamente o en cierto grado, con el fin de prevenir la ocurrencia de un incidente. El segundo enfoque se centra en el cambio de las consecuencias. Cuando una amenaza se materializa, los controles aplicados buscan detener el avance de la degradación o permiten una pronta recuperación del sistema de información tras un ataque.

4.2.4.3.2 Aceptar el riesgo

No se implementan controles que cambien el efecto o la probabilidad del riesgo, esta elección puede basarse en análisis que hayan determinado que el riesgo es bajo, imposible o que no es apropiado invertir en salvaguardas. Es una decisión crítica que corresponde a la alta dirección, y es necesario realizar un seguimiento continuo del riesgo.

4.2.4.3.3 Evitar el riesgo

Consiste en detener cierta actividad o proceso que representa un riesgo para la organización. Dado que el beneficio generado no justifica el peligro que se corre, ni las pérdidas que provocaría la materialización de una amenaza, es preferible buscar una alternativa que implique un riesgo menor.

4.2.4.3.4 Transferir el riesgo

En ocasiones, resulta más beneficioso para la organización contratar a una entidad especializada para solventar los riesgos identificados. Esta entidad se encargará de velar por la integridad de la información, haciendo uso de sus recursos especializados, garantizando una pronta respuesta o solución ante cualquier incidente.

4.2.4.4 Metodología MAGERIT – versión 3.0

La metodología MAGERIT, establecida por el gobierno español, analiza los riesgos que afectan los sistemas de información, siendo crucial en el contexto del crecimiento tecnológico actual. Su objetivo es reducir riesgos asociados al uso de sistemas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, generando así confianza en los clientes y mitigando la desconfianza. Además, sensibiliza a los responsables sobre los riesgos, ofreciendo un método para sistematizar el análisis, planificar salvaguardas y preparar a la organización para evaluaciones [4], [5]. MAGERIT responde al “Proceso de Gestión de los Riesgos” mencionado en la normativa ISO 31000, permitiendo a los órganos de gobierno tomar

decisiones informadas sobre riesgos tecnológicos, siguiendo la metodología PDCA aplicable en la implementación de un SGSI basado en ISO 27001 [7].

MAGERIT maneja elementos como activos de información, amenazas, vulnerabilidades, impacto, probabilidad, riesgo y salvaguardas, y su proceso se desarrolla en etapas de planificación, análisis, gestión y selección de salvaguardas. Estructurada en tres libros, el primero proporciona una introducción general, el segundo un catálogo de elementos y el último libro es una guía de técnicas específicas y generales para las fases de análisis [4]. La metodología sigue pasos específicos: identificar activos críticos, determinar amenazas, estimar impacto y probabilidad, y finalmente, estimar el riesgo y evaluar la eficacia de las salvaguardas existentes [7]. Este enfoque integral asegura una gestión de riesgos efectiva, alineada con estándares internacionales y buenas prácticas de seguridad de la información.

Con base en [7], [42] esta metodología propone las siguientes 4 fases para el análisis de riesgos:

- **Planificación:** Se establecen las consideraciones necesarias para dar inicio al proyecto, identificándose las amenazas a las que se encuentran expuestos los activos, en caso de que se haya omitido algún riesgo, en una próxima revisión se lo denominara como oculto o ignorado para ser tomado en cuenta.
- **Análisis de riesgos:** En esta fase por cada riesgo identificado se efectúa una valoración cuantitativa en la que se pueda determinar cuáles son los riesgos con un mayor impacto y probabilidad de ocurrir, por lo que, deben ser tratados prioritariamente.
- **Gestión de riesgos:** Aquí entra en juego cuestiones monetarias, estratégicas y de política, acerca de cuál será el tratamiento que se proveerá a cada uno de los riesgos, teniendo la opción de evitarlo al dar de baja cierto proceso que no genera un beneficio mayor al riesgo que causa, o de transferirlo en caso de poseer cierto aseguramiento con una empresa externa.
- **Selección de Salvaguardas:** Se determinan los mecanismos de salvaguarda que modificarán la situación del riesgo y por ende tendrán que ser implementadas.

4.2.4.4.1 Herramienta PILAR

PilarBasic es una aplicación informática que integra los activos del sistema, sus interdependencias y su valor para la organización. Una vez comprendido el sistema, posibilita la introducción de posibles amenazas en los aspectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, para definir los riesgos potenciales que enfrenta el sistema. Al identificarse los riesgos, se puede determinar las salvaguardas necesarias para proteger la información, así también, la herramienta

PilarBasic permite un seguimiento continuo y recurrente del sistema de protección de la organización, permitiendo afrontar nuevos riesgos y aumentar la confianza de su funcionamiento [63].

Existen diversas versiones de esta herramienta, entre las que se encuentran PilarBasic, PILAR y uPILAR. La diferencia entre estas versiones radica en las funcionalidades que ofrecen al usuario, lo cual se traduce en un valor monetario diferente para adquirir una licencia. En las tres versiones, los resultados pueden presentarse en varios formatos: informes RTF, gráficos y tablas para incorporar en hojas de cálculo. Es importante mencionar que se puede solicitar una licencia con fines académicos, como se ha hecho para el presente TIC [52].

4.2.5 Trabajos relacionados

En la **Tabla 3** se presenta una lista de los trabajos relacionados con el TIC.

Tabla 3. Trabajos relacionados.

Título	Descripción
Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio.	El trabajo de titulación se centra en diseñar un SGSI para el Hospital de Especialidades Fuerzas Armadas No.1, con el propósito de reducir los riesgos de seguridad y gestionar eficientemente los activos de información, adaptándose a estándares internacionales. Se emplean tres fases metodológicas basadas en normativas como ISO/IEC 27001:2013 y Magerit, para identificar los activos críticos, amenazas y vulnerabilidades, y establecer un plan de tratamiento de riesgos [4].
Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS.	La empresa GMS busca certificarse según la norma ISO/IEC 27001:2013 y necesita implementar controles para gestionar la seguridad de la información. Este proyecto define un plan para implementar el SGSI en un proceso de GMS, con el fin de facilitar la certificación. Se describe la metodología del proyecto, el estado de cumplimiento de los controles y se presentan conclusiones y recomendaciones [5].
Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indígena SAC.	El propósito del proyecto es fortalecer la seguridad de la información en la Cooperativa de Ahorro y Crédito SAC mediante la instauración de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la Norma ISO/IEC 27001. Se realizó un análisis del nivel de seguridad actual, se detectaron posibles vulnerabilidades, y se implementaron políticas de seguridad con el objetivo de asegurar la protección de la información de forma eficaz [6].
Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca.	Se plantea la implementación de un SGSI con el fin de manejar los riesgos operativos, será específicamente diseñado para salvaguardar la información en los procesos cruciales de la Universidad Nacional de Cajamarca (UNC), apoyado en estándares ISO/IEC 27003 y en metodologías como MagerIT. La viabilidad del sistema se corroboró a través de una encuesta de satisfacción dirigida a usuarios de tecnología de la información (TI), respaldada por análisis estadísticos [7].

Nota. Elaboración propia.

5 Metodología

5.1 Área de estudio

El presente Trabajo de Integración Curricular (TIC) se llevó a cabo durante el periodo académico de marzo-agosto 2024 en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL). La DTI es responsable de administrar y gestionar los sistemas de información e infraestructura tecnológica utilizados diariamente por el personal administrativo, docente y estudiantil.

La DTI se encuentra ubicada en la Av. Pío Jaramillo Alvarado, Administración Central, Bloque 41, Loja, Ecuador, en las coordenadas -4.0334694769439885, -79.20288654056017, como se puede observar en la **Figura 10**.

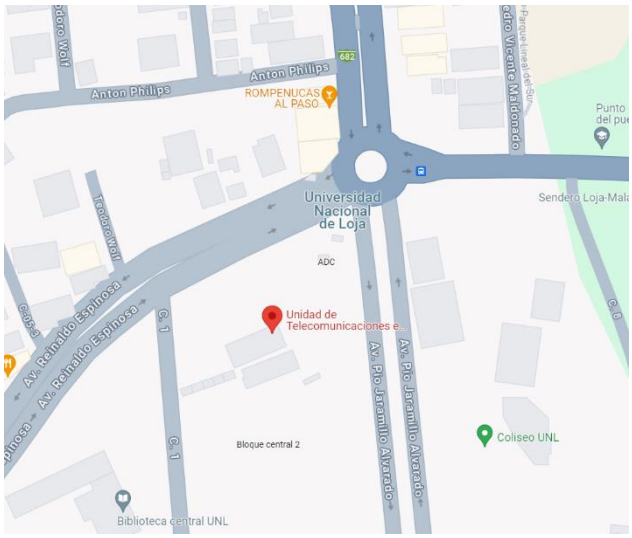

Figura 10. Ubicación de la Dirección de Tecnologías de Información – UNL.
Nota. Recuperado de Google Maps.

5.2 Procedimiento

A continuación, se presenta una descripción del procedimiento desarrollado para cumplir con los objetivos planteados en el TIC:

5.2.1 Objetivo 1: Implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL)

- **Fase 1: Planificar (P)**
  - Se determinó el grado de aplicabilidad de las cláusulas de la norma ISO/IEC 27001:2013 en el alcance del presente Trabajo de Integración Curricular (TIC) (ver sección **6.1.1.1**).
  - Se realizó un análisis del contexto interno de la DTI, para identificar sus atribuciones y responsabilidades, procesos, roles y actividades, así como, las políticas a las cuales se rigen actualmente (ver sección **6.1.1.2**).

- Se efectuaron dos entrevistas al Ingeniero Juan Carlos Riofrío, encargado del Proceso de Seguridad Informática (ver **Anexo 2**), para determinar el estado de la seguridad de la información en la DTI, por medio de un análisis GAP sobre el cumplimiento de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 (ver sección **Análisis de brechas (GAP)**).
- Se llevó a cabo una encuesta dirigida a los trabajadores de la DTI, con el propósito de conocer los requisitos de seguridad que tienen para la propuesta del SGSI (ver sección **Requisitos de las partes interesadas en el SGSI**).
- Se recopiló información sobre los activos de información gestionados por la Dirección (ver sección **Activos de información**).
- Se analizó el contexto externo de la DTI, determinándose los organismos reguladores y de innovación tecnológica relevantes, además, se revisaron las leyes, políticas, planes y estrategias desarrolladas en Ecuador sobre el uso de las TIC en ámbitos como el comercio electrónico, la protección de datos personales, la creación de un gobierno electrónico y la aplicación de la ciberseguridad en los sistemas de información nacionales (ver sección **6.1.1.3**).
- Se definió el alcance del SGSI, detallándose los procesos y servicios que ofrece la DTI a la comunidad universitaria, su estructura organizativa actual, las redes e infraestructura que administran y los límites del SGSI (ver sección **6.1.1.4**).
- Se formuló una política de alto nivel, que incluyó los objetivos de la seguridad de la información para el SGSI (ver sección **6.1.1.5**).
- Se establecieron los roles y responsabilidades para el cumplimiento de las actividades de seguridad de la información en el SGSI, de manera que formen parte de las actividades cotidianas que efectúa la DTI en la universidad (ver sección **6.1.1.6**).
- Se seleccionó la metodología de análisis y gestión de riesgos MAGERIT v.3, con la cual fue posible identificar y categorizar los activos de información para valorarlos según los criterios de confidencialidad, integridad y disponibilidad, obteniendo un valor total al promediar los valores definidos en cada una de las dimensiones de seguridad (ver sección **6.1.1.7**).
- Se caracterizaron las amenazas asociadas a dichos activos, definiendo criterios para la degradación en caso de que cierta amenaza se materializará. Estos valores se promediaron con el valor total del activo de

información, resultando en el impacto (ver sección **Caracterizar las amenazas**).

- Se definió una escala cuantitativa para el impacto y la probabilidad de los riesgos, de manera que, al multiplicar ambas variables, aplicando la técnica de análisis mediante tablas, se determine el nivel de riesgo (ver sección **Analizar y priorizar el riesgo**).
- Se definieron los diferentes tipos de tratamiento de riesgos: aceptar, reducir, evitar y transferir, seleccionando el tratamiento más adecuado con base en el apetito de riesgo de la DTI y el nivel de riesgo de cada activo de información (ver sección **Definir los diferentes tipos de tratamiento de riesgo**).
- Se diseñó una matriz de riesgos teniendo en cuenta los criterios del impacto y la probabilidad, así también, la matriz sirve como referencia para posicionar el valor del nivel de riesgo (ver **Tabla 20. Matriz de riesgos**.).
- Se elaboró un informe sobre la situación actual de la DTI, que incluyó toda la información previamente recopilada, analizada y evaluada. Este informe servirá para evaluar cuantitativamente la mejora de la DTI en el ámbito de la seguridad de la información tras la propuesta del SGSI (ver sección **6.1.1.8**).
- Se realizó la Declaración de aplicabilidad conforme a la norma ISO/IEC 27001:2013, cláusula 6.1.3, literal d); para analizar y seleccionar los controles de seguridad más oportunos, con los que se efectuará el tipo de tratamiento de riesgo previamente seleccionado (ver sección **6.1.1.9**).
- Se identificaron los recursos disponibles para la propuesta del SGSI (ver sección **6.1.1.10**).

- **Fase 2: Hacer (D)**
  - Se realizó un informe sobre la evaluación y tratamiento de riesgos (ver sección **6.1.2.1**).
  - Se elaboró un plan de tratamiento de riesgos, en donde se indicaron los controles de seguridad seleccionados para mitigar los riesgos identificados en los activos de información (ver sección **6.1.2.2**).
  - Se definieron un conjunto de políticas de seguridad de la información que abarcan los controles de seguridad seleccionados del Anexo A de la norma ISO/IEC 27001:2013 (ver sección **6.1.2.3**).

5.2.2 Objetivo 2: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3

- **Fase 3: Verificar (C)**
  - Se determinó cuantitativamente la efectividad de las salvaguardas en la reducción del nivel de riesgo por medio de la metodología MAGERIT v.3 (ver sección **6.2.1.1**).
  - Se evaluó el nivel de riesgo a través de la ejecución de casos de prueba basados en escenarios posibles junto con el Ing. Juan Carlos Riofrío, Mg, (ver **Anexo 3**) con el propósito de determinar la efectividad de los controles de seguridad definidos (ver sección **6.2.1.2**).
  - Se evaluó el nivel de madurez de la DTI junto con el Ing. Juan Carlos Riofrío, Mg, (ver **Anexo 4**) posterior a la propuesta del SGSI (ver sección **6.2.1.3**).
- **Fase 4: Actuar (A)**
  - Se hizo la entrega formal del SGSI al encargado del Proceso de Seguridad Informática (ver **Anexo 5**), quien será el responsable de llevar a cabo evaluaciones periódicas que permitan analizar el estado de los controles de seguridad. Además, se presentaron los resultados del TIC al Director de la DTI y a los encargados de los Procesos (ver sección **6.2.2**).

5.3 Recursos

Para llevar a cabo las actividades mencionadas anteriormente, se utilizaron diversos recursos científicos, técnicos y tecnológicos, que se detallan en las siguientes secciones.

5.3.1 Recursos científicos

❖ **Método analítico-sintético**

Se empleó este método para descomponer mentalmente en secciones a la DTI para su análisis, conociendo más sobre sus atribuciones, procesos, roles y activos de información. Luego, se sintetizó toda esta información, estableciendo relaciones y características generales entre los elementos.

❖ **Análisis de brechas (GAP)**

Permitió conocer el desempeño de la DTI en el ámbito de la seguridad de la información, al contrastar lo estipulado en las normas, con el nivel real de implementación que tiene el departamento.

❖ **Revisión Bibliográfica**

Se investigó en libros, artículos científicos, informes de seguridad, tesis de grado y otras fuentes de información científica. Toda la información obtenida permitió construir

el marco teórico y justificar el uso de recursos científicos, técnicos y tecnológicos en el desarrollo del TIC.

5.3.2 Recursos técnicos

- **Entrevista**

Fue aplicada al Ingeniero Juan Carlos Riofrío, encargado del Proceso de Seguridad Informática. A través de esta entrevista, se conoció el estado actual de la seguridad de la información en la DTI, determinándose la necesidad de una política de seguridad de la información que formalice las diversas actividades realizadas por los trabajadores del departamento.

- **Encuesta**

Se aplicó a los trabajadores de la DTI para identificar sus necesidades y expectativas respecto a la propuesta del SGSI. Se utilizó la herramienta Google Forms para facilitar el análisis y procesamiento de los datos obtenidos de cada una de las preguntas.

- **Norma ISO/IEC 27001:2013**

Guía que permitió planificar la propuesta de un SGSI en la DTI, incluyendo una lista de controles de seguridad de la información para la formulación de políticas.

- **Norma ISO/IEC 27002:2013**

Guía que describe con mayor profundidad cada uno de los controles de seguridad de la información indicados en el Anexo A de la norma ISO/IEC 27001:2013, permitiendo una mejor comprensión de su selección o exclusión al momento de ser considerados para su aplicación en la DTI.

- **Matriz de riesgos**

Esta técnica permitió visualizar de una mejor manera los riesgos identificados en los activos de información de la DTI y corroborar la reducción del nivel de riesgo al emplear los controles de seguridad.

- **Casos de prueba**

Se utilizó esta técnica para evaluar la efectividad de las políticas de seguridad de la información en la mitigación de los riesgos presentes en la DTI.

