

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA,

INFORMÁTICA Y MECÁNICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS



TESIS

**DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
BASADO EN LA NORMA TÉCNICA PERUANA NTP ISO 27001:2014 PARA LA
UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO**

PRESENTADO POR:

Br. VICTOR HUGO CUBA GAMARRA

Br. MARCO EMERSON SOLIS CANO

**PARA OPTAR EL TÍTULO PROFESIONAL
DE INGENIERO INFORMATICO Y DE
SISTEMAS**

ASESOR:

Mgt. JOSE MAURO PILLCO QUISPE

CUSCO – PERÚ

2024

INFORME DE ORIGINALIDAD

(Aprobado por Resolución Nro.CU-303-2020-UNSAAC)

El que suscribe, asesor del trabajo de investigación/tesis titulada:

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TÉCNICA PERUANA NTP ISO 27001:2014 PARA LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO "

presentado por:

CUBA GAMARRA, Víctor Hugo, DNI: **43131967** y SOLÍS CANO, Marco Emerson DNI **40981136** para optar el título profesional/grado académico de:

: INGENIERO INFORMÁTICO Y DE SISTEMAS

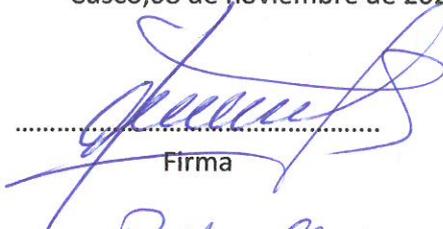
Informo que el trabajo de investigación ha sido sometido a revisión por 02 veces, mediante el Software Antiplagio, conforme al Art. 6° del Reglamento para Uso de Sistema Antiplagio de la UNSAAC y de la evaluación de originalidad se tiene un porcentaje de.....5%.....

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No se considera plagio.	X
Del 11 al 30 %	Devolver al usuario para las correcciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, quien a su vez eleva el informe a la autoridad académica para que tome las acciones correspondientes. Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de asesor, firmo el presente informe en señal de conformidad y **adjunto** la primera hoja del reporte del Sistema Antiplagio.

Cusco, 08 de noviembre de 2024


.....
Firma

Post firma.....

N° de DNI.....

ORCID del asesor: **0000-0002-0527-089X**

Se adjunta:

1. Reporte generado por el sistema antiplagio.
2. Enlace del reporte generado por el sistema antiplagio: **oid:27259:403259333**

solis, cuva marco emerson, victor hugo

TESIS PREGRADO_revision_final_APA_7.pdf

 Universidad Nacional San Antonio Abad del Cusco

Detalles del documento

Identificador de la entrega

trn:oid:::27259:403259333

Fecha de entrega

8 nov 2024, 9:32 a.m. GMT-5

Fecha de descarga

3 ene 2025, 10:48 a.m. GMT-5

Nombre de archivo

TESIS PREGRADO_revision_final_APA_7.pdf

Tamaño de archivo

2.2 MB

135 Páginas

33,396 Palabras

200,468 Caracteres

5% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- ▶ Bibliografía
- ▶ Texto citado
- ▶ Texto mencionado
- ▶ Coincidencias menores (menos de 20 palabras)

Exclusiones

- ▶ N.º de coincidencias excluidas

Fuentes principales

- 5%  Fuentes de Internet
- 0%  Publicaciones
- 3%  Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

DEDICATORIA

El presente trabajo en conjunto es dedicado a Dios, por brindarnos fortaleza, sabiduría y guía a lo largo de este arduo pero gratificante proceso académico. Impulsado por su constante amor, por sostenerme en los momentos de dificultad y por iluminar mi camino con esperanza y fe. Todo lo logrado ha sido posible gracias a su inagotable misericordia.

AGRADECIMIENTOS

Sobre todas las cosas a Dios por permitir sostenernos día a día con su gracia y amor para alcanzar nuestras metas y objetivos.

A nuestras familias quienes sin saber nos impulsan a crecer cada día y demostrar que no existen límites para cumplir los objetivos, este logro no habría sido posible sin su amor incondicional, paciencia y comprensión. A lo largo de este arduo camino, su constante apoyo emocional y su alegría inagotable han sido nuestra mayor fuente de inspiración. Cada paso que se he dado en esta travesía académica ha estado motivado por el deseo de brindarles un futuro mejor, y esta tesis es el fruto de ese anhelo.

A nuestros respetados y estimados docentes, cuya orientación experta, apoyo incondicional y sabiduría académica fueron fundamentales en la culminación de esta tesis. Su dedicación para transmitir conocimientos, su paciencia en responder a las inquietudes y su constante estímulo fueron esenciales para mi crecimiento académico y profesional.

¡Muchas Gracias!

INTRODUCCIÓN

En el mundo contemporáneo, la información se ha consolidado como uno de los activos más valiosos para las organizaciones, y las instituciones educativas no son la excepción. La Universidad Nacional de San Antonio Abad del Cusco (UNSAAC), como institución académica de prestigio, gestiona grandes volúmenes de datos relacionados con actividades administrativas, académicas e investigativas. No obstante, esta información enfrenta riesgos significativos debido a la falta de controles de seguridad adecuados y la ausencia de un marco normativo que garantiza su protección.

Un diagnóstico preliminar revela varias áreas críticas que requieren atención inmediata. En primer lugar, la Universidad Nacional de San Antonio Abad del Cusco (UNSAAC) carece de un análisis detallado de su situación actual en materia de seguridad de la información, especialmente en relación con los requisitos establecidos en la Norma Técnica Peruana NTP ISO/IEC 27001:2014, esta norma técnica está basada en un estándar internacional ISO/IEC 27001 que proporciona un marco para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

La gestión de la seguridad de la información es un proceso sistemático para afrontar eficazmente las amenazas y los riesgos de la seguridad de la información en una organización según lo indicado por (Yuan, 2014)

La falta de controles específicos expone a la universidad a vulnerabilidades frente a amenazas internas y externas, mientras que el incumplimiento normativo puede derivar en sanciones legales y pérdida de confianza por parte de la comunidad académica y administrativa. Además, se identifica una insuficiente concienciación y capacitación del personal en temas de seguridad de la información, lo que aumenta el riesgo de incidentes de seguridad de la información relacionados con errores humanos y ataques externos e internos como por ejemplo intrusiones no autorizadas.

La implementación de un SGSI conforme a la NTP ISO/IEC 27001:2014 no solo permite gestionar estos riesgos de manera efectiva, sino que también asegura el cumplimiento de requisitos legales, regula el acceso a la información y fortalece la resiliencia institucional frente a ciberataques. Según (Alberto G.

Alexander, 2007), “un SGSI proporciona un enfoque sistemático para proteger la información en términos de confidencialidad, integridad y disponibilidad, alineando los objetivos organizacionales con las mejores prácticas internacionales”.

Por ello, el objetivo principal de esta investigación es proponer un diseño de un SGSI basado en la NTP ISO/IEC 27001:2014 para la UNSAAC apuntando al proceso crítico considerado Tramite Documentario, que permitirá abordar los siguientes objetivos críticos:

Análisis de la situación actual basado en las normas técnicas peruanas NTP ISO/IEC 27001:2014 que permitieron identificar las brechas existentes en la gestión de la seguridad de la información.

Definición de controles de seguridad que permitirá proponer medidas específicas para mitigar riesgos detectados significativo o críticos.

Cumplimiento normativo que permitirá asegurar que las actividades de gestión de la información cumplan con los requisitos legales y regulatorios incluidos en la NTP ISO/IEC 27001:2014. Considerar también la Ley 29733– “Ley de Protección de datos personales”. De no cumplirse la organización está expuesta a multas y vulnera la imagen institucional, generando desconfianza en el tratamiento de los datos. Entre otras que fueron comentadas en las entrevistas desarrolladas en el presente proyecto.

Concienciación y capacitación que permitirá realizar el diseño de estrategias para sensibilizar y entrenar a los usuarios de forma transversal para la aplicación de prácticas seguras de manejo de información.

Para cumplir con estos objetivos, esta investigación utilizará una metodología PMBOK que tiene una guía que ofrece estándares y pautas para la gestión de proyectos ágiles, las mejores prácticas en gestión de proyectos (Institute., 2017) basada en el conocimiento del proceso y la NTP ISO/IEC 27001:2014, analizando el estado actual de la universidad, evaluando riesgos y proponiendo controles alineados con la norma mencionada. Asimismo, se recurre a una revisión bibliográfica que sustentó los conceptos claves y el diseño propuesto.

De acuerdo con las limitaciones de tiempo con el que se cuenta es escaso, para la implementación del proyecto, se consideró controles para los activos de información que presentan un riesgo crítico. Asimismo, establecer un diseño del sistema de gestión de seguridad de la información dejando de lado las fases de monitoreo, certificación y auditoría; por no ser fases necesarias para la propuesta, pero si para mantener un Sistema de Gestión de Seguridad de la información y optativamente la certificación de ISO/IEC 27001.

Con esta propuesta, se espera fortalecer la seguridad de la información en la Universidad Nacional de San Antonio Abad del Cusco (UNSAAC), levantar cuantiosas observaciones que se fueron identificando a nivel de áreas de control y auditoría, asegurando la protección de sus activos críticos y estableciendo un modelo que pueda ser replicado a nivel transversal a todos los procesos de la universidad para que se apliquen buenas prácticas de uso de los activos de información generando conciencia y cultura en la seguridad de la información.

RESUMEN

Este proyecto de investigación tiene como objetivo principal diseñar un modelo de referencia para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Universidad Nacional de San Antonio Abad del Cusco. Dicho modelo busca fortalecer la protección de la información sensible asociado al proceso de Gestión de Trámite Documental, alineándose con las mejores prácticas y estándares internacionales. A través de este diseño, se espera no solo mitigar los riesgos asociados a las amenazas y vulnerabilidades identificadas, sino también establecer una cultura de seguridad, garantizando la confidencialidad, integridad y disponibilidad de los datos. El modelo propuesto facilitará el cumplimiento normativo, contribuyendo al desarrollo de una gestión más eficiente y segura de la información, en concordancia con las disposiciones de la Resolución Ministerial N° 004-2016-PCM y la NTP ISO/IEC 27001:2014. Uno de los principales desafíos fue la identificación de la limitada cultura de seguridad en la universidad, junto con la escasez de recursos técnicos y humanos especializados en la gestión de la seguridad de la información.

El enfoque metodológico fue descriptivo y aplicado, utilizando como herramientas clave el análisis de riesgos, entrevistas con actores involucrados en los procesos administrativos, y la evaluación de las brechas de cumplimiento normativo. Se trazó un diseño estructurado que incluye políticas, gestión de incidentes, capacitación y un plan de mejora continua para garantizar su sostenibilidad.

Tomar en cuenta el diseño para su implementación permitirá que la UNSAAC no solo fortalezca su gestión de trámite documental, sino que también se posicione como un referente en la adopción de buenas prácticas en el ámbito educativo peruano.

Palabras Claves: Sistema de Gestión de Seguridad de la Información, NTP ISO/IEC 27001:2014, Gestión de Riesgos, Unidad de Trámite Documentario UTD.

ABSTRACT

This research project aims to design a reference model for the implementation of an Information Security Management System (ISMS) at the National University of San Antonio Abad of Cusco. This model aims to strengthen the protection of sensitive information associated with the Document Management Process, aligning with best practices and international standards. Through this design, it is expected not only to mitigate the risks associated with the identified threats and vulnerabilities but also to establish a security culture, ensuring the confidentiality, integrity, and availability of the data. The proposed model will facilitate regulatory compliance, contributing to the development of a more efficient and secure information management system, in accordance with the provisions of Ministerial Resolution No. 004-2016-PCM and NTP ISO/IEC 27001:2014. One of the main challenges was identifying the limited security culture at the university, along with the scarcity of specialized technical and human resources in information security management. The methodological approach was descriptive and applied, using key tools such as risk analysis, interviews with stakeholders involved in administrative processes, and the evaluation of compliance gaps. A structured design was outlined that includes policies, incident management, training, and a continuous improvement plan to ensure its sustainability. Taking the design into account for its implementation will allow UNSAAC not only to strengthen its document management but also to position itself as a benchmark in the adoption of best practices in the Peruvian educational field.

Keywords: Information Security Management System, NTP 27001: 2014, Risk Management, Documentary Processing Unit.

INDICE DE CONTENIDO

CAPÍTULO I: ASPECTOS GENERALES	14
1.1. Antecedentes	14
1.1.1. Antecedentes Internacionales	14
1.1.2. Antecedentes Nacionales.....	16
1.2. Planteamiento del problema	19
1.2.1. Problema General	19
1.2.2. Problemas Específicos.....	20
1.3. Objetivos	21
1.3.1. Objetivo General	21
1.3.2. Objetivos Específicos.....	21
1.4. Justificación.....	21
1.4.1. Falta de Análisis de situación actual en base a la NTP ISO 27001:2014	21
1.4.2. Falta de políticas, procedimientos y controles de seguridad de información	22
1.4.3. Incumplimiento normativo de la NTP ISO/IEC 27001:2014	23
1.4.4. Falta de capacitación y concienciación de Seguridad de la Información.....	23
1.5. Alcances y delimitaciones	24
1.5.1. Alcances.	24
1.5.2. Delimitaciones.....	24
1.6. Estudio de factibilidad.....	25
1.6.1. Factibilidad Técnica.....	25
1.6.2. Factibilidad Económica	26
1.6.3. Factibilidad Operativa	27
1.7. Metodología.....	27
1.7.1. Tipo de la Investigación.....	27
1.7.2. Nivel de la Investigación	28
1.7.3. Diseño de la Investigación.....	29
CAPÍTULO II: MARCO TEÓRICO.....	31
2.1. Bases Teóricas	31
2.1.1. Sistema De Gestión De Seguridad De La Información	31
2.1.2. Trámite Documentario.....	32
2.2. Términos Básicos.....	33
2.2.1. Activos de Información.	33
2.2.2. Ataque.....	34
2.2.3. Información.....	34
2.2.4. Seguridad de la Información	34
2.2.5. Confidencialidad	35
2.2.6. Integridad.....	35
2.2.7. Disponibilidad	36
2.2.8. Ciberseguridad	36
2.2.9. Amenazas	37
2.2.10. Vulnerabilidad	37
2.2.11. Riesgo.....	37
2.2.12. Impacto	38
2.2.13. Probabilidad	38

2.2.14.	Control	39
2.2.15.	Procedimiento.....	39
2.2.16.	Usuario	39
2.2.17.	Concienciación de usuarios.....	39
2.2.18.	Política de Seguridad de la Información.	40
2.2.19.	Análisis de riesgos	40
2.2.20.	Matriz de riesgos.....	41
2.2.21.	Gestión de Riesgos	43
2.3.	Marco Normativo.....	43
2.3.1.	Norma Técnica Peruana NTP ISO/IEC 27001:2014	43
2.3.2.	ISO 27000	44
2.3.3.	ISO 27001	45
2.3.4.	ISO 27002	45
2.3.5.	ISO 27003	47
2.3.6.	ISO 27005	47
2.3.7.	ISO 27008	48
2.3.8.	NIST CSF	49
2.4.	Marco Metodológico	50
2.4.1.	Ciclo de Deming Concepto y Descripción.....	50
2.4.2.	Método MAGERIT	52
2.4.3.	Establecimiento del Contexto	53
2.4.4.	Identificación de Riesgos.....	53
2.4.5.	Análisis de Riesgos	53
2.4.6.	Evaluación de Riesgos	54
2.4.7.	Tratamiento de Riesgos	54
2.4.8.	Monitoreo y Revisión	54
2.4.9.	Comunicación y Consulta.....	54
2.5.	Metodología PMBOK	54
2.5.1.	Estandarización y Estructura.....	55
2.5.2.	Gestión Integral del Proyecto	56
2.5.3.	Enfoque en la Calidad	56
2.5.4.	Gestión de Riesgos.....	56
2.5.5.	Adaptabilidad y Mejora Continua	56
2.5.6.	Documentación y Comunicación	56
2.5.7.	Definición de la Metodología del Proyecto.....	59
CAPÍTULO III: DESARROLLO DEL PROYECTO.....		61
3.1.	Inicio del Proyecto.....	61
3.1.1.	Entendimiento de la Organización.....	61
3.1.2.	Definición del alcance del proyecto.....	71
3.1.3.	Identificación de los interesados.	72
3.1.4.	Elaboración del Acta de Constitución del Proyecto	73
3.1.5.	Asignación de responsables del proyecto.....	73
3.2.	Planificación	73
3.2.1.	Desarrollo del plan de Gestión de proyecto	74
3.2.2.	Plan de Comunicación.....	75
3.3.	Ejecución:.....	76
3.3.1.	Elaborar un análisis de la situación actual en base a la NTP ISO 27001:2014	76

3.3.3.	Proponer controles de seguridad	97
3.3.4.	Plantear un procedimiento para Cumplimiento normativo	101
3.3.5.	Proponer Estrategias de Concienciación y capacitación.....	105
3.4.	Planes propuestos de Monitoreo y Control.....	106
3.4.1.	Planificación de Supervisión del rendimiento del SGSI.....	106
3.5.	Cierre del Proyecto	106
3.5.1.	Resultado del análisis de la situación actual en base a la NTP ISO 27001:2014.....	106
3.5.2.	Propuesta de políticas, procedimientos y controles de seguridad de información ...	109
3.5.3.	Planteamiento de Políticas y propuesta de procedimiento para Cumplimiento normativo.....	109
3.5.4.	Propuesta de Estrategias de Concienciación y capacitación	110
CONCLUSIONES.....		112
RECOMENDACIONES.....		114
ANEXOS		116
BIBLIOGRAFÍA		117

ÍNDICE DE TABLAS

Tabla 1 Presupuesto Estimado.....	26
Tabla 2 Controles de seguridad específicos.....	46
Tabla 3 Metodología del proyecto.....	59
Tabla 4 Cronograma de actividades del proyecto	74
Tabla 5 Escala y Valor de Importancia de un activo.....	79
Tabla 6 Escala de la importancia en la confidencialidad.....	80
Tabla 7 Escala de la importancia en la Integridad.....	80
Tabla 8 Escala de la importancia en la disponibilidad.....	81
Tabla 9 Escala de la importancia en la disponibilidad.....	83
Tabla 10 Catálogo de amenazas, agentes y vulnerabilidades.....	84
Tabla 11 Catálogo de vulnerabilidades	85
Tabla 12 Cuantificación y Calificación de las vulnerabilidades identificadas.....	90
Tabla 13 Nivel de impacto del riesgo	91
Tabla 14 Posibilidad de ocurrencia de un riesgo	91
Tabla 15 Degradación de activos de información.....	92
Tabla 16 Valoración de riesgos	93
Tabla 17 Efectividad de controles.....	99
Tabla 18 Propuestas para las políticas y directivas de seguridad de la información.....	102
Tabla 19 Resultado de valorización a activos de información de la UTD.....	107
Tabla 20 Resultados de autoevaluación de riesgos de seguridad de la información para la UTD	108
Tabla 21 Cantidad de Controles y Planes de tratamiento identificados.....	108

ÍNDICE DE FIGURAS

Figura 1 Componentes de un Sistema de Seguridad de la Información	32
Figura 2 La Gestión documental y trámite documentario	33
Figura 3 Etapas para el análisis de riesgos	41
Figura 4 Ejemplo de una Matriz de Riesgos	43
Figura 5 Familia de la ISO 27001	44
Figura 6 Estructura de la Norma ISO 27001.....	45
Figura 7 Norma ISO/IEC 27003.....	47
Figura 8 Ciclo PDCA Según ISO/IEC 27005	48
Figura 9 Dominios ISO/IEC 27001:2013	49
Figura 10 Plan de Mejora Continua - Ciclo de Deming	50
Figura 11 Proceso de gestión de riesgos según ISO 31000.....	53
Figura 12 Organigrama de la UNSAAC	62
Figura 13 Extracto ROF de UNSAAC	64
Figura 14 Ubicación de UTD dentro del organigrama de la UNSAAC	64
Figura 15 Manual de procedimientos de la Unidad de Trámite Documentario de la UNSAAC.....	66
Figura 16 Proceso de recepción de documentos en la UTD - UNSAAC.....	67
Figura 17 Proceso de Emisión de documentos en la UTD - UNSAAC.....	68
Figura 18 Proceso de archivo de documentos en la UTD - UNSAAC.....	69
Figura 19 Proceso de despacho de documentos en la UTD - UNSAAC.....	70
Figura 20 Identificación de activos de información	81
Figura 21 Mapa de calor de riesgos	92
Figura 22 Elementos que participan en el análisis de riesgos.....	94
Figura 23 Proceso de análisis de riesgos de activos de información	97
Figura 24 Proceso de propuesta de controles de seguridad de la información	101

CAPÍTULO I: ASPECTOS GENERALES

1.1. Antecedentes

1.1.1. *Antecedentes Internacionales*

Sistema de Gestión de Seguridad de la Información para la Subsecretaría de Economía y Empresas de menor tamaño - Tesis (NELSON ALEJANDRO YAÑEZ CACERES, 2017)

La tesis referida detalla la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Subsecretaría de Economía y Empresas de Menor Tamaño utilizando herramientas *open source* y modelos de desarrollo de mejora continua para dar cumplimiento a un subconjunto de 44 objetivos de control del anexo normativo de la norma ISO 27001:2013. La presente tesis no aborda la implementación de los 114 objetivos de control de la norma ISO 27001, pero acorta las principales brechas de seguridad de la información existentes en la entidad al cubrir en forma completa el primer ciclo PDCA del Sistema de Gestión de Seguridad de la Información, escogiendo un subconjunto de 44 objetivos de control priorizados por una análisis de brechas identificadas, incorporando las recomendaciones de DIPRES (Dirección de Presupuestos de Chile) y dicha selección se realizó por un comité de seguridad de la Información formado en el presente trabajo Las políticas y procedimientos son mantenidos en régimen mediante los seis sistemas que constituyen el SGSI y cuyo objetivo es administrar, monitorear, documentar y mejorar en forma continua la seguridad de la información La metodología que se utiliza esta tesis, se centra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información. Esta tesis plantea que la metodología de implementación de SGSI se apoye en la gestión de riesgos, utilizando las guías y buenas prácticas de la norma ISO 31000. Con ello los procesos estratégicos de la sub - secretaría son clasificados por prioridad según su exposición a los riesgos y su impacto. De esta forma se mejora la asignación de recursos a los proyectos de seguridad de la información, se favorece el aprendizaje y la creación de equipos de trabajo orientados a los objetivos prioritarios, sin que ellos desperdiciaran la visión de conjunto y objetivo final. Como análisis de la implementación del SGSI y de las políticas y

procedimientos de seguridad de la información se realizaron dos auditorías, una interna y otra realizada por una empresa externa. Ambas auditorías fueron totalmente independientes al equipo que diseñó e implementó tanto el SGSI como las políticas y procedimientos de seguridad de la información. Ambas auditorías obtuvieron a la conclusión que el estado actual de seguridad de la información está en un nivel medio. Esto es un avance valioso pues al inicio de la presente tesis no había un SGSI ni políticas y procedimientos efectivos para proteger la seguridad de la información. La principal recomendación transmitida por las auditorías fue ahondar la difusión de las políticas y procedimientos de seguridad de la información, continuar con la implementación de los restantes 70 objetivos de control de la norma ISO 27001:2013 y realizar una nueva valoración durante el 2017 del funcionamiento del SGSI, es decir se han implementado los restante objetivos de control y evaluar el grado de institucionalización de las políticas y procedimientos de seguridad de la información.

