UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERIA
CARRERA DE TELECOMUNICACIONES

Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000:2022 mediante el tratamiento de riesgos para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para mejorar el esquema de información.

Trabajo de Titulación para optar al título de:
Ingeniero en Telecomunicaciones

Autor:
Pilatuña Flores Ángeles María

Tutor:
Mgs. Santillán Valdiviezo Luis Gonzalo

Riobamba, Ecuador. 2025

DECLARATORIA DE AUTORÍA

Yo, **Ángeles María Pilatuña Flores**, con cédula de ciudadanía **060498262-9**, autora del trabajo de investigación titulado: **Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000-2022 mediante el tratamiento de riesgos para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para mejorar el esquema de información**, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 13 mayo de 2025.

Ángeles María Pilatuña Flores

C.I:060498262-9

ACTA FAVORABLE - INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN

En la Ciudad de Riobamba, a los 15 días del mes de mayo de 2025, luego de haber revisado el Informe Final del Trabajo de Investigación presentado por la estudiante **Ángeles María Pilatuña Flores** con CC: **060498262-9** de la carrera **Ingeniería en Telecomunicaciones** y dando cumplimiento a los criterios metodológicos exigidos, se emite el **ACTA FAVORABLE DEL INFORME FINAL DEL TRABAJO DE INVESTIGACIÓN** titulado **"Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000:2022 mediante el tratamiento de riesgos para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para mejorar el esquema de información"**, por lo tanto se autoriza la presentación del mismo para los trámites pertinentes.

Firmado electrónicamente por:
LUIS GONZALO SANTILLAN VALDIVIEZO
Validar únicamente con FirmaEC

Mgs. Luis Gonzalo Santillán Valdiviezo
TUTOR

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000-2022 mediante el tratamiento de riesgos para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para mejorar el esquema de información,** por **Ángeles María Pilatuña Flores,** con cédula de identidad número **060498262-9**, bajo la tutoría de **Mgs. Luis Gonzalo Santillán Valdiviezo;** certificamos que recomendamos la **APROBACIÓN** de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.

De conformidad a la normativa aplicable firmamos, en Riobamba 13 de junio de 2025

Alejandra Pozo, Mgs.
PRESIDENTE DEL TRIBUNAL DE GRADO

Antonio Meneses, PhD.
MIEMBRO DEL TRIBUNAL DE GRADO

José Jinez, Mgs.
MIEMBRO DEL TRIBUNAL DE GRADO

CERTIFICACIÓN

Que, **Pilatuña Flores Ángeles María** con CC: **0604982629**, estudiante de la Carrera **Telecomunicaciones**, Facultad de **Ingeniería**; ha trabajado bajo mi tutoría el trabajo de investigación titulado **" Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000:2022 mediante el tratamiento de riesgos para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para mejorar el esquema de información.**", cumple con el **2 %,** de acuerdo al reporte del sistema antiplagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 2 de junio de 2025

Firmado electrónicamente por:
LUIS GONZALO SANTILLAN VALDIVIEZO
Validar únicamente con FirmaEC

Mgs. Luis Santillán Valdiviezo.
TUTOR

DEDICATORIA

A mis seres queridos,

Carlos Pilatuña y María Flores, por ser mi primer amor, por su apoyo incondicional, por los sacrificios que hicieron para que llegara hasta aquí y por creer en mí incluso en los momentos más difíciles, cada logro mío lleva su esfuerzo.

A mis hermanos, mis cómplices de vida, mis críticos más honestos, por recordarme que, al final, la familia es el mejor refugio.

A Pablito y Paolita que sin compartir lazos de sangre han sido familia del alma, gracias por las risas, los silencios compartidos, los consejos sabios y el hombro firme, ustedes son hogar, abrigo y fuerza.

Esta meta también les pertenece.

A mis amigos,

El lujo que elegí, gracias por las risas compartidas, momentos únicos, gracias por hacer de esta trayectoria una aventura inolvidable. (G.A.J.J.J.K)

Con todo mi corazón,

Angie

AGRADECIMIENTO

Antes que todo, doy gracias a Dios por permitirme llegar hasta este punto de mi vida, por cada oportunidad que me brinda, por los desafíos que fortalecen mi espíritu y cada sorpresa que da sentido a mi camino.

Agradezco a la Universidad Nacional de Chimborazo, por dejarme ser parte de esta prestigiosa comunidad estudiantil.

A todos mis profesores, por su paciencia, dedicación y valiosas enseñanzas. En particular, quiero destacar al máster Luis Santillán, tutor de mi proyecto de investigación, con sus consejos y críticas constructivas que fueron fundamentales para dar forma a este trabajo.

Al máster Diego Caiza, por su tiempo y aportes que enriquecieron esta investigación.

A Fabian Noriega, por estar presente, por su apoyo sincero y por ser una parte valiosa de mi vida.

Con cariño, Angie

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

RESUMEN

La seguridad de la información es considerada unos de los pilares fundamentales dentro del desarrollo tecnológico, por ende, el objetivo de la presente investigación fue realizar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27000:2022 para la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo (UNACH). La propuesta está basada en el análisis de tratamiento de riesgos, para mejorar el esquema de información, garantizando la integridad de la institución.

El análisis de riesgos en la DTIC, presenta riesgos bajos, medios y altos, estos últimos se les dará un proceso de tratamiento para mitigar su nivel de riesgo, es por ello que se utilizó una metodología exploratoria y experimental, facilitando la identificación de factores esenciales de cada activo, permitiendo la manipulación de variables.

Para contribuir con la seguridad de la información en la DTIC, se elaboró un plan de tratamiento de riesgos basado en la Norma Internacional ISO 27000:2022, enfocándose principalmente en los controles y acciones de mejora pertinentes, buscando lograr la mitigación del nivel de riesgo de los activos a un nivel más aceptable.

Finalmente, tras una detallada evaluación posterior a la implementación del plan, se obtiene los primeros datos en los que se verifico que los riesgos altos fueron mitigados. De esta manera, la seguridad de la información en la DTIC de la UNACH se vería significativamente fortalecida, gracias a un sistema de protección más robusto y eficaz.

Palabras Clave: SGSI, Riesgo, Activo, Tratamiento, Seguridad.

ABSTRACT

Information security is considered one of the fundamental pillars within the technological development, therefore, the aim of this research was to develop an Information Security Management System (ISMS) based on the ISO 27000:2022 standard for the Dirección de Tecnologías de la Información y Comunicación (DTIC) of the Universidad Nacional de Chimborazo (UNACH). The proposal is based on the risk treatment analysis, to improve the information scheme, guaranteeing the integrity of the institution.

The risk analysis in the DTIC, presents low, medium and high risks, the latter will be given a treatment process to mitigate their level of risk, that is why an exploratory and experimental methodology was used, facilitating the identification of essential factors of each asset, allowing the manipulation of variables.

In order to contribute to information security in the DTIC, a risk treatment plan was developed based on the International Standard ISO 27000:2022, focusing mainly on the relevant controls and improvement actions, seeking to mitigate the risk level of the assets to a more acceptable level.

Finally, after a detailed evaluation after the implementation of the plan, first data were obtained, in which, it was verified that the high risks were mitigated. In this way, the information security in the DTIC of the UNACH would be significantly strengthened, thanks to a more robust and effective protection system.

Keywords: ISMS, Risk, Asset, Treatment, Security.

Reviewed by:
Mgs. Edison Salazar Calderón
ENGLISH PROFESSOR
I.D. 0603184698

CAPÍTULO I

1.1 INTRODUCCIÓN

En la actualidad, todas las organizaciones gestionan información confidencial, la cual constituye uno de sus principales activos. Con el creciente número de amenazas a las que se enfrentan diariamente, resulta imperativo que cada entidad adopte las medidas necesarias para salvaguardarse ante ataques a la seguridad de la información [1]. Ante esta situación, según el estándar internacional, la norma ISO 27000:2022 proporciona un marco sólido para implementaciones.

Los centros académicos en el presente periodo de digitalización, por la intensa variedad de información que recogen, pero también por la gama de tipos de datos que maneja, están obligadas a enfrentarse a necesidades realmente importantes para la gestión de la información. Para que ello sea posible, garantizando la integridad, la confidencialidad y la disponibilidad de la información obtenida y para que de esta manera se cumpla con el marco de regulaciones en relación a la privacidad y protección, para las universidades es necesario contar con un SGSI.

Por lo tanto, el objetivo principal de este trabajo es evaluar el estado del sistema de la información mediante el tratamiento de riesgos para la DTIC de la Universidad Nacional de Chimborazo, basado en la norma ISO 27000:2022 para establecer el esquema del SGSI [2]. Esto quiere decir que realizar un análisis de riesgos en la DTIC, es un proceso importante para diagnosticar, evaluar y entender los riesgos en relación con estos activos. Una vez se ha realizado el diagnóstico de riesgos en el SGI, es necesario propuesta de acciones específicas para gestionarlos y mitigarlos.

Así, se procederá a la evaluación de aquellos riesgos, pero dándoles importancia en función del potencial que estos tienen en la seguridad de la información. A partir de estos planteamientos de realiza un plan que contemple la puesta en práctica de los controles designados con cada riesgo que habremos determinado.

Además, las políticas y los procedimientos se modificarán y actualizarán para tener en cuenta los cambios resultantes del diagnóstico [1], [3]. Es esencial que el SGSI en la universidad enfatice los beneficios concretos y la mejora en la preparación de la universidad para abordar los desafíos del entorno de seguridad de la información. Además, debe establecer una base sólida para los futuros esfuerzo de seguridad.

1.2 ANTECEDENTES

En el año de 1995, el instituto Británico de Normas (BSI) publico la norma BS 7799, la cual es conocida como una de las primeras directrices que tratan de forma holística la administración de la seguridad. Este esquema planteo los cimientos para los fundamentos de la seguridad de la información, que incluyen la privacidad, la integridad y a la disponibilidad [4].

La norma BS 7799 de BSI se divide en dos partes 7799-1 siendo una guía de buenas prácticas cuya realidad es que el programa de certificación no está establecido y la segunda parte 7799-2 se anunció por primera vez en 1998, estableciendo los requisitos del sistema de seguridad de las dos partes de la norma se revisaron en 1999 y se adoptó la primera parte por ISO, sin cambios sustanciales y en 2002 la segunda parte se revisó para adecuarse a la filosofía de normas ISO de sistemas de gestión. información (SGSI) para ser certificable por una entidad independiente [5].

En 2005, tanto ISO como IEC implementaron oficialmente la serie ISO/IEC 27000, mediante la emisión de ISO/IEC 27001, que define las condiciones para un SGSI. Esta regla es esencial para las entidades, dado que proporciona un esquema exhaustivo para salvar la información y minimizar los peligros [6].

Freddy Reyes en el año 2012 propone una técnica para implementar de un Sistema de Gestión de la Información SGSI conforme a la norma ISO 27001. Esta diseñado específicamente para laboratorios de análisis microbiológicos, con la finalidad de asegurar la protección y privacidad de la información vital gestionada en estos ambientes [7].

SALCEDO explica las metas, el ámbito de aplicación, la expectativa del SGSI y la metodología vinculada a la definición, organización, reconocimiento y desarrollo del modelo de negocios. Seguridad de los datos para la entidad ISAGXXX, fundamentada en la norma ISO 27001:2013; comenzando desde la comprensión de la organización desde el punto de vista de los individuos, procedimientos vitales en el funcionamiento de la energía, realización del análisis de seguridad de la misma, información reconocimiento de las principales vulnerabilidades y amenazas, implementando una estrategia de metodología de gestión de riesgos para la gestión de riesgos de seguridad en el ámbito de la información, diseño de los planos para la gestión y creación del marco normativo del sistema de administración de protección de datos para ISAGXXX [8].