- **Metodología PDCA**

Es la metodología que mejor se adapta al despliegue de un SGSI basado en la norma ISO/IEC 27001:2013, permitiendo cumplir las cláusulas del estándar en sus respectivas fases y obteniendo resultados estructurados que fueron documentados para ser presentados a las partes interesadas.

- **Metodología MAGERIT v.3**

Utilizada durante la fase de planificación de la metodología PDCA, ofreció un proceso sistemático referente a la evaluación y tratamiento de riesgos, definiendo criterios para el impacto y la probabilidad, con los cuales se obtuvo el nivel de riesgo.

5.3.3 Recursos tecnológicos

- **Hardware**
  - **Laptop DELL modelo Inspiron 7559:** Equipo utilizado para el desarrollo de las actividades del TIC, desde la planificación, evaluación de los riesgos, selección de los controles, hasta la evaluación de la eficacia de los controles en la reducción del nivel de riesgo. Las características del equipo son: procesador i7-6700HQ, GPU: Intel(R) HD Graphics 530, 8 GB de memoria RAM.
- **Software**
  - **Office 2021:** Suite ofimática de Microsoft que incluye Word, Excel, PowerPoint; aplicaciones utilizadas para la realización del TIC.
  - **PilarBasic:** Aplicación utilizada para el registro de los activos de información, su respectiva valoración y la caracterización de amenazas.

6 Resultados

En la presente sección se exponen los resultados obtenidos a lo largo de la ejecución de los 2 objetivos planteados.

6.1 Objetivo 1: Implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL)

6.1.1 Fase 1: Planificar (P)

6.1.1.1 Determinar la aplicabilidad de la norma ISO/IEC 27001:2013 en el alcance del TIC

La propuesta del SGSI se elabora conforme a la norma ISO/IEC 27001:2013; sin embargo, por cuestiones de tiempo, el alcance del presente TIC no contempla el cumplimiento total de las cláusulas estipuladas en dicha norma. En la **Tabla 4** se indica la aplicabilidad de las cláusulas dentro del alcance del TIC.

Tabla 4. Aplicabilidad de la norma ISO/IEC 27001:2013.

Cláusula	Gestión	Cumplimiento	Observación
4	**Contexto de la organización**		
4.1	Comprensión de la organización y de su contexto	**Total**	Se realizó un análisis y recopilación de información sobre el contexto interno y externo de la DTI.
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	**Total**	Se efectuó una encuesta dirigida a los trabajadores de la DTI, con el objetivo de conocer sus requisitos sobre la propuesta de un SGSI.
4.3	Determinación del alcance del sistema de gestión de seguridad de la información	**Total**	El alcance del SGSI se documentó y fue aprobado por el encargado del Proceso de Seguridad Informática.
4.4	Sistema de gestión de seguridad de la información	**Parcial**	El cumplimiento del SGSI, y la evaluación del desempeño, quedan bajo la responsabilidad de la DTI.
5	**Liderazgo**		
5.1	Liderazgo y compromiso	**Total**	Se contó con el apoyo del Director del TIC, el encargado del Proceso de Seguridad Informática y los trabajadores de la DTI.
5.2	Política	**Parcial**	La política de seguridad de la información ha sido redactada, pero aún no ha sido comunicada a los trabajadores de la DTI.
5.3	Roles, responsabilidades y autoridades en la organización	**Parcial**	Se han definido roles y responsabilidades para tratar la seguridad dentro de la DTI, pero no se ha designado personal.
6	**Planificación**		
6.1	**Acciones para tratar los riesgos y oportunidades**		
6.1.1	Consideraciones generales	**Total**	Se realizó un estudio del contexto interno y externo de la DTI, así como

Cláusula	Gestión	Cumplimiento	Observación
			de los requisitos de las partes interesadas.
6.1.2	Apreciación de riesgos de seguridad de la información	**Total**	Se aplicó la metodología de análisis y gestión de riesgos MAGERIT v.3.
6.1.3	Tratamiento de los riesgos de seguridad de la información	**Total**	
6.2	Objetivos de seguridad de la información y planificación para su consecución	**Parcial**	Se definieron los objetivos de seguridad de la información, pero el cumplimiento de los mismos queda bajo la responsabilidad de la DTI.
7	**Soporte**		
7.1	Recursos	**Parcial**	Se proporcionaron recursos para la planificación y el establecimiento del SGSI.
7.2	Competencia	**Total**	El Director del TIC y el encargado del Proceso de Seguridad Informática, quienes poseen conocimiento sobre la seguridad de la información, brindaron su apoyo.
7.3	Concienciación	**No aplica**	El encargado del Proceso de Seguridad Informática debe proporcionar capacitación y concienciación a los trabajadores de la DTI, para que conozcan los beneficios del SGSI y las implicaciones de no cumplir con los requisitos del Sistema.
7.4	Comunicación	**No aplica**	El encargado del Proceso de Seguridad Informática es responsable de determinar los procesos de comunicación concernientes al SGSI.
7.5	**Información documentada**		
7.5.1	Consideraciones generales	**Total**	Se ha documentado la información requerida por la norma y la solicitada por la DTI.
7.5.2	Creación y actualización	**Parcial**	Se ha designado al responsable de verificar y actualizar la documentación de acuerdo con las necesidades de la DTI.
7.5.3	Control de la información documentada	**No aplica**	La DTI es responsable de proteger la información documentada y de asegurarse de que esté disponible para las partes interesadas.
8	**Operación**		
8.1	Planificación y control operacional	**Parcial**	Se han establecido lineamientos y directrices encaminadas a la protección de la información, pero su implementación y mejora son responsabilidad de la DTI.
8.2	Apreciación de los riesgos de seguridad de información	**No aplica**	La DTI es la encargada de realizar una nueva apreciación de los riesgos de seguridad a intervalos planificados o cuando se produzca una modificación importante.
8.3	Tratamiento de los riesgos de seguridad de información	**No aplica**	La ejecución de los controles seleccionados queda bajo la responsabilidad de la DTI.
9	**Evaluación del desempeño**		

Cláusula	Gestión	Cumplimiento	Observación
9.1	Seguimiento, medición, análisis y evaluación	**No aplica**	La evaluación del desempeño y eficacia del SGSI no está contemplada en el alcance del TIC.
9.2	Auditoría interna	**No aplica**	Una vez que el SGSI haya sido implementado en la DTI, se deberán efectuar auditorías internas a intervalos planificados para determinar si cumple con los requisitos de la norma ISO 27001.
9.3	Revisión por la dirección	**No aplica**	La alta dirección deberá revisar los resultados de las auditorías para determinar la efectividad del SGSI y asegurarse de que esté alineado con los objetivos estratégicos de la DTI.
10	**Mejora**		
10.1	No conformidad y acciones correctivas	**No aplica**	La detección de no conformidades, la planificación y la puesta en marcha de acciones correctivas quedan bajo la responsabilidad de la DTI.
10.2	Mejora continua	**No aplica**	La mejora continua del SGSI no está contemplada en el alcance del TIC.

Nota. Elaboración propia.

En la **Tabla 5** se observa que se cumple con el 35% de las cláusulas de la norma ISO/IEC 27001, vitales para la ejecución del presente TIC. Por otro lado, se cumple parcialmente un 27%, y un 38% de las cláusulas están fuera del alcance del TIC. La estimación de aplicabilidad de las cláusulas de la norma se realizó por cuestiones de tiempo, dado que el SGSI será entregado a la DTI, y ellos serán los encargados de su implementación y mejora.

Tabla 5. Resumen del grado de aplicabilidad de la norma ISO 27001.

Cumplimiento	Descripción		Porcentaje
Total	Esencial para la elaboración y desarrollo del TIC		35%
Parcial	Apoyan el cumplimiento de los objetivos planteados		27%
No aplica	No se encuentran dentro del alcance del TIC		38%
		Total	100%

Nota. Elaboración propia.

6.1.1.2 Recopilar información del contexto interno de la DTI

La recopilación de información a nivel interno permitió obtener una visión detallada de la situación actual de la DTI en materia de seguridad de la información. Se identificaron sus atribuciones y responsabilidades con la comunidad universitaria, los procesos efectuados, los roles y actividades, la política vigente, el estado de adecuación de las cláusulas y controles de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013, los requisitos de las partes interesadas en el SGSI y los activos de información administrados. Toda esta información se presenta en las siguientes secciones.

❖ **Atribuciones y responsabilidades**

Por medio de la revisión y análisis del Reglamento Orgánico de Gestión Organizacional por Procesos de la Universidad Nacional de Loja (ver **Anexo 6**), específicamente en su artículo 37, se determinó que la DTI es la encargada de proveer capacitaciones a los estamentos universitarios en la administración y uso de los servicios informáticos; siendo activos partícipes en la provisión de soporte técnico o mantenimiento del software y hardware institucional cuando sea necesario. Adicionalmente, la DTI asesora a las autoridades universitarias en la adquisición de nuevas tecnologías de la información, siguiendo un proceso de análisis que considera la instalación y manejo de estas tecnologías, determinando el grado de aceptación respecto a las capacidades y solicitudes de la universidad en sus actividades diarias.

❖ **Procesos efectuados**

La DTI pasó recientemente por una reestructuración que dio origen a la creación de cuatro Procesos: Infraestructura Tecnológica, Sistemas de Información, Seguridad Informática y Provisión de Servicios. A continuación, se presenta el portafolio de productos y servicios que cada uno de estos Procesos debe cumplir, conforme al artículo 37 del Reglamento Orgánico de Gestión Organizacional por Procesos de la Universidad Nacional de Loja (ver **Anexo 6**).

Portafolio de Productos y Servicios:

- **Infraestructura Tecnológica**
  - Documentación de infraestructura de Redes.
  - Centro de Datos funcionales.
  - Documentación de Electrónica y Telecomunicaciones.
  - Documentación de adquisiciones de bienes y servicios de TI.
  - Monitoreo de infraestructura tecnológica y sistemas de información.
- **Sistemas de Información**
  - Plan de Desarrollo de software.
  - Sistemas de TI desarrollados e implementados.
  - Documentos de Control de Calidad.
  - Fichas Técnicas de la Base de Datos.
  - Documentación Técnica y Funcional de los Sistemas, Aplicativos y Soluciones de TI.
  - Documento de control de cambios.
- **Seguridad Informática**
  - Informes de evaluación de vulnerabilidades y riesgos.
  - Registro de altas y bajas de usuarios.
  - Informe de cumplimiento de políticas de TI.

- Informe de atención a incidencia de seguridad informática.
- Informe de respaldos de TI.

- **Provisión de Servicios**
  - Reporte de atención a través de mesa de servicios.
  - Informes de mantenimiento preventivo (plan) y correctivo.
  - Inventario tecnológico.
  - Programas de Capacitación de TI.
  - Informe de gestión de sistemas institucionales.

❖ **Roles y actividades**

Se analizaron los manuales de puestos de carrera – LOSEP (ver **Anexo 7**), los cuales detallan cuestiones referentes a la instrucción formal, experiencia laboral, capacitación requerida, actividades esenciales, conocimientos adicionales y competencias técnicas para cada puesto de trabajo en los diferentes departamentos de la universidad. En la **Figura 11** se presenta un organigrama que ayuda a comprender mejor la estructura de la DTI, basado en la información proporcionada por estos manuales.

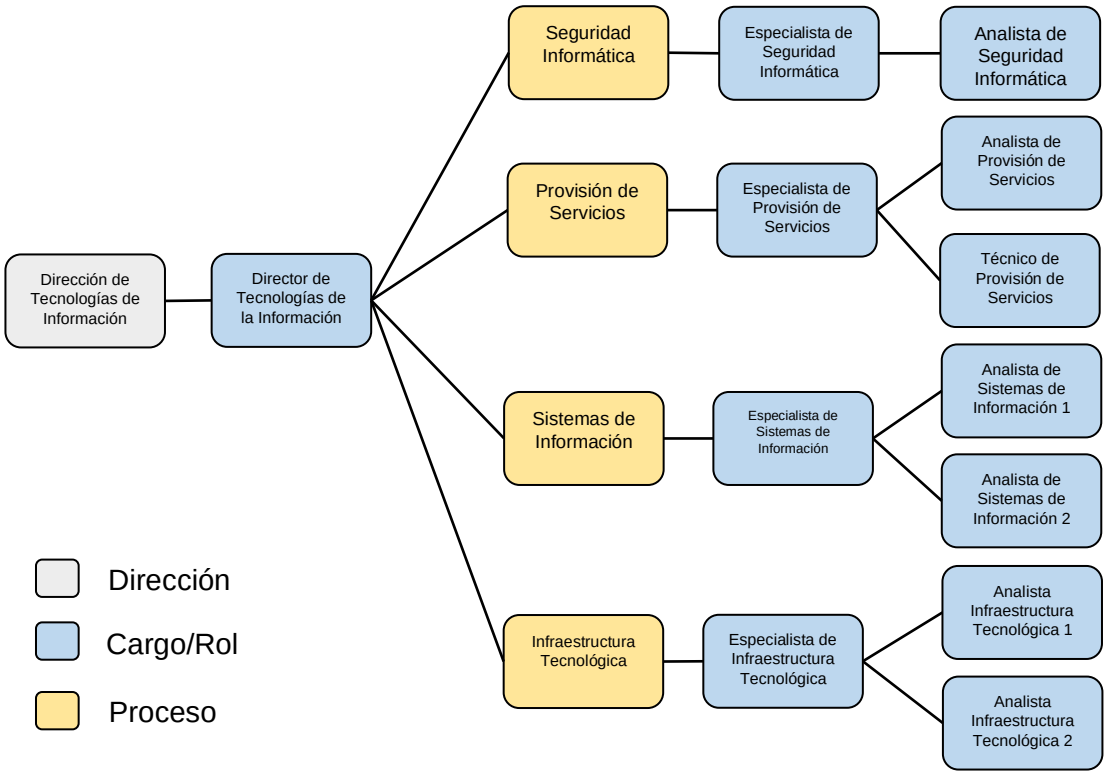

Figura 11. Organigrama de la DTI.
Nota. Elaboración propia.

A pesar de que los roles y actividades estén adecuadamente documentados, se identificó que la DTI carece de normativas dedicadas a resolver incidentes. La segregación de tareas no es adecuada, ya que son realizadas por trabajadores con un

perfil que no es afín al Proceso en el que desempeñan sus labores. En su mayoría, los trabajadores de la DTI llevan a cabo sus actividades basándose en el nivel de criticidad o en el momento en el que se recibe una solicitud, lo que resulta en una falta de formalidad y en la ausencia de un registro detallado para controlar la manipulación de los diferentes activos de información y determinar las medidas necesarias para prevenir que una amenaza aproveche una vulnerabilidad y cause un impacto negativo.

- **Políticas aplicadas en la DTI**

Las políticas actualmente vigentes en la DTI fueron creadas en el año 2012 bajo la dirección del Ing. Milton Palacios, quien era responsable de la entonces denominada Unidad de Telecomunicaciones e Información (UTI). Estas políticas, tituladas “Políticas de Telecomunicaciones, Desarrollo de Software y Redes de la Universidad Nacional de Loja”, han quedado obsoletas debido a la reestructuración organizacional en la DTI, generando incertidumbre y desestabilización en las actividades y funciones del personal. La ausencia de directrices y procedimientos formales ha relegado la seguridad a un segundo plano. Es fundamental establecer políticas actualizadas que guíen a los empleados sobre las mejores prácticas y las consecuencias de sus acciones en la seguridad de la información (ver **Anexo 8**).

- **Análisis de brechas (GAP)**

El análisis de brechas (GAP) permitió identificar las cláusulas y controles de las normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 que están siendo implementadas en la DTI, así como el grado de cumplimiento en el que se encuentran, por medio de la incorporación de un modelo de madurez. Para la ejecución de esta tarea, se consideraron los siguientes niveles de madurez indicados en la **Tabla 6**.

Tabla 6. Niveles de madurez.

Medida	Estado	Descripción
0	**No existe**	Se reconoce la importancia de la cláusula o el control para una correcta gestión de la seguridad de la información, pero no ha sido implementada por parte de la dirección.
1	**Ad-hoc (Básico)**	La cláusula o el control existen, pero se aplica únicamente cuando es necesario en casos específicos; por ende, no es generalizable y no se realiza un seguimiento de su aplicación.
2	**Ejecutado**	La cláusula o el control es aplicado frecuentemente por parte de los trabajadores, pero de manera informal al no estar debidamente aprobado ni documentado.
3	**Definido**	La cláusula o el control se aplica conforme a un procedimiento documentado, de acuerdo con la planificación, y se efectúa un seguimiento del mismo.
4	**Manipulable y medible**	La cláusula o el control se crean con base en un estándar y es documentado por la dirección, la cual hace uso de métricas para una gestión cuantitativa de su desempeño.
5	**Optimizado**	La dirección se encarga de analizar y evaluar el desempeño de la cláusula o el control, para determinar las no conformidades y las oportunidades de mejora, y así aplicar medidas preventivas y correctivas.

Nota. Elaboración propia.

El análisis fue realizado junto con el encargado del Proceso de Seguridad Informática, el Ingeniero Juan Carlos Riofrío (ver **Anexo 2**). En el caso de la norma ISO/IEC 27001:2013, se asignaron valores a partir de la cláusula 4 hasta la 10, mientras que en la norma ISO/IEC 27002:2013 se asignaron valores a cada uno de los 114 controles de seguridad de la información. La **Figura 12** presenta los resultados de una forma gráfica para una mayor comprensión del nivel de cumplimiento de las cláusulas de la norma ISO/IEC 27001:2013.