Conclusiones: La tesis destaca la jerarquiza de la seguridad de la información, la necesidad de implementar un SGSI y el desafío que enfrentan las entidades públicas en Chile para cumplir con las normativas establecidas.

Comentarios: En Perú, el Gobierno ha impulsado normativas que establecen la obligatoriedad de la implementación del SGSI en las Entidades Públicas, pero aún no se ha alcanzado el nivel de desarrollo definido en esas normas, así como el propósito del estudio es realizar una investigación estructurada y organizada, utilizando herramientas como las entrevistas, para identificar las limitaciones y facilidades que encuentran las entidades públicas en la implementación del SGSI. Se busca analizar y evaluar los aspectos que afectan el proceso de implementación y el desarrollo del Gobierno Electrónico Peruano.

1.1.2. Antecedentes Nacionales

Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca - Tesis (Roberto Carlos Fuentes Serrate, 2020)

Asegurar la confidencialidad, la integridad y la disponibilidad de la información, se ha convertido en una de las tareas fundamentales del gobierno de las tecnologías de la información (TI) en las organizaciones, sobre todo, si los procesos críticos son soportados por tecnologías de la información. Para gestionar los riesgos operativos que resultan de la dependencia de las TI, se hace necesario la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La presente tesis, plantea un SGSI para brindar seguridad a la información que se gestiona en los procesos críticos de la Universidad Nacional de Cajamarca (UNC), concretamente, en aquellos procesos que son la razón de ser de la organización, como la gestión académica y la investigación. El marco de referencia teórico que se tomó como guía para el desarrollo de la propuesta fue la ISO/IEC 27003, norma que propone una metodología de implementación de un SGSI, y que, a su vez, se sustenta en las buenas prácticas y recomendaciones de las normas hermanas, ISO/IEC 27001 e ISO/IEC 27002. Para el análisis de riesgos de TI, que es una etapa crítica de la implementación del SGSI, se tomó como referencia la metodología española MAGERIT. La validación de SGSI propuesto se realizó a través de un procedimiento no experimental, como una encuesta de satisfacción, aplicada a los usuarios de TI de la universidad. El análisis estadístico de los datos recopilados en la encuesta, que la propuesta de SGSI tiene un nivel aceptable para que pueda ser implementado.

Conclusiones: La tesis propone un SGSI basado en la norma ISO/IEC 27003 para mejorar la seguridad de la información en la Universidad Nacional de Cajamarca, abordando la evaluación de riesgos, la implementación del SGSI y validando a través de una encuesta de satisfacción.

Comentarios: La tesis propone un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27003, que consta de cinco capítulos que abordan la realidad, problemática, marco teórico, metodología de investigación, resultados, conclusiones y recomendaciones; La metodología de investigación utilizada incluye la evaluación de la situación actual de la seguridad de

la información y la gestión de riesgos, con el objetivo de identificar y tratar los niveles de riesgos no tolerables, La confidencialidad, integridad y disponibilidad de la información (CID) se consideran tareas fundamentales del gobierno de las tecnologías de la información (TI) en la universidad, especialmente cuando los procesos críticos dependen de la tecnología.

Establecimiento, Implementación, Mantenimiento y Mejora de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2013, para una Empresa de Consultoría de Software, - Tesis (Daniel Elías Santos Llanos, 2017)

Actualmente, las empresas de consultoría de desarrollo de software cuentan con muchos retos propios de este tipo de negocio. Entre estos, destacan los relacionados a la seguridad de información, pues, debido al perenne intercambio de información entre la empresa y sus clientes, aparecen riesgos potenciales que pueden comprometer el éxito e incluso el mantenimiento de la organización. La solución planteada para este problema es un Sistema de Gestión de Seguridad de Información (SGSI), el cual cuenta con el estándar ISO 27001:2013 como marco formal de requisitos a cumplir. Este sistema permitirá que los directivos y demás implicados gestionen y tomen decisiones adecuadas respecto a la seguridad de información de la organización, para asegurar que cuente con niveles apropiados para la confidencialidad, integridad y disponibilidad de la información crítica que se maneja como parte de su operación. En este informe se especifican las cuatro fases cíclicas del SGSI: el establecimiento, donde las bases del sistema se integran a los procesos del negocio; la implementación, que desarrolla los mecanismos para la adecuada administración de la seguridad; el mantenimiento, donde se detectan fallos que pueden existir en la organización o en el propio sistema; y la mejora, que finalmente permite cerrar el ciclo mediante la aplicación de todas las correcciones y optimizaciones significativas que han sido detectadas. Este modelo permite que el sistema opere bajo un principio de mejora continua, que beneficia permanentemente a la organización, propiciando un manejo adecuado de la seguridad de su información.

Conclusiones: Según lo citado resalta los desafíos de seguridad de información que enfrentan las empresas de consultoría de desarrollo de software y propone la implementación de un SGSI basado

en el estándar ISO 27001:2013. El SGSI se divide en cuatro fases cíclicas que permiten establecer, implementar, mantener y mejorar el sistema, asegurando un enfoque de mejora continua. Esto garantiza la adecuada gestión de la seguridad de la información en la organización.

Comentarios: Las empresas de consultoría de desarrollo de software enfrentan desafíos específicos relacionados con la seguridad de la información debido al intercambio constante de datos con los clientes. Estos riesgos potenciales pueden afectar el éxito y la supervivencia de la organización. La solución propuesta que aborde este problema sería la implementación de un Sistema de Gestión de Seguridad de Información (SGSI), que se basa en el estándar ISO 27001:2013. Este sistema permite a los directivos y demás involucrados gestionar y tomar decisiones adecuadas en relación con la seguridad de la información, garantizando niveles adecuados de confidencialidad, integridad y disponibilidad de la información crítica de la organización.

Desarrollo de una propuesta de implementación de la NTP ISO/IEC 27001:2014, Sistema de Gestión de Seguridad de la Información, para la Oficina funcional de Informática del Gobierno Regional Cusco -Tesis (Fressia Lisset Ariasca Suma, Sheny Katherine Quispe Borda, 2017)

La Oficina Funcional de Informática del Gobierno Regional del Cusco actualmente no cuenta con la implementación de controles eficientes, normas y estándares relacionados a seguridad de la información, siendo la información su activo más importante. Por tanto en respuesta a este problema se desarrolla el presente trabajo de tesis, que muestra las etapas de diseño y planificación de un Sistema de Gestión de Seguridad de la Información alineado a las especificaciones y requerimientos de la NTP ISO/IEC 27001:2014, adaptando este proceso al contexto de la Oficina Funcional de Informática; para lo cual se adquirió y utilizó la NTP ISO/IEC 27001:2014 para su revisión e interpretación, logrando así identificar los procesos críticos o sensibles de las etapas de desarrollo del proyecto, las cuales son: Organización, Planificación, Despliegue, Revisión y Consolidación. El objetivo de este trabajo es elaborar una propuesta de implementación de los requisitos especificados del capítulo 4 al 10 de la NTP ISO/IEC 27001:2014 que se exigen para la conformidad de un Sistema de Gestión de Seguridad de la Información. Inicialmente se realiza un diagnóstico de la situación actual

de la Oficina Funcional de Informática en función al cumplimiento de los requisitos de la norma, logrando así identificar las debilidades y falencias en temas de seguridad de la información relacionados al cumplimiento de las normas. A continuación, se identifican los procesos y actividades a llevarse a cabo en cada etapa del desarrollo del proyecto el cual es alineado a la metodología PHVA (Planificar, Hacer, Verificar y Actuar) donde a su vez se aplicaron conceptos y directrices sobre la gestión de proyectos utilizados en la guía PMBOK; posteriormente en los anexos del trabajo se realiza la documentación de los entregables que son exigidos en la norma. Finalmente, el desarrollo de esta propuesta es considerada para la institución como una guía y soporte para el inicio de las diligencias de implementación de un Sistema de Gestión de Seguridad de la Información como es exigido por ley (RM N° 004-2016-PCM).

Conclusiones: Se concluye que la implementación de la norma ISO/IEC 27001:2013 será un paso importante para garantizar la seguridad de la información en la Oficina Funcional de Informática del Gobierno Regional Cusco y mejorar la confianza en la gestión de la información.

Comentarios: La tesis propone la implementación de la norma ISO/IEC 27001:2013 en la Unidad Administrativa de Informática del Gobierno Regional Cusco, con el objetivo de garantizar la seguridad de la información. La propuesta incluye un análisis de la situación actual, la identificación de requisitos, una planificación detallada y una conclusión sobre los beneficios de implementar la norma.

1.2. Planteamiento del problema

1.2.1. Problema General

La Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco presenta ciertas carencias en seguridad de la información, lo cual compromete la confidencialidad, integridad y disponibilidad de los documentos y activos de información. La falta de un Sistema de Gestión de Seguridad de la Información basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 impide el establecimiento de controles y procesos adecuados, así como la identificación y mitigación de riesgos, lo que impacta negativamente en la eficiencia y confiabilidad de los servicios proporcionados por la Unidad de Trámite Documentario.

1.2.2. Problemas Específicos

Para proponer un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma técnica peruana NTP ISO/IEC 27001:2014 y mejorar la gestión y eficiencia en la Unidad de Trámite Documentario es necesario abordar los siguientes problemas específicos:

Falta un análisis de la situación actual en base a la NTP ISO 27001:2014

Esta dimensión consiste en desarrollar la situación actual de la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco en base a información recopilada mediante algunas reuniones y entrevistas al personal involucrado en la Gestión de la Unidad de Trámite Documentario.

Falta de políticas, procedimientos y controles de seguridad de la Información

Ausencia de políticas, procedimientos y controles técnicos y organizativos para proteger la información contra amenazas y riesgos, esto implica que no se están estableciendo medidas adecuadas o controles para garantizar la Confidencialidad, integridad y Disponibilidad de la Información en la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco.

Incumplimiento normativo de la NTP ISO 27001:2014

La Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco no cumple plenamente con los requisitos legales, regulaciones y normativas del territorio relacionadas con la seguridad de la información, así como, la NTP ISO 27001:2014, esto puede recaer en su reputación, sanciones legales, administrativas y aumenta el riesgo en incidentes de seguridad.

Falta de concienciación y capacitación sobre Seguridad de la Información

El personal de la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco no está suficientemente consciente ni capacitado en prácticas de seguridad de la información. La falta de concienciación y capacitación adecuada puede aumentar la probabilidad de cometer errores y de que los empleados no sigan prácticas seguras en la gestión de documentos y datos.

1.3. Objetivos

1.3.1. Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma técnica peruana NTP ISO/IEC 27001:2014 para la gestión en la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco.

1.3.2. Objetivos Específicos

1. Analizar la situación actual del proceso de Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco en base a la NTP ISO 27001:2014
2. Elaborar una propuesta de políticas, procedimientos y controles de seguridad de la Información para la Universidad Nacional de San Antonio Abad del Cusco en base a la NTP ISO 27001:2014
3. Proponer un modelo de mejora continua en el cumplimiento normativo de la Universidad Nacional de San Antonio Abad del Cusco basado en la NTP ISO 27001:2014
4. Establecer estrategias de concienciación y capacitación de seguridad de la información para la Universidad Nacional de San Antonio Abad del Cusco

1.4. Justificación

La justificación para abordar los problemas mencionados en el plan de tesis "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TÉCNICA PERUANA NTP ISO ISO/IEC 27001:2014 PARA LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO " se basa en varios aspectos:

1.4.1. Falta de Análisis de situación actual en base a la NTP ISO 27001:2014

La Universidad Nacional de San Antonio Abad del Cusco almacena y procesa una gran cantidad de datos sensibles, incluyendo información personal de estudiantes, profesores y empleados. Conocer la situación actual de seguridad de la información es esencial para proteger estos datos y evitar posibles violaciones de la privacidad.

Las instituciones educativas son un objetivo atractivo para los ciberdelincuentes debido a la cantidad de datos valiosos que manejan. La situación actual de seguridad debe evaluarse para identificar y

mitigar posibles amenazas cibernéticas.

Las violaciones de seguridad de la información pueden dañar seriamente la reputación de la universidad. Conocer y mejorar la seguridad de la información ayuda a mantener la confianza de los estudiantes, profesores, padres y otros interesados en la institución.

Un incidente de seguridad importante puede interrumpir las operaciones de la universidad. Conocer la situación actual de seguridad es esencial para garantizar la continuidad de las operaciones académicas y administrativas.

La evaluación de la situación actual de seguridad permite identificar y evaluar los riesgos relacionados con la información. Esto es fundamental para tomar decisiones informadas sobre la asignación de recursos y la implementación de medidas de seguridad.

Conocer la situación actual de seguridad es un primer paso importante para educar y concienciar a todos los miembros de la comunidad universitaria sobre la importancia de la seguridad de la información. Una comunidad informada es más propensa a colaborar en la protección de los datos.

La tecnología y las amenazas cibernéticas evolucionan constantemente. Conocer la situación actual de seguridad es crucial para mantenerse al día con las mejores prácticas y las soluciones de seguridad más recientes.

Comprender la situación actual de seguridad permite asignar recursos de manera más eficiente, identificando las áreas que requieren mayor atención y aquellos controles que pueden necesitar mejoras.

1.4.2. Falta de políticas, procedimientos y controles de seguridad de información

La Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco maneja documentos y datos sensibles que requieren una protección adecuada. La falta de un sistema de gestión de seguridad de la información y de controles efectivos pone en riesgo la confidencialidad, integridad y disponibilidad de esta información, lo cual puede tener consecuencias graves como la divulgación no autorizada, la alteración o la pérdida de datos valiosos.

1.4.3. Incumplimiento normativo de la NTP ISO/IEC 27001:2014

Las universidades a menudo están sujetas a regulaciones y leyes de protección de datos. Conocer la implementación de un SGSI basado en la norma NTP ISO/IEC 27001:2014 permite cumplir con los requisitos legales, regulaciones y normativas relacionadas con la seguridad de la información. Cumplir con estas exigencias es fundamental para evitar posibles sanciones legales, daños a la reputación de la institución y pérdida de confianza por parte de los usuarios y clientes.

1.4.4. Falta de capacitación y concienciación de Seguridad de la Información

Se brinda a los empleados la comprensión necesaria de las políticas y procedimientos de seguridad de la información establecidos. Esto les permite saber cómo manejar la información de manera segura, qué prácticas deben seguir y cómo responder adecuadamente a incidentes de seguridad. El conocimiento de las políticas y procedimientos contribuye a establecer una cultura de seguridad en toda la organización. Generando conciencia de aplicabilidad resiliente de Seguridad de la Información. Esto implica una mayor agilidad en los trámites, reducción de errores y garantía de la integridad de la información, lo cual contribuye a la satisfacción de los usuarios y a una mejor imagen institucional.

Finalmente, es importante; Porque definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva frente a otras entidades educativas que no aplican técnicas de capacitación en seguridad de la información, esto nos ayudará en mejorar el flujo en los procesos evitando la degradación de información. (Carlos Arturo Avenía, 2017)

1.5. Alcances y delimitaciones

1.5.1. Alcances.

Alcance Geográfico.

El proyecto se centrará exclusivamente en la Unidad de Tramite Documentario – UTD de la Universidad Nacional de San Antonio Abad del Cusco - UNSAAC, en la ciudad del Cusco.

Alcance de Normativas.

El estudio se basará y centra en la norma técnica peruana NTP ISO/IEC 27001:2014 así como las mejores prácticas internacionales para la gestión de seguridad de la información.

Alcance de Datos

El proyecto considerará la seguridad de la información relacionada con datos brindados por personal de la Unidad de Tramite Documentario – UTD, siendo ellos los dueños de los procesos de gestión documental. Esto se considera dentro de la metodología una autoevaluación de riesgos y es posible la omisión involuntaria de alguna información o activo por el dueño del proceso y/o personal de la unidad.

Alcance de Procesos

El diseño del sistema de gestión de seguridad de la información abordará procesos clave, como la clasificación de activos de información, clasificación de datos, acceso a sistemas usados en la unidad de trámite documentario, la gestión de incidentes, y la concienciación de seguridad de la información.

1.5.2. Delimitaciones.

Esta investigación sólo abarcará la fase de Diseño del Sistema de Gestión de Seguridad de Información para la Unidad de Trámite Documentario - UTD de la Universidad Nacional de San Antonio Abad del Cusco. Esta delimitación establece que la investigación no cubrirá otras fases del ciclo de vida del SGSI, como la implementación, la operación o la mejora continua, considerando que depende de la aprobación futura de los jefes de Unidad o de Departamento y las limitaciones de recursos financieros y humanos que pueden restringir la implementación completa del sistema de gestión de seguridad de la información. Esto será considerado en las recomendaciones.

Exclusión de Auditoría Externa y certificación del sistema de gestión de seguridad de la información no estará dentro del alcance del proyecto, será considerado en las recomendaciones para una etapa posterior.

El proyecto se llevará a cabo durante un período específico de tiempo, y las conclusiones se basarán en la situación de seguridad de la información en ese momento.

Se tiene considerando el análisis de riesgos determinados por el dueño del proceso de la Unidad de Tramite Documentario - UTD de la Universidad Nacional de San Antonio Abad del Cusco, excluyendo otras unidades o departamentos.

Las consideraciones legales y regulatorias específicas están fuera del alcance del proyecto, se considera en las recomendaciones finales el asesoramiento legal adicional.

Los talleres de análisis de riesgos se llevarán a cabo con los actores principales de ejecución del procedimiento.