Arana [9], El propósito principal de este estudio es instaurar el sistema de administración de seguridad de la información conforme a la norma ISO 27001:2013 en la compañía Core

Business Corp. SAC con el fin de salvar la información en los procesos de operación. Además, se emplearon métodos de observación y revisión documentada. El instrumento empleado fue la lista de verificación para verificar el acatamiento de la norma ISO 27001:2013 y la matriz de consistencia. Además, se utilizaron las herramientas del diagrama de Gantt y la matriz de riesgos con el propósito de cumplir con los objetivos de este estudio. La técnica empleada fue el ciclo PHVA y MAGERIT, lo que facilitó la implementación. En consecuencia, en el análisis organizacional se logró un 38% de cumplimiento, continuando con la aplicación de la norma ISO 27001:2013, finalizando de esta manera con un 100%. Además, la relación entre el costo y el beneficio fue de 1.96, lo que indica que la implementación es lucrativa para Core Business. Para concluir, la implementación posibilita la protección de los activos de información a través de los controles establecidos al llevar a cabo el análisis de riesgos de Sistemas de Información [9].

En Ambato, Ecuador, en la empresa privada MEGAPROFER S.A, de la venta de productor ferreteros en todo el país, se detectaron dificultades en la administración de seguridad de la información y los activos. Es evidente la ausencia de políticas apropiadas, procedimientos y controles en los procesos. Como solución Christian Torres propone un plan para la seguridad de la información considerando la norma ISO 27001 que proteja la información y activos de la empresa MEGAPROFER S.A del año 2020, que se centra en los datos que gestiona la compañía, incluyendo las políticas de seguridad, sistemas de control de acceso, gestión de activos, protección de los recursos humanos, entre otros aspectos. A partir de esto, se sugieren nuevas políticas de seguridad consistentes y dentro de los límites de cumplimiento institucional, para la implementación y mejora que proporciona un SGSI, a través del proceso de mejora continua [10]

En la UNACH, en 2024, ocurrió una auditoría para la seguridad física en la Facultad de Ingeniería, basada en el Estándar 27001 según las instrucciones. El análisis incluyo el estudio de las directrices de entrada, las normativas de observación y las estrategias de respuesta ante sucesos. Diversos problemas críticos requieren rectificación para cumplir con las normas de seguridad definidas por ISO 27001. Atendiendo a los resultados de las evidencias, se presenta una propuesta de un plan de contingencia que ofrece propuestas claras, donde las alternativas corresponden a acciones tales como la mejora de los sistemas de ingreso, la realización de controles periódicos sistemáticos de seguridad y la elaboración de talleres de capacitación para los trabajadores. Estas estrategias se elaboran para atacar los riesgos,

resguardar la información y proteger la vulnerabilidad de la Universidad Nacional de Chimborazo [11].

1.3 PLANTEAMIENTO DEL PROBLEMA

El manejo adecuado de los riesgos que ponen en peligro la seguridad de sus activos de la información es una preocupación principal para la DTIC de la UNACH. Esto incluye problemas como la seguridad física, la gestión ineficaz y las amenazas de ciberseguridad, que pueden dañar la integridad, la confidencialidad y la disponibilidad de los datos alojados en sus sistemas informáticos, los mismos que pertenecen a estudiantes, profesores y personal administrativo.

Acorde a la alerta por parte de la Unidad de Comunicaciones Institucionales de la UNACH el pasado 2 de diciembre de 2023, ha sido constatado el surgimiento de los correos electrónicos fraudulentos; esto supone una nueva y vigente fuente de preocupación dado que podría influir de forma negativa en la seguridad de la información, posicionándose como un medio del que valerse para suplantar a la universidad o engañar tanto a estudiantes como a personal, por lo cual la confianza en las comunicaciones oficiales se vería ampliamente afectada.

Como estrategia se plantea la mitigación de los riesgos identificados, proponiendo el desarrollo de un SGSI, el cual será conforme a lo establecido por la normativa ISO/IEC 27000:2022, ya que proporciona un marco estructurado que permitirá realizar la identificación y gestión de una forma proactiva de los riesgos inherentes a la seguridad de la información. La implementación de un SGSI, por lo tanto, permitirá que el DTIC sea capaz de anticiparse y de responder adecuadamente a las amenazas existentes, garantizándose la protección de los activos de la información de la UNACH.

Es fundamental que el SGSI se mantenga funcionando de forma efectiva en un entorno en el que las amenazas de ciberseguridad están cambiando constantemente. Para que la UNACH pueda desconectarse y hacerse cargo de forma adecuada de las nuevas vulnerabilidades y técnicas de ataque que puedan surgir en el futuro, la UNACH deberá implementar un proceso de mejora continua en el sistema de gestión de seguridad de la información que se base en la revisión de los incidentes de seguridad y las auditorías internas, externas, la actualización de las políticas y procedimientos. Esto garantiza que el sistema de gestión de seguridad de la información permanezca al tanto de los últimos avances y proporcione una conducción proactiva para la seguridad constantemente

1.4 JUSTIFICACIÓN

La DTIC de la UNACH deberá identificar los riesgos de activos de información y sus garantes, comprendiendo que todo es positivo para la DTIC, incluido el soporte físico (construcción o equipo), inteligencia o información (ideas, aplicaciones, proyectos) marca, reputación, etc. La finalidad de identificar cada activo es reconocer las vulnerabilidades, amenazas, riesgos de estos y así crear instrucciones específicas para proteger los mismos [2]. Por tal motivo, un SGSI basado en la norma ISO/IEC 27000 mediante el tratamiento de riesgos ayudará al DTIC a cumplir con requisitos legales y regulaciones relacionadas con la seguridad de la información. Permitiendo tomar decisiones informadas sobre la asignación de recursos para mitigar riesgos y reducir la probabilidad de incidentes de seguridad [3]. El planteamiento de un plan de mejora en la seguridad de la información para el DTIC es no solo viable, sino también esencial para mantener la seguridad y la eficiencia en un entorno tecnológico en constante cambio.

1.5 OBJETIVOS

1.5.1 Objetivo General

- Evaluar el estado del Sistema de la información mediante el tratamiento de riesgos para el DTIC de la Universidad Nacional de Chimborazo basado en la norma ISO 27000:2022 para la implementación del esquema del SGSI.

1.5.2 Objetivos Específicos

- Identificar los riesgos del área de Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para el desarrollo de la norma ISO 27000.
- Realizar un análisis de riesgos para la priorización de amenazas a la seguridad de la información de una manera sistemática mediante la documentación de resultados.
- Establecer un plan de tratamiento de riesgos y procedimientos de la seguridad de la información.
- Ejecutar una evaluación de las políticas y procedimientos implementados de la seguridad de información para la gestión de riesgos.

CAPÍTULO II

2. ESTADO DEL ARTE

ESET ha publicado un informe que indica un aumento del 60% en los ataques en Latinoamérica en 2018 en comparación con el 2017. Además, el informe indica que Ecuador es el país con mayor cantidad de empresas afectadas por phishing con un 20,9% y el país con el mayor índice de infecciones de ransomware con un 22%[12]. La norma ISO/IEC 27001 es un referente fundamental para la implementación de un SGSI. Autores como García Martínez, destacan la importancia de esta norma en la configuración de políticas y controles de seguridad[13].

Según las consideraciones el Modelo de un SGSI [14] que está basado en el estándar NTP ISO/IEC 27001:2014, un sistema de gestión de la información que incluye aspectos administrativos como la Dirección Ejecutiva de Difusión Estadística y la Dirección Ejecutiva de Producción Estadística se conforma utilizando el modelo PDCA y la metodología Magerit VS 3, el modelo PDCA o "Planificar-Hacer-Verificar-Actuar", consta de un conjunto de fases que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzada y el modelo Magerit está dirigido a los medios electrónicos, informáticos y telemáticos, hay que su uso en la actualidad es frecuente, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con preventivas para lograr tener confianza en utilizarlos.

En el trabajo de investigación de Lema Vinlasaca[15] se usó la aplicación llamada CRAMM V5.0, que es una herramienta desarrollada en 1978 por CCTA del gobierno de Reino Unido, evalúa los riesgos compatibles con la norma ISO 27001 enfocándose a la evaluación de impacto empresarial, identificación y evaluación de amenazas, en este caso de estudio sobre el cumplimiento del SGSI, se pudo evidenciar que los controles implementados para los riesgos, fueron mitigados dentro del periodo establecido dando resultados favorables a la organización. Siendo una metodología eficaz, eficiente y aceptable de las técnicas de la información a fin de garantizar que la organización siga sus principios.

El autor Guerra [16]presenta un análisis exhaustivo de los desafíos de seguridad y la gestión de riesgos en bibliotecas universitarias. Se revisan las amenazas específicas que enfrentan las bibliotecas en el entorno digital y se destacan las consecuencias potenciales de la perdida de información. Además, los métodos de identificación y análisis de riesgos se utilizan en contextos similares incluidos con énfasis en la capacidad de usar y la capacidad de ajustar

estos métodos en las bibliotecas universitarias. El autor también aborda las tendencias emergentes en seguridad de la información y presenta ejemplos de buenas prácticas en la implementación de sistemas de gestión de seguridad en bibliotecas universitarias.

Según la Escuela Europea de Excelencia [17], los protocolos de seguridad se revisan y actualizan con frecuencia. La última actualización de ISO 27001(ISO/IEC 27001:2022), una de las normas más importantes en cuanto a seguridad cibernética a nivel mundial, se presentó recientemente. Hay cinco características; dependiendo del tipo de control (prevención, detección, reparación), características de seguridad de la información (seguridad, integridad y usabilidad), conceptos de seguridad cibernética (identificación, protección, detección, reacción y recuperación), operativas (capacidad de seguridad de expertos o prácticas, como gestión o seguridad física) y también la gestión y ecosistemas). Además, el nuevo estándar reduce la cantidad de controles de seguridad a 93. De esta manera, se pueden identificar 8 controles humanos 14 controles físicos y 34 controles tecnológicos.

2.1 MARCO TEORICO

2.1.1 SISTEMA DE GESTIÓN DE LA INFORMACIÓN (SGSI)

El SGSI incluye una colección de políticas, procedimientos y reglas de liderazgo junto con recursos y actividades apropiadas que juntos administran la organización, para buscar sus principales recursos de información. El SGSI desde la visión de ISO/IEC 27001 es sistemático para crear, implementar, servicios, supervisión, revisión, mantenimiento y mejora de la seguridad de la información de la organización y lograr sus objetivos comerciales y/o mantenimiento comercial [18].

2.1.2 ESTRUCTURA DE UN SGSI V.2022

1. **Alcance:** Indica las limitaciones y el uso del sistema en la organización, creando campos, procesos, recursos y tecnología.
2. **Referencias Normativas:** ISO/IEC 27000
3. **Términos y Definiciones:** A los efectos de este documento, se aplican los términos y definiciones proporcionados en ISO/IEC27000.
4. C**ontexto de la organización:** Determinar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados esperados de un SGSI.
    - Comprender las necesidades y expectativas de las partes interesadas.

- Determinación del alcance del SGSI

5. **Liderazgo:** la alta dirección deberá demostrar liderazgo y compromiso con respecto al SGSI mediante:
    - Políticas
    - Funciones, responsabilidades y autoridades de la organización.
6. **Planificación:** La organización debe considerar los problemas mencionados en (4) y sus requisitos, determinar los riesgos y oportunidades que deben abordarse para:
    - Evaluación de riesgos de seguridad de la información.
    - Manejo de riesgos relacionados a la seguridad de la información.
    - Objetivos de seguridad y planificación para lograrlos.
    - Planificación de cambios.
7. **Soporte:** La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación y mantenimiento del SGSI.
8. **Operación:** La organización realiza acciones de planificación, implementación y control de procesos necesarios para cumplir los requisitos e implementar las acciones determinada en la cláusula (6).
9. **Evaluación del desempeño:** La organización determinara los métodos de seguimiento, medición, análisis y evaluación según corresponda para garantizar la valides de los resultados.
10. **Mejora:** La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del SGSI [19].

2.1.3 NORMA ISO 27000

La norma ISO 27000 es un conjunto de estándares creados para proteger los recursos de información de las organizaciones. La norma ISO 27000 también define y describe la colección de procesos organizados adecuadamente a las organizaciones para obedecer sus objetivos y metas comerciales con seguridad de la información. Esto muestra cómo las organizaciones de control de seguridad de la información, desde la construcción hasta la implementación, la supervisión, la reparación, la evaluación y el mantenimiento, protegen los recursos de información [20].