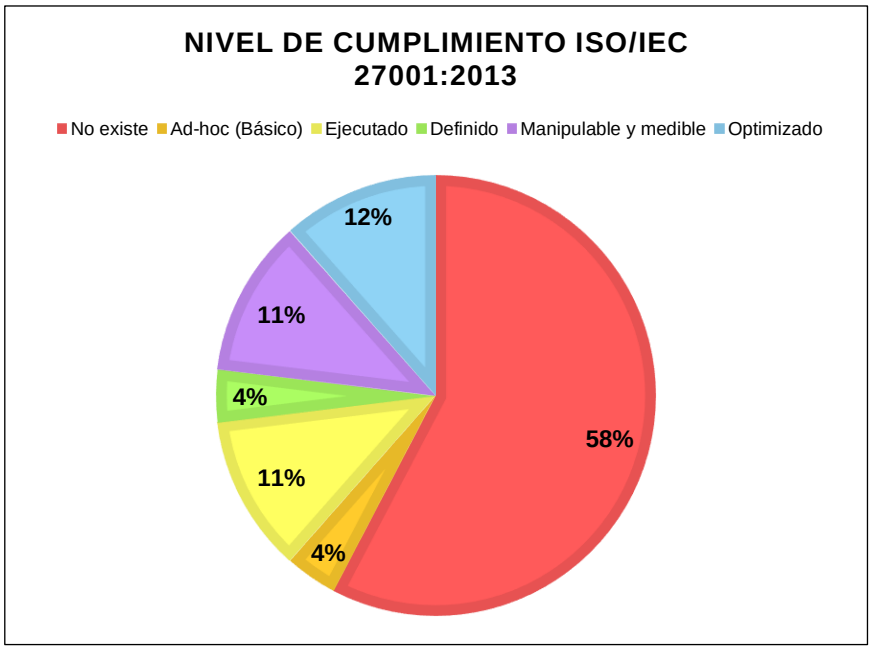

Figura 12. Nivel de Cumplimiento (ISO/IEC 27001:2013).
Nota. Elaboración propia.

Según los resultados del análisis GAP, un 58% de las cláusulas de la norma se encuentran en un nivel de madurez 0 (No existe). Por otro lado, el 12% está posicionado en un nivel de madurez 5 (Optimizado), debido a que son conscientes del contexto interno y externo, comprenden los requisitos de las partes interesadas y poseen una adecuada segregación de roles y responsabilidades. Por lo tanto, la DTI se encuentra en un nivel de madurez 2 (Ejecutado), reconociendo en su mayoría la importancia de una gestión adecuada de la seguridad de la información, aunque esta se lleve a cabo de manera informal.

La **Figura 13** presenta los resultados del nivel de cumplimiento de los controles de seguridad de la norma ISO/IEC 27002:2013.

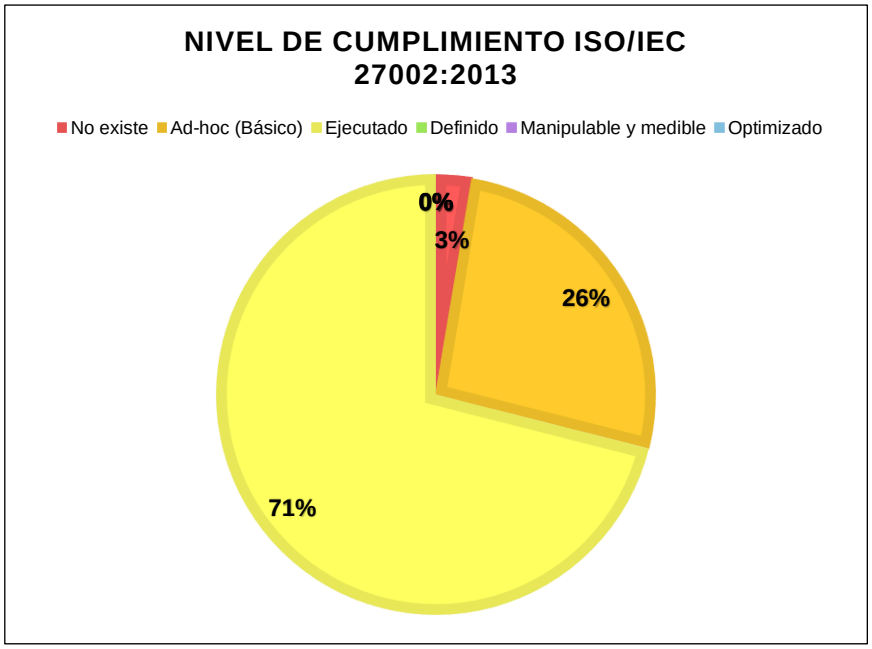

Figura 13. Nivel de Cumplimiento (ISO/IEC 27002:2013).
Nota. Elaboración propia.

Los resultados del análisis GAP realizado a la norma ISO/IEC 27002:2013 indican que, de los 114 controles de seguridad evaluados (representando el 100%), la mayoría (71%) se encuentran en un nivel de madurez 2 (Ejecutado). Un 26% se sitúa en un nivel de madurez 1 (Ad-hoc) y un 3% en un nivel de madurez 0 (No existe). Esto sugiere la necesidad de mejorar el estado de los controles de seguridad en la DTI, oficializándolos con el uso de políticas que sean conocidas por los trabajadores del departamento. De este modo, se generaría una cultura basada en la protección de la información y en la prevención y mitigación de riesgos que podrían causar perjuicios al departamento y a la universidad.

La información obtenida de los análisis es útil para la propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que ofrece una comprensión precisa de la situación actual de la Dirección de Tecnologías de Información (DTI). Esto permitió identificar las cláusulas y controles de seguridad que deben considerarse para aumentar la resiliencia ante las amenazas que puedan afectar los activos de información gestionados y administrados por la DTI, elevando su nivel de madurez (La información completa se encuentra en el **Anexo 9**).

- **Requisitos de las partes interesadas en el SGSI**

Se aplicó una encuesta a los trabajadores de la DTI, siguiendo la cláusula 4.2 de la norma ISO/IEC 27001:2013, con el objetivo de identificar y determinar las necesidades y expectativas con relación a la propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI). A continuación, se presentan los principales hallazgos:

- **Conocimiento y Capacitación:** La mayoría de los trabajadores tienen una noción general sobre la seguridad de la información. Sin embargo, se evidencia la falta de capacitaciones frecuentes y actualizadas en este ámbito. Se recomienda llevar a cabo capacitaciones periódicas para que los funcionarios adquieran conocimientos actualizados sobre los mejores procedimientos de seguridad.
- **Implementación de Normas y Políticas:** Se evidenció que la mayoría de trabajadores tenían una idea sobre lo que es la seguridad de la información, no obstante, más de la mitad no sabe cuál es el uso de la norma ISO/IEC 27001:2013. Adicionalmente, debido a que las políticas están desactualizadas, se resalta la necesidad de analizarlas para que estén acorde a la situación actual y a las mejores prácticas de seguridad.
- **Definición de Roles y Responsabilidades:** La correcta definición de roles y responsabilidades en seguridad de la información es reconocida como esencial por la mayoría de los trabajadores. Esto contribuirá a reducir errores y mejorar la eficacia de los controles de seguridad implementados.
- **Controles de Seguridad y Procedimientos:** Los trabajadores apoyan la formalización de controles de seguridad mediante políticas que aseguren la protección de los equipos y sistemas de información de la DTI.
- **Gestión de Incidentes y Continuidad Operativa:** La presente propuesta es vista como una medida necesaria por el personal de la DTI, ya que proporciona una respuesta eficiente ante incidentes de seguridad, minimizando su impacto en las operaciones y protegiendo la información crítica.
- **Cumplimiento Normativo y Auditorías:** La aplicación de acciones correctivas, conforme a estándares nacionales e internacionales en seguridad de la información, aporta un marco de trabajo que fortalece la resiliencia ante amenazas emergentes en los sistemas de información.
- La formalización de procedimientos para asegurar la protección de datos y equipos es una expectativa del personal de la DTI. Las políticas de seguridad de la información deben estar accesibles para todos, promoviendo la concienciación sobre los riesgos que pueden afectar a los activos (revisar el **Anexo 10** para acceder a la información completa).

❖ **Activos de información**

El personal técnico de la DTI se encarga de administrar y gestionar los activos de información, siendo responsables de asegurar un adecuado funcionamiento y

mantenimiento de los sistemas de información y equipos que son usados para proveer servicio a la comunidad universitaria, en conjunto de todos los trabajadores de la DTI se han formulado inventarios que poseen ciertos datos técnicos y de despliegue; sin embargo, estos no han sido formalizados.

6.1.1.3 Recopilar información del contexto externo de la DTI

El contexto externo juega un papel significativo en la forma en la que opera la DTI dentro de la UNL. La identificación de organismos reguladores es importante dado que, son aquellos que implantan leyes, políticas y acuerdos a nivel macro que las organizaciones e instituciones a nivel nacional deberán acatar para no verse inmersas en problemas legales. Se han redactado leyes y políticas para un aprovechamiento estratégico y equitativo de las Tecnologías de la Información y la Comunicación en variados ámbitos, la DTI al manejar datos personales de personal administrativo, trabajadores, docentes y estudiantes, debe cumplir los lineamientos establecidos al ser un factor clave en el aseguramiento de la seguridad de la información.

6.1.1.4 Definir el alcance del SGSI

El alcance del SGSI delimita la información crítica de la DTI que debe resguardarse. Este alcance abarca toda la información generada, almacenada y procesada por los sistemas de información de la Dirección, sin importar su formato, ya sea impreso o digital. Además, se detallan los procesos, servicios y equipos de comunicación que deben considerarse al formular las políticas de seguridad. Se establecen ciertas exclusiones, como las auditorías internas, debido a la limitación del tiempo que se tiene en la ejecución del proyecto (ver **Anexo 11**).

6.1.1.5 Establecer la Política de seguridad de la información

La política de alto nivel de la seguridad de la información fue el primer control que se aplicó conforme al Anexo A de la norma ISO/IEC 27001:2013. En ella se establecieron los objetivos del SGSI, así como el manejo de los requisitos y los controles de seguridad, detallándose las responsabilidades y el apoyo para la propuesta del SGSI, siendo la base para el establecimiento del resto de políticas (ver **Anexo 12**).

6.1.1.6 Establecer los Roles y Responsabilidades para el SGSI

La DTI debe definir los roles y responsabilidades presentados en la **Tabla 7** para asegurar una adecuada gestión de la seguridad de la información:

Tabla 7. Roles y Funciones.

Rol	Función
Comité de seguridad de la información	Respaldo de la Política de seguridad de la información
Oficial de seguridad	Seguimiento de la Política de seguridad de la información
Propietario de los datos	Clasificación de la información

Rol	Función
Personal de la DTI	Cumplimiento de la Política de seguridad de la información

Nota. Elaboración propia.

- **Comité de seguridad de la información**

El comité se encarga de revisar y aprobar las políticas de seguridad de la información de la DTI. Sus actividades incluyen:

- Revisión del plan estratégico de la DTI.
- Definición de proyectos orientados al fortalecimiento de la seguridad de la información.
- Creación de un plan de difusión para comunicar las políticas al personal de la DTI.

- **Oficial de seguridad**

El oficial de seguridad es responsable de definir y mantener las políticas de seguridad de la información, así como de asesorar al personal de la DTI sobre la implementación del SGSI. Las responsabilidades del oficial de seguridad incluyen:

- Implementar un plan para concienciar al personal de la DTI sobre la importancia de la seguridad según la criticidad de la información.
- Mantener, actualizar, distribuir y monitorear las políticas de seguridad de la información con base en los cambios del ambiente laboral.
- Desarrollar proyectos de seguridad para garantizar el establecimiento de una cultura de seguridad informática.
- Dar soporte a los usuarios finales en los Procesos de identificación de información sensible y de las medidas de seguridad necesarias en cada sistema, para cumplir con las políticas de seguridad de la información.

- **Propietario de los datos**

El propietario de los datos es responsable de los activos de información que administra la DTI. El comité de seguridad de la información debe informarles sobre sus responsabilidades. Estas incluyen:

- Identificar toda la información confidencial correspondiente a su Proceso de responsabilidad, independientemente de su estado o formato, y clasificarla conforme a la política de seguridad de la información.
- Autorizar el acceso a la información a personas o grupos debidamente autorizados.

- **Personal de la DTI**

Todo el personal que utiliza los activos de información para el cumplimiento de sus funciones tiene las siguientes responsabilidades:

- Cumplir con las medidas de seguridad definidas en las políticas de seguridad de la información.
- Participar activamente en las capacitaciones periódicas para estar al tanto de las actualizaciones o recomendaciones en el área de seguridad.

6.1.1.7 Aplicar la metodología de evaluación y tratamiento de riesgos

La metodología seleccionada para llevar a cabo esta actividad es MAGERIT v.3, debido a su enfoque estructurado y detallado en la identificación, evaluación y tratamiento de los riesgos de seguridad de la información, esencial para cumplir con los requisitos de la norma ISO 27001 en materia de gestión de riesgos.

❖ **Identificar los activos de información**

Los activos de información que son administrados por la DTI se clasificaron conforme a las siguientes categorías:

- **[D] Datos / Información:** Son el activo esencial de la organización, y al ser procesados, es posible cumplir con las metas trazadas internamente.
- **[S] Servicios:** Funciones propias o que pueden pertenecer a otra organización y son adquiridas para el procesamiento de la información.
- **[SW] Software – Aplicaciones informáticas:** Necesarias para gestionar, analizar y transformar los datos, permitiendo la explotación de la información para la prestación de los servicios.
- **[HW] Equipamiento informático (hardware):** Son los medios físicos en donde será almacenada la información y datos, de las aplicaciones y servicios que ofrece la organización.
- **[COM] Redes de comunicaciones:** Una colección de medios generales, tecnologías, protocolos y facilidades necesarias para el intercambio de información y documentos entre los usuarios de la red.
- **[L] Instalaciones:** Espacio físico en el que se encuentra alojado el hardware, así como los equipos de comunicaciones.
- **[P] Personal:** Grupo de individuos que interactúan tanto con el hardware como con el software.

En la **Tabla 8** se presenta el inventario de activos realizado conforme a lo estipulado en la norma ISO/IEC 27001:2013, específicamente en su Anexo A, cláusula A.8.1.1. El inventario se compone de los siguientes campos: Tipo, ID, Nombre, Descripción, Características, Responsable y Ubicación (La información completa se encuentra en el **Anexo 13**).

Tabla 8. Inventario de activos.

Tipo	ID	Nombre	Descripción	Características	Responsable	Ubicación
[D] [S] [SW]	[ACT01]	Sistema de Información Académico Administrativo y Financiero – SIAAF	Información Confidencial			
[D] [S] [SW]	[ACT02]	Repositorio Digital (DSpace)				
[D] [S] [SW]	[ACT03]	BIBLIOTECAS, KOHA				
[D] [S] [SW]	[ACT04]	Revistas de la Universidad Nacional de Loja				
[D] [S] [SW]	[ACT05]	Repositorio de Código Fuente - GitLab				
[D] [SW]	[ACT06]	POSTGRESQL (diferentes versiones)				

Nota. Elaboración propia.

* Datos enmascarados para garantizar la confidencialidad de la información.

❖ **Valoración de los activos de información**

Para la valoración de los activos se ha definido una escala de valores con un rango de 0 a 10, bajo las dimensiones de Confidencialidad, Integridad y Disponibilidad, tomando en cuenta los siguientes criterios:

Confidencialidad: Para la valoración de esta dimensión se debe responder la siguiente pregunta: ¿Qué daño causaría que lo conociera quien no debe? (ver **Tabla 9**).

Tabla 9. Confidencialidad.

Valor			Criterio
10	Muy alto	MA	Revelar este activo comprometería gravemente la confidencialidad de la información, potencialmente exponiendo datos altamente sensibles o críticos para la universidad a personas no autorizadas, resultando en pérdidas financieras significativas, violaciones de privacidad graves o consecuencias legales severas.
7-9	Alto	A	La divulgación de este activo afectaría significativamente la confidencialidad de la información, poniendo en riesgo datos sensibles y potencialmente causando daños financieros, problemas de reputación o violaciones regulatorias importantes.
4-6	Medio	M	Exponer este activo tendría un impacto importante, pero moderado en la confidencialidad de la información, pudiendo resultar en la revelación de datos confidenciales a individuos no autorizados, lo que podría provocar interrupciones operativas, pérdidas de competitividad o problemas de cumplimiento menores.
1-3	Bajo	B	La divulgación de este activo tendría un impacto limitado en la confidencialidad de la información, con consecuencias menores para la universidad, como la exposición de información interna a personas no autorizadas, ocasionando problemas de reputación o pérdidas financieras leves.
0	Muy Bajo	MB	No se espera que la divulgación de este activo tenga un impacto significativo en la confidencialidad de la información, ya que la información es de naturaleza pública, no confidencial o inexistente.

Nota. Elaboración propia.

Integridad: Para la valoración de esta dimensión se debe responder la siguiente pregunta: ¿Qué perjuicio causaría que estuviera dañado o corrupto? (ver **Tabla 10**).

Tabla 10. Integridad.