1.6. Estudio de factibilidad

1.6.1. Factibilidad Técnica

La factibilidad técnica del proyecto será utilizando recursos humanos y tecnológicos disponibles, conocimiento, compromiso y autorización respectiva de las Autoridades correspondientes. Para el caso del ofrecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) establecido acorde a la Norma Técnica Peruana NTP ISO/IEC 27001:2014, la factibilidad técnica se evaluó considerando que la Unidad de Tramite Documentario cuenta con personal idóneo y con la experiencia suficiente para poder brindar el entendimiento de los procesos del área.

Así también mediante buenas prácticas se gestionó las debidas autorizaciones y coordinaciones requeridas para la disponibilidad de tiempo e información, considerando tener un compromiso de confidencialidad con las partes.

La Unidad de Tramite Documentario tiene los equipos de cómputo necesarios para evidenciar la ejecución de procesos.

Por ende, el proyecto de tesis Diseño de un Sistema de Gestión de Seguridad de la Información establecido bajo la Norma Técnica Peruana NTP ISO/IEC 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco es factible.

1.6.2. *Factibilidad Económica*

La factibilidad económica del proyecto de tesis sobre el diseño de un SGSI establecido a base en la NTP ISO 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco parece positiva, dado que los beneficios esperados en términos de seguridad de la información mejorada, cumplimiento normativo, eficiencia operativa y reputación institucional superan los costos estimados de implementación. Invertir en un SGSI robusto no solo mitiga riesgos significativos, sino que también posiciona a la universidad como líder en la gestión de la seguridad de la información, proporcionando un retorno de inversión tanto tangible como intangible.

Costos estimados de recursos humanos

Los costos relacionados a la remuneración de los bachilleres de Ingeniería Informática y de Sistemas se estimaron según escala remunerativa acorde a este tipo de proyectos y experiencia según su certificación que se detallan a continuación:

Tabla 1
Presupuesto Estimado

Detalle	Cantidad	Monto
Servicios de consultoría	4 meses	20,000.00
Libros	3	460.00
ISO 27001	1	475.00
Analistas de Seguridad de la Información	4 meses x 2	24,000.00
Útiles de escritorio	-	120.00
Laptop	2	6,000.00
Servicio de internet	4 meses	400.00
Total		51,455.00

Fuente: Elaboración propia

En la tabla 1 se estima el costo del proyecto de implementación y es factible económicamente puesto que la unidad de Tramite Documentario de la Universidad Nacional San Antonio Abad de Cusco podría solicitar asignación de un presupuesto para desarrollo de proyectos.

Por ende, el proyecto de tesis Diseño de un Sistema de Gestión de Seguridad de la Información Basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco es factible Económicamente.

1.6.3. Factibilidad Operativa

La factibilidad operativa evalúa la capacidad de la organización para implementar y mantener el proyecto en términos de recursos tecnológicos, humanos, procesos y gestión operativa. Para el proyecto de tesis sobre el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma Técnica Peruana NTP ISO 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco de la unidad de Tramite Documentario, se deben considerar los siguientes aspectos:

El desarrolló un plan de gestión de cambios para abordar cualquier modificación producto de la implementación del SGSI y para asegurar una transición identificada.

La coordinación con las jefaturas de línea para involucrar a todas las partes interesadas desde el principio para obtener su apoyo y compromiso.

Validaciones necesarias para que la infraestructura tecnológica actual sea adecuada para soportar el SGSI.

Por ende, el proyecto de tesis Diseño de un Sistema de Gestión de Seguridad de la Información Basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 para la Universidad Nacional de San Antonio Abad del Cusco es factible Operativamente.

1.7. Metodología

1.7.1. Tipo de la Investigación

(Robert R. Sherman, Rodman B. Webb, 1988) Enfatiza que la investigación cualitativa busca comprender el significado de los fenómenos desde la perspectiva de los participantes. La orientación hacia la comprensión del significado de los fenómenos desde la perspectiva de los usuarios.

En el contexto de la seguridad de la información, esto significa comprender cómo los distintos usuarios

perciben las amenazas, las vulnerabilidades y puede accionar oportunidades de mejora y planes de acción y contrarrestarlas.

(Michael Quinn Patton, 2010) Define los datos cualitativos como descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones.

El enfoque cualitativo es ideal para obtener una comprensión profunda y contextualizada de los desafíos y necesidades específicas de la Universidad Nacional de San Antonio Abad del Cusco en relación con la seguridad de la información. Las descripciones detalladas proporcionadas por los datos cualitativos permitirán captar los eventos del entorno.

Definido el enfoque cualitativo está alineado con el objetivo de diseñar un sistema de gestión de seguridad de la información que sea efectivo y contextualmente adecuado. Al captar las percepciones y experiencias de los usuarios, podemos diseñar un sistema que no solo cumpla con los estándares técnicos, sino que también se adapte a las realidades y necesidades específicas de la Universidad Nacional de San Antonio Abad del Cusco.

(Willian Jhoel Murillo Hernandez, 2008) Indica que la investigación aplicada recibe el nombre de “investigación práctica o empírica”, que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad.

La investigación aplicada se centra en resolver problemas específicos y prácticos. En este caso, el objetivo es desarrollar un sistema de gestión de seguridad de la información que aborde las necesidades y desafíos particulares de la universidad, garantizando la protección de la información y el cumplimiento de las normativas pertinentes.

1.7.2. Nivel de la Investigación

Esta investigación adopta un enfoque descriptivo, el cual se basa en la observación e interpretación de los resultados obtenidos a partir de la recolección de información a través de encuestas y entrevistas. Méndez (2003) indica que en este tipo de estudio se observa, describe y

fundamentan varios aspectos del fenómeno, no existe la manipulación de las variables, tampoco la búsqueda de causa efecto. (Valmi D. Sousa, Martha Driessnack, Isabel Amélia Costa Mendes, 2007) Precisa que la investigación descriptiva utiliza criterios sistemáticos que permiten revelar la estructura de los fenómenos en estudio y también ayuda a identificar comportamientos específicos mediante el uso de técnicas particulares para la recopilación de información en búsqueda de describir y analizar los hechos y características de un fenómeno o situación específica.

En el caso de un proyecto de tesis para implementar un Sistema de Gestión de Seguridad de la Información con ISO 27001 para la gestión de trámite documentario de la Universidad Nacional San Antonio de Cusco, la investigación descriptiva se enfocará en describir y analizar los aspectos relacionados con la seguridad de la información en el proceso de trámite documentario en la Universidad Nacional San Antonio de Cusco. Finalmente, se describirán las conclusiones y recomendaciones de la investigación, incluyendo la importancia de implementar un sistema de gestión de seguridad de la información en el proceso de trámite documentario y cómo esto contribuirá a garantizar la seguridad de la información en la Universidad Nacional San Antonio de Cusco.

1.7.3. *Diseño de la Investigación*

Yin (2018) precisa que el estudio de caso es especialmente útil para investigaciones aplicadas cuando se necesita analizar un sistema, proceso o contexto organizacional con el objetivo de proponer mejoras basadas en un entendimiento detallado del entorno.

Esta afirmación sustenta la necesidad de utilizar un diseño de caso en el proyecto de tesis, ya que la implementación de un sistema de gestión de seguridad de la Información requiere comprender profundamente el entorno específico de la Unidad de Tramite Documentario. En este caso, la universidad tiene procesos únicos relacionados con la gestión de la información, que deben ser evaluados para identificar riesgos, brechas y necesidades particulares. Yin resalta la capacidad del estudio de caso para contextualizar soluciones prácticas y orientadas a la mejora organizacional, lo cual es esencial para alinear un SGSI con los estándares de la ISO 27001

Creswell (2014) indica que el diseño cualitativo aplicado es una herramienta poderosa para estudiar

problemas prácticos en contextos específicos, facilitando la generación de propuestas alineadas con las necesidades del entorno.

Esta perspectiva previa enfatiza el aspecto práctico del diseño cualitativo aplicado, lo que es particularmente relevante en un SGSI. La implementación de un sistema de gestión requiere más que un marco teórico, necesita propuestas viables y ajustadas a las limitaciones y capacidades de la organización. Un enfoque cualitativo permite recopilar información detallada de los involucrados, como los responsables de TI, usuarios finales y líderes organizacionales, para garantizar que las soluciones propuestas sean realistas, prácticas y efectivas dentro del contexto organizacional.

El diseño de la investigación con estudio de caso, debido a su enfoque en analizar el estado actual y proponer un sistema de gestión de seguridad de la información para mejorar los procesos de la Unidad de Tramite Documentario de la Universidad Nacional San Antonio Abada del Cusco.

En conclusión, la Investigación está definida para ser una Investigación Aplicada porque busca resolver un problema específico y práctico relacionado con la seguridad de la información en la universidad. Definida como Cualitativa porque se utilizarán métodos cualitativos para obtener una comprensión profunda de las necesidades y percepciones de los usuarios del sistema. Descriptiva considerando que el estudio describirá detalladamente la situación actual y las necesidades de seguridad de la información de la universidad. Con estudio de caso adecuado para el análisis y mejora del objetivo.

CAPÍTULO II: MARCO TEÓRICO

2.1. Bases Teóricas

2.1.1. *Sistema De Gestión De Seguridad De La Información*

Un SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. (Neira, 2005)

Un SGSI desde la visión del estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (por ejemplo, en empresas públicas, organizaciones sin ánimo de lucro, etc.). (Neira, 2005)

Un Sistema de Gestión de Seguridad de la Información (SGSI) consta de políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. (Ministros, 2024) El análisis de los requisitos para la protección de los activos de información y la aplicación de los controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI. (Ministros, 2024)

La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming” PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). (TI, 2019) en adelante se muestra en la Figura 1 los componentes que describen gráficamente los componentes de un SGSI.

Figura 1
Componentes de un Sistema de Seguridad de la Información



Fuente: (Anita Guerra, 2024)

En la figura 1 se muestra los componentes de un Sistema de Gestión de Seguridad de la Información, que contiene un conjunto de políticas, procedimientos, procesos y tecnologías diseñados para proteger la información de una organización contra amenazas internas y externas, garantizando su confidencialidad, integridad y disponibilidad, a través del Ciclo de Deming.

2.1.2. Trámite Documentario.

La gestión documental es el conjunto de prácticas, normas y tecnologías utilizadas para administrar los documentos en una organización. Esto incluye tanto los documentos recibidos como los creados internamente. Es esencial para mantener la integridad, accesibilidad y eficiencia de la información en una organización. (Docuware, 2024)

La gestión de trámite documentario es el registro, almacenamiento y recuperación de documentos. (Exact, 2021), que a continuación se ilustra en un gráfico referencial.

Figura 2
La Gestión documental y trámite documentario



Fuente: (Exact, 2021)

Según lo descrito anteriormente y como se muestra en la figura 2, se entiende que una gestión de trámite documentario es una base de datos de información variada y que debe ser utilizada alineada a buenas prácticas de gestión que podrían incluir tecnologías y normatividad para su administración.

2.2. Términos Básicos

2.2.1. *Activos de Información.*

En la Gestión de la Seguridad de la Información, los activos se refieren a cualquier elemento valioso para una organización que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso. Esta definición incluye no sólo herramientas tangibles, como hardware, software y equipos de red, sino también los intangibles, como información, conocimientos, propiedad intelectual y reputación. (Sophie Danby, 2023)

Es un recurso del sistema informático y necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no, ejemplo los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc. (Eduardo Amable Samaniego Mena, 2021)

Según las definiciones antes indicadas y para un Sistema de Gestión de Seguridad de la Información, los activos de información son todo lo significativamente valioso que posee, desde documentación en distintos tipos de almacenamiento (físico y/o digital) incluyendo a las personas que trabajan en ella

(recursos humanos), sus equipos de comunicación físicos y digitales para conseguir los objetivos trazados por la dirección de una organización. Estos activos deberán ser protegidos frente a situaciones o amenazas que puedan afectarlas de manera negativa.

2.2.2. Ataque

Es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control de este y pueden llegar a poner en riesgo una entidad o sistema. (Eduardo Amable Samaniego Mena, 2021)

En seguridad de la información un ataque es la manifestación de una vulnerabilidad en la que puede resultar afectada uno o varios activos de información y poner en riesgo la confidencialidad, integridad y/o disponibilidad de una organización.

2.2.3. Información

La información constituye un activo importante y esencial para las necesidades empresariales de una organización, la misma que puede existir de muchas maneras, puede ser impresa, escrita en papel, almacenada electrónicamente, ser transmitida por medio electrónicos, se puede mostrar en videos o exponer oralmente. (I&T Solutions, 2022)

Es la acción de la presentación de informes, sobre la base de un informe de noticias sobre algo, declarar aprendido. Este término también se utiliza para referirse a los conocimientos que añade a los que ya posee en una zona determinada, y por extensión, se llama de esta manera también a esos conocimientos. (Carlos Arturo Avenía, 2017)

Según lo descrito en el párrafo anterior, información es el conocimiento sobre una determinada materia que a su vez se convierte en conocimiento.

2.2.4. Seguridad de la Información

La seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. (Edgar Vega Briceño, 2021)

Es la protección de la información y de los sistemas de información del acceso, uso, divulgación y destrucción no autorizada a través de estándares, procesos, procedimientos, estrategias, recursos

informáticos, recursos educativos y recursos humanos. (Carlos Arturo Avenía, 2017).

En ese entender podemos afirmar que la seguridad de la información es un concepto que incluye términos y definiciones para mantener protegida la información en sus diferentes representaciones y medios de almacenamiento utilizando estándares, procesos, estrategias y recursos para evitar la destrucción o accesos a información no autorizada. Según diferentes autores añaden términos como Autenticidad y Protección de Datos Personales dentro del concepto de seguridad de la información. Para el desarrollo en este tema de investigación se tomará en cuenta lo definido por la ISO/IEC 27001 en todas sus publicaciones, que se enfoca básicamente en la protección de la triada C-I-D (Confidencialidad, Integridad y Disponibilidad)

2.2.5. Confidencialidad

La confidencialidad es la propiedad por la cual la información no esté disponible ni sea divulgada a individuos, organismos o procesos no autorizados. (I&T Solutions, 2022)

La confidencialidad asegura que sólo el personal autorizado accede a la información que le corresponde para usar los recursos que necesita en la realización de sus actividades. (Eduardo Amable Samaniego Mena, 2021)

Este concepto en seguridad de la información da conocer que la información deberá estar protegida contra accesos no autorizados, en tal sentido únicamente personas con autorizaciones permitidas o ciertos privilegios puedan acceder a ella.

2.2.6. Integridad

La integridad es la propiedad de proteger la precisión y la totalidad de los activos. (I&T Solutions, 2022)

Este principio garantiza la autenticidad y exactitud de la información en cualquier momento que se solicitó o se envía de un entorno tecnológico en que los datos no han sido alterados o destruidos de forma no autorizada. . (Carlos Arturo Avenía, 2017)

Consiste en asegurarse que la información no se pierda ni este comprometida, ya que el hecho de trabajar con información errónea puede acarrear que se forme una cadena de errores y se tomen

decisiones equivocadas. (Eduardo Amable Samaniego Mena, 2021)

Este concepto en el ámbito de seguridad de la información da a entender que la información almacenada debe ser íntegra y completa sin ningún tipo de daño, adulteración o cambio no autorizado o en su defecto se debe conocer al autor, momento del cambio y justificación.

2.2.7. Disponibilidad

La disponibilidad es la propiedad de estar accesible y ser utilizable a demanda por parte de un organismo autorizado. (I&T Solutions, 2022)

La disponibilidad permite que la información esté disponible para quien la necesita, para ello hay que implementar las medidas necesarias para que tanto la información como los permisos estén disponibles. (Eduardo Amable Samaniego Mena, 2021)

Disponición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio; la disponibilidad afecta directamente a la productividad de las organizaciones. (Miguel Angel Amutio Gómez, 2012)

Para seguridad de la información se deberá entender que “Disponibilidad” hace referencia a que la información deberá estar disponible a quien tenga los permisos necesarios para acceder a ella cuando se requiera.

2.2.8. Ciberseguridad

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes. (Kaspersky Lab, 2024)

Para este contexto, afirmamos que la ciberseguridad está comprometida con la protección de activos de información de una organización, para lo cual se utilizan diferentes herramientas, conceptos, metodologías, políticas, buenas prácticas entre otras actividades que nos ayudan a mantener segura la información, a sus usuarios y ambiente en el que interactúan.

2.2.9. Amenazas

Una amenaza es una acción que podría resultar en la violación, interrupción o corrupción de un sistema mediante la explotación de vulnerabilidades conocidas o desconocidas. (Eduardo Amable Samaniego Mena, 2021)

Una amenaza para un sistema informático es una circunstancia que tiene el potencial de causar daños o pérdidas. Es decir, las amenazas pueden dar lugar a un ataque en el equipo. (Carlos Arturo Avenía, 2017)

El término amenaza en seguridad de la información es una condición en la que un activo puede ser vulnerado causando o provocando que un sistema o subsistema presente funcionamiento defectuoso o no esperado, esta amenaza puede ser causa de un ataque o derivar de causas ajenas a un proceso o sistema en la organización.

2.2.10. Vulnerabilidad

Es cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo. (Eduardo Amable Samaniego Mena, 2021)

Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software. (Carlos Arturo Avenía, 2017) Según estas definiciones se entiende que una vulnerabilidad está asociada a un activo el cual contiene debilidad o **falta de control** en él y que puede representar un riesgo o futuro fallo en un sistema, aplicación o exposición negativa de los activos en la entidad.

2.2.11. Riesgo

Efecto de la incertidumbre sobre los objetivos, puede ser positivo o negativo o ambos y puede tratar, crear o dar lugar a oportunidades o amenazas. Los objetivos pueden tener diversos aspectos y categorías, y pueden ser aplicados en diversos niveles. El riesgo se expresa generalmente en términos de fuentes de riesgo, acontecimientos potenciales, sus consecuencias y su probabilidad. (ISO

31000:2018, 2018)

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. (Eduardo Amable Samaniego Mena, 2021)

Para seguridad de la información y según lo antes definido, riesgo es la existencia y exposición de una amenaza detectada y que esta pueda llegar a ocurrir y cause impactos negativos, positivos o ambos a los objetivos de una organización.

2.2.12. Impacto

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal; estas consecuencias para la empresa reciben el nombre de impacto. Dicho de otra forma, el impacto sería el alcance producido o daño causado en caso de que una amenaza se materialice. (Eduardo Amable Samaniego Mena, 2021)

Para la seguridad de la información un impacto se entiende por una pérdida o degradación de un activo debido a que una amenaza se ha concretado o se volvió en una realidad por falta de prevención o control. Este impacto puede afectar todo tipo de activo de información en una organización.

2.2.13. Probabilidad

En la terminología de administración/gestión de riesgos (3.2), la palabra “probabilidad” se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado). (ISO 31000:2018, s.f.)

El concepto o definición de probabilidad puede diferir según las materias del estudio dónde se aplique, pero para el caso de seguridad de la información el concepto antes mencionado nos da a entender que una probabilidad nos podría indicar la frecuencia y resultado de una situación específica realizada mediante un experimento.

2.2.14. Control

Un control es una medida para ayudarnos a mitigar el riesgo, podemos establecer que un control o controles nos ayudan a garantizar contra un tipo determinado de amenaza. Estas medidas se denominan controles. (Edgar Vega Briceño, 2021)

Medida que modifica un riesgo. (ISO 31000:2018, s.f.)

Esta definición de control da a comprender que nos ayuda a disminuir, modificar o reducir un riesgo una vez este sea identificado.

2.2.15. Procedimiento

Se denomina procedimiento al conjunto de instrucciones, controles, etc. que hacen posible la resolución de una cuestión específica. (Licencia Creative Commons, 2024)

Entonces podemos diferenciar que existe una diferencia entre un Proceso y Procedimiento, mientras un proceso se ejecuta en un determinado momento para llevar a cabo una tarea común, un procedimiento es una manera de realizar las cosas, sigue un método o un esquema para ejecutar una actividad asignada.

2.2.16. Usuario

Persona que utiliza un equipo. Si el equipo está conectado a una red, un usuario puede tener acceso a los programas y archivos del equipo, así como a los programas y archivos que se encuentran en la red (en función de las restricciones de cuenta determinadas por el administrador de la red) En definitiva, es cualquier persona que precise o utilice un sistema de proceso de datos. (Licencia Creative Commons, 2024)

Se entiende por Usuario que es una persona a quien se le asigno un recurso o servicio definido para realizar una actividad definida, un usuario no necesariamente debería ser una persona con experiencia en administrar, crear o modificar un sistema, un usuario podría ser una persona sin mucha experiencia a quien se le puede capacitar previamente para realizar una determinada actividad.