2.1.4 NORMA ISO 27001:2022

La ISO 27001:2022 se presenta como la normativa internacional para los sistemas SGSI para proporcionar privacidad, integridad y disponibilidad continua de la información, así como cumplimiento legal [21]. Esta norma no solo es aplicable a organizaciones de cualquier tamaño y sector, sino que también puede adaptarse a sus necesidades específicas y requisitos comerciales. Al seguir los principios y directrices establecidas en la ISO 27001, las instituciones pueden asegurar la información, mejorar la confianza de los clientes y partes interesadas, manteniéndose a la vanguardia en un entorno empresarial cada vez más digital y globalizado.

2.1.5 CAMBIOS DE VERSIONES DE LA ISO 27001

Esta versión ISO es un cambio importante en cantidad y método para clasificar el control de seguridad, además de revisar las regulaciones para determinar los requisitos de configuración, implementación, servicio, monitoreo, revisión, mantenimiento y mejora de SGSI.

Ilustración 1:Controles de seguridad en las versiones de ISO/IEC 27001
Fuente: [3]

- Los problemas relacionados con el método de clasificación del control de seguridad se pueden encontrar 4 temas o formas de clasificación: controlar a las personas, físico, tecnología y organización.
- Existen cinto tipos de atributos: basado en el tipo de control, propiedades de seguridad de la información, conceptos de ciberseguridad, capacidades operativas y dominios de seguridad.
- Además, los nuevos estándares reducen el número de factores de gestión de seguridad a 93. Por lo tanto, 8 factores de gestión para todos pueden identificar 14 controles físicos, 34 controles tecnológicos y 37 controles organizacionales [3]

2.1.6 CONTROLES PARA PERSONAS

Como se puede observar en [3] lo controles para personas son los siguientes:

- Selección
- Términos y condiciones de empleo.
- Concienciación, educación y formación en seguridad de la información.
- Proceso disciplinario.
- Obligaciones después de completar o cambiar de trabajo.
- Contratos de seguridad y no divulgación.
- Trabajo bajo modalidad remota.
- Informar eventos de seguridad de la información.

2.1.7 CONTROLES FÍSICOS

De la misma manera en [22]al hablar de los controles físicos tenemos los siguientes:

- Perímetros de seguridad física
- Entrada física
- Establecimiento de la seguridad en oficinas, instalaciones y despachos.
- Seguridad física
- Ante amenazas externas y ambientales establecer protecciones.
- Trabajo en áreas seguras
- Puesto de trabajo despejado y pantalla limpia
- Ubicación y protección de equipos
- Seguridad de los activos fuera de las instalaciones
- Medios de almacenamiento
- Servicios de soporte
- Seguridad del cableado
- Mantenimiento de equipo
- Eliminación segura o reutilización de equipos.

2.1.8 CONTROLES TECNOLÓGICOS

En cuanto a los controles tecnológicos presentes en [3] podemos nombrar los siguientes:

- Dispositivos de usuario final
- Derechos de acceso privilegiado

- Restricción de acceso a la información
- Acceso al código fuente
- Autenticación segura
- Gestión de la capacidad
- Protección contra malware
- Gestión de vulnerabilidades técnicas
- Gestión de la configuración
- Eliminación de información
- Enmascaramiento de datos
- Prevención de fuga de datos
- Copia de seguridad de la información
- Redundancia de las instalaciones de tratamiento de información
- Registro de eventos
- Actividades de monitoreo
- Sincronización del reloj
- Utilizar privilegios para programas
- Instalar software
- Seguridad de redes
- Seguridad de los servicios de red
- Separación en las redes
- Filtrado web
- Uso de criptografía
- Ciclo de vida de desarrollo seguro
- Cumplimiento de estándares de seguridad de aplicaciones
- Ingeniería y sistemas seguros
- Codificación oportuna con seguridad
- Desarrollo y aceptación en las pruebas de seguridad
- Subcontrato de desarrollo
- Desarrollo, prueba y producción de entornos
- Cambios gestionados
- Pruebas de información
- Auditoria en la protección de los sistemas de información

2.1.9 CONTROLES ORGANIZACIONALES

En [22] se puede identificar los siguientes controles organizacionales:

- Políticas orientadas a la seguridad de información
- La seguridad de la información debe tener funciones y responsabilidades
- Funciones segregadas
- Contacto permanente con autoridades
- Tener contacto en los grupos de interés
- Las amenazas deben ser tratadas con inteligencia
- La gestión de proyectos vinculada a la seguridad de la información
- Tener al día los inventarios relacionados con información y otros activos
- La información y activos deben ser utilizados de manera adecuada
- Retorno de activos
- Clasificación de información
- Etiquetado de información
- Transferencia de información
- Control de acceso
- Gestión de identidad información de autenticación.
- Información de autenticación.
- Derechos de acceso.
- Seguridad de la información en la relación con los proveedores.
- Acercamiento a la seguridad de la información en acuerdos con proveedores.
- La seguridad de la información debe estar acorde con la cadena de suministros ICT
- Los servicios del proveedor deben tener monitoreo, revisión y gestión
- Los servicios en la nube garantizados por la seguridad de la información
- Los accidentes de seguridad de la información deben ser tratados con planificación y preparación
- Los eventos de seguridad de la información deben someterse a evaluación y decisión
- Los accidentes de seguridad de información deben tener su respuesta
- Los incidentes de seguridad de información deben ser utilizados como aprendizaje
- Recolección de pruebas.
- Seguridad de la información durante interrupción.

- Preparación de ICT para continuidad de actividad
- Requisitos legales, reglamentarios y contractuales.
- Derechos de propiedad intelectual.
- Protección de registros.
- Privacidad y protección de PII
- Revisión independiente de seguridad de la información.
- Cumplimiento de políticas, reglas y normas se seguridad de la información.
- Procedimientos operativos documentados.

2.2 PRINCIPIOS DE SEGURIDAD DE LA INFORMACION

2.2.1 Confidencialidad

La información solo debe ser conocida por el personal autorizado que al requiera por el desarrollo de sus funciones [23]

2.2.2 Integridad

Es importante mencionar que la información siempre debe ser precisa y sin cambios, así como los procedimientos responsables de usarla. En cualquier caso, los datos no se pueden cambiar o sin el consentimiento de la empresa [24].

2.2.3 Disponibilidad

Es indiscutible que la información no debe estar disponible fácilmente, la disponibilidad va de acuerdo con su nivel de responsabilidad, permisos y autorización [14].

2.2.4 Amenaza

Una posible causa de un incidente no deseado puede dañar un sistema u organización [14].

2.2.5 Vulnerabilidad

Las amenazas pueden utilizar la debilidad de un activo [23]

2.3 CICLO DE VIDA DEL SGSI

El ciclo de Deming, también conocido como PDCA (Plan, Do, Check, Act), debe usarse para implantar el SGSI. Se trata de un sistema diseñado para mejorar continuamente la ejecución de procesos y la gestión.

- **Planificar (Plan).** Evaluar todas las amenazas y riesgos de información que surja en diferentes áreas de DTIC. Se deben instalar factores de gestión apropiados para medir los riesgos de datos en las corrientes internas y externas, y también deben establecer las políticas necesarias para cumplir con las medidas de seguridad [24]
- **Hacer (Do).** Para medir los riesgos, se implementa los controles apropiados en esta etapa. Para la detección y evaluación de riesgos y amenazas, se pone en marcha el SGSI en esta etapa [25].
- **Verifique (Check).** Esta etapa en la que se debe evaluar y revisar la eficacia y eficiencia. Se puede determinar si están alcanzando los objetivos mediante métricas asociadas a objetivos. Es la etapa en la que se encuentran los errores que deben corregirse[24]
- **Actuar (Act).** En esta última etapa, se realizan los cambios o correcciones del sistema necesarios para maximizar el rendimiento que se descubrieron en la etapa anterior de evaluación [24]

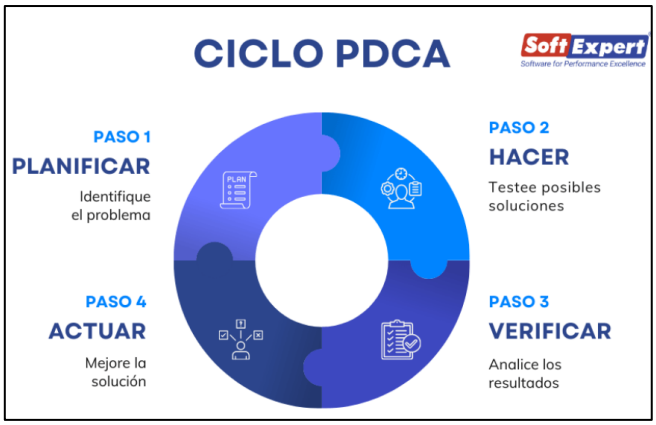


Ilustración 2: Ciclo PDCA
Fuente: [25]

CAPÍTULO III

3. Metodología

3.1 Tipo de estudio y metodología

Para el desarrollo del siguiente proyecto de investigación, se optó por un método exploratorio, con el objetivo de examinar y entender el estado actual del DTIC de la UNACH.

Como no se dispone de un SGSI oficialmente establecido, este análisis facilitará la identificación de factores esenciales, vulnerabilidades y peligros que impactan en la salvaguarda de la información institucional. Los hallazgos obtenidos ofrecerán una base sólida para posteriores estudios descriptivos o de aplicación que se concentren en el diseño e implementación de un SGSI de acuerdo con buenas prácticas y normas internacionales.

3.2 Métodos de Investigación

3.2.1 Investigación Experimental

La investigación experimental es un tipo de investigación científica que se caracteriza por manipular variables independientes para observar sus efectos sobre las variables dependientes, controlando otros factores que puedan en los resultados[26]. La investigación experimental implica la implementación de cambios controlados en el sistema con el propósito de evaluar su efectividad y rendimiento, una vez ya implementado el SGSI en el DTIC de la UNACH, dando como propósito un informe detallado de los cambios implementados y los resultados obtenidos.

3.2.2 Población

En la presente investigación la población está constituida por datos de la variable Nivel de riesgo. La población total se definirá considerando todas las categorías del riesgo, como la criticidad de los activos, nivel del riesgo, la frecuencia de acceso, la complejidad de los sistemas, entre otros. Esto dará una visión completa de la extensión del riesgo.

3.2.3 Muestra

La selección de la muestra se realiza de manera estratégica para obtener una visión precisa y representativa de la situación de seguridad de la información en la organización, siendo una parte de la población, evaluando una muestra de 70 riesgos de la DTIC de la UNACH.

3.3 Operación de variables

3.3.1 Variable Dependiente

Tabla 1: Variable Dependiente
Fuente: Autor

Variable Dependiente	Descripción	Evaluación
Nivel de riesgo.	Este componente evalúa las posibles consecuencias o daños que podrían surgir si un riesgo específico se materializa.	Una escala cualitativa

A continuación, se muestra en la tabla 2 con la evaluación de la variable nivel de riesgo.

Tabla 2: Descripción de Niveles de Riesgo
Fuente: Autor

NIVEL DE RIESGO	DESCRIPCION
BAJO	Se refiere a los riesgos cuya probabilidad de ocurrencia e impacto son poco elevadas. Por lo general, no representan una muy alta amenaza para la organización y puede continuar tolerándose y sin acciones inmediatas.
MEDIO	Se habla de riesgos de probabilidad de ocurrencia media, con un impacto medianamente afectando el correcto funcionamiento de los procedimientos institucionales o, por ejemplo, la seguridad de la información. Se requiere desplazarlos de manera planificada o, en caso de no ser controlados, pueden convertirse en amenazas críticas.
ALTO	Contiene riesgos de alta probabilidad y su impacto puede ser grave o muy grave para la organización, esto es información institucional muy importante, segura y disponible. Este tipo de riesgo requiere una intervención inmediata y un plan de prioridad para reducir su nivel a un tipo aceptable.