Valor			Criterio
10	Muy alto	MA	La corrupción o daño en este activo ocasionaría consecuencias extremadamente graves, impactando significativamente la veracidad y exactitud de los datos críticos. La restauración a su estado original sería altamente compleja y requeriría un tiempo considerable, afectando gravemente el desempeño de las actividades.
7-9	Alto	A	La alteración no autorizada de este activo resultaría en consecuencias graves, comprometiendo la veracidad y exactitud de datos sensibles que podrían afectar el funcionamiento normal. Requeriría esfuerzos significativos para su restauración y provocaría impactos considerables en las actividades operativas.
4-6	Medio	M	La modificación no autorizada de este activo podría acarrear consecuencias importantes pero moderadas, afectando la veracidad y exactitud de datos relevantes para la universidad. Esto podría generar impactos moderados en las operaciones y requerir un tiempo y recursos significativos para su corrección.

Valor			Criterio
1-3	Bajo	B	La alteración no deseada de este activo conllevaría consecuencias leves, con un impacto mínimo en la veracidad y exactitud de los datos. Probablemente ocasionaría efectos menores en las actividades normales y podría corregirse relativamente fácil.
0	Muy Bajo	MB	La modificación no autorizada de este activo tendría un impacto insignificante en la veracidad y exactitud de los datos, ya que se trata de información puramente informativa que no afecta sustancialmente las operaciones o actividades.

Nota. Elaboración propia.

Disponibilidad: Para la valoración de esta dimensión se debe responder la siguiente pregunta: ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? (ver **Tabla 11**).

Tabla 11. Disponibilidad.

Valor			Criterio
10	Muy alto	MA	La falta de disponibilidad de este activo tiene consecuencias extremadamente graves, afectando significativamente la capacidad de la universidad para llevar a cabo sus funciones críticas. Si el tiempo de inactividad es menor o igual a 2 horas, el impacto es catastrófico, interrumpiendo gravemente las operaciones esenciales.
7-9	Alto	A	La falta de disponibilidad de este activo provoca consecuencias graves, causando interrupciones significativas en las operaciones. Si el tiempo de inactividad es mayor a 2 horas y menor o igual a 4 horas, el impacto es considerable, afectando en gran medida la capacidad de llevar a cabo las actividades críticas.
4-6	Medio	M	La falta de disponibilidad de este activo tiene consecuencias importantes pero moderadas, generando interrupciones en las actividades. Si el tiempo de inactividad es mayor a 4 horas y menor o igual a 6 horas, el impacto es moderado, causando perturbaciones en el funcionamiento normal.
1-3	Bajo	B	La falta de disponibilidad de este activo tiene un impacto menor, con interrupciones menores en las actividades. Si el tiempo de inactividad es mayor a 24 horas, el impacto en el funcionamiento normal es mínimo, ya que se trata de información pública o informativa que no es crítica.
0	Muy Bajo	MB	La disponibilidad de este activo es irrelevante, ya que su falta de disponibilidad no afecta significativamente las operaciones normales de la universidad.

Nota. Elaboración propia.

La valoración de las tres dimensiones de seguridad (**Tabla 9**, **Tabla 10**, **Tabla 11**) se lleva a cabo individualmente para cada activo de información específico. Luego, se suman los valores de las tres dimensiones para obtener un promedio, el cual será redondeado al entero más cercano. El valor máximo posible en esta escala es 10, indicando la importancia de implementar controles que garanticen su correcto funcionamiento dentro de la DTI. Por otro lado, el valor mínimo es 0, sugiriendo que se puede prescindir del activo al no afectar directamente las actividades diarias de la comunidad universitaria. La valoración total del activo será clasificada con base en la siguiente escala de colores:

Tabla 12. Criterios de valoración.

Valor			Criterio
10	Muy alto	MA	El activo de información es crítico para el cumplimiento de los objetivos estratégicos de la universidad y su pérdida tendría un impacto extremadamente grave en la confidencialidad, integridad y/o disponibilidad.
7-9	Alto	A	El activo de información es fundamental para alcanzar los objetivos estratégicos de la universidad y su pérdida tendría consecuencias graves en la confidencialidad, integridad y/o disponibilidad.
4-6	Medio	M	El activo de información es relevante para el logro de los objetivos estratégicos de la universidad y su pérdida tendría implicaciones significativas en la confidencialidad, integridad y/o disponibilidad.
1-3	Bajo	B	El activo de información aporta valor, pero su pérdida no tendría un impacto crítico en la confidencialidad, integridad y/o disponibilidad.
0	Muy Bajo	MB	El activo de información no es fundamental para el logro de los objetivos estratégicos de la universidad y su pérdida tendría un impacto mínimo en la confidencialidad, integridad y/o disponibilidad.

Nota. Elaboración propia.

Considerando los criterios de valoración (**Tabla 12**), en la **Tabla 13** se presentan los resultados obtenidos (La información completa se encuentra en el **Anexo 14**).

Tabla 13. Valoración total del activo.

Tipo	ID	Nombre	Valoración			Valor Final [(C+I+D)/3]
			Confidencialidad	Integridad	Disponibilidad	
[D] [S] [SW]	[ACT01]	Sistema de Información Académico Administrativo y Financiero – SIAAF	9	9	9	**9**
[D] [S] [SW]	[ACT02]	Repositorio Digital (DSpace)	0	4	3	**2**
[D] [S] [SW]	[ACT03]	BIBLIOTECAS, KOHA	0	5	3	**3**
[D] [S] [SW]	[ACT04]	Revistas de la Universidad Nacional de Loja	0	5	3	**3**
[D] [S] [SW]	[ACT05]	Repositorio de Código Fuente - GitLab	10	9	9	**9**
[D] [SW]	[ACT06]	POSTGRESQL (diferentes versiones)	10	10	9	**10**

Nota. Elaboración propia.

- **Caracterizar las amenazas**

La metodología MAGERIT v.3, en su Libro I – Método, capítulo 3, sección 3.1.2, y en el Libro II – Catálogo de Elementos, capítulo 5, describe las diversas categorías de amenazas típicas que pueden afectar el rendimiento de los activos. A continuación, se detallan brevemente estas categorías:

- **[N] Desastres naturales:** Se refiere a eventos naturales como incendios, inundaciones y otros accidentes, que, aunque son de origen accidental, pueden afectar al sistema de forma pasiva.
- **[I] De origen industrial:** Desastres que ocurren dentro de la organización, como contaminación o fallos eléctricos, que pueden ser causados tanto por factores externos como internos, ya sea de forma accidental o deliberada por parte de los trabajadores.
- **[E] Errores y fallos no intencionados:** Se refiere a los errores cometidos por personas que tienen acceso al sistema de información, los cuales, ya sea por falta de capacitación o por descuido, pueden causar fallos no intencionados.
- **[A] Ataques intencionados:** Las personas que tienen acceso al sistema o agentes externos pueden ser autores de ataques intencionados, con el fin de obtener beneficios o simplemente hacer daño directamente a la organización.

La herramienta PilarBasic asigna las amenazas pertinentes según la naturaleza del activo de información, es decir, según la categoría en donde se encuentra con base en lo mencionado en el Libro II - Catálogo de Elementos.

De acuerdo con la clasificación de amenazas proporcionada por PilarBasic, la **Tabla 14** presenta las amenazas para cada tipo de activo y la dimensión que se ve comprometida (La información completa se encuentra en el **Anexo 14**).

Tabla 14. Amenazas.

Amenaza	Activos de información	Dimensión afectada
[N.1] Fuego	[ACT52] – [ACT53] – [ACT54] – [ACT55] – [ACT56] – [ACT57] – [ACT58] – [ACT59] – [ACT60] – [ACT61] – [ACT62] – [ACT64] – [ACT65] – [ACT66] – [ACT69]	[D] disponibilidad
[N.2] Daños por agua	[ACT52] – [ACT53] – [ACT54] – [ACT55] – [ACT56] – [ACT57] – [ACT58] – [ACT59] – [ACT60] – [ACT61] – [ACT62] – [ACT64] – [ACT65] – [ACT66] – [ACT69]	[D] disponibilidad
[N.*] Desastres naturales	[ACT52] – [ACT53] – [ACT54] – [ACT55] – [ACT56] – [ACT57] – [ACT58] – [ACT59] – [ACT60] – [ACT61] – [ACT62] – [ACT64] – [ACT65] – [ACT66] – [ACT69]	[D] disponibilidad
[I.1] Fuego	[ACT52] – [ACT53] – [ACT54] – [ACT55] – [ACT56] – [ACT57] – [ACT58] – [ACT59] – [ACT60] – [ACT61] – [ACT62] – [ACT64] – [ACT65] – [ACT66] – [ACT69]	[D] disponibilidad

Nota. Elaboración propia.

La **Tabla 15** ofrece una descripción de cada una de las amenazas, con la finalidad de proporcionar una mayor comprensión del espectro que abarcan (La información completa se encuentra en el **Anexo 14**).

Tabla 15. Descripción de las amenazas.

Amenaza	Descripción
[N.1] Fuego	Incendios: representan la posibilidad de que el fuego consuma los recursos del sistema.
[N.2] Daños por agua	Inundaciones: riesgo de que el agua destruya los recursos del sistema.
[N.*] Desastres naturales	Otros incidentes que ocurren sin la participación humana incluyen fenómenos como rayos, tormentas eléctricas, terremotos, ciclones, avalanchas y deslizamientos de tierra.
[I.1] Fuego	Incendios: provenientes de entornos industriales debido a la actividad humana, ya sea accidental o intencionalmente, provocando la destrucción de los recursos del sistema por el fuego.

Nota. Elaboración propia.

- **Analizar y priorizar el riesgo**

Una vez identificadas las amenazas a las que está expuesto un activo, es necesario evaluar el grado de influencia de dicha amenaza, considerando el siguiente aspecto:

Degradación: Evalúa el nivel de daño causado por un incidente, generalmente definido como una fracción del valor total del activo. Así, es posible concluir que ha sido "parcialmente degradado" o "totalmente degradado".

En la **Tabla 16** se proporciona una escala que sirve como referencia para evaluar la degradación del activo de información.

Tabla 16. Degradación.

Escala				
10	MA	Muy alta	Casi seguro	Fácil
7-9	A	Alta	Muy alto	Medio
4-6	M	Media	Posible	Difícil
1-3	B	Baja	Poco probable	Muy difícil
0	MB	Muy baja	Muy raro	Extremadamente difícil

Nota. Elaboración propia.

Para determinar el valor del impacto, es necesario comparar la valoración total del activo de información con la degradación que representaría la materialización de una amenaza. Con el fin de obtener un valor cuantitativo, se aplicará la Fórmula **(1)**:

$$\textbf{Impacto} = (\text{Valor del activo total} * \text{Degradación}) / 2 \qquad (1)$$

El resultado se redondea al entero más cercano, en la **Tabla 17** se proporciona la estimación del impacto junto con los valores numéricos.

Tabla 17. Impacto.

Impacto				
0	1-15	16-34	35-49	50
MB	B	M	A	MA

Nota. Elaboración propia.

Antes de continuar, es necesario introducir una nueva variable: la probabilidad. La probabilidad se refiere a la frecuencia con la que una amenaza específica se materializa o podría materializarse. Determinar y expresar esta probabilidad puede ser complejo y se puede realizar de manera cuantitativa a través de una escala nominal, tal como se presenta en la **Tabla 18**.

Tabla 18. Probabilidad.

Escala					
10	MA	100	Muy frecuente	A diario	10
7-9	A	10	Frecuente	Mensualmente	7-9
4-6	M	1	Normal	Una vez al año	4-6
1-3	B	1/10	Poco frecuente	Cada varios años	1-3
0	MB	1/100	Muy poco frecuente	Siglos	0

Nota. Elaboración propia.

Para llevar a cabo la evaluación del impacto y la probabilidad, la metodología MAGERIT v.3, en el Libro III – Guía de Técnicas, capítulo 2, sección 2.1, hace referencia a la técnica de Análisis mediante tablas. Un método simple, pero que ha demostrado ser muy útil al identificar la importancia relativa de los diferentes activos sujetos a amenazas. Adicionalmente, para obtener un valor cuantitativo, se debe aplicar la Fórmula **(2)**:

Nivel de Riesgo = Impacto * Probabilidad (2)

En la **Tabla 19**, se presenta una matriz que sirve como referencia para posicionar el valor del nivel de riesgo, teniendo en cuenta los valores del impacto y probabilidad.

Tabla 19. Nivel de riesgo.

Riesgo		Probabilidad				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Nota. Elaboración propia.

- **Definir los diferentes tipos de tratamiento de riesgo**

La norma ISO/IEC 27001:2013, en su Cláusula 6: Planificación, hace referencia a la necesidad de implementar procesos o acciones destinadas a reducir los riesgos identificados a un nivel tolerable o aceptable. Dicho proceso se conoce como tratamiento de los riesgos para la seguridad de la información y se fundamenta en dos criterios:

- Aceptar el riesgo
- Tratar el riesgo (tratamiento de riesgos)

Cuando un riesgo identificado representa un perjuicio notable para las operaciones de la institución, en este caso de la DTI, la norma menciona diversas opciones para el tratamiento de los riesgos, las cuales han sido detalladas en la sección **4.2.4.3**.

- **Determinar el nivel de riesgo**

Se definió el apetito por el riesgo, lo cual se refiere a la disposición de una organización para aceptar riesgos en función de los servicios y/o productos que ofrece a sus clientes. En el contexto de la DTI, se propuso un apetito por los riesgos categorizados como “Muy Bajo (MB)”, “Bajo (B)” y “Medio (M)”. Los riesgos clasificados como “Alto (A)” y “Muy Alto (MA)” deben ser reducidos seleccionando controles de seguridad de la información especificados en el Anexo A de la norma ISO/IEC 27001:2013.

Se desarrolló una matriz de riesgos en donde se registraron los riesgos asociados a ciertos activos de información. Además, se agregó el valor total de cada uno de los activos y se asignaron valores para la variable “Degradación” de acuerdo con lo estipulado en la **Tabla 16**.

Aplicando la Fórmula **(1)**, se determinó el valor del “Impacto” (redondeado al entero más cercano). Luego, se asignaron valores a la variable “Probabilidad” según la **Tabla 18**. Posteriormente, se aplicó la Fórmula **(2)**, y con la técnica de Análisis mediante tablas, basada en la **Tabla 19**, se determinó el nivel de riesgo, finalmente teniendo en cuenta la sección **Tratamiento de riesgos**, se seleccionó un tratamiento. Toda esta información se presenta en la **Tabla 20** (La información completa se encuentra en el **Anexo 14**).

Tabla 20. Matriz de riesgos.

ID Riesgo	ID Amenaza	Riesgo	ID Activo	Valor del activo	Degradación	Impacto	Probabilidad	Valor	Nivel de riesgo	Tratamiento
[R01]	[N.1]	Pérdida de datos y daños a la infraestructura debido a incendios, causando interrupciones comerciales y afectando la reputación y las finanzas de la organización.	[ACT52]	6	10	30	3	**90**	**Medio**	Aceptar el riesgo
			[ACT53]	5		25		**75**		
			[ACT54]	9		45		**135**	**Alto**	Reducir el riesgo
			[ACT55]	8		40		**120**		
			[ACT56]	8		40		**120**		
			[ACT57]	8		40		**120**		
			[ACT58]	7		35		**105**		
			[ACT59]	8		40		**120**		
			[ACT60]	8		40		**120**		
			[ACT61]	7		35		**105**		
			[ACT62]	7		35		**105**		
			[ACT64]	4		20		**60**	**Medio**	Aceptar el riesgo
			[ACT65]	8		40		**120**	**Alto**	Reducir el riesgo
			[ACT66]	7		35		**105**		
			[ACT69]	8		40		**120**		
[R02]	[N.2]	Destrucción de recursos del sistema por inundaciones, causando interrupciones operativas y pérdida de datos críticos.	[ACT52]	6	10	30	3	**90**	**Medio**	Aceptar el riesgo
			[ACT53]	5		25		**75**		
			[ACT54]	9		45		**135**	**Alto**	Reducir el riesgo
			[ACT55]	8		40		**120**		
			[ACT56]	8		40		**120**		
			[ACT57]	8		40		**120**		
			[ACT58]	7		35		**105**		
			[ACT59]	8		40		**120**		
			[ACT60]	8		40		**120**		
			[ACT61]	7		35		**105**		
			[ACT62]	7		35		**105**		
			[ACT64]	4		20		**60**	**Medio**	Aceptar el riesgo
			[ACT65]	8		40		**120**	**Alto**	Reducir el riesgo
			[ACT66]	7		35		**105**		
			[ACT69]	8		40		**120**		

ID Riesgo	ID Amenaza	Riesgo	ID Activo	Valor del activo	Degradación	Impacto	Probabilidad	Valor	Nivel de riesgo	Tratamiento
[R03]	[N.*]	Interrupción y daños causados por desastres naturales, como rayos, tormentas, terremotos y ciclones, resultando en pérdida de datos y daños a la infraestructura, requiriendo medidas de protección y planes de contingencia.	[ACT52]	6	10	30	3	**90**	**Medio**	Aceptar el riesgo
			[ACT53]	5		25		**75**		
			[ACT54]	9		45		**135**	**Alto**	Reducir el riesgo
			[ACT55]	8		40		**120**		
			[ACT56]	8		40		**120**		
			[ACT57]	8		40		**120**		
			[ACT58]	7		35		**105**		
			[ACT59]	8		40		**120**		
			[ACT60]	8		40		**120**		
			[ACT61]	7		35		**105**		
			[ACT62]	7		35		**105**		
			[ACT64]	4		20		**60**	**Medio**	Aceptar el riesgo
			[ACT65]	8		40		**120**	**Alto**	Reducir el riesgo
			[ACT66]	7		35		**105**		
			[ACT69]	8		40		**120**		
[R04]	[I.1]	Destrucción de recursos del sistema por incendios industriales, ya sea accidental o intencional, causando interrupciones operativas, pérdida de datos y daños a la infraestructura.	[ACT52]	6	10	30	3	**90**	**Medio**	Aceptar el riesgo
			[ACT53]	5		25		**75**		
			[ACT54]	9		45		**135**	**Alto**	Reducir el riesgo
			[ACT55]	8		40		**120**		
			[ACT56]	8		40		**120**		
			[ACT57]	8		40		**120**		
			[ACT58]	7		35		**105**		
			[ACT59]	8		40		**120**		
			[ACT60]	8		40		**120**		
			[ACT61]	7		35		**105**		
			[ACT62]	7		35		**105**		
			[ACT64]	4		20		**60**	**Medio**	Aceptar el riesgo
			[ACT65]	8		40		**120**	**Alto**	Reducir el riesgo
			[ACT66]	7		35		**105**		
			[ACT69]	8		40		**120**		

Nota. Elaboración propia.