2.2.17. Concienciación de usuarios

La concienciación es una actividad que tiene como objetivo el poder educar a los usuarios técnicos y no técnicos que hace vida activa con tecnologías, sobre las amenazas y riesgos que existen

y a los que se exponen diariamente al compartir información a través de un dispositivo. (Martín Frias, 2021)

Es importante la concientización o concienciación de todos los usuarios dentro de una organización, esto para evitar posibles riesgos y pérdidas asociados a los activos de información. Como parte de la concientización es muy importante la capacitación de los usuarios para que no sean víctimas de engaños por parte de actores externos/internos a la organización, esto es vital dentro de organizaciones, ya que de esta depende que los riesgos o pérdidas se minimicen o mitiguen mediante planes de seguridad o capacitación constante a los usuarios de la organización.

2.2.18. Política de Seguridad de la Información.

La Política de Seguridad de la Información persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio. (GRUPO ACS, 2022)

Podemos entender por Políticas de Seguridad de la Información como un instructivo desarrollado o creado para mantener a buen recaudo la información física o digital de una entidad u organización, y que esta política debe de ser que ser divulgada o informado a los interesados o responsables de los procesos de negocio y debe de tener el apoyo y compromiso de los principales directivos o funcionarios de la entidad.

2.2.19. Análisis de riesgos

En un sistema de seguridad de la información de una organización debe tener en cuenta todos los elementos o activos que lo comprenden, analizar su nivel de vulnerabilidad de cada uno, con el fin de identificar y evaluar las posibles amenazas del impacto causaría un ataque contra el sistema.

El personal y el equipo de seguridad serán responsables de analizar cuidadosamente cada uno de los elementos que lo conforman, a veces el abandono mínimo de un elemento débil en cuestión, ha producido fallos de seguridad importantes. Ellos se interrelacionan y a cualquier descuido puede

causar errores inesperados en los efectos de negocio sobre la organización . (Carlos Arturo Avenía, 2017).

Figura 3
Etapas para el análisis de riesgos



Fuente: (Escuela Superior de Administración Pública., 2020)

En la figura 3 se muestra las etapas de un análisis de riesgo, que consta en la clasificación de todos los activos de una organización, estos activos deben ser analizados con la finalidad de detectar posibles vulnerabilidades o amenazas que pudieran causar impacto negativo o un ataque en la organización, es responsabilidad del personal verificar los activos para minimizar posibles fallas que traigan consecuencias que puedan degradar a la organización.

2.2.20. *Matriz de riesgos*

La matriz de riesgos es un documento que permite identificar las actividades de una empresa, los riesgos inherentes a las mismas y la probabilidad de que estos riesgos se acaben materializando. Por lo general, es una herramienta flexible, que ha de documentar los procesos y evaluar el riesgo integral de una organización. Por ello, es necesario que participen en su elaboración las unidades de negocios, operativas y funcionales de la compañía.

Esta matriz consta de dos ejes:

Horizontal: Se sitúa el impacto o consecuencias que tendría la materialización de cada uno de los riesgos identificados.

Vertical: Se representa la probabilidad de que cada uno de los riesgos anteriores ocurra o se materialice.

Los riesgos en una matriz sirven para tomar decisiones, ya que los riesgos que estén más arriba y a la derecha, por ejemplo, pueden ser los riesgos en los que hay que tomar acciones directas y radicales. Por el contrario, los que estén abajo y a la izquierda, pueden ser los que tengan menor probabilidad y consecuencia. Estos últimos no serán tratados o serán aceptados simplemente.

La elaboración de la matriz de riesgo ha de contar con los siguientes elementos:

1. Identificación de riesgos: El documento debe contener la identificación de los riesgos asociados a las actividades de la empresa. Estos riesgos pueden ser inherentes a la propia actividad de la empresa (por ejemplo, que un banco se vea afectado por una crisis financiera mundial). Unos factores o riesgos inherentes pueden ser más relevantes que otros, por lo que es necesario establecer una prioridad.

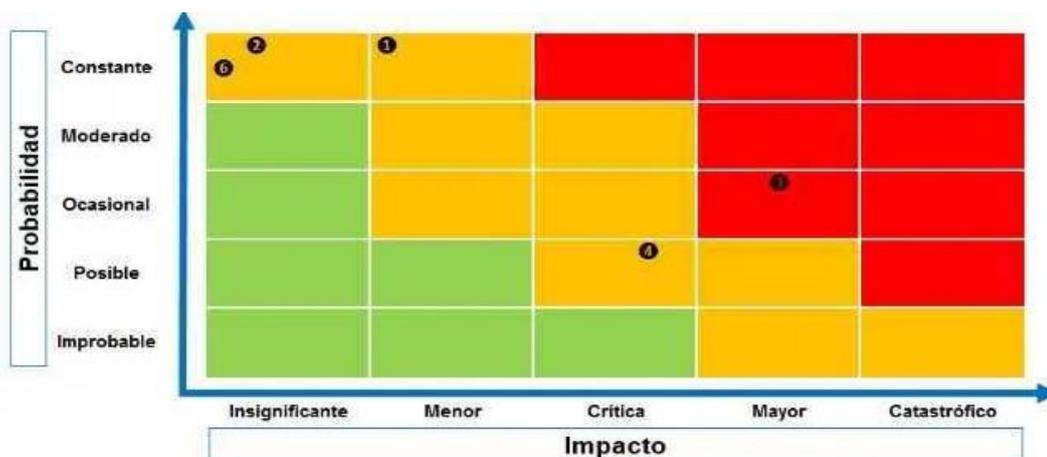
2. Determinar la probabilidad y el impacto de los riesgos: Como vimos en su definición, otro elemento que debe contener toda matriz de riesgos es el apartado de probabilidad. Es decir, se ha de establecer una clasificación donde se establezca la probabilidad de que un riesgo ocurra. Esta clasificación puede ser cualitativa o cuantitativa. Además de la probabilidad de que ocurran los riesgos, es necesario incluir en este apartado el impacto que puede tener sobre la compañía (puede ser bajo, medio o alto, por ejemplo).

3. Evaluación de la calidad de gestión: Tras realizar la valoración del riesgo, el siguiente paso imprescindible a la hora de crear una matriz de riesgos es evaluar si los controles establecidos por la empresa para mitigar los riesgos son eficaces. Esto ayudará a reducir el indicador de riesgo inherente neto de la empresa.

4. Calcular el riesgo neto o residual: Este elemento se calcula teniendo en cuenta el grado de materialización de los riesgos inherentes y la gestión establecida por la administración para mitigar esos riesgos. Conociendo el "riesgo residual", la dirección de la empresa podrá tomar mejores decisiones para continuar o no con una actividad, en función de su nivel de riesgo, o reforzar los controles sobre los mismos. (Alejandro Riveros, 2023).

A continuación, en la figura 4 se muestra gráficamente lo indicado sobre una matriz de riesgos:

Figura 4
Ejemplo de una Matriz de Riesgos



Fuente: (Alejandro Riveros, 2023)

2.2.21. Gestión de Riesgos

Es el proceso que se realiza para **identificar y gestionar los riesgos a los que puede estar expuesta la organización**, además, para validar la eficiencia de los controles y crear planes de acción que ayude a mitigarlos, aprovecharlos o en caso de que no se puedan prevenir contar con una estrategia que permita reducir las pérdidas.

En muchas ocasiones, estas amenazas o riesgos también pueden crear valor, pues las empresas establecen métodos para generar un equilibrio entre los objetivos de crecimiento, rentabilidad y los riesgos a los que están asociados para contar con una consecución adecuada.

Aunque la gestión de riesgos es liderada por los directores o la junta directiva, es importante saber que es un tema que debe involucrar a todos los miembros de la entidad y por ende se debe crear e implementar una cultura de riesgos. (Pirani Risk, 2024)

2.3. Marco Normativo

2.3.1. Norma Técnica Peruana NTP ISO/IEC 27001:2014

Esta norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de una organización, También incluye requisitos para su evaluación y tratamiento de los riesgos de seguridad de la información. Los requisitos de esta norma son genéricos y están hechos para aplicarse a todas las organizaciones sin importar su tamaño, tipo o naturaleza. (Gobierno del Perú, 2023)

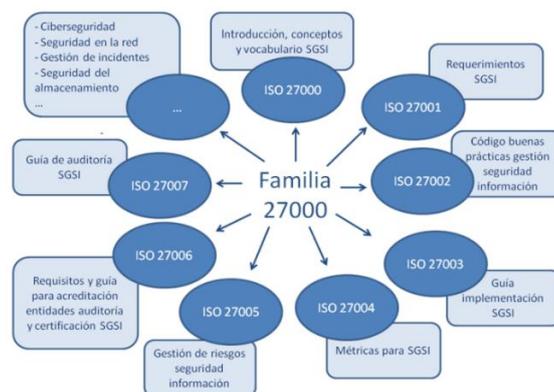
El plan de desarrollo está descrito en la Resolución Ministerial N°004-2016-PCM, del 8 de enero del 2016, en la cual se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de Seguridad, Sistema de Gestión de Seguridad de la Información. Requisitos 2da Edición, en todas las entidades integrantes del sistema Nacional de Informática. (Presidencia de Consejo de Ministros., 2016)

En resumen, la NTP ISO/IEC 27001:2014 es un estándar de referencia para la implementación y el mantenimiento de un sistema de gestión de seguridad de la información efectivo y eficiente, que ayuda a las organizaciones a proteger los activos informáticos y la información confidencial y sensible.

2.3.2. ISO 27000

ISO/IEC 27000 es un conjunto de estándares internacionales que se centran en la gestión de la seguridad de la información en las organizaciones. Estos proporcionan un marco integral para establecer, implementar, mantener y mejorar continuamente la seguridad de la información dentro de una empresa; En particular, la serie ISO 27000 se centra en proporcionar un marco para la gestión de la seguridad de la información en las organizaciones. (Soraya Jiménez Beamud, 2016)

Figura 5
Familia de la ISO 27001



Fuente: (Soraya Jiménez Beamud, 2016)

La figura 5 nos muestra algunos integrantes de la familia 27000.

En resumen, la ISO 27000 contiene y proporciona las bases y el lenguaje común para el resto de las normas de la serie.

2.3.3. ISO 27001

ISO/IEC 27001 es el estándar más conocido del mundo para sistemas de gestión de seguridad de la información (SGSI). Define los requisitos que debe cumplir un SGSI. (International Organization for Standardization, 2022)

La norma ISO/IEC 27001 proporciona a empresas de cualquier tamaño y de todos los sectores de actividad orientación para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. (International Organization for Standardization, 2022)

La conformidad con ISO/IEC 27001 significa que una organización o empresa ha implementado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja la empresa, y que este sistema respeta todas las mejores prácticas y principios consagrados en esta Norma Internacional. (International Organization for Standardization, 2022)

Figura 6
Estructura de la Norma ISO 27001



Fuente: (Jorge García Martínez, 2024)

En la figura 6 se muestra el contenido de la estructura de la norma ISO/IEC 27001.

2.3.4. ISO 27002

ISO/IEC 27002 es un estándar internacional que proporciona orientación para las organizaciones que buscan establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) centrado en la ciberseguridad. Mientras que ISO/IEC 27001 describe los requisitos para un SGSI, ISO/IEC 27002 ofrece mejores prácticas y objetivos de control relacionados

con aspectos clave de ciberseguridad, incluido el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta a incidentes. (International Organization for Standardization., 2022)

Tabla 2
Controles de seguridad específicos.

Controles	Descripción
Marco de Control:	Detalla los 14 dominios de control y los 114 controles específicos que abarca ISO 27002. Estos controles abordan áreas clave de seguridad de la información, desde la gestión de activos hasta la gestión de incidentes.
Políticas y Procedimientos de Seguridad:	Explica cómo desarrollar políticas y procedimientos de seguridad efectivos que reflejen las necesidades y riesgos de la organización.
Gestión de Acceso y Control:	Describe cómo establecer controles de acceso adecuados, autenticación, autorización y auditoría para garantizar la protección de los sistemas y datos.
Gestión de Activos de Información:	Detalla cómo identificar, clasificar y gestionar activos de información, incluyendo datos confidenciales y críticos.
Seguridad Física y del Entorno:	Explica cómo proteger los activos físicos, como instalaciones y equipos, para prevenir accesos no autorizados o daños.
Gestión de Comunicaciones y Operaciones:	Describe cómo asegurar la seguridad de las redes, sistemas y operaciones diarias, incluyendo la gestión de vulnerabilidades y parches.
Gestión de Incidentes de Seguridad:	Detalla cómo prepararse y responder a incidentes de seguridad, incluida la planificación de la respuesta y la recuperación.
Cumplimiento Normativo y Legal:	Explica cómo cumplir con las regulaciones y leyes aplicables relacionadas con la seguridad de la información.
Gestión de la Continuidad del Negocio:	Describe cómo garantizar la disponibilidad continua de los servicios incluso en caso de interrupciones graves.
Gestión de la Seguridad de Recursos Humanos:	Detalla cómo abordar la seguridad en la contratación, el entrenamiento y la terminación de personal.
Gestión de la Seguridad de las Comunicaciones y Operaciones:	Describe cómo proteger las comunicaciones y las operaciones de TI para garantizar su integridad y confidencialidad.
Gestión de la Seguridad de Abastecimiento:	Explica cómo evaluar y gestionar los riesgos de seguridad asociados con los proveedores y terceros.
Gestión de la Seguridad de la Información en Relaciones con Terceros:	Detalla cómo establecer acuerdos de seguridad sólidos con socios comerciales y terceros.

Fuente: Elaboración propia

2.3.5. ISO 27003

Es una norma internacional que proporciona guías para la implementación de un sistema de gestión de seguridad de la información (SGSI). Se trata de una parte de la serie de normas ISO 27000 y es complementaria a la norma ISO 27001. (International Organization for Standardization, 2017)

La norma ISO/IEC 27003 establece los requisitos para la *planificación, implementación, monitoreo y revisión* de un SGSI y proporciona recomendaciones para el mismo. Incluye un proceso detallado para la implementación de un SGSI, desde la identificación de los riesgos hasta la evaluación y mejora continua del mismo. (International Organization for Standardization, 2017)

Figura 7
Norma ISO/IEC 27003



Fuente: Internet

En la figura 7 se representa la guía de implementación del SGSI para el presente trabajo de investigación utilizando el proceso de “planificación”.

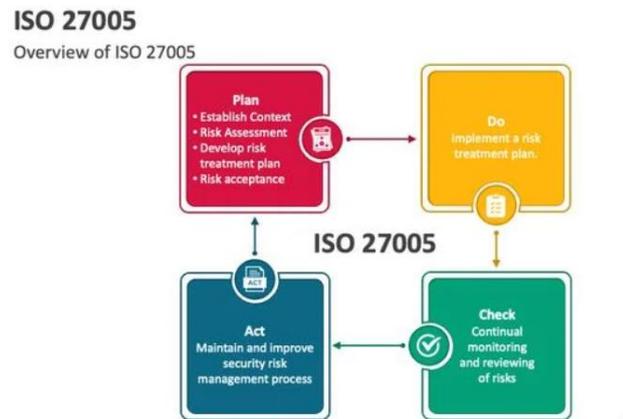
Además, podemos decir que el objetivo principal de la norma ISO/IEC 27003 es ayudar a las organizaciones a implementar de manera efectiva un SGSI, garantizar la protección de la información importante, mejorar su seguridad de la información y cumplir con los requisitos legales y reguladores.

2.3.6. ISO 27005

Esta norma contiene recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la Información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada como soporte para aplicar satisfactoriamente un SGSI basado en un enfoque de gestión de riesgos.

Los indicadores de riesgo muestran si la organización está sujeta o tiene una alta probabilidad de ser sometida a un riesgo que excede el riesgo permitido. (SegWeb Blog Spot, 2012)

Figura 8
Ciclo PDCA Según ISO/IEC 27005



Fuente: (Yangaly, s.f.)

La figura muestra el ciclo de mejora continua parte de la familia ISO/IEC 27001, la ISO/IEC 27005 tiene su enfoque orientado a la gestión de riesgos en un Sistema de Gestión de Seguridad de la Información SGSI y cuenta con una metodología y procedimientos para la evaluación, clasificación y seguimiento continuo a los riesgos de Seguridad de la Información que pueden ser afectados dentro de una determinada organización.

2.3.7. ISO 27008

Es un estándar que suministra orientación acerca de la implementación y operación de los controles, es aplicable a cualquier tipo y tamaño de empresa, tanto pública como privada que lleve a cabo revisiones relativas a la seguridad de la información y los controles de seguridad de la información. (ESG Innova Group, 2014)

Es compatible con otras normas como ISO 27001 o ISO 27002, y sirve como plataforma estratégica para garantizar la seguridad de la información así mismo soporta tanto la planificación como la ejecución del SGSI y el proceso de gestión del riesgo del sistema de la organización. (ESG Innova Group, 2014)

Figura 9
Dominios ISO/IEC 27001:2013



Fuente: (Jaime Andrés Bello Vieda, 2017)

En la figura 9 muestra el anexo A de la norma ISO/IEC 27001:2013 (14 dominios y sus 114 controles) Para el presente trabajo la aplicación del ISO/IEC 27008 será de utilidad para una correcta implementación de los controles que se vean por conveniente aplicarse conjuntamente con la revisión de la ISO/IEC 27002.

2.3.8. NIST CSF

El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia no reguladora que promueve la innovación mediante el fomento de la ciencia, los estándares y la tecnología de la medición. El marco de ciberseguridad del NIST (CSF del NIST) consta de estándares, pautas y mejores prácticas que ayudan a las organizaciones a mejorar su gestión de riesgos de ciberseguridad.

El diseño del CSF del NIST tiene una flexibilidad que le permite integrarse con los procesos de seguridad existentes dentro de cualquier organización, en cualquier industria. Proporciona un excelente punto de partida para implementar la seguridad de la información y la gestión de riesgos de ciberseguridad en prácticamente cualquier organización. (IBM Corporation, 2024)

Es un marco totalmente voluntario, las empresas deciden si ejecutarlo o no. Este sistema de prácticas brinda un mejor enfoque a las empresas para saber hacerle frente a amenazas, como ataques cibernéticos y evitar robos de información.

Identificar, proteger, detectar, responder y recuperar, son las cinco funciones que se exponen en el marco NIST para ayudar a mejorar la ciberseguridad de cualquier empresa. Por muy simple puede llegar a verse, estos pasos en conjunto mejoran significativamente la gestión organizacional. (Ikusi Redes de Telecomunicaciones, 2024)

Según lo referido NIST es un marco de trabajo usado en muchas organizaciones y empresas con la finalidad de mejorar la calidad de las tecnologías de información TIC's aplicando su estrategia y/o metodología (Identificar, proteger, detectar, responder y recuperar) para reducir los riesgos asociados a una gestión de la seguridad de la información y ciberseguridad utilizados comúnmente en entidades públicas y privadas del mundo entero

2.4. Marco Metodológico

2.4.1. Ciclo de Deming Concepto y Descripción

El Ciclo de Deming, también conocido como el Ciclo PDCA en inglés (Plan-Do-Check-Act), es una metodología de gestión iterativa utilizada para la mejora continua de procesos y productos. Fue popularizado por W. Edwards Deming, un estadístico y consultor de calidad que contribuyó significativamente a la gestión de calidad en el siglo XX. El ciclo proporciona un marco estructurado para identificar problemas, implementar soluciones, verificar resultados y realizar ajustes necesarios. (William Edwards Deming, s.f.)

Figura 10
Plan de Mejora Continua - Ciclo de Deming



Fuente: (Digital Learning, 2021)

La figura 10 muestra el ciclo de Deming, conocido también como ciclo de mejora continua que a continuación será descrito.

Descripción del Ciclo de Deming

Plan (Planificar)

Definición: Identificar un problema o una oportunidad de mejora. Establecer objetivos específicos y desarrollar un plan de acción para lograr estos objetivos.

Actividades:

Recolección y análisis de datos.

Identificación de causas raíz de problemas.

Formulación de estrategias y planes para abordar las áreas identificadas.

Ejemplo: En el contexto de un SGSI, esta fase podría involucrar la evaluación inicial de riesgos y la planificación de políticas de seguridad.

Do (Hacer)

Definición: Implementar el plan desarrollado en la fase anterior. Ejecutar las acciones planificadas a pequeña escala para probar su efectividad.

Actividades:

Capacitación y comunicación con el personal involucrado.