3.3.2 Variables Independientes

Tabla 3: Variables Independientes
Fuente: Autor

Variable Dependiente	Descripción	Evaluación
Impacto	Grado de daño o consecuencia que una	Variable cualitativa

	amenaza puede causar a un activo de información. El impacto depende de la confidencialidad, integridad, disponibilidad.	
Probabilidad de ocurrencia	Es la frecuencia con la que un riesgo puede ocurrir dentro de un periodo determinado	Variable cualitativa

En la tabla 4, se observa la evaluación de la Probabilidad de ocurrencia de un riesgo.

Tabla 4: Evaluación de la Variable Probabilidad de ocurrencia
Fuente: Autor

PROBABILIDAD DE OCURRENCIA		
CRITERIO	**VALOR**	**PERIODICIDAD**
IMPROBABLE	1	No ha sucedido
MEDIANAMENTE PROBABLE	2	Ha ocurrido o podría ocurrir en un periodo a largo plazo
MUY PROBABLE	3	Ha ocurrido o podría ocurrir en un periodo a corto plazo

3.4 Procedimiento y Análisis

3.4.1 Descripción del área de estudio

La Dirección de Tecnologías de la Información y Comunicación, forma una parte esencial de la Universidad Nacional de Chimborazo, supervisa la administración y la preservación del marco tecnológico y los mecanismos que ayudan a los deberes académicos[27].

La DTIC supervisa los datos sensibles y vitales ligados con los alumnos, educadores, personal administrativo, lo que lo convierte en un área crítica para salvaguardar, dar accesibilidad, brindar precisión y confidencialidad de los datos, en consecuencia, este estudio analiza la condición actual de la DTIC con respecto a la gestión de la seguridad de la información.

3.4.2 Situación Actual.

En esta etapa se recaba toda la información actual de la DTIC de la UNACH, para ello se empieza detallando la infraestructura de la DTIC, buscando analizar cada subproceso y sus respectivos activos.

Ilustración 3: Estructura de la DTIC, UNACH
Fuente: [28]

El estado actual del proceso del SGSI en la DTIC de la UNACH, nos basamos en la estructura de la ISO 27001, teniendo como resultado la siguiente evaluación de cada sección. En la ilustración 4, tenemos el estado actual de la sección 4 del estándar ISO 27001, en la Dirección de Tecnologías de la Información y Comunicación de la UNACH.

Estado de la implementación del SGSI en el DTIC

Sección	Requisito ISO/IEC 27001	Status	Notas
4	**Contexto de la organización**		
4,1	**Contexto organizacional**		
4,1	Determinar los **objetivos del SGSI** de la organización y cualquier cuestión que pueda comprometer su efectividad	Inexistente	Definir y acordar con todas las partes interesadas los objetivos del SGSI precautelando su eficacia durante la implementación.
4,2	**Partes interesadas**		
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	? Desconocido	Analizar e identificar los factores internos externos, así como las tendencias en el entorno de negocio que pueda influir en el programa.
4.2 (b)	Determinar sus requisitos relevantes al respecto de la seguridad de la información y sus obligaciones	? Desconocido	Analizar los diversos requerimientos obtenidos, conforme a las obligaciones.
4,3	**Alcance del SGSI**		
4,3	Determinar y documentar el **alcance del SGSI**	? Desconocido	Alcance se realizara en el Departamento de Tecnologías de la Información y Comunicación de la UNACH
4,4	**SGSI**		
4,4	Establecer, implementar, mantener y mejorar continuamente un SGSI de conformidad con la norma	Inexistente	La DTIC no cuenta con un SGSI.

Ilustración 4: Estado de la Sección 4 de la ISO 27001
Fuente: ISO/IEC 27001:2022, Autor

En la ilustración 5, tenemos la Sección 5, indicándonos el estado actual del liderazgo, en la sección 5.2 referente a políticas tenemos una evaluación de gestionado, esto se refiere que la DTIC tiene en estado vigente dichas políticas.

5	Liderazgo		
5,1	**Liderazgo & compromiso**		
5,1	La alta dirección debe demostrar **liderazgo & compromiso** en relación con el SGSI	Limitado	Las partes interesadas en implementar un SGSI, deberán firmar un acta de compromiso.
5,2	**Política**		
5,2	Establecer la **política de seguridad de la información**	Gestionado	La DTIC documenta las políticas que tiene implementadas.
5,3	**Roles, responsabilidades & autoridades en la organización**		
5,3	Asignar y comunicar los **roles & responsabilidades** de la seguridad de la información	Inicial	Establecer, acordar y comunicar los roles y responsabilidades a todo el personal.

Ilustración 5:Estado de la Sección 5 de la ISO 27001
Fuente: ISO/IEC 27001:2022, Autor

En la ilustración 6, tenemos la Sección 6, indicándonos el estado actual de planificación.

6	Planificación		
6,1	**Acciones para tratar con los riesgos & oportunidades**		
6.1.1	Diseñar / planificar el SGSI para satisfacer los requisitos, tratando con los riesgos & oportunidades	Inicial	La DTIC no cuenta con un SGSI.
6.1.2	Definir y aplicar un **proceso de apreciación de riesgos de seguridad de la información**	Inicial	La DTIC no cuenta con un SGSI.
6.1.3	Documentar y aplicar un proceso de **tratamiento de riesgos de seguridad de la información**	Inicial	La DTIC no cuenta con un SGSI.
6,2	**Objetivos & planes de seguridad de la información**		
6,2	Establecer y documentar los objetivos y planes de seguridad de la información	Inicial	La DTIC no cuenta con un SGSI.
6,3	**Planificación de cambios**		
6,3	Los cambios sustanciales al SGSI deben ser llevados a cabo de manera planificada	Inicial	La DTIC no cuenta con un SGSI se trabaja con la versión 2022

Ilustración 6: Estado de la Sección 6 de la ISO27001
Fuente: ISO/IEC 27001:2022, Autor

En la ilustración 7, tenemos la Sección 7, indicándonos el estado actual de soporte, cabe recalcar como la DTIC no consta con un SGSI, sus niveles a evaluar son iniciales e inexistentes.

7	Soporte		
7,1	**Recursos**		
7,1	Determinar y proporcionar los recursos necesarios para el SGSI	Inicial	No tiene asignación de recursos para el área.
7,2	**Competencias**		
7,2	Determinar, documentar y poner a disposición las **competencias** necesarias	Inexistente	No cuentan con documentación de SGSI referentes a aplicar
7,3	**Concientización**		
7,3	Establecer un programa de **concientización en seguridad**	Inicial	Proponer un programa de comunicación de forma eficaz usando los medios de comunicación.
7,4	**Comunicación**		
7,4	Determinar la necesidad para las **comunicaciones internas y externas** relevantes al SGSI	Inicial	La DTIC no cuenta con un SGSI
7,5	**Información documentada**		
7.5.1	Proveer la **documentación** requerida por la norma así como la requerida por la organización	Inicial	Tener compromisos en proveer la información necesaria para la implementación.
7.5.2	Proveer **títulos**, autores, etc. para la documentación, **adecuar el formato** consistentemente, **revisarlos & aprobarlos**	Inicial	Tener compromisos en proveer la información necesaria para la implementación.
7.5.3	**Controlar la documentación** adecuadamente	Inicial	Tener compromisos en proveer la información necesaria para la implementación.

Ilustración 7: Estado de la Sección 7 de la ISO 27001
Fuente: ISO/IEC 27001:2022, Autor

En la ilustración 8, tenemos la sección 8, indicándonos el estado actual de Operación, de igual manera como la DTIC no consta con un SGSI, sus niveles a evaluar son inexistentes.

8	Operación		
8,1	Planificación y control operacional		
8,1	Planificar, implementar, controlar & documentar el proceso del SGSI para gestionar los riesgos (i.e. un **plan de tratamiento de riesgos**)	Inexistente	La DTIC no cuenta con un SGSI
8,2	Apreciación del riesgo de seguridad de la información		
8,2	**(Re)hacer la apreciación & documentar los riesgos de seguridad de la información en forma regular** & ante cambios o modificaciones	Inexistente	La DTIC no cuenta con un SGSI
8,3	Tratamiento del riesgo de seguridad de la información		
8,3	Implementar el plan de tratamiento de riesgos (**tratar los riesgos!**) y documentar los resultados	Inexistente	La DTIC no cuenta con un SGSI

Ilustración 8: Estado de la Sección 8 de la ISO 27001
Fuente: ISO/IEC 27001:2022, Autor

En la ilustración 9, tenemos la sección 9, indicándonos el estado actual de Evaluación del desempeño, de igual manera como la DTIC no consta con un SGSI, sus niveles a evaluar son inexistentes.

9	Evaluación del desempeño		
9,1	Seguimiento, medición, análisis y evaluación		
9,1	**Hacer seguimiento, medir, analizar y evaluar** el SGSI y los controles	Inexistente	La DTIC no cuenta con un SGSI
9,2	Auditoría interna		
9,2	Planificar y llevar a cabo **auditorías internas** del SGSI	Inexistente	La DTIC no cuenta con un SGSI
9,3	Revisión por la dirección		
9,3	Emprender **revisiones por la dirección** del SGSI regularmente	Inexistente	La DTIC no cuenta con un SGSI

Ilustración 9: Estado de la Sección 9 de la ISO27001
Fuente: ISO/IEC 27001:2022, Autor

En la ilustración 10, tenemos la sección 10, indicándonos el estado actual de Mejora, de igual manera como la DTIC no consta con un SGSI, sus niveles a evaluar son inexistentes.

10	Mejora		
10,1	Mejora continua		
10,1	**Mejorar** continuamente el SGSI	Inexistente	La DTIC no cuenta con un SGSI
10,2	No conformidad y acciones correctivas		
10,2	Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones	Inexistente	La DTIC no cuenta con un SGSI

Ilustración 10: Estado de la Sección 10 de la ISO 27001
Fuente: ISO/IEC 27001:2022, Autor

El estado de implementación del SGSI en la DTIC, evidencio varias limitaciones, no existen procedimientos ni normativas internas para regular el acceso, tratamiento y almacenamiento seguro de los datos de la información.

3.4.3 Identificación de activos

La información que se presenta a continuación se obtuvo directamente de cada responsable de los subprocesos, previo al acuerdo de confidencialidad (Véase ANEXO A), se especifica que dicha documentación será utilizada solamente para fines investigativos.

Para la identificación de activos de cada subproceso definimos el tipo de activo, y sus parámetros a evaluar.

Tabla 5: Tipos de activos
Fuente: Autor

Tipo de Activos	Descripción
Información	Se constituye como un recurso abstracto que se guardará en información o soporte (generalmente se agrupa en archivos o bases de datos) o se enviará de un lugar a otro, lo que significa transmisión de datos. INF - DIG (Información Digital): Base de datos y archivos de datos, contratos y documentos del sistema, informes técnicos, pautas operativas, procesos operativos o de soporte, planes comerciales continuos, contratos relacionados con la cancelación de fondos, programas y almacenamiento de información física o electrónica, entre otros planes, correspondientes a esto. INF - FIS (Físico): Corresponde a todos los documentos, carpetas que se encuentran impresas.
Software	El software consta de todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos. Ejemplos: Sistemas Operativos (Windows/ Linux) , Software de paquete o software estándar (Software de gestión de bases de datos, software de mensajería electrónica, software colaborativo, software de directorio, software de servidor web, etc.) , Aplicaciones Empresariales (Software de contabilidad, software de control de máquinas herramienta, software de atención al cliente, software de gestión de competencias del personal, software administrativo, Mesa de Ayuda etc.)
Hardware	Equipamiento visible, físico y tangible tal como equipos de computación, equipos de comunicación, equipos de redes, medios de almacenamiento, componentes físicos, como Impresoras, Discos Duros, CPU. etc.
Servicios	Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema que sean consolidados por el proceso, personas y herramientas tecnológicas Ejemplos: Servicio de Contabilidad, servicio de mensajería, servicio correo electrónico
Personas	Todo el recurso humano que intervenga en las actividades, tareas, procedimientos, etc. Ejemplos: Analistas, Operadores, Coordinadores, jefes, Gerentes
Instalaciones	Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)
Red	El tipo de red consta de todos los dispositivos de telecomunicaciones que se utilizan para interconectar varios equipos o elementos de un sistema de información físicamente remotos. Ejemplos: Puente, enrutador, concentrador, conmutador, intercambio automático

En cada subproceso, se identificaron todos los activos y sus propietarios, se evaluaron, con valores de 1 a 3, para encontrar el valor del impacto de cada activo, evaluando su confidencialidad, integridad y disponibilidad de cada uno.