De acuerdo con la matriz de riesgo efectuada para cada uno de los riesgos vinculados a los activos de información controlados por la DTI, se logró determinar el Mapa de Calor (ver **Tabla 21**). Se concluyó que hay 114 riesgos con un nivel Muy Alto, 285 con nivel Alto, 217 con nivel Medio, 57 con nivel Bajo y 21 con nivel Muy Bajo.

Tabla 21. Mapa de calor.

Impacto \ Probabilidad	MB	B	M	A	MA
MA	0	6	4	8	0
A	0	69	87	82	14
M	0	59	92	104	25
B	0	20	28	53	13
MB	0	12	9	6	3

MA: Muy Alto
A: Alto
M: Medio
B: Bajo
MB: Muy Bajo

Nota. Elaboración propia.

En la **Figura 14** se muestran los resultados de la evaluación de riesgos en la DTI de una forma gráfica para una mayor comprensión.

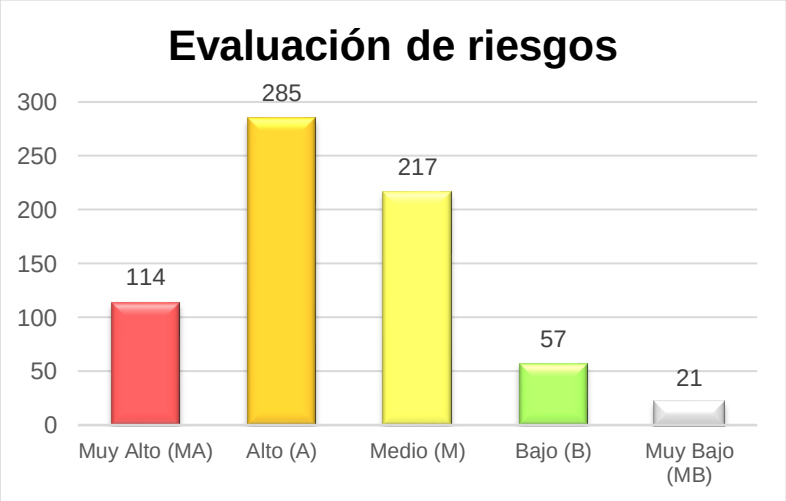

Figura 14. Evaluación de riesgos en la DTI.
Nota. Elaboración propia.

6.1.1.8 Elaborar un informe de la situación actual de la DTI

En el informe se recopiló, analizó y evaluó la información tanto del contexto interno como externo de la DTI, incluyendo el resultado de la evaluación de riesgos aplicando la metodología MAGERIT v.3. El propósito del documento es proporcionar una visión sobre el estado inicial de la DTI antes de la propuesta del SGSI, y verificar los cambios en aspectos relacionados con la seguridad de la información (ver **Anexo 15**).

6.1.1.9 Realizar la Declaración de aplicabilidad con base al Anexo A

La Declaración de aplicabilidad documenta el análisis y evaluación de cada control de seguridad indicado en el Anexo A de la norma ISO/IEC 27001:2013. Se justificó la selección o exclusión de cada control, determinándose la idoneidad de 113 controles de seguridad agrupados en políticas de seguridad de la información. El control "A.12.7.1 Controles de auditoría de sistemas de información" fue excluido, ya que las auditorías internas no están contempladas en el alcance del SGSI ni del TIC (ver **Anexo 16**).

6.1.1.10 Identificar los recursos del SGSI

Se identificaron tres recursos clave para la propuesta del SGSI: la ayuda del encargado del Proceso de Seguridad Informática, quien contribuyó en la selección de controles y desarrollo de políticas; los trabajadores de la DTI, que aportaron información sobre sus necesidades y expectativas; y el Director del TIC, quien revisó la documentación requerida por la norma ISO 27001 y facilitó materiales para la implementación de la metodología MAGERIT v.3.

6.1.2 Fase 2: Hacer (D)

6.1.2.1 Realizar un informe sobre la evaluación y tratamiento de riesgos

Concluida la evaluación y tratamiento de riesgos, se elaboró un informe que incluye información sobre el alcance de la evaluación, los documentos utilizados, el período de tiempo, y los resultados obtenidos, presentados en un mapa de calor y un gráfico de barras (ver **Anexo 17**).

6.1.2.2 Elaborar el Plan de tratamiento de riesgos

El plan de tratamiento de riesgos relaciona los controles de seguridad seleccionados previamente y su mecanismo de cumplimiento con los riesgos identificados como elevados, con el objetivo de mitigar dichos riesgos a niveles más manejables (ver **Anexo 18**).

6.1.2.3 Definir políticas de seguridad de la información para la DTI

Una vez identificados los riesgos asociados a los activos de información cuyo nivel es "Alto" y "Muy Alto", y seleccionados los controles de seguridad del Anexo A de la norma ISO 27001 para mitigarlos, el método de instauración es la formulación de un conjunto de políticas que dictaminen las actividades que deberán ser realizadas por los trabajadores de la DTI. Esto busca disminuir el nivel de riesgo y cumplir con los requisitos del SGSI.

Las políticas de seguridad de la información que se han desarrollado se presentan a continuación:

- **Política de roles y responsabilidades de seguridad**

Se formalizaron los roles y responsabilidades del SGSI, asignando tareas según los puestos de trabajo y actividades realizadas por cada empleado, siempre enmarcadas en los Procesos de la DTI. El Director de la DTI tiene la responsabilidad de crear y garantizar un canal permanente de comunicación con las autoridades de control competentes, servicios auxiliares y grupos de interés especial, para mantenerse actualizado sobre las últimas noticias en seguridad que ayuden a mejorar el SGSI. Se establecieron términos y condiciones para empleados y proveedores, quienes deberán firmar compromisos de confidencialidad antes de acceder a los sistemas de información. Se realizarán capacitaciones periódicas sobre las políticas y procedimientos de la DTI y, en caso de incumplimiento, se aplicarán sanciones según el reglamento creado por el Director de la DTI (ver **Anexo 19**).

- **Política sobre dispositivos móviles y teletrabajo**

Se definieron reglas básicas para el uso de dispositivos móviles dentro o fuera de la DTI, con el objetivo de proteger la información confidencial de la Dirección contra agentes externos. También se detallaron lineamientos para los empleados en modalidad de teletrabajo, quienes deben regirse a las reglas de dispositivos móviles y proteger los datos sensibles contra intrusiones no autorizadas en el lugar de trabajo (ver **Anexo 20**).

- **Política trae tu propio dispositivo (BYOD)**

Se establecieron reglas para el uso de dispositivos personales en la DTI, con el objetivo de mantener el control sobre la información sensible y confidencial procesada y almacenada en dichos dispositivos. Se aplicarán controles de autenticación, como contraseñas, lectores biométricos, SMS y correo electrónico, y no se deberán instalar aplicaciones que eludan los controles de seguridad. Los empleados de la DTI deberán cumplir con todas las normas establecidas (ver **Anexo 21**).

- **Política de uso aceptable**

Se definió una política para el uso aceptable de los activos de información, incluyendo responsabilidades y obligaciones de los empleados de la DTI, así como las actividades prohibidas al utilizar equipos y sistemas de información de la Dirección. El cuidado y mantenimiento de los equipos, tanto a nivel físico como lógico, será responsabilidad del personal de la DTI. Los funcionarios son responsables de las acciones realizadas con las cuentas proporcionadas por la DTI. Por ello, se establecen reglas claras para el uso de dichas cuentas (ver **Anexo 22**).

- **Política de seguridad para proveedores**

Se establecen directrices para la relación con proveedores, incluyendo cláusulas contractuales para aclarar las responsabilidades en el manejo de información confidencial de la DTI. En servicios como desarrollo de software, deben aplicarse

mecanismos de seguridad en todas las fases del sistema de información (ver **Anexo 23**).

- **Procedimiento para la gestión de incidentes**

El objetivo es detectar incidentes de seguridad en los activos de información, siguiendo un proceso de recepción, clasificación y tratamiento conforme a su criticidad, con retroalimentación para decisiones sobre medidas preventivas y correctivas (ver **Anexo 24**).

- **Política de clasificación de la información**

Las actividades y responsables en el proceso de clasificación se describen basándose en criterios que determinan el nivel de confidencialidad requerido para cada tipo de información. Esto permite que únicamente el personal técnico autorizado acceda o manipule dicha información, minimizando riesgos de divulgación y alteración (ver **Anexo 25**).

- **Política de eliminación y destrucción**

Se establece el procedimiento para la eliminación segura de la información almacenada en equipos, dispositivos móviles y formatos físicos, conforme a los lineamientos de la Política de clasificación de la información. Esta medida evita la eliminación accidental de información crítica. Además, se llevará un registro de la destrucción o eliminación de los soportes, notificando al responsable del activo en caso de que no sea la misma persona quien ejecute esta actividad (ver **Anexo 26**).

- **Procedimientos operativos para tecnología de la información (TI) y la comunicación**

La política establece los lineamientos para gestionar vulnerabilidades técnicas en los sistemas de información y proteger los equipos a nivel físico y lógico, incluyendo la realización de copias de seguridad en función de la criticidad de la información (ver **Anexo 27**).

- **Política de control de acceso**

El acceso a los servicios tecnológicos se gestiona mediante cuentas de usuario asignadas con permisos ajustados a las funciones específicas de cada empleado en la DTI. Cada funcionario es responsable de mantener sus credenciales en confidencialidad. Asimismo, se detallan normas para el uso y control de los servicios de red (ver **Anexo 28**).

- **Política del uso de controles criptográficos**

La aplicación de la criptografía asegura que solo los usuarios autorizados puedan acceder a la información. Esta política especifica un conjunto de normas para la gestión de claves y los activos de información que deben emplear herramientas criptográficas con algoritmos de encriptación (ver **Anexo 29**).

- **Política de seguridad física y ambiental**

Se presentan factores a considerar al elegir el emplazamiento de los equipos y dispositivos de comunicación de la DTI. El acceso al Centro de Datos estará supervisado, prohibiéndose el ingreso de equipos de registro de información. También se presentan lineamientos para proteger los equipos ante amenazas externas y ambientales, y asegurar los activos fuera de las instalaciones (ver **Anexo 30**).

- **Política de pantalla y escritorio limpio**

Las pautas establecidas previenen la filtración y manipulación de información en los puestos de trabajo. El personal de la DTI deberá bloquear la pantalla de su equipo al ausentarse y retirar cualquier documento confidencial de equipos compartidos, como impresoras (ver **Anexo 31**).

- **Política de gestión de cambios**

Se efectúa un procedimiento para la solicitud de cambios que incluirá detalles sobre su implementación y procedimientos de reversión en caso de inconvenientes. Una vez aprobado el cambio, el usuario asignado llevará a cabo las acciones necesarias, y la documentación se actualizará para garantizar su disponibilidad a todo el personal de la DTI (ver **Anexo 32**).

- **Política de desarrollo seguro**

Las reglas básicas para el desarrollo seguro de sistemas de información en la DTI incluyen una evaluación de riesgos y control de software no autorizado. Se aplican principios de ingeniería segura para que los desarrolladores, internos o externos, cumplan con requisitos de seguridad definidos y métodos de análisis de código que aseguren la preparación del sistema para producción (ver **Anexo 33**).

- **Política de creación de copias de seguridad**

La periodicidad de las copias de seguridad se define según la criticidad de la información, y se ejecutarán pruebas para verificar que los datos sean confiables, íntegros y estén disponibles en caso de ser requeridos (ver **Anexo 34**).

- **Política de gestión de registros y eventos de seguridad**

La política establece directrices para el control y seguimiento de las actividades de los administradores y usuarios en los activos de la DTI. Los registros deberán ser protegidos, y se recomienda mantener copias en tiempo real en sistemas que eviten accesos no autorizados, con el fin de salvaguardarlos (ver **Anexo 35**).

- **Política de transferencia de la información**

Se delimitaron canales de comunicación para la transferencia de información, según su complejidad y criticidad. Se establecieron lineamientos para el uso de mensajería electrónica y se hizo obligatoria la instauración de medidas de seguridad al utilizar servicios accesibles por redes públicas (ver **Anexo 36**).

- **Política de la continuidad del negocio**

Los productos y servicios clave, considerados críticos durante la evaluación y tratamiento de riesgos, estarán bajo la supervisión del Director de la DTI y del responsable del Proceso de Seguridad Informática ante cualquier incidente que interrumpa las operaciones de la DTI y afecte sus actividades diarias en la Universidad. La efectividad de los planes de continuidad del negocio será evaluada de forma periódica (ver **Anexo 37**).

- **Política de cumplimiento legal, regulatorio y contractual**

Se detallaron las entidades regulatorias y la legislación aplicable que influyen en las actividades de la DTI. Se establecieron directrices para los requisitos contractuales que garantizan el cumplimiento de las políticas de seguridad de la información (ver **Anexo 38**).

- **Política de revisión y cumplimiento de la seguridad de la información**

Se debe establecer un responsable para llevar a cabo una revisión independiente para evaluar controles, políticas, procesos y procedimientos de seguridad de la información, con el objetivo de conocer la efectividad del SGSI y las no conformidades detectadas. Se definió un responsable para garantizar el cumplimiento de los procedimientos de seguridad en cada Proceso de la DTI y se dictaminó la ejecución de una comprobación técnica para verificar que los sistemas de información cumplen con los lineamientos de las políticas de seguridad (ver **Anexo 39**).

- **Políticas de la DTI**

La Dirección de Tecnologías de Información (DTI) tenía políticas desactualizadas que no reflejaban su situación actual ni cumplían con los objetivos de la Institución. Estas políticas estaban desalineadas de la misión y visión de la Universidad Nacional de Loja. Se realizó un análisis exhaustivo y se actualizaron de acuerdo con los Procesos actuales de la comunidad universitaria.

Como resultado, se crearon seis nuevas políticas. Una de carácter general para la DTI, una específica para cada Proceso (exceptuando Seguridad Informática, ya que es un eje transversal que debe aplicarse en todas las actividades de la Dirección), y dos políticas de apoyo para la elaboración de sistemas y el uso de equipos computacionales (ver **Anexo 40**).

6.2 Objetivo 2: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3

6.2.1 Fase 3: Verificar (C)

6.2.1.1 Determinar la efectividad de las salvaguardas

Se aplicó la metodología MAGERIT v.3 para determinar la manera en el que las salvaguardas ingresan al cálculo del riesgo, esto lo hacen de dos formas:

- **Reduciendo la probabilidad:** La salvaguarda disminuye las oportunidades de que un riesgo ocurra; sin embargo, si ocurre, el perjuicio generado será el mismo.
- **Limitan el daño causado:** Las salvaguardas son capaces de limitar el impacto del riesgo, permitir una pronta detección para frenar la degradación o aplicar una rápida recuperación del sistema una vez que el riesgo ha finalizado.

En el caso del presente TIC las salvaguardas son las políticas de seguridad de la información. Se definieron los tipos de protección de las salvaguardas enmarcadas dentro del efecto que producen al riesgo. En la **Tabla 22** se detallan cada uno de ellos junto a algunos ejemplos para una mayor comprensión:

Tabla 22. Tipos de protección.

Efecto	ID	Nombre	Descripción	Ejemplos
Preventivas: reducen la probabilidad	[PR]	Prevención	La salvaguarda reduce las oportunidades de que un riesgo ocurra; si falla, el impacto del riesgo será el mismo.	• Controles de acceso. • Privilegios mínimos. • Metodologías de desarrollo seguro de software. • Asignación clara de roles y responsabilidades. • Gestión de capacidades.
	[DR]	Disuasión	Actúan sobre el atacante para disuadirlo de llevar a cabo el ataque; no tienen influencia en los daños si se ejecuta.	• Guardias de seguridad. • Comunicación de sanciones por incumplimiento o infracciones.
	[EL]	Eliminación	Eliminan equipos, servicios o sistemas de información innecesarios que puedan generar brechas de seguridad.	• Eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios; equipos y dispositivos de comunicación que ya no sean utilizados.
Acotan la degradación	[IM]	Minimización del impacto	Limitan las consecuencias del riesgo materializado.	• Desconexión de redes o equipos en caso de ataque. • Detención de servicios en caso de ataque. • Seguros de cobertura.