Implementación de los cambios o mejoras propuestas.

Recolección de datos durante la implementación para futura evaluación.

Ejemplo: Implementación inicial de controles de seguridad y procedimientos operativos.

Check (Verificar)

Definición: Evaluar los resultados de la implementación. Comparar los resultados obtenidos con los objetivos esperados para determinar si las acciones han sido efectivas.

Actividades:

Monitoreo y medición de resultados.

Análisis de las diferencias entre los resultados esperados y los obtenidos.

Identificación de problemas y áreas de mejora adicionales.

Ejemplo: Realización de auditorías internas y revisión de efectividad de los controles

implementados.

Act (Actuar)

Definición:

Tomar acciones basadas en los resultados de la fase de verificación. Si las acciones han tenido éxito, implementarlas a mayor escala; si no, ajustar el plan y repetir el ciclo.

Actividades:

Establecimiento de nuevas políticas y procedimientos basados en los aprendizajes.

Implementación de mejoras a mayor escala.

Documentación y comunicación de los cambios realizados.

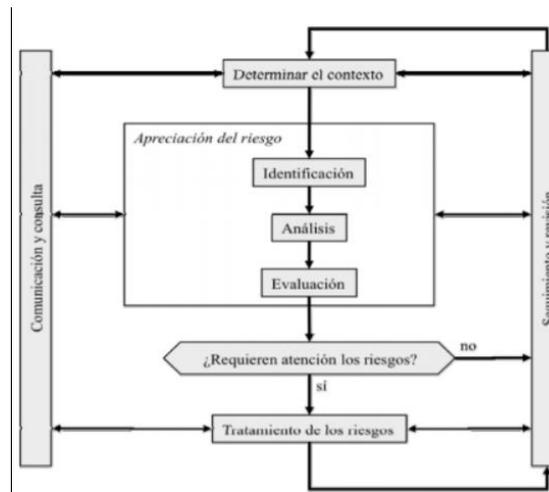
Ejemplo: Ajuste de políticas de seguridad y procedimientos según los resultados de la verificación y extensión de la implementación a toda la organización.

2.4.2. Método *MAGERIT*

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) está elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas, Actualmente está en su versión 3 y ofrece una aplicación para el análisis y gestión de riesgos de un sistema de información. (es.wikipedia.org, 2024)

Es así como esta metodología se basa en un enfoque proactivo para la gestión de riesgos y es compatible con otros marcos de gestión de riesgos basado en la ISO 31000 como son ISO 27005 y NIST SP 800-30. Estas son herramientas eficaces para la gestión de riesgos de seguridad de la información en organizaciones de todos los tamaños y sectores. A continuación, en la figura 11 se muestra el proceso de gestión de riesgos.

Figura 11
Proceso de gestión de riesgos según ISO 31000



Fuente: (interpolados.wordpress.com, 2020)

A Continuación, se menciona las etapas para la gestión de riesgos utilizando la metodología

MAGERIT 3.0

2.4.3. Establecimiento del Contexto

- Identificación del entorno organizativo y técnico.
- Definición de los objetivos del análisis.
- Delimitación del alcance del sistema a analizar.
- Identificación de activos, amenazas y salvaguardas iniciales.

2.4.4. Identificación de Riesgos

- Identificar combinaciones de activos, amenazas y vulnerabilidades que puedan ser un riesgo.
- Considerar los impactos posibles sobre la organización.

2.4.5. Análisis de Riesgos

- Evaluar el nivel de riesgo, considerando:
 - **Impacto:** Efecto negativo de la amenaza sobre los activos.
 - **Probabilidad:** Frecuencia esperada de ocurrencia del riesgo.

- Uso de matrices o herramientas para determinar el nivel de riesgo.

2.4.6. Evaluación de Riesgos

- Comparar los niveles de riesgo con los criterios de aceptación definidos.
- Determinar qué riesgos son aceptables y cuáles requieren tratamiento.

2.4.7. Tratamiento de Riesgos

- Diseñar y aplicar planes para mitigar, transferir, aceptar o evitar los riesgos identificados.
- Identificar salvaguardas adicionales que reduzcan el nivel de riesgo.

2.4.8. Monitoreo y Revisión

- Supervisar los riesgos y la eficacia de las medidas adoptadas.
- Realizar revisiones periódicas para reflejar cambios en el contexto o en los riesgos.

2.4.9. Comunicación y Consulta

- Garantizar que las partes interesadas comprendan el proceso de análisis y gestión de riesgos.
- Promover la participación activa y la transparencia durante el ciclo de gestión de riesgos.

2.5. Metodología PMBOK

Es un conjunto de estándares, mejores prácticas, directrices y terminología comúnmente aceptados en la gestión de proyectos. Publicado por el *Project Management Institute* (PMI), el PMBOK proporciona un marco estructurado para la gestión de proyectos, facilitando la planificación, ejecución, control y cierre de proyectos de manera eficiente y efectiva. Según Pinto, (Jeffrey K. Pinto, 2021) se destaca la relevancia del PMBOK (*Project Management Body of Knowledge*) como una guía integral y estandarizada que proporciona un marco esencial para la gestión de proyectos. Pinto señala

que el PMBOK ofrece a los profesionales de proyectos un conjunto de mejores prácticas, procesos y terminología que facilitan la planificación, ejecución y control de proyectos de manera eficaz. Al adherirse a los estándares del PMBOK, las organizaciones pueden mejorar su capacidad para entregar proyectos exitosos, cumplir con los requisitos de los interesados y lograr ventajas competitivas en sus respectivas industrias.

Según (Phd Harold Kerzner) La metodología PMBOK proporciona un enfoque sistemático para la gestión de proyectos, incluyendo proyectos tecnológicos, y explica cómo los principios del PMBOK pueden aplicarse en diferentes tipos de proyectos.

Utilizar la metodología PMBOK en el proyecto de tesis para la propuesta de un SGSI basado en la Norma Técnica Peruana NTP ISO 27001:2014 en la Universidad Nacional de San Antonio Abad del Cusco proporciona un marco estructurado y estandarizado que ayuda a gestionar eficazmente todos los aspectos del proyecto. La estandarización y la estructura del PMBOK garantiza que todas las áreas críticas del SGSI se aborden de manera integral y sistemática, asegurando la calidad, mitigando riesgos y facilitando la comunicación y la documentación. Esto resultará en un SGSI robusto y alineado con los mejores estándares internacionales, asegurando la protección efectiva de la información.

La metodología PMBOK (*Project Management Body of Knowledge*) proporciona un marco estructurado y estandarizado que es altamente beneficioso para la gestión de proyectos complejos, como el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). el enfoque sistemático del PMBOK debido a sus siguientes características:

2.5.1. Estandarización y Estructura

El PMBOK proporciona un conjunto de procesos y áreas de conocimiento bien definidos que aseguran una gestión organizada y coherente del proyecto. Para un proyecto de SGSI, esto es crucial para garantizar que todos los aspectos de seguridad de la información sean considerados y gestionados adecuadamente.

2.5.2. *Gestión Integral del Proyecto*

La metodología PMBOK cubre todas las fases del ciclo de vida del proyecto, desde el inicio y la planificación hasta la ejecución, monitoreo, control y cierre. Esto asegura que el proyecto de SGSI esté bien planificado desde el principio, con una clara definición de objetivos, alcance, cronograma y presupuesto.

2.5.3. *Enfoque en la Calidad*

El PMBOK incluye la gestión de la calidad como una de sus áreas de conocimiento. En un proyecto de SGSI, asegurar la calidad de los procesos y controles de seguridad es esencial para garantizar la protección de la información y cumplir con los estándares y normativas relevantes.

2.5.4. *Gestión de Riesgos*

La gestión de riesgos es una parte integral del PMBOK. En el contexto de un SGSI, la identificación, análisis y mitigación de riesgos relacionados con la seguridad de la información son fundamentales para proteger los activos de información de la organización.

2.5.5. *Adaptabilidad y Mejora Continua*

Aunque el PMBOK es un enfoque tradicional y estructurado, también permite la adaptación a las necesidades específicas del proyecto y la organización. Esto es particularmente útil para un proyecto de SGSI, donde las amenazas y vulnerabilidades pueden evolucionar, requiriendo ajustes y mejoras continuas en el sistema de gestión de seguridad.

2.5.6. *Documentación y Comunicación*

La metodología PMBOK enfatiza la importancia de la documentación y la comunicación efectiva. En un proyecto de SGSI, la documentación detallada de políticas, procedimientos y controles, así como la comunicación clara con todos los interesados, es crucial para asegurar la comprensión y el cumplimiento de las medidas de seguridad.

Técnicas e instrumentos

Las técnicas e instrumentos utilizados en el presente proyecto de investigación son los siguientes:

Técnicas

Análisis Documental.

Se revisaron y analizaron documentos relevantes, tales como la Norma Técnica Peruana NTP ISO 27001:2014, políticas y procedimientos de seguridad de la información existentes en la universidad. Mediante la aplicación nos ayudó a comprender los requisitos normativos y las prácticas actuales de seguridad de la información.

Entrevistas.

Se realizaron coordinaciones con la Jefaturas respectivas para poder entrevistar a sus trabajadores con formatos semi estructurados, en esta ocasión fue al personal de la Oficina de Tramite Documentario, como usuarios dueños de proceso y actores relevantes.

Se obtuvo información detallada sobre las prácticas actuales, eventos significativos, desafíos y expectativas en torno a la seguridad de la información.

Cuestionarios.

Se realizaron cuestionarios estructurados a los usuarios de la Oficina de Tramite Documentario con la intención de recolectar datos sobre el conocimiento y las prácticas relacionadas con la seguridad de la información.

Esta recolección de datos para poder tener un alcance del conocimiento sobre la cultura de seguridad de la información y la percepción del personal.

Observación Directa.

Se observó directamente las prácticas y procedimientos de seguridad de la información en los procesos críticos de la Unidad de Tramite Documentarios en búsqueda de la identificación de posibles brechas de seguridad de la información e identificar mejoras en las prácticas actuales de seguridad de la información.

Análisis de Riesgos.

En base a un marco de trabajo con una matriz diseñada se buscó identificar, evaluar y priorizar los riesgos de seguridad de la información proporcionando una base para desarrollar controles de

seguridad adecuados y priorizar los procesos que requieren atención inmediata.

Revisión de Literatura

Se revisó investigaciones previas, algunos artículos modernos académicos y publicaciones relevantes sobre la implementación de SGSI, la NTP 27001:2014 y la ISO 27001 con el fin de tener un contexto claro del proyecto en el marco de investigaciones existentes e identificación de mejores prácticas.

Instrumentos

Guía de Entrevistas

Un conjunto de preguntas abiertas y semiestructuradas diseñadas para obtener información detallada y específica de los entrevistados facilita la realización de entrevistas en profundidad con expertos y personal dueño de la ejecución de procesos relevantes.

Cuestionario

Un formulario estructurado con preguntas cerradas y abiertas para recolectar datos de una muestra amplia de empleados.

Recolección de datos estandarizados y comparables sobre la percepción y prácticas de seguridad de la información.

Matriz de Riesgos

El uso de un instrumento para evaluar y priorizar los riesgos de seguridad de la información ayudó a visualizar los riesgos y su impacto potencial, facilitando la identificación conjunta de Planes de Acción y Oportunidades de Mejora en los Controles Necesarios a implementar.

El uso de estas técnicas e instrumentos permitió una recolección de datos exhaustiva y detallada, proporcionando una comprensión profunda de las prácticas actuales, desafíos y necesidades de seguridad de la información en la Universidad Nacional de San Antonio Abad del Cusco. Esto, a su vez, facilitó el desarrollo de la propuesta de diseño de un SGSI siendo este robusto y alineado con la Norma Técnica Peruana NTP ISO 27001:2014, asegurando que las recomendaciones y medidas implementadas sean efectivas y pertinentes.

2.5.7. Definición de la Metodología del Proyecto

Metodología del Proyecto

El uso de estas técnicas e instrumentos permitió una recolección de datos exhaustiva y detallada, proporcionando una comprensión profunda de las prácticas actuales, desafíos y necesidades de seguridad de la información en la Universidad Nacional de San Antonio Abad del Cusco. Esto, a su vez, con esta metodología PMBOK que nos facilitó el desarrollo de la propuesta de diseño de un SGSI siendo este robusto y alineado con la Norma Técnica Peruana NTP ISO 27001:2014, asegurando que las recomendaciones y medidas implementadas sean efectivas y pertinentes.

Tabla 3
Metodología del proyecto

Fases	Descripción
INICIO DEL PROYECTO	<ul style="list-style-type: none"> Entendimiento de la Organización Definición del alcance de la implementación del SGSI Identificación de los interesados Elaboración del Acta de Constitución del Proyecto Asignación de responsables del proyecto
PLANIFICACIÓN	<ul style="list-style-type: none"> Desarrollo del Plan de gestión del proyecto. (plan que incluya el cronograma, costos y recursos). Plan de Comunicación (definir como comunicar los avances y decisiones). Análisis de riesgos. Plan de Gestión de Seguridad (identificación de controles políticas y procedimientos)
EJECUCIÓN	<ul style="list-style-type: none"> Implementación del SGSI (desarrollo e implementación de controles de seguridad y Diseño de Políticas y Procedimientos de Seguridad) Propuesta de Plan Estratégico de concientización
MONITOREO Y CONTROL	<ul style="list-style-type: none"> Monitoreo y supervisión de rendimiento de los planes de acción propuestos en el SGSI. (Evaluar y medir el desempeño de los controles a implementar)
CIERRE	<ul style="list-style-type: none"> Evaluación Final y Documentación: Revisar los logros del proyecto y documentar el desempeño

Fases	Descripción
	y los aprendizajes. <ul style="list-style-type: none"><li data-bbox="651 315 1272 421">• Informe de Cierre del Proyecto: Crear un informe detallado del proceso de implementación, resultados y recomendaciones futuras.

Fuente: Elaboración propia

CAPÍTULO III: DESARROLLO DEL PROYECTO

3.1. Inicio del Proyecto

3.1.1. *Entendimiento de la Organización*

Descripción de la Organización

La Universidad Nacional de San Antonio Abad del Cusco – UNSAAC dirigida en la actualidad por el Dr. Eleazar Crucinta Ugarte con documento Resolución N° 016-2021-CU-UNSAAC es el representante legal de la universidad a dedicación exclusiva en la gestión y dirección del gobierno universitario a todo nivel y en los parámetros establecidos en la Ley Universitaria N°30220 y de su estatuto.

Misión

“Brindar formación profesional científica, tecnológica y humanística de calidad, a los estudiantes universitarios, con valores y principios y responsabilidad social; afirmando la interculturalidad, reconociendo la diversidad natural, cultural y fortaleciendo nuestra identidad andino-amazónica”.

Visión

“Los peruanos acceden a una educación que les permite desarrollar su potencial desde la primera infancia y convertirse en ciudadanos que valoran su cultura, conocen sus derechos y responsabilidades, desarrollan sus talentos y participan de manera innovadora, competitiva y comprometida en las dinámicas sociales, contribuyendo al desarrollo de sus comunidades y del país en su conjunto”.

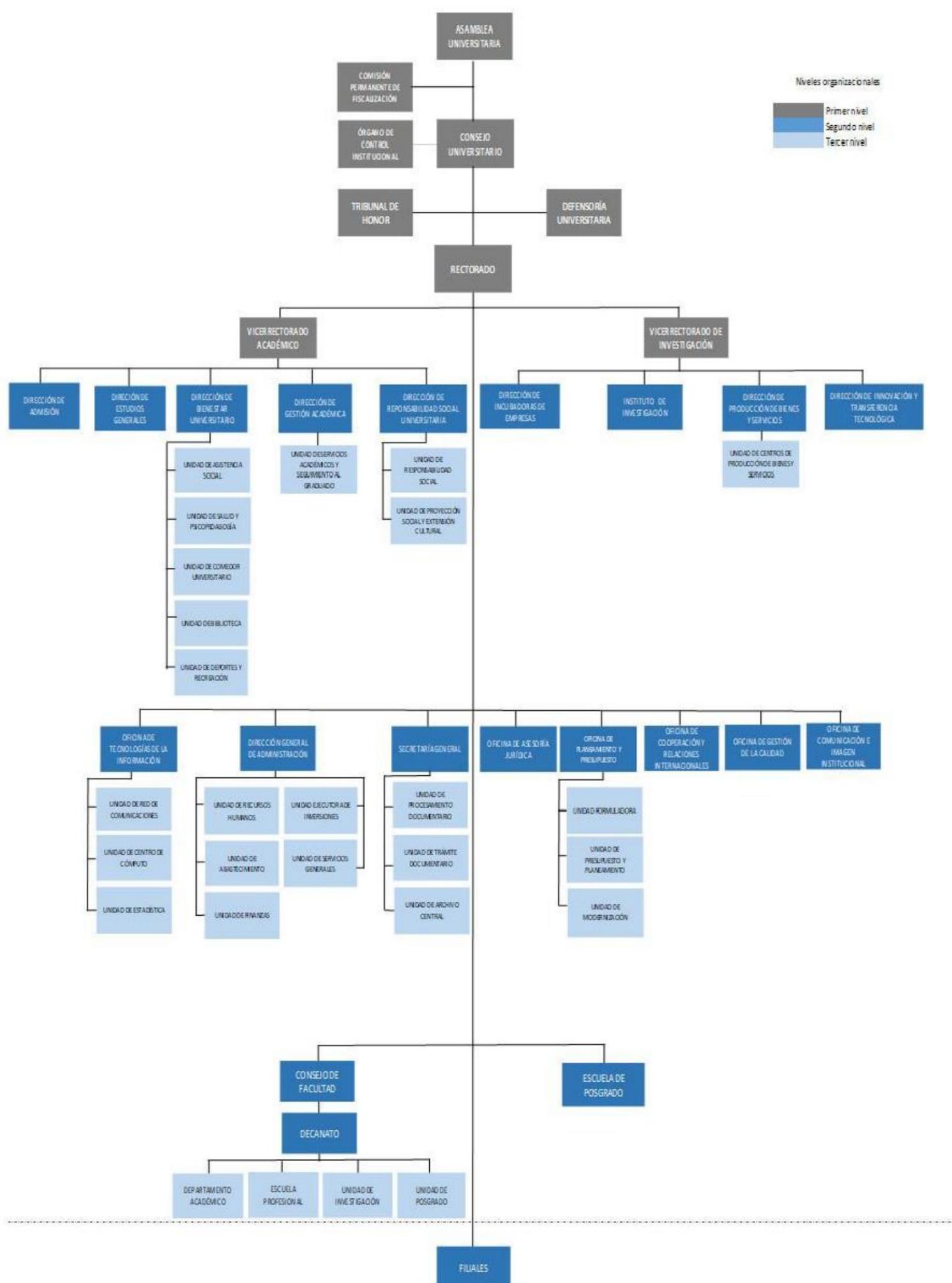
Organigrama

La universidad tiene como áreas funcionales al Rectorado, Vicerrectorado académico, Vicerrectorado de Investigación y Decanos de facultad, cada una de estas áreas con sus respectivas unidades, centros de producción y oficinas administrativas y académicas según lo estipulado en el organigrama actual, que se muestra a continuación:

Figura 12
Organigrama de la UNSAAC

REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES DE LA UNSAAC

ANEXO: ORGANIGRAMA DE LA UNIVERSIDAD UNSAAC



Aprobado por Resolución N°
CU-265-2021-UNSAAC

Fuente: (UNSAAC, 2021)

Datos Generales

La Universidad Nacional de San Antonio Abad del Cusco (UNSAAC), es una Universidad Pública ubicada en la ciudad del Cusco, Perú.

1. Fundación: 1 de marzo de 1692 por el obispo Mollinedo y Angulo bajo el nombre de "Universidad Nacional de San Antonio Abad del Cusco".

2. Ubicación:

- Dirección Legal: Av. de la Cultura Nro. 733
- Distrito / Ciudad: Cusco
- Departamento: Cusco, Perú

3. Facultades: La UNSAAC ofrece una amplia variedad de carreras en áreas como Ciencias de la Salud, Ingeniería, Ciencias Sociales, Ciencias Económicas y Administrativas, Humanidades, Ciencias Exactas, cada una de ellas con diferentes carreras profesionales acorde a su rama principal.