Tabla 2: Valoración de Activos
Fuente: Autor

VALORACIÓN DE ACTIVOS DE INFORMACIÓN				
VALOR	**ESCALAS**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**
3	**ALTO (A)**	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente a toda la Empresa. La información es de carácter CONFIDENCIAL y en caso de ser accedida por personas no autorizadas el impacto final sobre el proceso o resultado de la Empresa sería muy grave.	La pérdida de exactitud y estado completo de la información y métodos de procesamientos impacta negativamente a toda la Empresa. La información es base para la toma de decisiones estratégicas o es fundamental para la protección de los individuos de la organización. La ocurrencia de un fraude o errores sobre la misma ocasionará pérdidas graves o catastróficas, por lo cual, la información deberá estar libre de error	La falta del activo de información impacta negativamente a la Empresa. El tiempo máximo para recuperar la información y volver a iniciar el procesamiento es menor a 4 horas.
2	**MEDIO (M)**	**El conocimiento o divulgación no autorizada** de este activo de información impacta negativamente **a algunos procesos del negocio**. La información es de carácter CONFIDENCIAL/ INTERNA y **de ser accedida por personas no autorizadas podría afectar el resultado de varios procesos o poner en riesgo la empresa.**	**La pérdida de exactitud** y estado completo de la información y métodos de procesamientos **impacta negativamente a algunos procesos del negocio**. La información es crítica y es aquella en la cual se basan decisiones importantes del proceso. La ocurrencia de un fraude o errores sobre la misma **ocasionará pérdidas importantes o severas**, por lo cual, la información necesita **un nivel razonable de protección contra error y fraude.**	La falta del activo de información **impacta negativamente algunos procesos del negocio.** **El tiempo máximo para recuperar la información** y volver a iniciar el **procesamiento es menor a un día**.
1	**BAJO (B)**	**El conocimiento** o divulgación no autorizada de este activo de información **impacta negativamente al proceso.** La información a pesar de ser de carácter INTERNA/PUBLICA y ha sido clasificada y nutrida por la organización y d**e ser accedida por personas no autorizadas podría afectar el proceso**	**La pérdida de exactitud** y estado completo de la información y métodos de procesamientos **impacta negativamente al proceso. La información no es crítica, pero es básica para algunas decisiones del proceso**. **La ocurrencia de un fraude** o errores sobre la misma **podría ocasionar pérdidas.**	La falta del activo de información **impacta negativamente al proceso**. **El tiempo máximo para recuperar la información** y volver a iniciar el procesamiento debe **ser menor a una semana**.

3.4.4 Identificación de riesgos

Para la identificación de riesgos nos orientamos hacia el enfoque centrado en activos[29], evaluando así cuales son los principales vulnerabilidades y amenazas, identificando, clasificando y centrándonos en los riesgos más críticos de la organización.

Tabla 6: Ejemplos de Vulnerabilidades y Amenazas
Fuente: Autor

TIPO	AMENAZA	VULNERABILIDAD
Base de Datos	Acceso lógico no autorizado a la base de datos	Falta de controles de acceso lógico
Base de Datos	Ataque Informático	Configuración débil y/o por defecto
Hardware	Alteración, Eliminación, Pérdida o Robo de los dispositivos	Falta de consideraciones de seguridad para la ubicación de los equipos
Hardware	Alteración, Eliminación, Pérdida o Robo de los dispositivos	Falta de políticas / normas / procedimientos / estándares
Información Electrónica	Divulgación de información	Falta de políticas / normas / procedimientos / estándares
Información Electrónica	Fuga, robo o perdida de información	Falta de clasificación y condiciones de manejo de la información
Información Física	Desastres medioambientales	Falta de monitoreo de las condiciones ambientales
Información Física	Fuga, robo o perdida de información	Falta de acuerdos de confidencialidad

Con base en la información recabada, es posible realizar un análisis de cómo se maneja actualmente el DTIC, e identificar los riesgos podría afectar a los activos de información.

Ilustración 11:Identificación de Riesgo
Fuente: [30]

3.4.5 Análisis y Evaluación de Riesgos

Este paso consta dos partes, en la primera se realiza el análisis de un riesgo y el segundo la evaluación del mismo.

El análisis consta en identificar los activos a proteger, la probabilidad, el impacto, el propietario del activo, identificación de controles existentes, obteniendo así el nivel de riesgo de cada activo.

Para la evaluación del riesgo consiste en comparar los niveles frente a los criterios para la evaluación del riesgo.

Criterios para aceptar un Riesgo (BAJO):

- Impacto Bajo: La pérdida es menor y no afecta operaciones de importancia.
- Probabilidad Muy Baja: Ocurre menos de una vez cada 5 años.
- No viola requisitos legales: No hay obligación regulatoria de mitigarlo.

Criterios para NO aceptar un Riesgo (MEDIO / ALTO)

- Impacto Alto: Fuga de datos.
- Probabilidad Media/Alta: Ocurre en un periodo a corto plazo.
- Afecta la reputación de la organización: Falta de cifrado

3.4.5.1 Tratamiento de Riesgos

Una vez identificado los riesgos ALTOS y MEDIOS se toma en cuenta un método de tratamiento con su respectivo control del Anexo A de la norma ISO/IEC 27001, se escogieron controles que puedan disminuir o corregir el riesgo a un nivel aceptable.

Criterios para tratamiento de riesgos

- **Mitigación de riesgos:** Es importante realizar el control de seguridad de la información para reducir la posibilidad de un riesgo.
- **Evitar riesgos**: Es importante la prevención del riesgo antes que suceda.
- **Transferencia de riesgos:** Se puede adquirir un seguro para que el riesgo pueda ser transferido a un tercero
- **Aceptación de riesgos:** Es fundamental que se acepte el riesgo ya que el costo de sufrirlo suele ser muy alto [29].

Los factores de gestión propuestos de acuerdo con el Anexo A adjunto ISO/IEC 27001: 2022, menciona el nivel de prioridad en aquellos que reducen los niveles de riesgo altos y medianos al nivel aceptable, conforme los criterios aceptados por el DTIC.

En esta parte se procede a dar solución a los riesgos por medio del plan de tratamientos presentado, y entregado a la DTIC. (Véase ANEXO B), desarrollado para tratar y mitigar los riesgos identificados, bajo el acuerdo de confidencialidad, no se puede indicar el Plan de tratamiento de riesgos.

3.4.5.2 Políticas

La Dirección de Tecnologías de la Información y Comunicación, presento a inicios del año 2025, un conjunto de políticas de seguridad respecto a los activos de información institucional [31], así como obligaciones, responsabilidades y buen uso asociados a la vulneración de los mismos, entrando en vigencia de forma inmediata.

Políticas de la UNACH 2025

Sección	Politicas	Estado	Notas
1	**Gestión de activos de la información**		
1,1	Identificación y clasificación de los activos de la información	Optimizado	Protocolo de clasificación de activos de la información AIP_IC_ProtGS_UNACH_01. Para el Uso y acceso se regulo mediante el Protocolo de configuración y usi de activos de la información AIP_IUI_ProtGS_UNACH_02.
1,2	Propiedad y uso de los activos de la información	Optimizado	
1,3	Información confidencial	Optimizado	
1,4	Gestión de copias de seguridad.	Optimizado	Base al protocolo de respaldo de datos AIP_IC_ProtGS_UNACH_05
1,5	Gestión de medios extraíbles.	Gestionado	No se utilice el medio extraíble para almacenar otro tipo de información.
1,6	Borrado o eliminación de activos de información	Optimizado	
1,7	Gestión de activos de información de teletrabajo.	Optimizado	
2	**Gestión de Credenciales**		
2,1	Roles de acceso.	Optimizado	
2,2	Credenciales de usuario operador y final.	Optimizado	La activación, modificación y revocación de credenciales de usuario para el acceso a: equipos tecnológicos, red de comunicaciones, correo electrónico, sistemas, bases de datos se cumple conforme el Protocolo de configuración y uso de activos de la información AIP_IUI_ProtGS_UNACH_02.
2,3	Credenciales de usuario final.	Optimizado	
2,4	Credenciales de super usuario	Optimizado	

Ilustración 12: Políticas Vigentes de la UNACH
Fuente: ISO/IEC 27001;2022, Autor, [31]

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En esta sección se presentan los resultados obtenidos del estudio realizado en la DTIC de la UNACH, evidenciando que con la inclusión de una SGSI considerando la norma ISO 27000 produjo cambios notables en el esquema de gestión de la información.

Los resultados que se obtuvieron se presentan a continuación:

4.1.1 Estado Actual de la DTIC

La UNACH carece de un Sistema de Gestión de la Seguridad de la Información (SGSI); por lo tanto, la evidencia es otra: una protección disminuida para salvaguardar la información; ni siquiera existen protocolos definidos para la atención de incidentes, lo que puede reflejar la urgente necesidad de implementar un SGSI.

Ilustración 13: Estado Actual del SGSI
Fuente: Autor

Tabla 7: Estado Actual del SGSI
Fuente: Autor

Estado	Significado	Proporción del Estado SGSI
? Desconocido	No ha sido siquiera revisado aún	**11%**
Inexistente	Falta total de una política, procedimiento, control, etc. Comprensible	**39%**
Inicial	El progreso apenas ha iniciado y demandará un esfuerzo considerable para cumplir con los requisitos	**43%**
Limitado	Avanzando adecuadamente pero aún no finalizado	**4%**
Definido	El desarrollo se encuentra bastante completo, aunque carece de detalles y/o aún no ha sido implementado, no cumple con la normativa actual ni cuenta con el respaldo activo de la alta dirección	**0%**
Gestionado	El desarrollo ha finalizado, el proceso / control ha sido puesto en marcha y recientemente ha comenzado a funcionar	**4%**
Optimizado	El requisito cumple completamente, es totalmente funcional como se anticipa, está bajo supervisión activa y mejora continua, y hay pruebas contundentes que demuestran lo mencionado anteriormente a los auditores	**0%**
No Aplica	Todos los requisitos en el contenido principal de la norma ISO/IEC 27001 son obligatorios SI se desea certificar su SGSI. De lo contrario, la dirección responsable puede desestimarlos	**0%**

El estado de implementación de un SGSI en la DTIC al inicio tenemos un 43 % de los componentes evaluados se encuentran en un estado inicial, lo cual indica que apenas se han dado los primeros pasos hacia la implementación. Además, un 39% en estado inexistente, lo que evidencia la ausencia de procedimientos, políticas controles, etc.

Tenemos un 11% de los elementos fueron clasificados en estado desconocido, refiriéndose a que no han sido revisados y un 4%, presentaba un estado limitado, es decir, existen avances parciales, pero sin consolidarse ni completarse de forma efectiva.

4.1.2 Evaluación de Políticas

Las políticas de seguridad fueron evaluadas obteniendo como resultado que un 68% se encuentra optimizado, indicando que se encuentran operando de forma exitosa, funcionando de manera efectiva, el 33% se encuentra en nivel gestionado, lo que significa que han sido

desarrolladas completamente e implementadas recientemente y han comenzado a operar dentro de la Universidad.