Efecto	ID	Nombre	Descripción	Ejemplos
				• Cumplimiento de la legislación vigente.
	[CR]	Corrección	Reparan los daños producidos por un incidente, reduciendo el impacto dentro de la Institución.	• Gestión de incidentes. • Líneas de comunicación alternativas. • Fuentes de alimentación redundantes.
	[RC]	Recuperación	Permiten regresar a un estado previo a la materialización del riesgo, acotando los daños a un periodo menor de tiempo.	• Copias de seguridad (back-up).
Consolidan el efecto de las demás	[MN]	Monitorización	Mantienen un registro actualizado de actividades, detectando intentos de ataque para limitar el impacto.	• Registros de actividad. • Registro de descargas web. • Monitoreo de la red.
	[DC]	Detección	Informan de la ocurrencia de un ataque, permitiendo implementar medidas adicionales para limitar su progresión.	• Anti-virus. • Sistema de detección de intrusos (IDS). • Detectores de incendio.
	[AW]	Concienciación	Capacitan en el uso adecuado de equipos y sistemas, previniendo errores y mejorando la eficacia de salvaguardas.	• Cursos de concienciación. • Cursos de formación.
	[AD]	Administración	Gestionan adecuadamente los controles de seguridad aplicados, evitando desconocimiento y posibles ataques exitosos.	• Inventario de activos. • Evaluación y tratamiento de riesgos. • Plan de continuidad.

Nota. Elaboración propia.

Para medir la efectividad de las políticas de seguridad de la información, se han definido dos escalas de madurez tanto para el impacto como para la probabilidad, teniendo en cuenta lo mencionado en la metodología MAGERIT v.3.

En la **Tabla 23** se presentan los criterios de valoración de las salvaguardas contra el impacto:

Tabla 23. Criterios de valoración de salvaguardas contra el impacto.

Efectividad	Nivel	Significado	Criterio
0%	**L0**	**Inexistente**	La salvaguarda no es útil para limitar el impacto de un riesgo. Además, puede que no haya sido implementada ni propuesta.

Efectividad	Nivel	Significado	Criterio
5%	L1	Inicial / ad – hoc	La salvaguarda limita el impacto del riesgo de manera marginal y se aplica sólo en casos específicos, por lo que no es generalizable.
25%	L2	Reproducible, pero intuitivo	La salvaguarda se aplica frecuentemente por diferentes personas, pero su efectividad depende del conocimiento individual, reduciendo moderadamente el impacto de los riesgos sobre los activos de información.
50%	L3	Proceso definido	La salvaguarda se aplica de manera adecuada y conforme a un procedimiento documentado, limitando significativamente el impacto del riesgo.
75%	L4	Gestionado y medible	La salvaguarda es efectiva y permite un seguimiento cuantitativo de su desempeño mediante métricas, limitando considerablemente el impacto del riesgo.
100%	L5	Optimizado	La salvaguarda es idónea y se encuentra en un proceso continuo de análisis y mejora, limitando de manera óptima el impacto del riesgo.

Nota. Elaboración propia.

En la **Tabla 24** se presentan los criterios de valoración de las salvaguardas preventivas:

Tabla 24. Criterios de valoración de salvaguardas preventivas.

Efectividad	Nivel	Significado	Criterio
0%	L0	Inexistente	La salvaguarda no es útil para impedir que un riesgo se materialice. Además, puede que no haya sido implementada ni propuesta.
5%	L1	Inicial / ad – hoc	La salvaguarda reduce la probabilidad del riesgo de manera marginal y se aplica sólo en casos específicos, por lo que no es generalizable.
25%	L2	Reproducible, pero intuitivo	La salvaguarda se aplica frecuentemente por diferentes personas, pero su efectividad depende del conocimiento individual, reduciendo moderadamente la probabilidad de los riesgos sobre los activos de información.
50%	L3	Proceso definido	La salvaguarda se aplica de manera adecuada y conforme a un procedimiento documentado, reduciendo significativamente la probabilidad del riesgo.
75%	L4	Gestionado y medible	La salvaguarda es efectiva y permite un seguimiento cuantitativo de su desempeño mediante métricas, reduciendo considerablemente la probabilidad del riesgo.
100%	L5	Optimizado	La salvaguarda es idónea y se encuentra en un proceso continuo de análisis y mejora, reduciendo de manera óptima la probabilidad del riesgo.

Nota. Elaboración propia.

6.2.1.2 Evaluar el nivel de riesgo posterior a la implementación de controles de seguridad

Se elaboraron 45 casos de prueba según los riesgos identificados en el Plan de tratamiento de riesgo. Cada caso de prueba se diseñó con un escenario posible para analizar y determinar, junto con el encargado del Proceso de Seguridad Informática, el

Ingeniero Juan Carlos Riofrío (ver **Anexo 3**), la efectividad de las políticas de seguridad de la información, siguiendo la metodología MAGERIT v.3 en cuanto a los tipos y valoración de las salvaguardas.

La **Tabla 25** presenta una descripción de los campos dentro de la matriz de casos de prueba:

Tabla 25. Descripción de la matriz de casos de prueba.

Campo	Descripción
Nro.	Utilizado para controlar que se han realizado los 45 casos de prueba.
ID Riesgo	Identificador del riesgo asociado al caso de prueba, cuyo impacto y probabilidad se busca reducir.
ID caso de prueba	Identificador del caso de prueba.
Caso de prueba	Nombre del caso de prueba.
Escenario posible	Descripción del escenario donde se podría materializar un riesgo en la DTI.
Salvaguarda	Política de seguridad de la información diseñada para reducir la probabilidad y/o el impacto de un riesgo específico.
Tipo	Tipo de salvaguarda con base en la **Tabla 22**.
ID activo	Identificador del activo de información.
Nivel (Impacto)	Efectividad de la salvaguarda según los criterios de la **Tabla 23**.
Impacto	Cálculo del impacto considerando la efectividad de la salvaguarda, redondeado al entero más cercano.
Nivel (Probabilidad)	Efectividad de la salvaguarda según los criterios de la **Tabla 24**.
Probabilidad	Cálculo de la probabilidad considerando la efectividad de la salvaguarda, redondeado al entero más cercano.
Valor del riesgo	Resultado de la multiplicación del impacto por la probabilidad.
Nivel de riesgo	Categorización del riesgo de acuerdo a la metodología de evaluación y tratamiento de riesgos.

Nota. Elaboración propia.

En la **Tabla 26** se presenta la matriz de casos de prueba (La información completa se encuentra en el **Anexo 41**):

Tabla 26. Matriz de casos de prueba.

Nro.	ID Riesgo	ID Caso de prueba	Caso de prueba	Escenario posible	Salvaguarda	Tipo	ID Activo	Nivel (I)	Impacto	Nivel (P)	Probabilidad	Valor del riesgo	Nivel de riesgo residual
1	[R01]	[C01]	Incendios	Incendios causados por factores naturales como rayos solares concentrados por vidrio o relámpagos durante fuertes lluvias.	La política de seguridad física y ambiental, en la sección "3.4. Protección contra las amenazas externas o ambientales," establece que deben instalarse y aplicarse sistemas de prevención y extinción de incendios.	[PR] [IM]	[ACT54]	**L3 (50%)**	23	**L3 (50%)**	2	46	**Medio**
							[ACT55]		20			40	
							[ACT56]		20			40	
							[ACT57]		20			40	
							[ACT58]		18			36	
							[ACT59]		20			40	
					La política de la continuidad del negocio, en la sección "3.6. Lineamientos para la continuidad operativa," dicta la implementación de soluciones de respaldo y recuperación de datos, asegurando	[RC]	[ACT60]		20			40	
							[ACT61]		18			36	
							[ACT62]		18			36	
							[ACT65]		20			40	
							[ACT66]		18			36	
							[ACT69]		20			40	

Nro.	ID Riesgo	ID Caso de prueba	Caso de prueba	Escenario posible	Salvaguarda	Tipo	ID Activo	Nivel (I)	Impacto	Nivel (P)	Probabilidad	Valor del riesgo	Nivel de riesgo residual
					copias de seguridad regulares almacenadas en ubicaciones geográficamente separadas de las instalaciones de la DTI.								
2	[R02]	[C02]	Inundaciones	Inundaciones causadas por factores naturales como lluvias intensas.	La política de seguridad física y ambiental, en la sección "3.4. Protección contra las amenazas externas o ambientales," establece que los centros de datos y el cableado deben ubicarse lejos de áreas con riesgos de inundaciones.	[PR] [RC]	[ACT54]	**L3 (50%)**	23	**L3 (50%)**	2	46	**Medio**
							[ACT55]		20			40	
							[ACT56]		20			40	
							[ACT57]		20			40	
							[ACT58]		18			36	
							[ACT59]		20			40	
					La política de la continuidad del negocio, en la sección "3.6. Lineamientos para la		[ACT60]		20			40	
							[ACT61]		18			36	
							[ACT62]		18			36	
							[ACT65]		20			40	
							[ACT66]		18			36	
							[ACT69]		20			40	

Nro.	ID Riesgo	ID Caso de prueba	Caso de prueba	Escenario posible	Salvaguarda	Tipo	ID Activo	Nivel (I)	Impacto	Nivel (P)	Probabilidad	Valor del riesgo	Nivel de riesgo residual
					continuidad operativa," dicta la implementación de soluciones de respaldo y recuperación de datos, asegurando copias de seguridad regulares almacenadas en ubicaciones geográficamente separadas de las instalaciones de la DTI.								
3	[R03]	[C03]	Desastres naturales	Desastres naturales, como rayos, tormentas, terremotos y ciclones.	La política de seguridad física y ambiental, en la sección "3.4. Protección contra las amenazas externas o ambientales," establece la implementación de un sistema de alerta temprana conectado a	[DC] [RC]	[ACT54]	**L3 (50%)**	23	**L3 (50%)**	2	46	**Medio**
							[ACT55]		20			40	
							[ACT56]		20			40	
							[ACT57]		20			40	
							[ACT58]		18			36	
							[ACT59]		20			40	
							[ACT60]		20			40	
							[ACT61]		18			36	
							[ACT62]		18			36	
							[ACT65]		20			40	
							[ACT66]		18			36	
							[ACT69]		20			40	

Nro.	ID Riesgo	ID Caso de prueba	Caso de prueba	Escenario posible	Salvaguarda	Tipo	ID Activo	Nivel (I)	Impacto	Nivel (P)	Probabilidad	Valor del riesgo	Nivel de riesgo residual
					organismos oficiales de monitoreo de desastres naturales, con protocolos de respuesta y evacuación claramente definidos y comunicados a todo el personal de la DTI.								
					La política de la continuidad del negocio, en la sección "3.6. Lineamientos para la continuidad operativa," dicta la implementación de soluciones de respaldo y recuperación de datos, asegurando copias de seguridad regulares almacenadas en								

Nro.	ID Riesgo	ID Caso de prueba	Caso de prueba	Escenario posible	Salvaguarda	Tipo	ID Activo	Nivel (I)	Impacto	Nivel (P)	Probabilidad	Valor del riesgo	Nivel de riesgo residual
					ubicaciones geográficamente separadas de las instalaciones de la DTI.								
4	[R04]	[C04]	Incendios industriales	Incendios provocados por fallos en equipos eléctricos, sobrecalentamiento de maquinaria, o errores en el manejo del cableado eléctrico por parte del personal de la DTI.	La política de seguridad física y ambiental, en la sección "3.4. Protección contra las amenazas externas o ambientales," establece que deben instalarse y aplicarse sistemas de prevención y extinción de incendios.	[PR] [IM] [RC]	[ACT54]	**L3 (50%)**	23	**L3 (50%)**	2	46	**Medio**
							[ACT55]		20			40	
							[ACT56]		20			40	
							[ACT57]		20			40	
							[ACT58]		18			36	
							[ACT59]		20			40	
							[ACT60]		20			40	
							[ACT61]		18			36	
					La política de la continuidad del negocio, en la sección "3.6. Lineamientos para la continuidad operativa," dicta la implementación de soluciones de		[ACT62]		18			36	
							[ACT65]		20			40	
							[ACT66]		18			36	
							[ACT69]		20			40	

Nro.	ID Riesgo	ID Caso de prueba	Caso de prueba	Escenario posible	Salvaguarda	Tipo	ID Activo	Nivel (I)	Impacto	Nivel (P)	Probabilidad	Valor del riesgo	Nivel de riesgo residual
					respaldo y recuperación de datos, asegurando copias de seguridad regulares almacenadas en ubicaciones geográficamente separadas de las instalaciones de la DTI.								

Nota. Elaboración propia.

En la **Tabla 27** se presenta el mapa de calor obtenido después de la ejecución de los casos de prueba, cabe mencionar que se incluyen los riesgos residuales que habían sido aceptados en la Declaración de aplicabilidad.

Tabla 27. Mapa de calor final.

Impacto	MB	B	M	A	MA
MA	0	0	0	0	0
A	0	0	0	0	0
M	0	85	178	0	0
B	0	20	105	53	14
MB	0	12	9	6	3

Probabilidad

MA: Muy Alto
A: Alto
M: Medio
B: Bajo
MB: Muy Bajo

Nota. Elaboración propia.

En la **Figura 15** se presentan los resultados de la mitigación de riesgos en la DTI de una forma gráfica para una mayor comprensión.

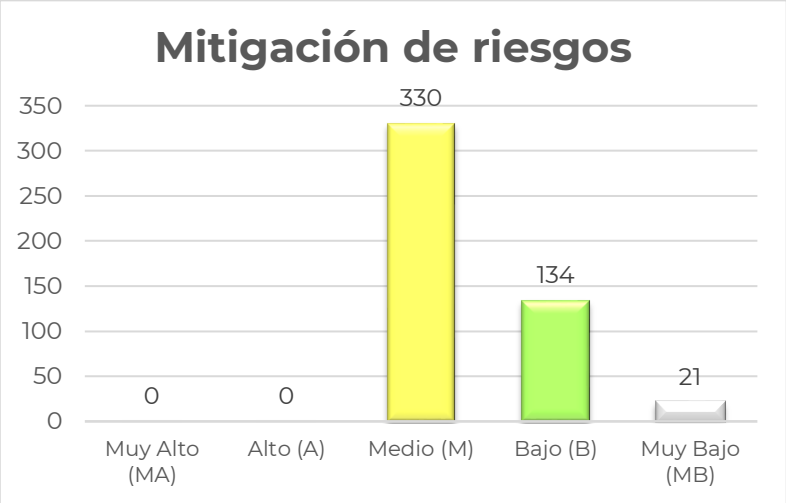

Figura 15. Mitigación de riesgos en la DTI.
Nota. Elaboración propia.

Con base en los resultados presentados se determinó que las políticas de seguridad de la información están en un Nivel L3, ya que se encuentran documentadas, pero aún no se han establecido métricas para medir su desempeño y así poder optimizarlas, así también, se comprobó que su implementación mitiga los riesgos asociados a los activos de información de la DTI. Es crucial actualizar estos documentos periódicamente para asegurar su utilidad en las actividades de la Dirección en la Universidad.

Se logró una redistribución completa de los riesgos categorizados como “Muy Alto” y “Alto”, puesto que, se redujeron a cero; sin embargo, los riesgos medios aumentaron de 217 a 330, un incremento del 52,53% y los riesgos bajos aumentaron de 57 a 134, es decir un aumento del 135,09%, reflejando la efectividad de las políticas en reducir riesgos a niveles más manejables. Finalmente, los riesgos muy bajos no experimentaron cambios, ya que eran irrelevantes.

6.2.1.3 Evaluar el nivel de madurez de la DTI posterior a la propuesta del SGSI

Se efectuó una nueva evaluación del nivel de madurez de la DTI referente al estado de la seguridad de la información aplicando el análisis de brechas (GAP), los resultados se presentan a continuación:

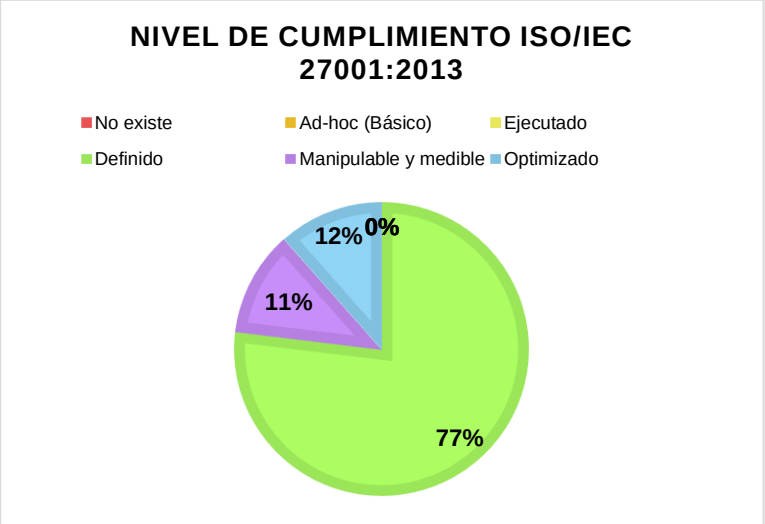

Figura 16. Nivel de Cumplimiento posterior al SGSI (ISO/IEC 27001:2013).
Nota. Elaboración propia.