Unidad De Tramite Documentario

La Unidad de Trámite Documentario – UTD de la Universidad Nacional de San Antonio Abad del Cusco según el Proyecto de Reglamento de Organización y Funciones – ROF, aprobado con RESOLUCIÓN N° CU- 265 -2021-UNSAAC se encuentra en su estructura orgánica dentro de la ADMINISTRACIÓN INTERNA como un *órgano de apoyo* adscrito a la Oficina de Secretaría General como una de sus unidades, de las cuales se conforman de la siguiente manera:

- 05.3 Secretaría General
 - 05.3.1. Unidad de Procesamiento Documentario.
 - 05.3.2. Unidad de Trámite Documentario.
 - 05.3.3. Unidad de Archivo Central.

Podemos visualizar lo mencionado anteriormente en el cuadro siguiente:

Figura 13
Extracto ROF de UNSAAC

05. ADMINISTRACIÓN INTERNA: ÓRGANOS DE APOYO

05.1. Dirección General de Administración

05.1.1. Unidad de Recursos Humanos

05.1.2. Unidad de Abastecimiento

05.1.3. Unidad de Finanzas

05.1.4. Unidad Ejecutora de Inversiones

05.1.5. Unidad de Servicios Generales

05.2. Oficina de Tecnologías de la Información

05.2.1. Unidad de Red de Comunicaciones.

05.2.2. Unidad de Centro de Cómputo

05.2.3. Unidad de Estadística.

DIRECCION DE PLANIFICACION/UNIDAD DE ORGANIZACIÓN Y METODOS

REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES DE LA UNSAAC

05.3 Secretaría General

05.3.1. Unidad de Procesamiento Documentario.

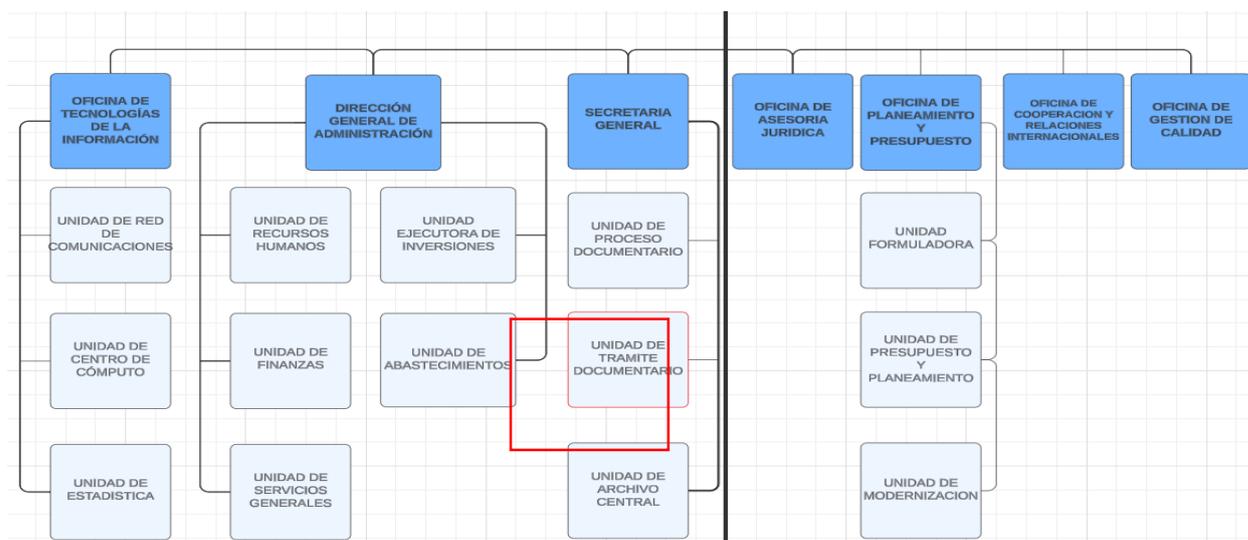
05.3.2. Unidad de Trámite Documentario.

05.3.3. Unidad de Archivo Central.

Fuente: (Universidad Nacional De San Antonio Abad del Cusco, 2021)

Orgánicamente la Unidad de Trámite Documentario pertenece a Secretaría General, siendo esta un Órgano que pertenece directamente del Rectorado como se muestra en la siguiente figura:

Figura 14
Ubicación de UTD dentro del organigrama de la UNSAAC



Fuente: (<https://www.unsaac.edu.pe/>)

Funciones, Objetivos Generales y Descripción de Procesos de la Unidad de Trámite Documentario y Comunicaciones.

La Unidad de Trámite Documentario y Comunicaciones, depende de Secretaría General, responsable de administrar, ejecutar y coordinar las actividades relacionadas con el procesamiento, clasificación, verificación, distribución y control del ingreso documentario general de la Institución, aplicando los principios de simplicidad y celeridad, brinda también el servicio de información a los administrados. (UNSAAC, 2021)

Funciones. - Son funciones de la Unidad de Trámite Documentario y Comunicaciones:

a. Organizar, coordinar y desarrollar las actividades referidas a la recepción, registro, clasificación, distribución y control de la documentación que emite y recibe secretaria general y Unidades académicas y administrativas de la Universidad.

b. Supervisar y coordinar el proceso de trámite documentario de los procedimientos administrativos de la Universidad con la celeridad y plazo establecidos en el TUPA.

c. Brindar información clara, completa, oportuna y precisa sobre los servicios que presta la Institución, así como orientar sobre quejas, reclamos y consultas formulados por los usuarios de la universidad.

d. Orientar al administrado en el seguimiento de un procedimiento administrativo logrando la conformidad del servicio brindado.

e. Velar por la confidencialidad de la información presentada por los usuarios y la Institución.

f. Brindar atención al ciudadano, bajo los principios de transparencia, imparcialidad, observando el Código de Ética de la función pública y las normas que la regulan.

g. Participar o proponer diseños de sistemas de información que aseguren el funcionamiento de trámite documentario.

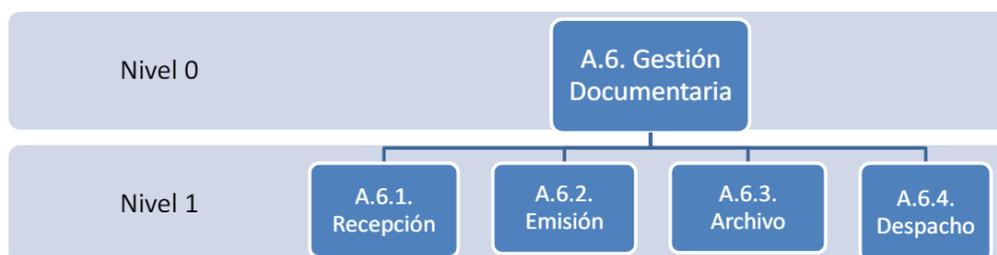
h. Administrar y custodiar el Libro de Reclamaciones de la Institución, para que los usuarios puedan expresar la insatisfacción o disconformidad de los servicios recibidos.

i. Las demás que le asigne el secretario general. (UNSAAC, 2021)

Descripción de procesos de la unidad de trámite documentario.

Los procesos de la Unidad de trámite documentario se describen a continuación:

Figura 15
Manual de procedimientos de la Unidad de Trámite Documentario de la UNSAAC



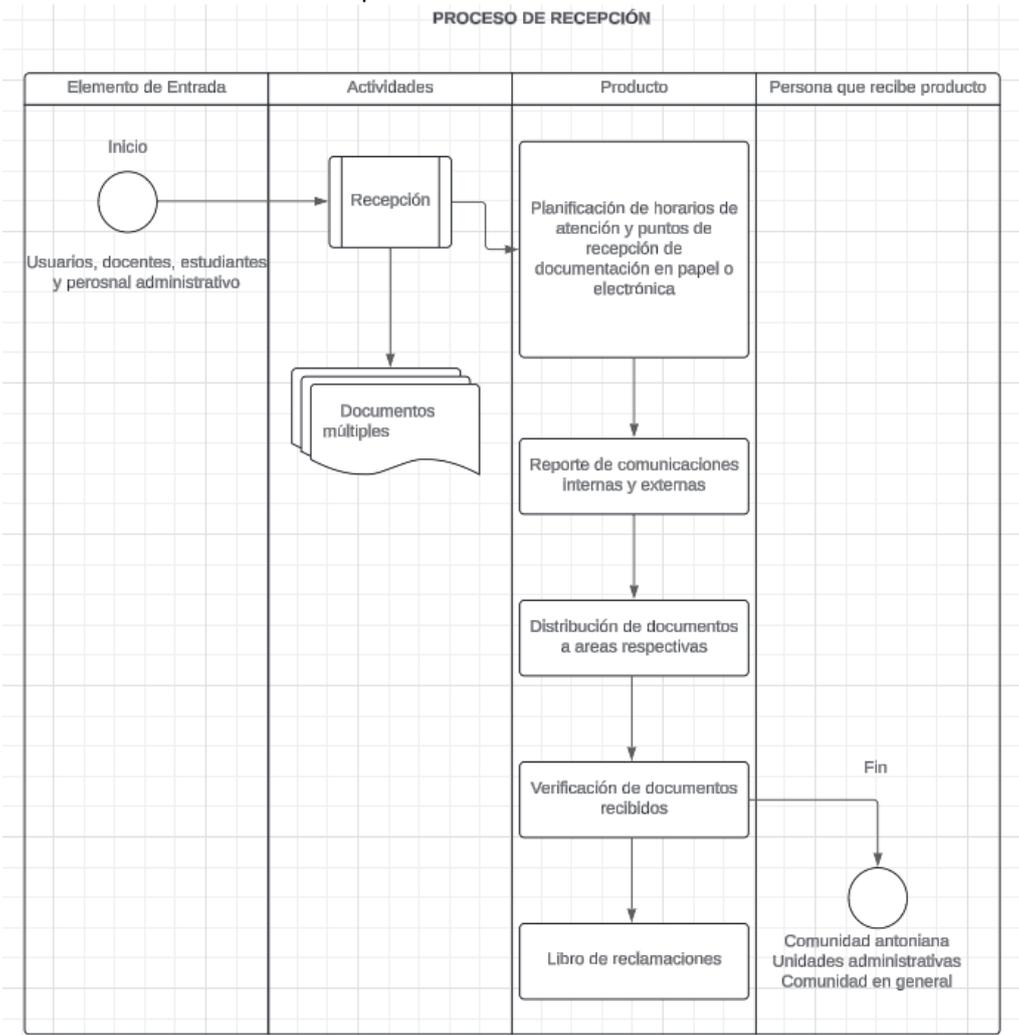
FICHA TÉCNICA DEL PROCESO NIVEL 0		CÓDIGO: A.6	
1) Nombre	A.6. Gestión Documentaria	3) Dueño del Proceso	Jefe de Secretaría General
2) Objetivo	Gestionar la simplificación administrativa con el propósito de mejorar la gestión institucional, con énfasis en la atención al estudiantado, sustentado en estándares y buenas prácticas en gestión documental priorizando y optimizando el uso de los recursos públicos. Nota. - Documento: Información creada. Recibida y conservada como evidencia y como activo por una organización o individuo, en el desarrollo de sus actividades o en virtud de sus obligaciones legales.	4) Requisitos	Ley N° 27444 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado D.L. N° 1310 Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI Estatuto Universitario ROF Instrumentos de gestión y normas nacionales
DESCRIPCIÓN DEL PROCESO			
5) Elementos de Entrada	6) Actividades: Procesos Nivel 1	7) Producto	8) Persona que recibe el producto
- Requerimientos de los usuarios, docentes, estudiantes y personal administrativo - Presupuesto Institucional - Misión, Visión, Objetivos y Procedimientos	A.6.1. Recepción A.6.2. Emisión A.6.3. Archivo A.6.4. Despacho	A.6.1.1 Planificación de Horarios de atención y puntos de recepción de documentación en papel o electrónicos. A.6.1.2 Reporte de comunicaciones internas y externas. A.6.1.3 Distribución de documentos a áreas respectivas A.6.1.4 Verificación de documentos recibidos. A.6.1.5. Libro de Reclamaciones A.6.2.1 Plan de Mejora para Emisión de Resoluciones en forma oportuna A.6.2.2 Plan de Implementación de formatos electrónicos con firma digital: Creación de Firmas, Validación de Firma A.6.3.1 Plan de Organización, Descripción; Selección, Conservación y Acceso de documentos y Servicios archivísticos. A.6.3.2 Reglamento de Valoración de documentos A.6.4.3 Plan de Implementación de Conservación de Documentos. A.6.4.1 Plan de Mejora en la distribución de documentos A.6.4.2 Plan de Registro y control de documentos despachados en forma manual o automatizada	Comunidad Antoniana Unidades Administrativas comunidad en general. Comunidad Antoniana Unidades Administrativas comunidad en general. Comunidad Antoniana Unidades Administrativas comunidad en general. Comunidad Antoniana Unidades Administrativas comunidad en general.
IDENTIFICACIÓN DE RECURSOS CRÍTICOS PARA LA EJECUCIÓN Y CONTROL DEL PROCESO			
9) Recursos		10) Controles o inspecciones	
Recursos Humanos capacitados en GESTIÓN DOCUMENTAL; Recursos Financieros Infraestructura y Ambiente de Trabajo: Oficinas, equipos de cómputo, escritorios, archivadores, sillas, software. De acuerdo a lo establecido por las normas.		Cumplimiento de dispositivos legales de gestión documental Política de Gestión Documental Manejo de Versiones	
EVIDENCIAS E INDICADORES DEL PROCESO			
11) Indicadores de desempeño			
<ul style="list-style-type: none"> Grado de satisfacción de los usuarios al año Tiempo de respuesta a Requerimientos de información por año, por unidad académico o administrativa % de usuario con Acceso, transparencia y derecho a la información vía internet /requerimiento de información 			

Fuente: (UNSAAC, 2021)

Mapa de Procesos

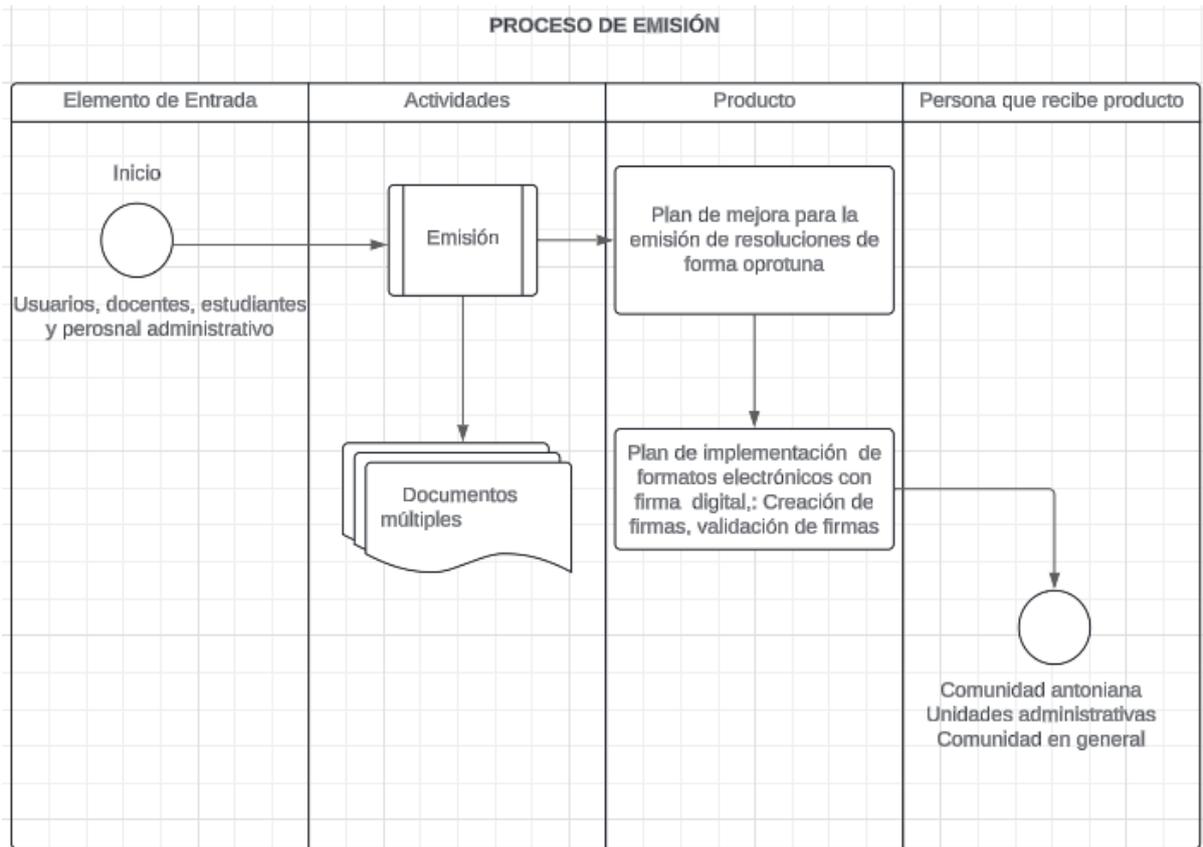
Los presentes mapas de procesos que se muestran a continuación fueron diagramados por los tesistas en base a la información recopilada del Reglamento de Obligaciones y Funciones – ROF de la página de transparencia de la UNSAAC.