Ilustración 14: Evaluación de las Políticas en la UNACH
Fuente: Autor

Tabla 8:Estado de Políticas de la UNACH
Fuente: Autor

Estado	Significado	Proporción del Estado SGSI
? Desconocido	No ha sido siquiera revisado aún	**0%**
Inexistente	Falta total de una política, procedimiento, control, etc. comprensible	**0%**
Inicial	La evolución apenas está iniciando y demandará un esfuerzo considerable para cumplir con los requisitos	**0%**
Limitado	Avanzando adecuadamente, pero aún no finalizado	**0%**
Definido	El proceso de desarrollo está prácticamente finalizado, aunque carece de detalles y/o todavía no se ha implementado, cumpliendo con lo vigente ni cuenta con el respaldo activo de la alta dirección.	**0%**

Gestionado	El desarrollo se ha finalizado, el proceso / control ha sido instaurado y recientemente ha empezado a funcionar	**33%**
Optimizado	El requisito cumple completamente, está funcionando según lo previsto, se encuentra en constante supervisión y mejora, y hay pruebas significativas para respaldar todo lo mencionado ante los auditores	**68%**
No Aplica	Todos los requisitos en el núcleo de la norma ISO/IEC 27001 son compulsorios SI su SGSI va a ser acreditado. De lo contrario, la gerencia responsable puede pasarlos por alto	**0%**

4.1.3 Tratamiento de Riesgos en la DTIC

Dentro del tratamiento de riesgos, se evaluaron los riesgos de los activos de la DTIC. Los resultados obtenidos son de 70 riesgos evaluados según su impacto y probabilidad de ocurrencia, se clasificaron después de analizarlos en 3 niveles de riesgos: Bajo, Medio, Alto. En estado inicial se obtuvo como resultado:

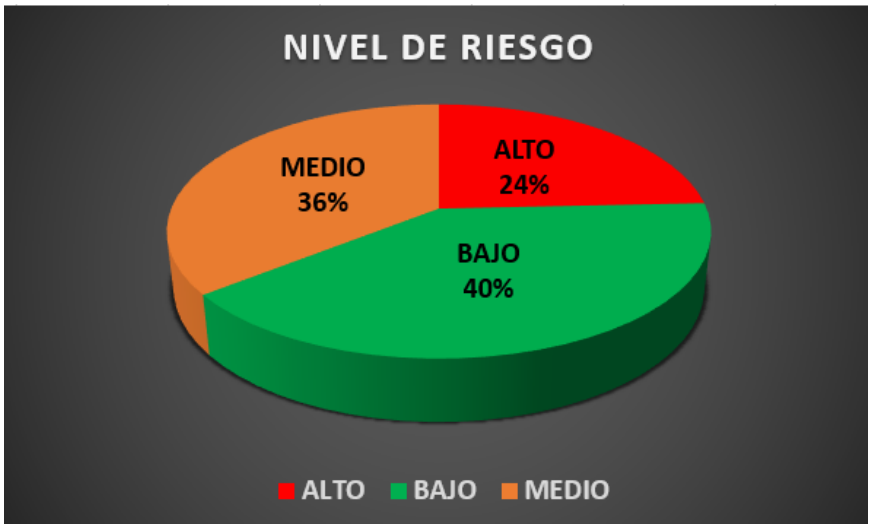


Ilustración 15: Nivel de Riesgo Inicial
Fuente: Autor

- El 40% se clasificó con riesgo bajo, teniendo una exposición mínima de amenazas, aunque se recomienda tenerlos bajo monitoreo continuo para prevenir posibles cambios en su nivel de riesgo.
- Un 36 % se encuentra con el riesgo promedio, que muestra ser una amenaza moderada para la seguridad de la información si no están controlados adecuadamente.
- El 24% se clasificó con riesgo alto, evidenciando las vulnerabilidades críticas, afectando a los activos. Estos deben ser tratados como prioritarios.

Se anticipa que la ejecución del plan de manejo de riesgo sugerido disminuirá notablemente el nivel de riesgo de los activos.

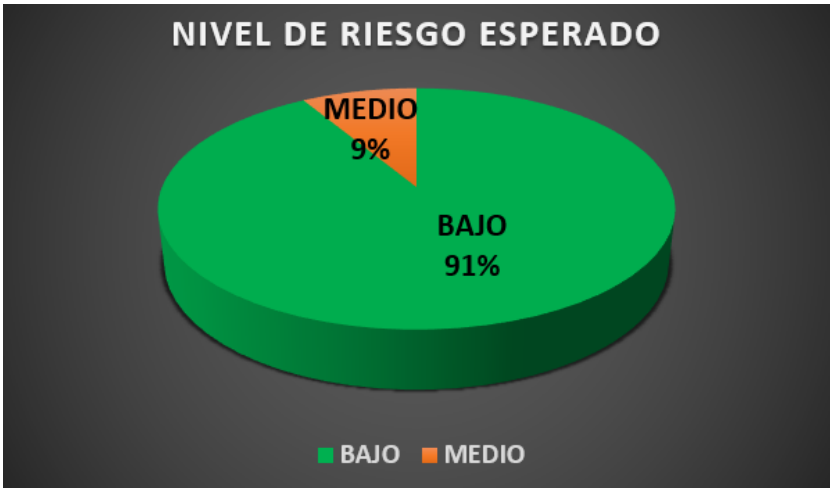


Ilustración 16: Nivel de Riesgo Esperado
Fuente: Autor

- Con un 91% se clasifica en nivel de riesgo bajo, lo que representa una mejora significativa, generando mayor seguridad de la información.
- El 6% se clasifica en nivel de riesgo medio lo que indica que aún se tienen riesgos que representan una amenaza moderada.

4.1.4 Prueba de Hipótesis

Para llevar a cabo la prueba de hipótesis en esta investigación, se utilizó el valor de significancia (p-valor) establecido en 0.05, mediante dicho valor se determina si se acepta la hipótesis nula H_O o se considera a la hipótesis alternativa H_α.

El análisis se realizó mediante la prueba de Chi- cuadrado, con el objetivo de evaluar una diferencia significativa. Para este proceso estadístico se empleó el software Statistical Package for the Social Sciences (SPSS), una herramienta especializada que facilita las evaluaciones estadísticas y su validación.

4.1.5 Hipótesis nula

H_O:Las variables no presentan una asociación significativa (son independientes).

4.1.6 Hipótesis alternativa

H_α:Las variables presentan una asociación significativa (son dependientes).

4.1.7 Tabla cruzada

Se procede a realizar una tabla cruzada con los datos de nivel de riesgo I y nivel de riesgo F.

Tabla 9. Tabla Cruzada de Niveles de Riesgo
Fuente: Autor

Recuento		NIVEL DE RIESGO F		
		BAJO	MEDIO	TOTAL
NIVEL DE RIESGO I	ALTO	14	3	17
	MEDIO	26	2	28
	BAJO	24	1	25
TOTAL		64	6	70

4.1.7.1 Interpretación

En la tabla 4, se observa una reducción de riesgos evidente, de los 17 riesgos en estado alto, 14 pasaron a nivel bajo y solo 3 se permanecieron en nivel bajo, lo que nos muestra que ninguno se mantuvo en nivel alto. Esto es una mejora significativa.

De los 28 riesgos, en un nivel promedio, 26 de los cuales han disminuido en un nivel bajo y solo 2 al mismo nivel. La aprobación se redujo significativamente

Y de los 25 riesgos que estaban en nivel bajo solo 1 subió a nivel medio, esto sugiere que la mayoría mantuvo su nivel de riesgo.

4.1.8 Prueba de Chi- Cuadrado

Tabla 10: Prueba de Chi-Cuadrado
Fuente: Autor

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	2.256[a]	2	,283
Razón de verosimilitud	2,300	2	,317
N de casos validos	70		

4.1.8.1 Interpretación

Se establece la hipótesis nula y alternativa

Ho: Las variables no presentan una asociación significativa (son independientes)

Hα: Las variables presentan una asociación significativa (son dependientes)

Nivel de significancia	α=0.05
Grados de Libertad	2
P-valor	0.283

Según la tabla de prueba de Chi-Cuadrado, se observa que el P-valor es 0,283 > 0.05 se acepta **Ho:** Las variables no presentan una asociación significativa (son independientes), al 95% de confianza.

4.1.9 Comparación Nivel de Riesgo

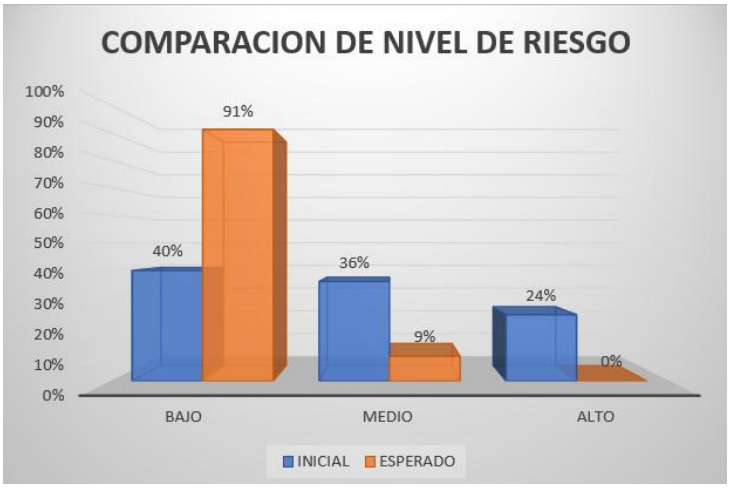


Ilustración 17: Comparación de Nivel de Riesgo
Fuente: Autor

En la ilustración 17, presenta un análisis comparativo entre el nivel de Riesgo Inicial vs Nivel de Riesgo Esperado.

- **El riesgo Bajo**: Se espera que el 40% aumente hasta 91%, esto muestra que el nivel de riesgo está en el nivel A con el nivel más bajo de exposición.
- **El riesgo Medio:** Se redujo considerablemente pasando del 36% inicial al 9% esperado.
- **El riesgo Alto**: Fue totalmente mitigado, reduciéndolo del 24%inicial a un 0% esperado.

Mostrándonos que hay una mejora sustancial, demostrando que las medidas propuestas son efectivas para el tratamiento de riesgos.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Después de los resultados de la prueba de Chi-Cuadrado, que se realiza con respecto a la comparación de los niveles de riesgo inicial con el nivel de riesgo esperado y teniendo en cuenta el valor de P es 0.283, el valor excede el nivel significativo entre el nivel confiable se pasa a aceptar la hipótesis nula, teniendo el 95% de confianza ya que no existe asociación significante respecto a las variables.
- Afrontando el presente proyecto, se llevó a cabo la identificación de los principales riesgos a la que está expuesta la DTIC, clasificando los riesgos teniendo en cuenta su impacto y su probabilidad de ocurrencia. En esta identificación se va a poder conocer la criticidad de cada uno de los activos y determinar los puntos más expuestos del entorno de la institución en cuestión.
- Se considera esencial identificar y evaluar los riesgos aceptables para definir la clasificación pormenorizada de activos significativos según su grado de exposición (bajo, medio, alto). Esta valoración representa la base fundamental para la elaboración de un plan de riesgos, desarrollado según los requisitos de ISO/IEC 27001: 2022, garantizando la gestión sistemática y eficaz de la seguridad de la información
- El SGSI representa el avance más significativo vinculado a las instituciones en lo que respecta a la seguridad de la información. Esto no solo optimiza el proceso interno del DTIC, sino que también eleva la capacidad tecnológica de la universidad para enfrentar nuevas amenazas, lo que fortalece la continuidad de los servicios y la confianza en la universidad.

5.2 RECOMENDACIONES

- Se recomienda que la Universidad Nacional de Chimborazo incorpore la gestión de seguridad de la información como una línea estratégica en su planificación institucional, promoviendo la conformación de un comité interdisciplinario que supervise la implementación del SGSI y garantice su mejora conforme el ciclo PDCA.
- Realizar un proceso continuo de actualización del inventario de activos y su valoración, incluyendo nuevos sistemas, servicio o personal que interactúe con la infraestructura tecnológica, con el fin de mantener vigente el análisis de riesgos y adaptarse a los cambios del entorno institucional.
- Teniendo en cuenta que la DTIC incluye un nuevo subproceso de seguridad informática en su estructura, es aconsejable implementar un plan de estudios específico diseñado para los participantes. Esto garantiza el funcionamiento apropiado de los subprocesos auxiliares.
- Establecer un programa con evaluaciones periódica, para adaptarse a nuevas amenazas y vulnerabilidades emergentes.