Con base en los resultados del análisis GAP, efectuados después de la propuesta del SGSI, en la **Figura 16** se observa que un 77% de las cláusulas se encuentra en un nivel de madurez 3 (Definido), dado que se ha realizado la documentación conforme a lo indicado por la norma; sin embargo, la DTI tiene la responsabilidad de aplicar métricas y optimizar los procedimientos definidos en las políticas de seguridad de la información. Un 11% de las cláusulas se mantiene en el nivel de madurez 4 (Manipulable y medible) debido a que el encargado del Proceso de Seguridad Informática posee la competencia necesaria para contribuir a la eficacia del SGSI en la DTI. Anteriormente, se realizaba una apreciación y tratamiento de los riesgos de seguridad de forma informal; ahora, se cuenta con documentación detallada que podrá ser aplicada por los trabajadores de la Dirección. El 12% restante se posiciona en el nivel de madurez 5 (Optimizado).

Por lo tanto, la DTI se puede posicionar en un nivel de madurez 3 (Definido) al ejecutar procesos encaminados a la seguridad de la información conforme a

documentos formalizados y aprobados, los cuales podrán ser mejorados mediante la aplicación de métricas.

Realizado el análisis y evaluación de los controles de seguridad, evidenciado en la Declaración de aplicabilidad, se determinó la aplicabilidad de 113 controles de seguridad, los cuales fueron definidos a través de políticas de seguridad de la información. En la **Figura 17**, se observa que un 97% de los controles se encuentra en un nivel de madurez 3 (Definido). Esto sugiere una considerable mejora en el estado de la seguridad de la información en la DTI, al contar con documentación formalizada a la cual pueden recurrir los trabajadores para el desempeño adecuado de sus actividades.

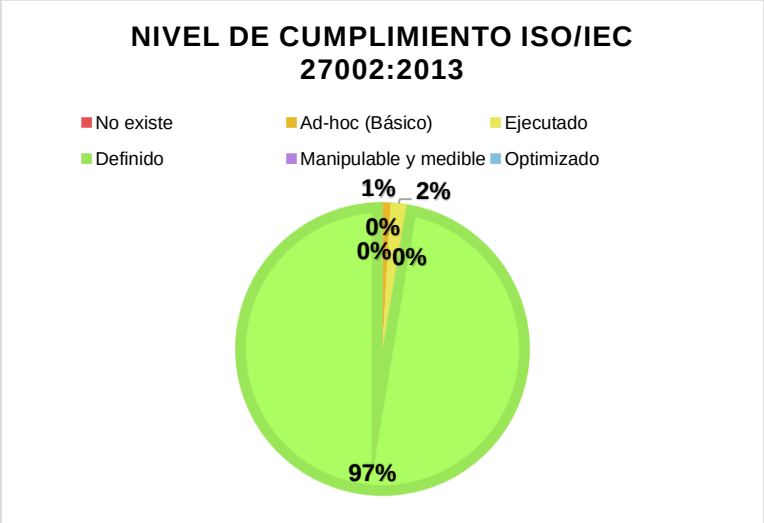

Figura 17. Nivel de Cumplimiento posterior al SGSI (ISO/IEC 27002:2013).
Nota. Elaboración propia.

La información obtenida de los análisis comprueba la mejora en la seguridad de la información de la DTI, al formalizar procesos previamente realizados de forma interna. Estos procesos ahora podrán ser monitoreados, permitiendo identificar no conformidades y oportunidades de mejora que beneficiarán la administración y gestión de los activos de información (La información completa se encuentra en el **Anexo 42**).

6.2.2 Fase 4: Actuar (A)

En esta última fase, aunque no se aplicó la cláusula 10 de la norma ISO 27001 relativa a la mejora continua por limitaciones de tiempo, se entregó formalmente la documentación del SGSI al encargado del Proceso de Seguridad Informática (ver **Anexo 5**), quien será responsable de realizar evaluaciones periódicas para identificar y corregir no conformidades mediante acciones preventivas y correctivas, mejorando el rendimiento del SGSI (ver **Anexo 43**). De igual manera, se presentó al Director de la DTI y a los encargados de los Procesos, los resultados del TIC, para que tengan noción sobre el procedimiento que se siguió, la documentación generada y el nivel de madurez en el que se encuentran actualmente (ver **Anexo 44**).

7 Discusión

7.1 Objetivo 1: Implementar controles de seguridad alineados con la norma ISO/IEC 27001:2013, empleando el ciclo PDCA para desarrollar políticas destinadas a reducir los riesgos de seguridad de la información en la Dirección de Tecnologías de Información (DTI) de la Universidad Nacional de Loja (UNL)

Para cumplir con el primer objetivo, se evaluó la aplicabilidad de las cláusulas de la norma ISO/IEC 27001:2013 en el contexto del Trabajo de Integración Curricular (TIC) para la propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Dirección de Tecnologías de Información (DTI). Se determinó una aplicabilidad total del 35%, una aplicabilidad parcial del 27% y un 38% no aplicable, debido a que en el lapso de tiempo que dura un ciclo académico no es posible realizar un seguimiento de las no conformidades en los controles formalizados, esta responsabilidad recae en la DTI. En los trabajos relacionados [4], [5], [7], no se menciona el porcentaje de aplicabilidad de la norma, a pesar de que este aspecto es crucial para definir el alcance del SGSI que será implementado en una empresa o institución; uno de los problemas potenciales derivados de esta omisión es la falta de personal especializado que pueda evaluar los controles de seguridad y aplicar acciones correctivas.

La recopilación de información sobre el contexto interno de la DTI permitió identificar que las políticas vigentes se encuentran desactualizadas, ya que no reflejan los cambios derivados de la reestructuración en la que se crearon nuevos Procesos. El análisis de brechas (GAP) confirmó la ausencia de documentación formal a la que los trabajadores puedan recurrir para desempeñar sus actividades de manera eficiente, manteniendo una adecuada protección de los activos, situando a la DTI en un nivel de madurez 2 (Ejecutado). Esta información, junto con los requerimientos de las partes interesadas, fue fundamental para seleccionar los controles de seguridad del Anexo A de la norma ISO 27001 que se implementarían a través de políticas de seguridad de la información.

El ciclo PDCA se acopla de manera óptima con la norma ISO 27001:2013, proporcionando un marco efectivo para la propuesta del SGSI. Mediante su aplicación, se logró cumplir con las cláusulas de la ISO 27001 dentro del alcance del TIC, obteniendo información clave que permitió determinar el estado de la seguridad de la información en la DTI y documentar el SGSI de manera apropiada. Su empleo se ha visualizado en trabajos relacionados [4], [5], [6], [7], debido a que la ISO 27001 adopta y promueve el enfoque de mejora continua para asegurar la efectividad del SGSI. No obstante, la aplicación de la metodología varía según el contexto de cada organización, institución o negocio.

La metodología MAGERIT v.3, empleada para la evaluación y tratamiento de riesgos, demostró ser compatible con la norma ISO 27001. Posibilitó la identificación y valoración de los activos de información administrados en la DTI. Esta metodología incluye una herramienta informática denominada PilarBasic, con la cual se identificaron las amenazas asociadas a dichos activos. De acuerdo con la matriz de riesgos diseñada, se detectaron 114 riesgos con nivel “Muy Alto”, 285 con nivel “Alto”, 217 con nivel “Medio”, 57 con nivel “Bajo” y 21 con nivel “Muy Bajo”. Esto evidencia la necesidad de implementar controles de seguridad para mitigar los riesgos categorizados como “Muy Alto” y “Alto”. La aplicación de MAGERIT v.3 coincide con los trabajos relacionados [4], [5], [6], [7], lo que destaca su utilidad y su relación directa con la propuesta de un SGSI. Sin embargo, cada estudio, incluyendo el presente TIC, adapta la metodología a su contexto, creando criterios de valoración y análisis del nivel de riesgo únicos.

El análisis y la evaluación de los controles de seguridad estipulados en el Anexo A de la norma ISO 27001 se reflejan en la Declaración de aplicabilidad, donde se identificó la idoneidad de 113 controles de seguridad. Se excluyó el control “A.12.7.1 Controles de auditoría de sistemas de información”, ya que no se incluye en el alcance del TIC. El diseño de políticas permitió implementar los controles de seguridad en la DTI, formalizando las actividades que el personal técnico y administrativo realiza diariamente. Las políticas muestran similitudes con trabajos relacionados, dado que se basaron en los lineamientos de la norma ISO 27002, que proporciona una guía para la instauración de cada uno de los controles de seguridad.

7.2 Objetivo 2: Evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de un entorno de casos de prueba aplicando la metodología MAGERIT v.3

La mitigación de los riesgos asociados a los activos de información se logró aplicando la metodología MAGERIT v.3, la cual permitió cuantificar la eficacia de las políticas de seguridad de la información del SGSI. Se diseñaron 45 casos de prueba basados en escenarios posibles y, junto con el Ingeniero Juan Carlos Riofrío, encargado del Proceso de Seguridad Informática, se confirmó que estas políticas efectivamente contribuyen a reducir el nivel de riesgo.

Las políticas de seguridad apoyaron en gran medida a la reducción de riesgos en la DTI, puesto que, al situarse en un nivel de madurez L3 (Proceso definido), con una efectividad del 50%, se demostró su capacidad para disminuir la probabilidad y/o limitar el impacto de los riesgos. Este nivel de efectividad fue el adecuado para redistribuir completamente los 114 riesgos catalogados como “Muy Alto” y los 285 como “Alto”, incrementando los riesgos de nivel “Medio” en un 52,53% y los de nivel “Bajo” en un

135,09%. Como resultado, se alcanzaron 330 riesgos con nivel “Medio”, 134 con nivel “Bajo”, y se mantuvieron los 21 riesgos con nivel “Muy Bajo”.

La ejecución de un nuevo análisis de brechas (GAP) posterior a la propuesta del SGSI corroboró un aumento en el nivel de madurez de la DTI en relación con la aplicabilidad de las cláusulas de la norma ISO/IEC 27001:2013 y los controles de la norma ISO/IEC 27002:2013, logrando un nivel de madurez 3 (Definido). Se actualizó la documentación necesaria para guiar a los funcionarios de la Dirección, asegurando el cumplimiento de las medidas para mantener la confidencialidad, integridad y disponibilidad de la información. Los resultados difieren de trabajos relacionados [4], [5], [6], [7], donde no se emplea una evaluación que determine la efectividad de las salvaguardas diseñadas e implementadas, limitándose a la entrega del SGSI.

Debido a la limitación de tiempo por el lapso que dura un ciclo académico, los casos de prueba se ejecutaron a través de escenarios simulados en lugar de un entorno real controlado. Esta limitación podría abordarse en un TIC centrado específicamente en la ejecución de casos de prueba, donde se apliquen métricas que evalúen el nivel de cumplimiento práctico de los controles de seguridad en la DTI, permitiendo obtener valores cuantitativos que mejoren el SGSI al identificar no conformidades que requieran acciones correctivas.

8 Conclusiones

Culminado el presente TIC se concluye lo siguiente:

- El desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2013, como se estableció en el objetivo general, permitió la formulación de 27 políticas de seguridad específicas. Paralelamente, se implementó un proceso estructurado utilizando la metodología MAGERIT v.3 para valorar los activos de información, identificar y priorizar riesgos, y formalizar las actividades del personal de la Dirección de Tecnologías de Información (DTI), garantizando así el cumplimiento de los requisitos de seguridad en la protección de los equipos y sistemas de información.
- La integración del ciclo PDCA con la norma ISO 27001 resultó altamente efectiva, ya que alineó cada una de sus fases con la documentación esencial que cualquier institución, organización o negocio necesita para mejorar la seguridad de la información. Esto permitió evaluar y seleccionar los controles de seguridad más adecuados al contexto interno y externo de la DTI, facilitando el desarrollo de políticas que contribuyen a la reducción de los riesgos asociados a los activos de información que administran y utilizan diariamente.
- La evaluación de la eficacia del SGSI, definida en el segundo objetivo específico, se realizó mediante la ejecución de 45 casos de prueba basados en escenarios posibles, aplicando la metodología MAGERIT v.3. Esta evaluación logró una redistribución significativa de los 114 riesgos clasificados como “Muy Alto” y de los 285 con nivel “Alto” identificados en la fase de planificación (P), evidenciándose, como los riesgos medios aumentaron un 52,53% y los bajos un 135,09%, lo que indica una mejora sustancial en la gestión y mitigación de riesgos para la seguridad de la información.
- El diseño de 27 políticas específicas de seguridad dentro del SGSI contribuyó significativamente a la reducción de los 114 riesgos clasificados como “Muy Alto” y los 285 riesgos con nivel “Alto”. La disminución en la probabilidad y el impacto de estos riesgos permitió su recategorización a niveles “Medio” y “Bajo”, resultando en un incremento de los riesgos medios de 217 a 330 y de los riesgos bajos de 57 a 134, de esta forma, las políticas implementadas han creado un entorno más seguro y controlado en la DTI.
- La información proporcionada por el encargado del Proceso de Seguridad Informática, junto con la investigación realizada y la participación activa del personal de la DTI, fue fundamental para identificar las necesidades específicas en materia de seguridad de la información y para la exitosa propuesta de un

SGSI adaptado a su contexto y expectativas, conforme a la norma ISO/IEC 27001:2013.

- La propuesta del SGSI posicionó a la DTI en un nivel de madurez 3 (Definido), asegurando una adecuada ejecución de sus actividades de acuerdo a procesos documentados y aprobados, enmarcados en el mantenimiento de la confidencialidad, integridad y disponibilidad de la información.

9 Recomendaciones

Culminado el presente TIC se recomienda:

- Efectuar evaluaciones de riesgo periódicas utilizando la metodología MAGERIT v.3 u otra metodología que se adapte a las necesidades de la DTI, con el fin de analizar y mejorar la efectividad de los controles de seguridad en la reducción del nivel de riesgo.
- Implementar un Sistema de Gestión de la Continuidad del Negocio (SGCN) conforme a la norma ISO 22301, y combinarlo con el SGSI para fortalecer la capacidad de recuperación ante riesgos que puedan causar interrupciones prolongadas en las operaciones de la DTI.
- Ejecutar casos de prueba en entornos reales controlados dentro de la DTI, con el objetivo de verificar el cumplimiento de los controles de seguridad establecidos en las políticas de seguridad de la información.
- Planificar auditorías internas en la DTI utilizando herramientas informáticas de análisis de riesgos asociados a los sistemas de información, generando información útil para la alta dirección en la implementación de acciones correctivas o de mejora.
- Utilizar este trabajo como base para su aplicación en otros departamentos de la Universidad Nacional de Loja, logrando un manejo adecuado de la información clasificada como confidencial y crítica, de la cual dependen las actividades académicas y económicas de la institución.

10 Bibliografía

[1] D. Villavicencio, L. Fuentes, R. Silva y O. Ibarra, “Las TIC en la Educación Superior y su Implementación en la Universidad de Guayaquil,” *593 Digital Publisher CEIT*, pp. 292-301, mayo, 2023. doi: https://doi.org/10.33386/593dp.2023.4.1935

[2] P. Uriguen, F. Vega y Á. Luna, “El uso de las TIC en el aprendizaje en la Universidad caso UTMACH,” *INNOVA Research Journal*, vol. 5, no. 1, pp. 31-46, enero-abril, 2020. doi: https://doi.org/10.33890/innova.v5.n1.2020.1120

[3] M. Pallero y J. Heguiabehere, *Seguridad de la información y ciberseguridad*, Argentina: Fundación Sadosky, 2023.

[4] M. Guano y M. Jaramillo, “Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio,” Tesis, Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, Ecuador, 2020.

[5] J. Recalde, “Plan de Implementación de un SGSI y Aplicación de controles críticos en el Centro de Operaciones de Seguridad en la empresa GMS,” Tesis, Escuela Politécnica Nacional, Quito, Ecuador, 2019.

[6] O. Muñoz, “Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indígena SAC,” Tesis, Universidad Técnica de Ambato, Ambato, Ecuador, 2020.

[7] R. Fuentes, “Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca,” Tesis, Facultad de Ingeniería Civil, de Sistemas y Arquitectura, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú, 2020.

[8] C. Barreto y F. Iriarte, *Las TIC en la educación superior. Experiencias de innovación*, Colombia: Universidad del Norte, 2017.

[9] W. Paredes-Parada, *Tecnologías para las instituciones de educación superior (IES) y sus experiencias*, Ecuador: CEDIA, 2021.

[10] S. Gellibert, S. Zapata y J. Díaz, “Las TIC en la educación superior durante la pandemia de la COVID-19.,” *Revista Sinapsis*, vol. 1, no. 19, junio, 2021.

[11] Fundación Telefónica, *Sociedad Digital en España 2023*, España: Penguin Random House Grupo Editorial, 2023.

[12] J. Harán, (2023, ago. 31). “ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina”. [en línea]. Disponible en: https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/ [Consultado: mayo 01, 2024]

[13] ESET, *Security Report Latinoamérica 2023*, 2023.

[14] E. Vega, *Seguridad de la Información*, Costa Rica: Editorial Área de Innovación y Desarrollo, S.L., 2021.

[15] E. Camargo y M. Rinconc, “La importancia de la seguridad de la información en el sector público en Colombia,” *Revista Ibérica de Sistemas y Tecnologías de Información*, enero-abril, 2022. doi: 10.17013/risti.46.87–99

[16] M. Di Luca, “Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso,” *Avances - Centro de Información y Gestión Tecnológica*, vol. 21, no. 2, pp. 248-263, abril-junio, 2019. [en línea]. Disponible en: http://www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/440/1426

[17] G. Escrivá, R. Romero, D. Ramada y R. Onrubia, *Seguridad informática*, España: Macmillan Profesional, 2013.