Figura 16
Proceso de recepción de documentos en la UTD - UNSAAC



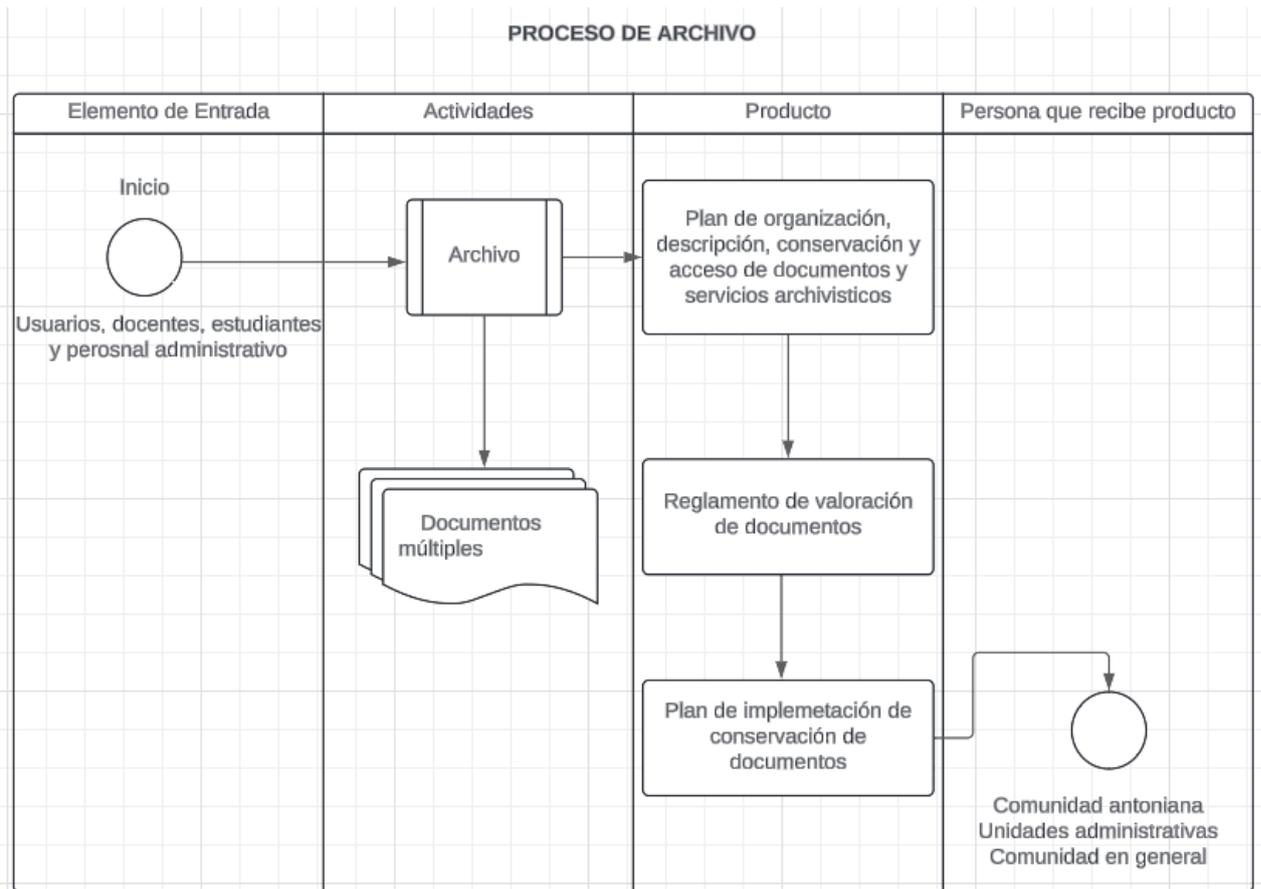
Fuente: Elaboración propia

Figura 17
Proceso de Emisión de documentos en la UTD - UNSAAC



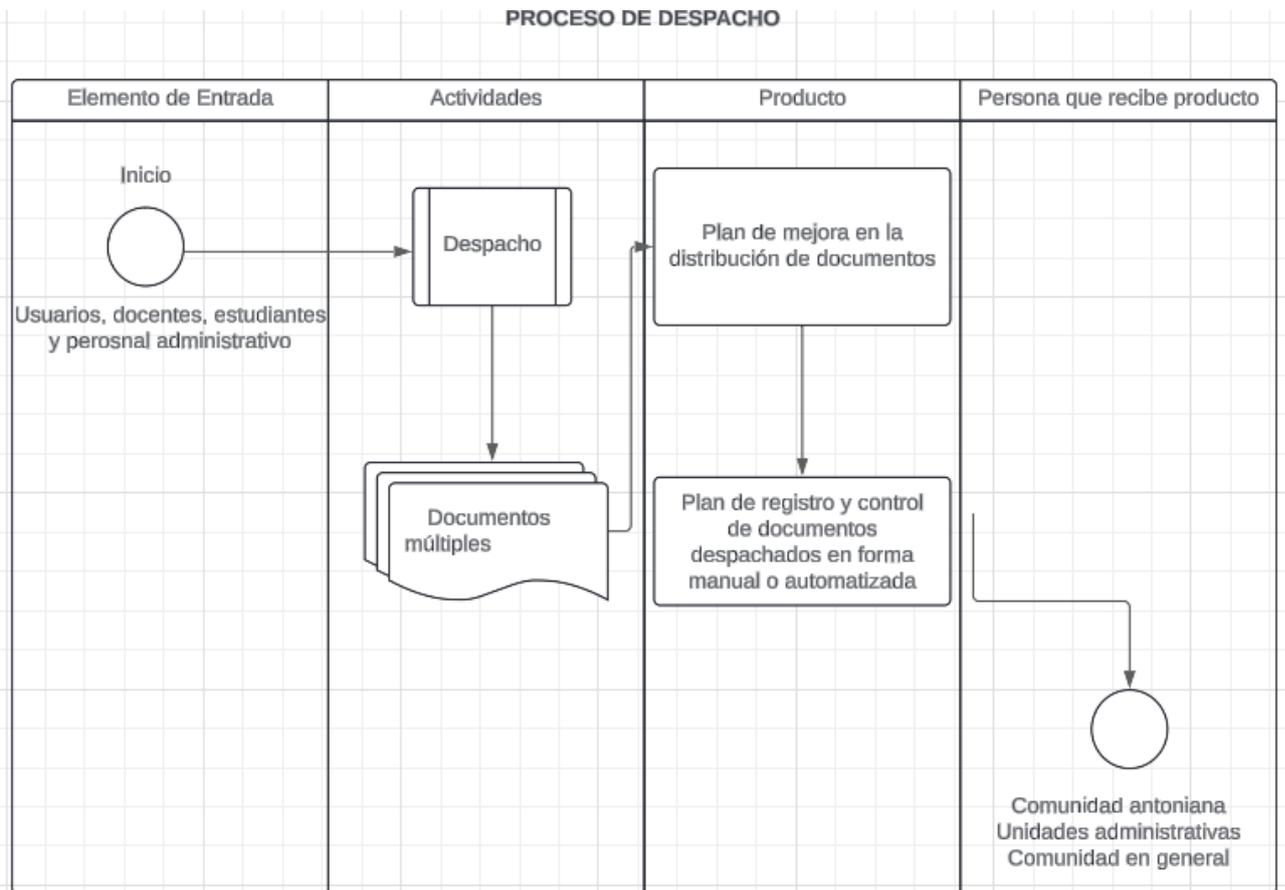
Fuente: Elaboración propia

Figura 18
Proceso de archivo de documentos en la UTD - UNSAAC



Fuente: Elaboración propia

Figura 19
Proceso de despacho de documentos en la UTD - UNSAAC



Fuente: Elaboración propia

3.1.2. Definición del alcance del proyecto.

Establecer un Sistema de Gestión de Seguridad de la Información en los aspectos más críticos dentro del proceso más crítico considerado “Gestión Documentaria” de la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco. Teniendo establecido límites claros, identificado los activos de información más importantes, implementado controles alineados con la NTP ISO 27001:2014, y garantizar el cumplimiento normativo y la asegurando la seguridad de la información.

Se trata de definir los límites en la aplicación del sistema de gestión de la seguridad de la información.

Los elementos que debemos tener en cuenta para la definición del alcance son:

- El contexto de la organización: Las cuestiones Internas y Externas
- Los requisitos y expectativas de las partes interesadas

Identificar el alcance correcto del SGSI es crucial porque ayudará a las organizaciones a cumplir sus requisitos de seguridad y planificar la implementación del SGSI

Una correcta definición del alcance permitirá:

- Determinar los recursos necesarios evitando el uso innecesario de recursos (en términos de tiempo, costo y esfuerzo)
- Planificar la implementación del SGSI determinando el calendario y el presupuesto necesarios.
- Alinear los requisitos de seguridad de la organización con los ejercicios de análisis y evaluación de riesgos.

Ejemplos de preguntas que pueden guiar a las organizaciones a la hora de definir el alcance y los límites del SGSI:

- ¿Qué productos y servicios en su organización estarán cubiertos por el SGSI?
- ¿Cómo y por qué el producto o servicio seleccionado es crítico para su organización?
- Cuáles son las características del servicio seleccionado; ¿es decir, el negocio, la organización, sus ubicaciones, activos y tecnologías para ser incluidos en el SGSI?

- ¿Va a requerir que las partes externas, proveedores cumplan con su SGSI?
- ¿Si las actividades realizadas por la organización requieren de interfaces o dependencias externas o de actividades realizados por terceros? ¿Deberían ser considerados dentro del alcance del SGSI?

Consideraciones antes de definir el Alcance del SGSI

1. Considere los requisitos de seguridad de la información que se han identificado en la Cláusula 4.1 – Definir los requisitos de seguridad de la información;
2. Considerar los servicios críticos que pueden causar un gran impacto en la organización o en sus clientes y partes interesadas como resultado de pérdidas de confidencialidad, integridad o disponibilidad;
3. Definir el alcance y los límites de la organización;
4. Definir el alcance y los límites de la Tecnología de Comunicación de Información (TIC)
5. Definir el alcance físico y los límites
6. Integre alcance y límites elementales para obtener el alcance y los límites del SGSI.
7. Considere las actividades externalizadas, así como las interfaces y dependencias requeridas

3.1.3. Identificación de los interesados.

La jefatura de la Unidad de Trámite Documentario que pertenece a la secretaría general, es el principal interesado por ser dueño del proceso considerado el más importante transversalmente en la universidad.

El Órgano de Control Institucional para cumplimiento normativo relacionado y Cumplir con los requisitos de las leyes de protección de datos.

El personal Administrativo para poder proporcionar un ambiente de trabajo seguro y apropiado con una información resguardada y disponible en cuanto a la ejecución de sus procesos.

El público en general, considerado los docentes y alumnado para poder contener con la debida privacidad la información que se maneja dentro del entorno educativo.

3.1.4. *Elaboración del Acta de Constitución del Proyecto*

Se tiene en el Anexo 01 el Acta de Constitución del Proyecto, dicho documento incluye los objetivos del SGSI, el alcance, propósito del proyecto, descripción del proyecto, objetivos del proyecto, alcance del proyecto, requisitos del proyecto, cronograma tentativo, presupuesto estimado, roles y responsabilidades, riesgos iniciales, criterios de éxito del proyecto, aprobación del acta de constitución del proyecto:

Los recursos asignados, el cronograma preliminar, los riesgos iniciales y el presupuesto general.

3.1.5. *Asignación de responsables del proyecto*

Se nombra a una persona responsable de liderar el proyecto, y a otra para realizar la coordinación y gestión de los procesos:

- BCH. VICTOR HUGO CUBA GAMARRA LÍDER DEL PROYECTO
- BCH. MARCO EMERSON SOLÍS CANO COORDINADOR DEL PROYECTO

Con el respaldo de la Jefatura de la Unidad de Trámite Documentario, para elevar cualquier necesidad y requerimiento del proyecto.

3.2. Planificación

Es la fase más extensa y crítica. Aquí se detallan todos los aspectos del proyecto, como actividades, plazos, calidad y los costos que previamente fueron detallados en la factibilidad económica. El éxito del proyecto depende de una planificación sólida.

3.2.2. Plan de Comunicación

El objetivo es asegurar la comunicación clara, precisa y oportuna entre los diferentes grupos interesados, facilitando la coordinación, minimizando los riesgos asociados a malentendidos y garantizando que todos los actores conozcan su rol y responsabilidad en el proyecto de implementación del SGSI. Facilitar la coordinación de actividades y el flujo de información, reduciendo riesgos de malentendidos o retrasos.

Identificación de Canales de Comunicación

Reuniones presenciales de avance: Con los responsables del proyecto para revisar el progreso, identificar problemas y ajustar el plan de acción.

Frecuencia y Tipo de Comunicación

Actualizaciones operativas diarias dentro del equipo de implementación a través de correo o cargando versiones distintas en el desarrollo continuo.

Reuniones por plataforma virtuales semanales en las cuales se desarrolle la revisión con el equipo de proyecto.

Roles y Responsabilidades en la Comunicación

Jefe de Proyecto: Responsable de coordinar las comunicaciones principales y de reportar el estado del proyecto a la alta dirección.

Responsable de Seguridad de la Información: Encargado de transmitir cambios y políticas de seguridad, así como coordinar las sesiones de capacitación.

Jefe de la Unidad de Trámite Documentario: Recibe los informes de estado y toma decisiones estratégicas en función de la información recibida.

Retroalimentación

Mecanismos de Retroalimentación: Encuestas post-capacitación y espacios de retroalimentación en las reuniones para evaluar la comprensión de las políticas de seguridad y los Planes de acción propuestos.

3.3. Ejecución:

3.3.1. *Elaborar un análisis de la situación actual en base a la NTP ISO 27001:2014*

El desarrollo de un análisis de situación actual se desarrolla en base a una metodología MAGERIT la cual describe diferentes fases las cuales se describen a continuación:

Identificación de Activos de Información

La información que es creada, utilizada y gestionada por los procesos de la Unidad de Trámite Documentario, es un recurso importante y vital para su operación de trámite diario para lograr los objetivos estratégicos. Debido a la importancia de la información, esta se convierte en un activo con valor para la Universidad Nacional San Antonio Abad del Cusco y requiere ser tratada con la seguridad adecuada.

Por lo tanto, es importante tener en cuenta:

- El jefe de la Unidad de Trámite Documentario es el propietario de los activos de información y de los riesgos de seguridad de la información que afectan al activo de información y tiene la responsabilidad de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

- Los Técnicos Administrativos son el soporte y apoyo para todos los procesos del área.

Los portapliegos son partícipes de algunos de los procesos incluidos en la Unidad de Trámite Documentario.

- El jefe de la Unidad de Trámite Documentario como propietario de la información y los activos de información, es la persona más idónea para determinar la clasificación y valoración para la Unidad de Trámite Documentario acorde sus características.

Pasos Previos:

Si la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco cuenta con un inventario y tasación de activos de información debe ser revisado por el propietario del activo de información en coordinación con el custodio del activo de información bajo la asesoría y supervisión del especialista de seguridad de la información o a quien se asigne esas funciones, verificando si los activos de información relevados se encuentran vigentes o han presentado alguna

variación y que deben ser tomados en cuenta durante el proceso de registro y actualización de la nueva matriz de inventario y tasación de activos de información. En caso de no contar con un inventario y tasación de activos, los propietarios del activo de información en coordinación con los custodios del activo de información bajo la asesoría y supervisión del especialista de seguridad de la información o a quien se asigne esas funciones deben elaborar el nuevo inventario y tasación de activos de información que están bajo su responsabilidad.

Se debe identificar los activos de información involucrados en los procesos de negocio que estén definidos dentro del alcance del Sistema de Gestión de Seguridad de la Información de la Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco para determinar cuáles de ellos están bajo riesgo y así establecer su priorización.

La Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco cuenta con diversos activos de información y son utilizados para realizar tareas que le permitan alcanzar sus objetivos estratégicos. En tal sentido, en esta etapa se identifican y listan los activos de información que son necesarios para soportar la ejecución de estas tareas y actividades. Los propietarios de los activos de información en coordinación de los custodios son los únicos responsables de identificar y evaluar estos activos, pudiendo tomar como referencia el inventario de activos anterior (si hubiera) con el apoyo del designado Analista de Seguridad de la Información.

Tipo del activo Para la tipificación de los activos de información se ha tomado como referencia el Catálogo de elementos de MAGERIT. De acuerdo con ello, los activos de información deben ser tipificados según las siguientes categorías generales:

Activos de Información

- Información electrónica.
- Información escrita.
- Información hablada.
- Otro tipo de información

Activos de Software

- Software comercial o herramientas, utilitarios.
- Software desarrollado por terceros.
- Software desarrollado internamente.
- Software de administración de base de datos.
- Otro software.

Activos Físicos

- Equipo de procesamiento.
- Equipo de comunicaciones.
- Medio de almacenamiento.
- Mobiliario y equipamiento.
- Otros equipos.

Servicios

- Procesamiento y comunicaciones.
- Servicios generales.
- Otros servicios

Personal

- Clientes.
- Empleados.
- Personal Externo.

Para cada activo de información identificado, se le debe asignar un tipo de activo según la tipificación y categorías generales de acuerdo con la previa descripción.

Propietario del activo El propietario del activo tiene la absoluta responsabilidad de identificar, evaluar y gestionar el ciclo de vida del activo de información para lo cual debe establecer quiénes tienen acceso, qué pueden hacer con la información y cuáles son los requisitos para que se salvaguarde su confidencialidad, integridad y disponibilidad de la información cuando corresponda, así como

establecer qué se hace con la información una vez que ya no sea requerida.

Custodio del activo El custodio del activo de información tiene la responsabilidad de mantener los niveles de protección de acuerdo con los criterios de confidencialidad, integridad y disponibilidad de la información, así como las especificaciones definidas por el propietario del activo. En tal sentido, para la Universidad Nacional de San Antonio Abad del Cusco; el jefe de la Unidad de Trámite Documentario es el custodio de los activos de información y tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones definidas por el propietario del activo.

Tasación de activos Basados en las necesidades del negocio, los propietarios de los activos de información establecen un nivel de tasación de cada activo que está bajo su responsabilidad, de acuerdo con sus niveles de importancia con respecto a la privacidad y a las dimensiones de seguridad de la información: confidencialidad, integridad y disponibilidad. La tasación de activos permite priorizar las acciones de evaluación de riesgos de seguridad de la información, y realizar la estimación del perjuicio para la institución, así como la implementación de controles que permitan tratar los riesgos a los que se encuentra expuesto.

Criterios para la tasación de activos de información por seguridad de la información Los criterios para la tasación de activos de información se realizan de acuerdo con las dimensiones de seguridad de la información que se detallan a continuación:

Tabla 5
Escala y Valor de Importancia de un activo

ESCALA	VALOR DE IMPORTANCIA
1	MUY ALTO
2	ALTO
3	MEDIO
4	BAJO
5	MUY BAJO

Fuente: Elaboración propia

Los valores de Importancia de los Activos CID

La estimación del valor de importancia de un activo de información está en función a la Confidencialidad-Integridad-Disponibilidad (CID), tomando en cuenta las obligaciones o requisitos del

negocio, la parte legal y lo contractual. Esta importancia es definida por el responsable del activo con el apoyo del analista de seguridad. A continuación, se definen estos términos, así como los valores de importancia:

Confidencialidad.

Esta dimensión se aplica mayormente a la información. Estos valores se obtienen según la clasificación identificada para cada Activo:

Tabla 6
Escala de la importancia en la confidencialidad

ESCALA	VALOR DE IMPORTANCIA	TIPO DE INFORMACIÓN
1	MUY ALTO	NO CLASIFICADA
2	ALTO	GENERAL
3	MEDIO	INTERNA
4	BAJO	RESERVADA
5	MUY BAJO	SECRETA

Fuente: Elaboración propia

Integridad.

Podríamos involucrar la siguiente pregunta para un mejor entendimiento: ¿Qué tan importante es para el Proceso el que este activo mantenga su integridad?

La falta de Integridad del activo (por error / adulteración / accidente):

Tabla 7
Escala de la importancia en la Integridad

ESCALA	VALOR DE IMPORTANCIA	INTEGRIDAD
1	MUY ALTO	Tiene el potencial de replicarse y afectar el objetivo del proceso.
2	ALTO	Afecta la integridad de una parte de la información del proceso
3	MEDIO	Afecta la integridad de la información de una o más actividades medianamente importantes.
4	BAJO	Afecta la integridad de una actividad del proceso no importante del proceso.
5	MUY BAJO	Afecta la integridad de un activo que tiene poca importancia.

Fuente: Elaboración propia

Disponibilidad.

Podríamos involucrar la siguiente pregunta para un mejor entendimiento: ¿Qué tan importante es

para la Institución que este activo mantenga su disponibilidad?

La falta de disponibilidad del activo:

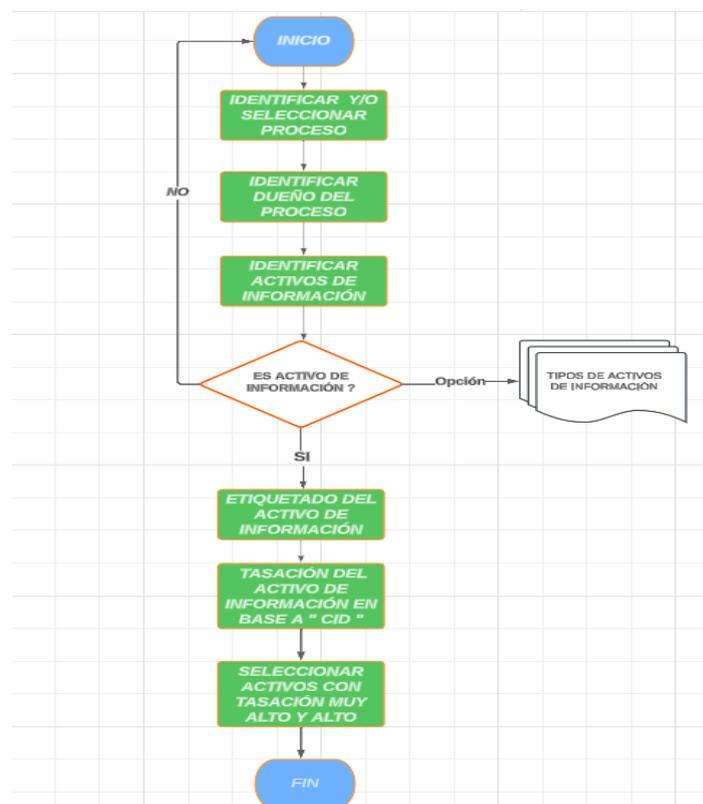
Tabla 8
Escala de la importancia en la disponibilidad

ESCALA	VALOR DE IMPORTANCIA	DISPONIBILIDAD
1	MUY ALTO	Tiene el potencial de replicarse y afectar el objetivo del proceso.
2	ALTO	Afecta la integridad de una parte de la información del proceso
3	MEDIO	Afecta la integridad de la información de una o más actividades medianamente importantes.
4	BAJO	Afecta la integridad de una actividad del proceso no importante del proceso.
5	MUY BAJO	Afecta la integridad de un activo que tiene poca importancia.

Fuente: Elaboración propia

A continuación, se ilustra el flujo a seguir para el proceso de identificación de activos de información:

Figura 20
Identificación de activos de información



Fuente: Elaboración propia.

Valoración del Activo de Información Para estimar el valor del activo de información, se estima de manera individual el valor de cada una de las dimensiones de seguridad de la información (confidencialidad, integridad y disponibilidad), luego se promedian cada uno de estos valores, tal como se expresa en la siguiente fórmula:

$$\text{Valor del activo} = \frac{(\text{Valor Confidencialidad} + \text{Valor Integridad} + \text{Valor Disponibilidad})}{3}$$

Clasificación de activos El objetivo de clasificar los activos de información es asegurar que los activos de información reciban el nivel de protección adecuado, conforme con su importancia para Unidad de Tramite Documentario de la Universidad Nacional San Antonio Abad del Cusco. La clasificación de activos entrega a los colaboradores que se encargan de operar o gestionar los activos de información una indicación concisa sobre cómo manejarlos y protegerlos. En esta etapa, usando como insumo los registros de los activos de información se procede a la clasificación de la sensibilidad y criticidad del activo de información identificado.