CAPÍTULO VI

6. PROPUESTA

Como resultado del trabajo de investigación en la DTIC de la UNACH muestra que se necesita un sistema adecuado para manejar la seguridad de la información.

Actualmente el esquema de seguridad de la información, presenta limitaciones referentes a la identificación de activos, aplicación de controles y políticas existentes, exponiendo y comprometiendo la confidencialidad, integridad y disponibilidad de la información.

En este caso se sugiere la implementación del SGSI siguiendo el estándar ISO 27001:2022, mejorando así el esquema de información, identificando, evaluando y tratando los riesgos asociados, aplicando controles para reducir el riesgo.

Para la ejecución de esta propuesta, se requiere la participación de toda la infraestructura de la DTIC, teniendo el compromiso por parte de la universidad, esto lograra un decrecimiento en los niveles de riesgo, teniendo una mayor eficacia en la gestión de información y aumentando la confianza institucional.

Para concluir, esta propuesta se basa en los resultados del análisis anterior y satisface de manera directa las demandas identificadas en la DTIC de la UNACH.

BIBLIOGRÁFIA

[1] Mayra Gabriela Cordero Núñez, "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.," Trabajo de titulación, UNIVERSIDAD TÉCNICA DE AMBATO, Ambato, 2022. Accessed: Aug. 05, 2024. [Online]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/34814/1/t1959si.pdf

[2] Baloa Rodriguez Nazareth Andreina, "Análisis, diseño e implementación de un proceso hardening para la protección del servidor de la página web institucional de la Dirección de Tecnologías de la Información y Comunicación de la UNACH," Universidad Nacional de Chimborazo, Riobamba, 2023.

[3] Mendoza Miguel Angel, "ISO 27001:2022: ¿qué cambios introdujo el nuevo estándar de seguridad?," Seguridad para Empresas.

[4] UNIT, "UNIT-ISO/IEC 27000." Accessed: Jan. 16, 2025. [Online]. Available: https://www.unit.org.uy/normalizacion/sistema/27000/

[5] OSCAR ANDRES RIOS GUTIERREZ, "Historia y evolución de la ISO serie 27000, ISO 17799," UNIVERSIDAD NACIONAL SEDE MIZALES, COLOMBIA, 2010. Accessed: Jan. 09, 2025. [Online]. Available: https://studylib.es/doc/845974/3.-historia-y-evoluci%C3%B3n-de-la-iso-serie-27000--iso-17799

[6] Aguilar Adriana, "Historia y Evolución de ISO 27001," ISO 27001, Cumplimiento Normativo. Accessed: Oct. 16, 2024. [Online]. Available: https://blog.tecnetone.com/historia-y-evoluci%C3%B3n-est%C3%A1ndar-iso-27001

[7] BUITRAGO ESTRADA JOHANNA CAROLINA, BONILLA PINEDA DIEGO HERNANDO, and MURILLO VARON CAROL ESTEFANIE, "DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI, EN EL SECTOR DE LABORATORIOS DE ANALISIS MICROBIOLOGICOS, BASADO EN ISO 27001.," UNIVERSIDAD EAN, BOGOTÁ, 2012. Accessed: Jan. 09, 2025. [Online]. Available: https://repository.universidadean.edu.co/server/api/core/bitstreams/92c04fed-8caf-417e-82d6-711e3196f1d0/content

[8] SALCEDO B. ROBIN J., "PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013," UNIVERSIDAD OBERTA CATALUNYA, ESPAÑA, 2014.

[9] ARANA WALDE LUCERO ALESSANDRA, "Implementación del sistema de gestión de información basado en la ISO 27001:2013 para proteger la

información de los procesos operativos en la empresa Core Business Corporation SAC, Lima - 2021," UNIVERSIDAD PRIVADA DEL NORTE, LIMA. PERU, 2021.

[10] Torres Chango Christian Damian, ""PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A," CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES, UNIVERSIDAD TÉCNICA DE AMBATO, Ambato - Ecuador, 2020.

[11] Tenorio Ordoñez Ivana Jolima, "Auditoría informática de seguridad física en el área de redes en la Universidad Nacional de Chimborazo utilizando norma ISO 27001," UNIVERSIDAD NACIONAL DE CHIMBORAZO, Riobamba, 2024.

[12] ESET, "SECURITY REPORT Latinoamérica 2018," Jun. 2018. Accessed: May 04, 2024. [Online]. Available: https://web-assets.esetstatic.com/wls/2018/06/ESET_security_report_LATAM2018.pdf

[13] María José Bravo Ramos, "DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA BIBLIOTECAS BASADO EN UNA METODOLOGÍA MEJORADA DE ANÁLISIS DE RIESGOS COMPATIBLE CON LA NORMA ISO/IEC 27001:2013," ESCUELA POLITÉCNICA NACIONAL, Quito, 2018. Accessed: May 04, 2024. [Online]. Available: https://bibdigital.epn.edu.ec/bitstream/15000/19880/3/CD-9295.pdf

[14] SUPERINTENDENCIA, "SISTEMA de Gestión de Seguridad de la Información (SGSI)," Jan. 2021, Accessed: May 04, 2024. [Online]. Available: https://www.seps.gob.ec/wp-content/uploads/Norma-ISO-27001.pdf

[15] R. C. D. G. D. F. LEMA VINLASACA, "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL CONTROL FÍSICO Y DIGITAL DE DOCUMENTOS APLICADO A LA EMPRESA LOCKERS S.A," ESPE, SANGOLQUÍ, 2018. Accessed: May 04, 2024. [Online]. Available: https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/eb7dfb3c-d128-4aaa-b7c1-fac60a2504b7/content

[16] Erick Guerra, Harold Neira, Jorge L., and Janns Patiño, "Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias," *Información Tecnológica*, Barranquilla, Colombia, pp. 145–156, oct. 2021. doi: 10.4067/S0718-07642021000500145.

[17] Escuela Europea de Excelencia, "Norma ISO 27001:2022: todo lo que debes saber sobre el nuevo estándar de Seguridad de la Información," *Artículos*

Técnicos, Destacado, Seguridad de la información, Dec. 06, 2022. Accessed: May 04, 2024. [Online]. Available: https://www.escuelaeuropeaexcelencia.com/2022/12/norma-iso-270012022-todo-lo-que-debes-saber-sobre-el-nuevo-estandar-de-seguridad-de-la-informacion/#:~: %20cinco%20a%C3%B1os

[18] Interfacing, "ISO/IEC 27000," Serie de normas ISO 27000. Accessed: Jan. 16, 2025. [Online]. Available: https://interfacing.com/es/iso-27000

[19] ISO/IEC 2022, "INTERNATIONAL STANDARD ISO/IEC27001,2022," 2022.

[20] Organismo de Certificación Global, "ISO 27001: Sistemas de gestión de seguridad de la información." Accessed: Jan. 16, 2025. [Online]. Available: https://www.nqa.com/es-pe/certification/standards/iso-27001-2022#:~:text=La%20ISO%2027001%3A2022%20es%20la%20norma%20internacional%20que%20proporciona,informaci%C3%B3n%2C%20as%C3%AD%20como%20cumplimiento%20legal.

[21] ISO27000.ES, "SGSI," Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información. Accessed: Nov. 16, 2024. [Online]. Available: https://www.iso27000.es/sgsi.html

[22] MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN, " ACUERDO Nro. MINTEL-MINTEL-2024-0003," Mar. 2024.

[23] "Sistema de Gestión de Seguridad de la Información (SGSI)," Nov. 2021.

[24] ambit, "¿Para qué sirve un SGSI? Controles y fases." Accessed: Mar. 18, 2025. [Online]. Available: https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases

[25] Soft Expert, "¿Qué es el Ciclo PDCA ?"

[26] Equipo de Enciclopedia Significados, "Investigación experimental." Accessed: Apr. 15, 2025. [Online]. Available: https://www.significados.com/investigacion-experimental/

[27] UNACH, "Dirección de Tecnologías de la Información y Comunicación." Accessed: Apr. 15, 2025. [Online]. Available: https://dtic.unach.edu.ec/

[28] UNACH, "Reglamento de Gestión Organizacional por Procesos ROGOP-2022," Riobamba, Aug. 2022.

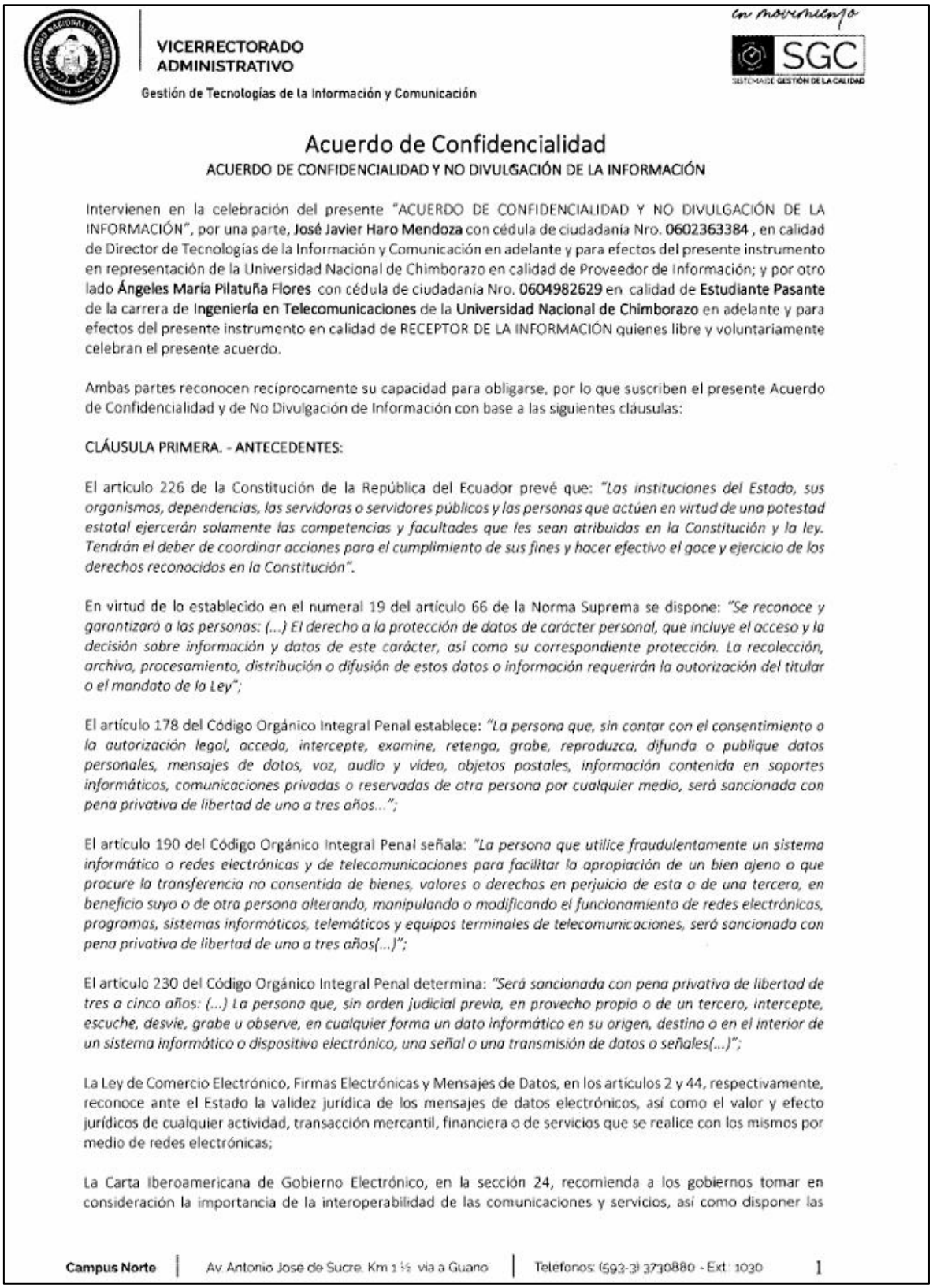
[29] Bonnie Emily, "El Enfoque ISO 27005," SECUREFRAME.