[18] I. Coronel, D. Quirumbay, “Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web,” *Revista Científica Y Tecnológica UPSE*, vol. 9, no. 2, pp. 97-109, diciembre, 2022. doi: https://doi.org/10.26423/rctu.v9i2.672

[19] E. Samaniego, J. Ponce, *Fundamentos de seguridad informática*. Ecuador: Editorial Grupo Compás, 2021.

[20] A. Arreola, *Ciberseguridad ¿Por qué es importante para todos?*, México: Siglo XXI Editores México, 2019.

[21] J. Candau, “Ciberseguridad. Evolución y tendencias,” *Boletín ieee bie3*, n. 23, pp. 460-494, noviembre, 2021.

[22] M. Jiménez, (2023, jul. 26). “Diferencias entre seguridad de la información y ciberseguridad”. [en línea]. Disponible en: https://www.piranirisk.com/es/blog/diferencias-entre-seguridad-informacion-y-ciberseguridad [Consultado: mayo 01, 2024]

[23] Universidad Francisco de Vitoria, (2023, ago. 22). “¿Qué diferencia hay entre seguridad informática y ciberseguridad?”. [en línea]. Disponible en: https://www.ufv.es/que-diferencia-hay-entre-seguridad-informatica-y-ciberseguridad-preguntas-grados/ [Consultado: mayo 01, 2024]

[24] J. Figueroa, R. Rodríguez, C. Bone y J. Saltos, “La seguridad informática y la seguridad de la información,” *Polo del Conocimiento*, vol. 2, no. 12, pp. 145-155, diciembre, 2017. doi: 10.23857/pc.v2i12.420

[25] M. Sánchez, (2016, ene. 14). “Perfilado de Activos de Información”. [en línea]. Disponible en: https://technologyincontrol2.wordpress.com/2016/01/14/perfilado-de-activos-de-informacion/ [Consultado: mayo 01, 2024]

[26] UNIR, (2021, mar. 31). “Confidencialidad en seguridad informática: claves para garantizarla”. [en línea]. Disponible en:

https://www.unir.net/ingenieria/revista/confidencialidad-seguridad-informatica/ [Consultado: mayo 01, 2024]

[27] Organización de los Estados Americanos. Departamento de Derecho Internacional. Secretaría de Asuntos Jurídicos, *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. Washington DC: Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la OEA. 2022.

[28] J. Solleiro, R. Castañón, Á. Guillén, T. Hernández y N. Solís, *Vigilancia tecnológica en CIBERSEGURIDAD*. México: Universidad Nacional Autónoma de México, 2022.

[29] M. Bermúdez, *Integridad de los datos*. Costa Rica: Universidad San Marcos, 2020.

[30] Comillas Universidad Pontificia, (2023, may. 8). "Confidencialidad, Integridad y Disponibilidad". [en línea]. Disponible en: https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/ [Consultado: mayo 01, 2024]

[31] UNIR, (2021, mar. 03). "Disponibilidad en seguridad informática: ¿en qué consiste este término?". [en línea]. Disponible en: https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/ [Consultado: mayo 01, 2024]

[32] C. Martín, (2023, sept. 25). "Estándares y normas ISO para mejorar la ciberseguridad". [en línea]. Disponible en: https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/ [Consultado: mayo 01, 2024]

[33] Becolve Digital, (2021, jul. 29). "Estándares de ciberseguridad. Qué son y para qué sirven". [en línea]. Disponible en: https://becolve.com/blog/estandares-de-ciberseguridad-que-son-y-para-que-sirven/ [Consultado: mayo 01, 2024]

[34] Universidad EAFIT, *NORMAS ISO Y SU COBERTURA*, Colombia: Universidad EAFIT, 2016.

[35] ISO, (s.f). "Sobre nosotros". [en línea]. Disponible en: https://www.iso.org/es/sobre [Consultado: mayo 01, 2024]

[36] IEC, *Bienvenidos a IEC*, Suiza: IEC, 2016.

[37] Servicio de Acreditación Ecuatoriano, (2017, jun. 27). "Sobre la Comisión Electrotécnica Internacional (IEC)". [en línea]. Disponible en: https://www.acreditacion.gob.ec/sobre-iec/ [Consultado: mayo 01, 2024]

[38] P. Castillo, "Propuesta de Implementación de la Norma ISO 27001:2005 Grupo PCDATA TECHNOLOGIES en la ciudad de Santo Domingo 2013," Tesis, Escuela de Graduados, Universidad APEC, Santo Domingo, República Dominicana, 2013.

[39] S. Bortnik, (2010, abr. 10). “La serie de normas ISO 27000”. [en línea]. Disponible en: https://www.welivesecurity.com/la-es/2010/04/16/la-serie-de-normas-iso-27000/ [Consultado: mayo 01, 2024]
[40] V. Camacho, “Diseño de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001:2013, para una fábrica de cuero y calzado,” Tesis, Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, Quito, Ecuador, 2021.
[41] C. Alonso, (2023, sept. 27). “ISO 27000 y el conjunto de estándares de Seguridad de la Información”. [en línea]. Disponible en: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/ [Consultado: mayo 01, 2024]
[42] M. Orellana, “Elaboración de una guía de implementación de un SGSI para la corporación ecuatoriana para el desarrollo de la investigación y la academia – CEDIA,” Tesis, Carrera de Ingeniería de Sistemas, Universidad Politécnica Salesiana, Cuenca, Ecuador, 2022.
[43] Colegio Oficial Ingenieros de Telecomunicación, “Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001,” Madrid, España.
[44] ISO/IEC 27000:2018, “Information technology - Security techniques - Information security management systems - Overview and vocabulary”, Geneva, Suiza, 2018.
[45] J. Russell, “ISO 27001:2013 Guía de Implantación para la Seguridad de la Información”, Londres, Inglaterra, 2018.
[46] Advisera, (s.f). “¿Qué es norma ISO 27001?”. [en línea]. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/ [Consultado: mayo 01, 2024]
[47] ISO, (s.f). “¿Qué es la norma ISO/IEC 27001?”. [en línea]. Disponible en: https://www.iso.org/es/contents/data/standard/08/28/82875.html [Consultado: mayo 01, 2024]
[48] CTMA Consultores, (2021, oct. 13). “¿Cuál es el objetivo de la norma ISO 27001?”. [en línea]. Disponible en: https://ctmaconsultores.com/objetivo-de-la-norma-iso-27001/ [Consultado: mayo 01, 2024]
[49] GlobalSuite Solutions, (2023, sept. 22). “¿Qué es la norma ISO 27001 y para qué sirve?”. [en línea]. Disponible en: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/ [Consultado: mayo 01, 2024]
[50] L. Huamani, *Programa de Estudio de Computación e Informática*, Perú: Instituto Superior Tecnológico Público Julio Cesar Tello, 2023.
[51] M. Cruz y S. Fukusaki, “Diseño e implementación de un Sistema de Gestión de Seguridad de la Información para proteger los activos de información de la clínica

Medcam Perú SAC. 2017," Tesis, Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Computación y Sistemas, Lima, Perú, 2017.
[52] K. Moron, "Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C," Tesis, Universidad Señor de Sipán, Pimentel, Perú, 2023.
[53] C. Torres, "Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer s.a.," Tesis, Universidad Técnica de Ambato, Ambato, Ecuador, 2020.
[54] Y. Andrade, (2016, abr. 18). "Entendiendo el SGSI," Universidad Piloto de Colombia. [en línea]. Disponible en: https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2748/Trabajo%20de%20grado2987.pdf?sequence=1&isAllowed=y [Consultado: mayo 01, 2024]
[55] Universidad de Concepción, "Aplicación del ciclo de Deming o PDCA para la Gestión de la Calidad en la Educación Superior: Una Introducción.", Concepción, Chile, 2020.
[56] Gobierno Electrónico, (s.f). "Ciclo de Deming (PDCA)". [en línea]. Disponible en: https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/ [Consultado: mayo 01, 2024]
[57] Escuela Europea de Excelencia, (2020, jul. 28). "¿En qué consiste el ciclo PDCA para la mejora continua?". [en línea]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2020/07/en-que-consiste-el-ciclo-pdca-para-la-mejora-continua/ [Consultado: mayo 01, 2024]
[58] Escuela Europea de Excelencia, (2022, dic. 14). "Qué es la gestión de riesgos de TI y qué competencias requiere". [en línea]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2022/12/que-es-la-gestion-de-riesgos-de-ti-y-que-competencias-requiere/ [Consultado: mayo 01, 2024]
[59] J. Ramírez, "Marco de Gestión de Riesgos de Tecnologías de Información y Comunicación en un entorno multi empresarial, basado en análisis de datos de seguridad (logs) para la empresa CasaLuker S.A," Tesis, Facultad de Administración, Departamento de informatica y Computación, Universidad Nacional de Colombia, Manizales, Colombia, 2021.
[60] R. Naveiro y D. Ríos., *Análisis de riesgos*, España: Los Libros de La Catarata, 2022.
[61] Centro Criptológico Nacional (CCN), *MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1: Marco general. Ministerio de Asuntos Económicos y Transformación Digital*, España: Gobierno de España, 2012.

[62] ISOTools, (s.f). “4 opciones de mitigación en el tratamiento de riesgos según ISO 27001”. [en línea]. Disponible en: https://www.isotools.us/2017/08/20/4-opciones-mitigacion-tratamiento-riesgos-segun-iso-27001/ [Consultado: mayo 01, 2024]
[63] N. Alvear y S. Plaza, “Control de riesgos en el departamento de servicio técnico de la empresa Servindurama en la ciudad de Cuenca,” Tesis, Universidad de Cuenca, Cuenca, Ecuador, 2011.

11 Anexos

Anexo 1: Entrevista inicial al Ing. Juan Carlos Riofrío, Mg.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 2: Actas de reunión con el Ing. Juan Carlos Riofrío, Mg, para determinar el estado de la seguridad de la información en la DTI.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1U807XPGN90V_NLQ1HGiHSUHWBqLm9sI6?usp=sharing

Anexo 3: Acta de reunión con el Ing. Juan Carlos Riofrío, Mg, para evaluar la eficacia de las políticas de seguridad de la información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1awkjiqs1tsfGpyXNRx51z4VrBDH3NIVZ?usp=sharing

Anexo 4: Acta de reunión con el Ing. Juan Carlos Riofrío, Mg, para evaluar el nivel de madurez de la DTI posterior a la propuesta del SGSI.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1krUsSiy8iAgZPRJ8Kt0omWLSdV9_Ulvf?usp=sharing

Anexo 5: Acta de entrega y aceptación de la documentación del SGIS al Ing. Juan Carlos Riofrío, Mg.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/14m2X3kvKQOxFBmoV3H_G6WzblJnL24Ff?usp=sharing

Anexo 6: Reglamento Orgánico de Gestión Organizacional por Procesos de la Universidad Nacional de Loja.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1NTSyhjNSGdoIymFuqcpf3BEkQ7hkbik2?usp=drive_link

Anexo 7: Manuales de puestos de carrera – LOSEP.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1zDONqQyKcj3eAQBER3jp3T9rJfX_kmbt?usp=drive_link

Anexo 8: Políticas de Telecomunicaciones, Desarrollo de Software y Redes de la Universidad Nacional de Loja.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1pbERMLf0lpohX6sYN0AGKhPH_Ig_86ql?usp=drive_link

Anexo 9: Informe sobre el estado de la seguridad de la información en la Dirección de Tecnologías de Información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1uVg3wsksJeQNd_Zb57pMZ-eeb7YhtanA?usp=drive_link

Anexo 10: Informe sobre las necesidades y expectativas de las partes interesadas en el SGSI.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1q90BkOplHmVJACt-gUI7jnS3JK2E1n3v?usp=drive_link

Anexo 11: Documento sobre el Alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 12: Política de seguridad de la información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1v_qhUpoDSSwPVp9GX-lEgx1DUWSRbAKY?usp=drive_link

Anexo 13: Inventario de activos.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 14: Metodología de evaluación y tratamiento de riesgos.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 15: Informe de la situación actual de la DTI.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1-ewk6g-7WgbhVUb9M1hQQuxINMuX3YG4?usp=sharing

Anexo 16: Declaración de aplicabilidad.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1hZ1Lq-WE0CbWGf6QzZY9SbljDgy2G59n?usp=sharing

Anexo 17: Informe sobre la evaluación y tratamiento de riesgos.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1--gimvWLfkS_bMC5hA55m89ECaaqVlsS?usp=drive_link

Anexo 18: Plan de tratamiento de riesgo.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1fWiWbARCaBlcBu32Q_Si0kWdX2eKyQG5?usp=drive_link

Anexo 19: Política de roles y responsabilidades de seguridad.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/14rdX3QwjVKmlcKNkAr7FjKLLC2qAXSI3?usp=drive_link

Anexo 20: Política sobre dispositivos móviles y teletrabajo.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1U61U3GLEEN7Eb54RXrvKqF32_gXr7zFg?usp=drive_link

Anexo 21: Política trae tu propio dispositivo (BYOD).

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/18oJiUlBXzCCSmE_BcDkliEi-_VOH0mWT?usp=drive_link

Anexo 22: Política de uso aceptable.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1RRzRe7DIOdmV7nFhiQwJUlq7coMhc-BC?usp=sharing

Anexo 23: Política de seguridad para proveedores.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1seinGNLj46ZMupbm1Urf-MBnND9txqmG?usp=sharing

Anexo 24: Procedimiento para la gestión de incidentes.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/17dISkbHQB22WzYk4tDQxvTXx5MySVCQU?usp=drive_link

Anexo 25: Política de clasificación de la información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1_Uu5ZmmKzvDZNxNrW_TrAEqTMgEvgXxm?usp=drive_link

Anexo 26: Política de eliminación y destrucción.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1Hy4h_JmpVwU2hqto8NaqLEFaR_ax_-Du?usp=drive_link

Anexo 27: Procedimientos operativos para tecnología de la información (TI) y la comunicación.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1rf2SdYEHkqNBKwA-LcCEbELmFEL-E4Jj?usp=drive_link

Anexo 28: Política de control de acceso.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1rhBDMZLdA6swOcxhPl20ie5WWhRTe11s?usp=drive_link

Anexo 29: Política del uso de controles criptográficos.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 30: Política de seguridad física y ambiental.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1XpeF5fmIcTyg2YlO8KEMhU8hBD8FHTIJ?usp=drive_link

Anexo 31: Política de pantalla y escritorio limpio.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1lcvI_zUHwf5JlWSSUP_FNp4InrVPkvrn?usp=drive_link

Anexo 32: Política de gestión de cambios.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1yt0zkmtbT1KwKsIqmWOeUGXrTb9IX9BE?usp=drive_link

Anexo 33: Política de desarrollo seguro.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1OyZSEqj0lPkxIUaNMCaHJXRwJ4N2zegG?usp=drive_link

Anexo 34: Política de creación de copias de seguridad.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1T2xrcePU1vFrRoZW4EFszgvfGzaVovZR?usp=drive_link

Anexo 35: Política de gestión de registros y eventos de seguridad.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1nDMXJfhJMIJP36OXoawrSchHONhbELME?usp=drive_link

Anexo 36: Política de transferencia de la información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1HQoDnn22eAp8mcOwtF_tIcYI0i42CcHl?usp=drive_link

Anexo 37: Política de la continuidad del negocio.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 38: Política de cumplimiento legal, regulatorio y contractual.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1MsQ00z3ohXXQjE_3__tE_kSp-QJfJVK1?usp=drive_link

Anexo 39: Política de revisión y cumplimiento de la seguridad de la información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1QIGCP5XpVw5IF8xDmqKE3HFxgtF_3p-O?usp=drive_link

Anexo 40: Políticas de la DTI.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1rKBD6SEi6WkbgElPxWfR5C0uFRSESzZ9?usp=drive_link

Anexo 41: Informe de casos de pruebas.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 42: Informe sobre la reevaluación del nivel de madurez en la Dirección de Tecnologías de Información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1UrBaFf33ZEGUiHHzzxhooUwuuAT7T4Hb?usp=drive_link

Anexo 43: Certificado de la Dirección de Tecnologías de Información.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1pOlDa85fooIwoG6bhBfYvaRDJctTCZ22?usp=drive_link

Anexo 44: Evidencias de la presentación de los resultados del TIC en la Dirección de Tecnologías de Información.

Documento confidencial: Uso exclusivo de la DTI.

Este documento está protegido bajo la *Ley Orgánica de Protección de Datos Personales*, que regula la seguridad, prohibición y adecuado tratamiento de datos personales sensibles, conforme a lo dispuesto en el Capítulo IV (Categorías Especiales de Datos, Artículo 26), Capítulo VI (Seguridad de Datos Personales, Artículo 37) y Capítulo VII (Del Responsable, Encargo y Delegado de Protección de Datos Personales, Artículo 47). Asimismo, su manejo está sujeto al *Acuerdo de Confidencialidad de No Divulgación* firmado en la DTI, que estipula que toda información clasificada como confidencial es propiedad exclusiva de la Universidad y de la DTI, y debe ser

resguardada y no divulgada por ningún medio. El acceso y tratamiento de este contenido es estrictamente limitado a personal autorizado.

Anexo 45: Certificado de traducción del resumen en inglés.

Ingrese al siguiente enlace para visualizar el Anexo: https://drive.google.com/drive/folders/1oMdOZgPj_ES7t_07gbIIv4lmhPW4nBjS?usp=sharing