[30] Tania López, "SGSI: Qué es y Como implementarlo," INNEVO. Accessed: Mar. 11, 2025. [Online]. Available: https://innevo.com/blog/que-es-sgsi

[31] UNACH, "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 2025," Riobamba, Jan. 2025.

ANEXOS

ANEXO A - CARTA DE CONFIDENCIALIDAD



VICERRECTORADO ADMINISTRATIVO

Gestión de Tecnologías de la Información y Comunicación

En movimiento

SGC

SISTEMA DE GESTIÓN DE LA CALIDAD

Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN

Intervienen en la celebración del presente "ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN", por una parte, **José Javier Haro Mendoza** con cédula de ciudadanía Nro. **0602363384** , en calidad de Director de Tecnologías de la Información y Comunicación en adelante y para efectos del presente instrumento en representación de la Universidad Nacional de Chimborazo en calidad de Proveedor de Información; y por otro lado **Ángeles María Pilatuña Flores** con cédula de ciudadanía Nro. **0604982629** en calidad de **Estudiante Pasante** de la carrera de **Ingeniería en Telecomunicaciones** de la **Universidad Nacional de Chimborazo** en adelante y para efectos del presente instrumento en calidad de RECEPTOR DE LA INFORMACIÓN quienes libre y voluntariamente celebran el presente acuerdo.

Ambas partes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información con base a las siguientes cláusulas:

CLÁUSULA PRIMERA. - ANTECEDENTES:

El artículo 226 de la Constitución de la República del Ecuador prevé que: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución".*

En virtud de lo establecido en el numeral 19 del artículo 66 de la Norma Suprema se dispone: *"Se reconoce y garantizará a las personas: (...) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley";*

El artículo 178 del Código Orgánico Integral Penal establece: *"La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años...";*

El artículo 190 del Código Orgánico Integral Penal señala: *"La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años(...)";*

El artículo 230 del Código Orgánico Integral Penal determina: *"Será sancionada con pena privativa de libertad de tres a cinco años: (...) La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales(...)";*

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en los artículos 2 y 44, respectivamente, reconoce ante el Estado la validez jurídica de los mensajes de datos electrónicos, así como el valor y efecto jurídicos de cualquier actividad, transacción mercantil, financiera o de servicios que se realice con los mismos por medio de redes electrónicas;

La Carta Iberoamericana de Gobierno Electrónico, en la sección 24, recomienda a los gobiernos tomar en consideración la importancia de la interoperabilidad de las comunicaciones y servicios, así como disponer las

Campus Norte | Av. Antonio José de Sucre. Km 1 ½ vía a Guano | Teléfonos: (593-3) 3730880 - Ext: 1030 1

medidas necesarias, para que todas las entidades públicas, cualquiera que sea su nivel y con independencia del respeto a su autonomía, establezcan sistemas que sean interoperables;

La Ley del Sistema Nacional de Registro de Datos Públicos publicada en el Registro Oficial No. 162 de 31 de marzo de 2010, en su artículo 4, cita: *"Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información...";*

El artículo 27 de la Ley ibídem establece: *"Las Registradoras o Registradores y máximas autoridades, a quienes se autoriza el manejo de las licencias para el acceso a los registros de datos utilizados por la ley, serán las o los responsables directos administrativa, civil y penalmente por el mal uso de las mismas";*

Bajo este marco regulatorio, la información que se dispone en los servicios institucionales se clasifica como reservada y/o confidencial, a tal efecto se acuerda suscribir el presente "Acuerdo de Confidencialidad y No Divulgación de la Información" entre quien solicita el acceso a los servicios institucionales y la entidad proveedora del servicio con la finalidad de proteger la información que se consuma cuando ésta tenga el carácter de reservada y/o confidencial.

Se garantizará la confidencialidad, integridad, disponibilidad, reserva y protección de los datos e información que se comparta e intercambie entre las entidades, de acuerdo a la normativa vigente.

CLÁUSULA SEGUNDA. - OBJETO:

En virtud de los antecedentes expuestos, por medio del presente instrumento el RECEPTOR DE LA INFORMACIÓN se obliga expresamente a guardar sigilo, confidencialidad y reserva sobre el contenido de toda la información generada, verbal o escrita, que se comparta entre las partes.

Además, el RECEPTOR DE LA INFORMACIÓN se compromete a hacer uso de la información, únicamente para las actividades relacionadas con las funciones que desempeña, conforme a las obligaciones y prohibiciones legales pertinentes.

CLÁUSULA TERCERA. - DERECHOS Y OBLIGACIONES:

Son obligaciones de la Universidad Nacional de Chimborazo las siguientes:

1. Suministrará al RECEPTOR DE LA INFORMACIÓN el informe/la información que estime necesaria para el desarrollo de sus funciones (contrato laboral y/o proyecto)

Son deberes de quien haga las veces de RECEPTOR DE LA INFORMACIÓN:

1. Guardar la reserva y confidencialidad, sin el deterioro de cualquier tipo de información que se le suministre o a la cual llegare a tener acceso o conocimiento;
2. Todo funcionario de la Universidad, pasante de prácticas pre profesionales, funcionario público de cualquier entidad pública y/o empleado de empresa privada que haga uso y tenga acceso a la información proporcionada por la Universidad Nacional de Chimborazo, deberá suscribir el presente instrumento.
3. Mantener en forma estrictamente reservada y confidencial toda la información que por razón de su competencia tendrá acceso, por lo tanto, se obliga a abstenerse de usar, disponer, divulgar y/o publicar por cualquier medio, oral, escrito, y/o tecnológico y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los intereses de la Institución a la cual pertenece.
4. Utilizar la información suministrada por la Universidad Nacional de Chimborazo, únicamente para los fines acordados por las partes.

No realizar copia o duplicado alguno de la información mencionada en este acuerdo sin la autorización previa y escrita de la otra parte; tampoco podrán divulgar dicha información a terceras personas sin que medie igualmente

la respectiva autorización previa y escrita de la otra parte. Se excluye de esta obligación la información que sea de dominio público o que sea del conocimiento previo de la Universidad Nacional de Chimborazo, sin constituir discreción de la información en los términos del presente acuerdo y, cuya revelación no cause agravio o perjuicio alguno a su titular.

CLÁUSULA CUARTA. - PATRÓN DE CONDUCTA, IMPLICACIONES DE LA RECEPCIÓN DE LA INFORMACIÓN Y RESPONSABILIDAD:

Las partes actuarán con responsabilidad en el buen uso de la información, lo que supone entre otros deberes, el de limitar la divulgación autorizada al menor número de personas, y el de tomar las medidas idóneas y eficaces para evitar el tráfico y fuga indebida de la información, así como su uso por fuera de los límites de este convenio.

El incumplimiento del deber de reserva establecido en la Cláusula Cuarta de este acuerdo, constituye violación de secreto y justa causa de terminación unilateral de la relación, sin desmedro de las indemnizaciones (sólo para proveedores) legales correspondientes.

El RECEPTOR DE LA INFORMACIÓN reconoce que la información confidencial a la que se refiere el presente acuerdo posee una valoración en imagen institucional y su indebida divulgación o utilización causa un perjuicio.

CLÁUSULA QUINTA. - MATERIALES:

Todos los materiales como, documentos físicos y digitales, que son entregadas al RECEPTOR DE LA INFORMACIÓN por parte de la Universidad Nacional de Chimborazo se considera como información confidencial y se debe guardar absoluta reserva de la misma.

CLÁUSULA SEXTA. - SANCIONES:

Para la aplicación de sanciones se tomará en cuenta lo establecido en la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Código Orgánico Integral Penal, Ley Orgánica del Sistema Nacional de Registro de Datos Púbicos y demás normativa aplicable; sin perjuicio de las acciones civiles y penales que procedan en cada caso.

Los funcionarios públicos que incumplieren las estipulaciones de este instrumento, podrán ser sancionados por la máxima autoridad de la entidad en la que prestan sus servicios, de conformidad con lo determinado en la Ley Orgánica del Servicio Público y su Reglamento.

CLÁUSULA SÉPTIMA. – EXCEPCIONES:

En los casos en que la información sea calificada como "Reservada" o "Confidencial" por mandato legal, las entidades que suscriben el presente acuerdo evaluarán la pertinencia de entregar o no dicha información.

CLÁUSULA OCTAVA. - VIGENCIA:

El presente instrumento tendrá una vigencia de cinco años a partir de la fecha de suscripción.

CLÁUSULA NOVENA - ACUERDO TOTAL:

Este acuerdo incluye el total entendimiento entre las partes con relación a la materia de la cual se trata este documento. Cualquier añadidura o modificación a este acuerdo deberá ser hecha por escrito y firmada por ambas partes.

CLÁUSULA DÉCIMA PRIMERA: NOTIFICACIONES. –

En el evento de que se produzca el incumplimiento de alguna de las cláusulas estipuladas en el presente acuerdo,

la parte afectada, notificará del incumplimiento a la máxima autoridad de la Universidad Nacional de Chimborazo, sin perjuicio de las acciones y sanciones previstas en la normativa vigente.

Una vez comprendido por los comparecientes el contenido y efectos del presente instrumento expresamente se ratifican en él, para fe y constancia se firma el presente documento por quienes en él intervinieron, en la ciudad de Riobamba, el día 30 de enero de 2025, en dos ejemplares del mismo tenor y validez.

Ing. José Javier Haro Mendoza
DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Ángeles María Pilatuña Flores
RECEPTOR DE LA INFORMACIÓN

ANEXO B – PLAN DE TRATAMIENTO DE RIESGOS

Riobamba, 16 de mayo de 2025

Javier Haro
Director de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo
Presente. –

De mi consideración:

Yo, **Ángeles María Pilatuña Flores**, estudiante de la carrera de **Ingeniería en Telecomunicaciones**, me permito presentar a usted el documento titulado **"Plan de Tratamiento de Riesgos de Seguridad de la Información en el DTIC de la UNACH"**, desarrollado en el marco de mi proyecto de investigación **Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27000:2022 mediante el tratamiento de riesgos para la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo para mejorar el esquema de información.**

El presente plan tiene como finalidad proponer acciones especificas para la gestión adecuada de los riesgos identificados, en concordancia con las buenas prácticas de seguridad de la información, y con el objetivo de fortalecer la protección de los activos tecnológicos e informáticos de la institución.

Agradezco la apertura brindada por el departamento para el desarrollo de este trabajo.

Atentamente,

Ángeles María Pilatuña Flores
Estudiante de la carrera de Ingeniería en Telecomunicaciones
Correo electrónico: angeles.pilatuna@unach.edu.ec
Teléfono: 0990937529

Recibido
16/05/2025

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN EL DTIC DE LA UNACH

UNIVERSIDAD NACIONAL DE CHIMBORAZO
DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

8 DE ABRIL DE 2025
ECUADOR

0

6. APROBACION Y RESPONSABLES

6.1 FIRMAS Y APROBACION.

ELABORADO POR:

ELABORACION
NOMBRE: Ángeles María Pilatuña Flores
CARGO: Estudiante de la Facultad de Ingeniería
FIRMA: 

REVISORES:

REVISION	REVISION
NOMBRE: Mgs. Luis Gonzalo Santillán Valdiviezo	**NOMBRE:** Mgs. Diego Gustavo Caiza Méndez
CARGO: Docente de la UNACH	**CARGO:** Analista de DTIC de la UNACH
FIRMA: 	**FIRMA:** 

APROBACION:

APROBACION	APROBACION
NOMBRE: Ph. D Carlos Peñafiel	**NOMBRE:** Mgs. José Javier Haro Mendoza
CARGO: Director de la carrera de Telecomunicaciones	**CARGO:** Director de DTIC de la UNACH
FIRMA: 	**FIRMA:** 

ANEXO C

Ilustración 18: Entrega de Documentación
Fuente: Autor