Por su nivel de sensibilidad La clasificación de la sensibilidad de los activos de información se realiza con el propietario del activo de información, en donde se le asigna al activo de información una etiqueta de sensibilidad que puede ser: Uso Público, Uso Interno, Uso Confidencial y Uso Restringido de acuerdo con lo establecido en el dominio de gestión de activos de la Política de los Dominios de Seguridad de la Información. Para efectuar la clasificación de la sensibilidad del activo de información se desarrolla con la guía de la siguiente tabla el Nivel de sensibilidad de los activos de información.

Tabla 9
Escala de la importancia en la disponibilidad

Nivel de Sensibilidad	Detalle
USO PÚBLICO	Información accedida tanto por miembros de la Universidad como por personas externas a ella (público en general), sin estar sujetos a ningún control.
USO INTERNO	Información accedida exclusivamente por personal interno autorizado de la Unidad de Tramite Documentario y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso. Su revelación requiere la aprobación del custodio en coordinación con el propietario del activo.
USO CONFIDENCIAL	Información que por su naturaleza debe ser accesible sólo a aquellos que se encuentren debidamente autorizados y de manera excepcional personal externo (auditores, entidades reguladoras, consultores externos, entre otros), puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso. Su revelación requiere la aprobación de su propietario, es de uso exclusivo de la Universidad, en el caso de terceros se debe firmar acuerdo de confidencialidad y no divulgación.
USO RESTRINGIDO	Información cuyo acceso se da a un grupo determinado de individuos, seleccionados a partir de un proyecto estratégico o de interés institucional que pertenecen a un grupo o nivel específico de poder dentro de la entidad. Su revelación requiere la aprobación de las altas autoridades como la ASAMBLEA UNIVERSITARIA, por lo tanto, deben ser gestionados con todas las precauciones y controles posibles, determinando exactamente qué personas tienen acceso a los mismos y vigilando su uso, transporte y almacenamiento.

Fuente: Elaboración propia

Identificación de amenazas y vulnerabilidades.

Amenaza es una causa potencial de un incidente no deseado, que puede resultar en un daño para la Unidad de Tramite Documentario de la Universidad Nacional San Antonio Abad del Cusco. El responsable del Activo en este caso el dueño del proceso debe listar las amenazas que afectan a los activos a su cargo y cuáles son las causas por las cuales se produce la amenaza. Asimismo, poder determinar el vector de ataque que podría permitir su materialización.

El agente que genera la amenaza puede ser Interno o Externo y pueden ser humanos o no humanos.

Los agentes internos están dentro de la Universidad. Los agentes externos incluyen las personas ajenas

a la Universidad.

De igual manera, no todos los tipos de amenaza requieren un agente de fuente de amenazas; tomando como referencia la publicación especial: NIST SP 800-30.

Es necesario tener en cuenta que entre las amenazas existen dependencias como por ejemplo la denegación de un servicio que es causado por una mala operación o por un código malicioso, adicionalmente el código malicioso es una amenaza que es causada por un hacker, el impacto de esta amenaza esta dado que puede paralizar un servicio y a la vez puede paralizar todo un proceso critico de un negocio en este caso el de la Unidad de Tramite Documentario. Si bien las amenazas pueden ser de tipos muy variados, para propósitos de análisis se establecen algunos tipos de amenaza que se van a utilizar:

Tabla 10
Catálogo de amenazas, agentes y vulnerabilidades

Amenazas	Agente
Fuego	Natural, falla eléctrica, agente externo
Daños por agua	Baños, tuberías, lluvias
Desastres naturales (terremotos, tormenta, huaico, etc.)	Naturales
Desastres industriales	Empresas cercanas, equipos industriales
Contaminación mecánica (vibraciones, polvo, suciedad, etc.)	Ambiente
Contaminación electromagnética (radio, campos magnéticos, etc.)	Equipos de comunicación
Fallas en equipos	Fabricación, falta o mal tratamiento
Falla lógica (fallos en los programas, etc.)	Programador, empresa, control calidad
Corte de suministro eléctrico	Falla cables, tablero, empresa
Condiciones inadecuadas de temperatura y humedad.	Mala o falla en la ambientación, Natural
Falla de servicios de comunicación	Equipos de comunicación, proveedor, cable
Interrupción de otros servicios y suministros esenciales.	Equipos, empresas

Amenazas	Agente
Errores humanos	Usuarios no capacitados o incompetentes, Administrador no capacitado o incompetente, Personal no capacitado o incompetente
Fuga de información	Personal interno y/o externo
Alteración de la información	Error humano o deliberado
Destrucción de la información	Falla proceso, deliberado, mal manejo
Caída de sistemas por agotamiento de recursos	Incumplimiento de especificaciones, saturación
Ausencia del personal	Huelga, enfermedad, vacaciones
Denegación de servicio	Hacker, mal proceso
Vandalismo	Hacker, personal descontento
Sabotaje	Hacker, personal interno o externo
Código malicioso	Hacker, personal interno, programador
Otros	Otros

Fuente: Elaboración propia

Así también se presenta un abanico de vulnerabilidades:

Tabla 11
Catálogo de vulnerabilidades

Tipo	Vulnerabilidad
Hardware	Falta de mantenimiento Preventivo y Correctivo
	Ausencia de esquemas de reemplazo periódico.
	Susceptibilidad a la humedad, el polvo y la suciedad.
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
Copia no controlada	
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencia de pistas de auditoría
Asignación errada de los derechos de acceso	

	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y usos no controlados de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Falla en la producción de informes de gestión
	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables.
	Punto único de falla
Red	Ausencia de identificación y autenticación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
Personal	Falta de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en un área susceptible de inundación
Lugar	Red energética inestable
	Ausencia de protección física de la edificación, puertas y ventanas
	Ausencia de procedimiento formal para el registro y retiro de usuarios
Organización	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso

	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información
	Ausencia de auditorías (supervisiones) regulares
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento del servicio
	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.
	Ausencia de procedimiento de control de cambios
	Ausencia de procedimiento formal para el control de la documentación del SGSI
	Ausencia de procedimiento formal para la supervisión del registro del SGSI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso del correo electrónico
	Ausencia de procedimientos para la introducción del software en los sistemas operativos
	Ausencia de registros en las bitácoras (logs) de administrador y operario.
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla
	Ausencia de autorización de los recursos de procesamiento de la información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad
	Ausencia de revisiones regulares por parte de la gerencia
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
	Política de Seguridad de la Información
	Organización de seguridad
Concientización	Roles y responsabilidad de seguridad
	Procedimientos y estándares
	Programa de concientización sobre seguridad
	Control de acceso físico
Seguridad física	Monitoreo (Ej. CCTV)
	Vigilancia
	Alarmas

	Seguridad perimetral
	Falta de Controles Preventivos y Detectivos de incendios
Perímetro	Firewall
	Pruebas de penetración
	Web application firewall (WAF)
	Sistemas de detección / prevención e intrusos (IDS/IPS)
	VPN, NAC
	Red interna
	VLANs
	ACLs
	Auditoría de seguridad
Host	Controles de contraseñas
	Estándares de endurecimiento
	Gestión de parches de seguridad
	Prevención de intrusiones de host (HIPS)
	Falta de Anti-malware
	Logs seguridad
	Escaneo de vulnerabilidades
	Aplicación
	Técnicas de programación segura
	Políticas de contraseñas
	Controles de acceso
	Web application firewall (WAF)
	Evaluación de seguridad
	Datos
	Encriptación, ofuscación
	Clasificación
	ACLs
	Data Leak Prevention (DLP)
	Sanitización de datos
Digital Rights Management (DRM)	

Fuente: Elaboración propia

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso.

Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal Configurado que permite que un agente de amenaza acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en

función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta.

Metodología de cuantificación de las vulnerabilidades (CVSS)

(Common Vulnerability Scoring System)

El CVSS es una iniciativa pública concebida por la *National Infrastructure Assurance Council* (NIAC) de EE. UU, un grupo que provee de recomendaciones al *Department of Homeland Security* de los EE.UU. Entre las organizaciones que lo adoptaron tempranamente destacan Cisco, US *National Institute of Standards and Technology* (NIST), *Qualys* y Oracle. En la actualidad, el CVSS está bajo la custodia del *Forum for International Response Teams* (FIRST) y es aceptada por diversas organizaciones relacionadas a seguridad de información: IBM, HP, CISCO, MICROSOFT, McAfee, Symantec, etc.

Entre los beneficios que ofrece el CVSS están:

1. Puntuación estándar de vulnerabilidades: El CVSS es neutro desde el punto de vista de las aplicaciones, permitiendo que distintas organizaciones asignen una puntuación a sus vulnerabilidades de TI a través de un único esquema.

2. Puntuación contextualizada: La puntuación asignada por una organización corresponde al riesgo que la vulnerabilidad representa para dicha organización.

3. Sistema abierto: El CVSS provee todos los detalles sobre los parámetros usados en la generación de cada puntuación permitiendo comprender tanto el razonamiento que sustenta una puntuación como el significado de diferencias entre puntuaciones.

Las puntuaciones asignadas por el CVSS se derivan de los tres grupos de métricas siguientes:

- Base: Este grupo representa las propiedades de una vulnerabilidad que son inmutables en el tiempo, específicamente: complejidad de acceso, vector de acceso, y grado en que compromete la confidencialidad, integridad y disponibilidad del sistema.
- Temporal: Este grupo mide las propiedades de una vulnerabilidad que sí cambian en el tiempo, como por ejemplo la existencia de parches o código para su explotación.

- Entorno: Este grupo mide las propiedades de una vulnerabilidad que son representativas de los ambientes de uso de las TI como por ejemplo la prevalencia de sistemas afectados y pérdidas potenciales.

Tabla 12
Cuantificación y Calificación de las vulnerabilidades identificadas

CATEGORÍA DEL RIESGO	NIVEL CID	
1	CRITICO	9-10
2	ALTO	7-8.9
3	MEDIO	4-6.9
4	BAJO	0.1-3.9
5	NINGUNO	0

Fuente: Elaboración propia

Evaluación de riesgos y probabilidad de ocurrencia.

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos, y por ello han surgido una multitud de guías informales, aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están dichos activos y no llamarse a engaño

El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular (Thomas R. Peltier, 2001)

El objetivo del análisis de riesgo es identificar los riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades (Alberto G. Alexander, 2007)

Para identificar el nivel de impacto del riesgo se utilizará la siguiente tabla de valoración; considerando Factores de impacto de un ciberataque. Cabe mencionar, que los factores de impacto establecidos han sido seleccionados tomando como Nota: el informe “Debajo de la Superficie de un Ciberataque” publicado por Deloitte en el año 2016.

Tabla 13
Nivel de impacto del riesgo

VALOR DEL IMPACTO	NIVEL CID	IMPACTO
1	MUY ALTO	INSIGNIFICANTE
2	ALTO	MENOR
3	MEDIO	MODERADO
4	BAJO	MAYOR
5	MUY BAJO	CATASTRÓFICO

Fuente: Elaboración propia

La probabilidad es la posibilidad de ocurrencia de un riesgo en un periodo de tiempo determinado. Puede ser calculada en función a cuantas veces históricamente ha ocurrido o se prevé que pueda suceder en el futuro. Para identificar la probabilidad de ocurrencia del riesgo se utilizará la siguiente tabla de valoración:

Tabla 14
Posibilidad de ocurrencia de un riesgo

Valores	Rango de Probabilidad				
	Raro	Improbable	Posible	Probable	Casi certeza
Frecuencia	1 VEZ EN 3 AÑOS	1 VEZ POR AÑO	1 VEZ POR SEMESTRE	1 VEZ AL TRIMESTRE	1 VEZ CADA MES
Probabilidad Matemática	< 10%	10.1% - 20%	20.1% - 50%	50.1% - 90%	> 90%

Fuente: Elaboración propia

De acuerdo con la metodología MAGERIT se va a valorizar la degradación de la confidencialidad, integridad y disponibilidad considerando las amenazas, las vulnerabilidades y los controles existentes para cada riesgo, luego se va a poner el valor de degradación máximo el cual es asumido como el nivel de impacto de la seguridad de la información.

Luego se define la probabilidad según la tabla el cual nos indica la posibilidad en las condiciones actuales que se llegue a materializar la amenaza.

Con el valor del impacto y la probabilidad de cada riesgo se determina con la matriz de riesgo el nivel bajo, medio, alto y extremo.

Tabla 15
Degradación de activos de información

Valores de Degradación		
Degradación-Confidencialidad		
5	MUY ALTO	Un activo secreto es vulnerado.
4	ALTO	Un activo reservado es factible que sea vulnerado.
3	MEDIO	Un activo confidencial es poco factible que sea vulnerado.
2	BAJO	Un activo interno es vulnerado.
1	MUY BAJO	Un activo público es vulnerado.
Degradación -Integridad		
5	MUY ALTO	Imposible de reconstruir la información al 100%.
4	ALTO	Se puede reconstruir, pero su obtención es muy costosa.
3	MEDIO	Se puede reconstruir a un costo razonable.
2	BAJO	Resulta fácil reconstruir el activo dañado.
1	MUY BAJO	No se necesita reconstruir.
Degradación -Disponibilidad		
5	MUY ALTO	Disponible en más de una semana.
4	ALTO	Disponible en un lapso de entre un día y una semana.
3	MEDIO	Disponible en un lapso de entre medio día y un día.
2	BAJO	Disponible en un lapso de entre una hora y medio día.
1	MUY BAJO	Disponible en menos de una hora

Fuente: Elaboración propia

El riesgo potencial de un activo de información corresponde al nivel de riesgos sin considerar (en ausencia) los controles existentes o planificados para disminuir la probabilidad o impacto, de ser el caso. En este paso, los propietarios o custodios de los activos de información calculan el valor del riesgo potencial mediante la combinación de la probabilidad de ocurrencia del riesgo por el impacto que ocasiona sobre los activos de información. Así tenemos:

Figura 21
Mapa de calor de riesgos

PROBABILIDAD	CASI CERTEZA	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO
	PROBABLE	MEDIO	ALTO	ALTO	EXTREMO	EXTREMO
	POSIBLE	BAJO	MEDIO	ALTO	EXTREMO	EXTREMO
	IMPROBABLE	BAJO	BAJO	ALTO	ALTO	EXTREMO
	RARO	BAJO	BAJO	MEDIO	ALTO	ALTO
		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
		IMPACTO				

Fuente: Elaboración propia

Tabla 16
Valoración de riesgos

Riesgo	Significado
EXTREMO	Cuando el activo se encuentra expuesto a riesgos altos o extremos que ameritan ser tratados.
ALTO	Cuando el activo se encuentra expuesto a riesgos altos o extremos que ameritan ser tratados.
MEDIO	Es un riesgo aceptable, cuando el activo se encuentra expuesto a riesgos bajos o moderados, por lo que no amerita que pase al proceso de Tratamiento de Riesgo
BAJO	Es un riesgo aceptable, cuando el activo se encuentra expuesto a riesgos bajos o moderados, por lo que no amerita que pase al proceso de Tratamiento de Riesgo

Fuente: Elaboración propia

3.3.2. Análisis de Riesgos

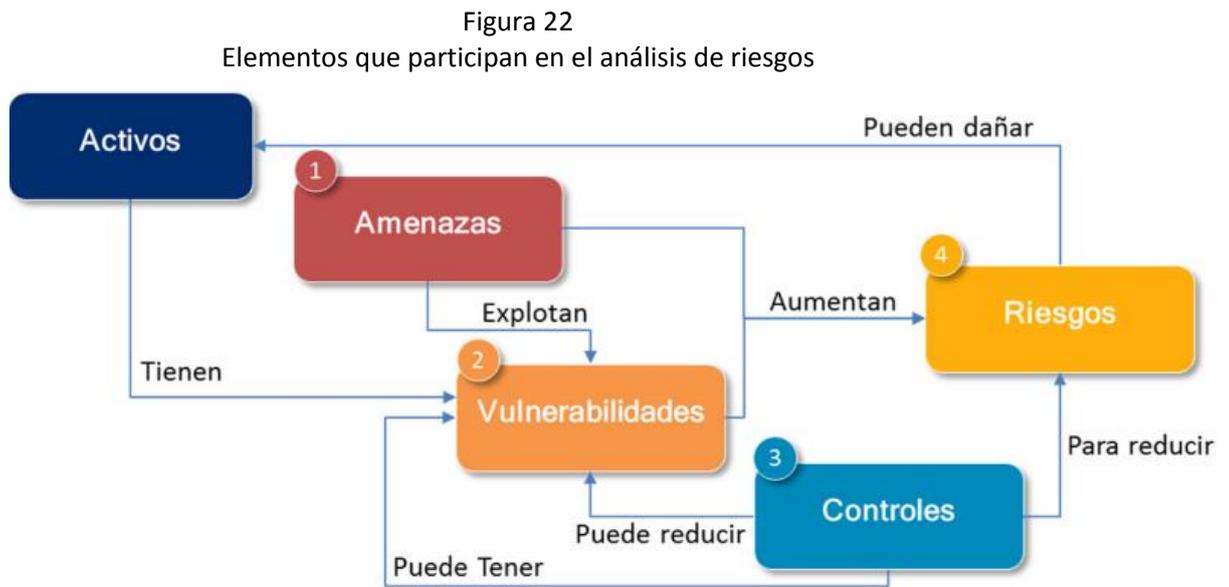
Esta etapa de evaluación de riesgos de seguridad de la información se centra en aquellos riesgos que puedan tener impacto negativo sobre la confidencialidad, integridad y disponibilidad de los activos de información que fueron identificados en el inventario y tasación de activos de información. La identificación y el análisis de los riesgos de seguridad de la información de los activos de información, sirve de base para la evaluación y tratamiento y como deben ser gestionados.

En el despliegue de esta etapa, el Especialista de Seguridad de la Información, asiste metodológicamente a los propietarios de los activos de información (jefe de la Unidad) en el análisis detallado, identificación de amenazas, vulnerabilidades, riesgos, controles, probabilidad e impacto. Asimismo, la información recogida en esta etapa debe ser registrada en la matriz elaborada en el ANEXO 04 Matriz de Análisis de Riesgos. Para desplegar las actividades antes listadas, es importante tener en cuenta:

- Los activos de información que van a ser considerados en esta etapa serán aquellos cuya tasación final sea relevante, es decir, con tasación final Medio, Alto o Muy Alto. En la etapa de tratamiento de riesgos de seguridad de la información, los riesgos con nivel de riesgo real “Bajo” son aceptados dentro del apetito de riesgos de la Unidad de Tramite Documentario de la Universidad Nacional San Antonio Abad del Cusco y no requieren tratamiento adicional, mientras que aquellos con un nivel de riesgo real “Moderado” queda a criterio del propietario del activo de información aplicar

tratamiento. Para los que tienen un nivel de riesgo real “Alto” y “Extremo” requiere tomar la decisión por parte del Propietario del Activo de información y, de ser necesario, contar con la participación del Custodio del activo de información para aceptar, mitigar, transferir o evitar el riesgo, que será aprobado por el Comité de Seguridad de la Información.

A continuación, se muestran los elementos que participan en el análisis de riesgos:



Asimismo, es importante entender las relaciones que se presentan entre los distintos elementos que la componen. Estas relaciones se listan a continuación y muestran en la Figura previa.

- Los activos y los controles pueden presentar vulnerabilidades que pueden ser explotadas por las amenazas.
- La combinación de las amenazas y vulnerabilidades pueden aumentar el efecto potencial del riesgo
- Los controles permiten reducir las vulnerabilidades y riesgos.

Pasos Previos

Antes de efectuar una evaluación de riesgos se debe llevar a cabo un inventario y tasación de activos de información para identificar los activos de información cuya tasación final es relevante y por lo cual debe centrarse el análisis de riesgos y su posterior evaluación de riesgos.

Objetivos

Analizar e identificar los riesgos a los que están expuestos los activos de información, determinando las amenazas, vulnerabilidades y controles aplicados para su tratamiento.

Conceptos y supuestos

Conceptos: Independientemente del método de análisis que se utilice, se asume la relación siguiente:

Supuestos.

El especialista de seguridad de la información o a quien se asigne esas funciones cuenta con una metodología para realizar el análisis y evaluación de riesgos de seguridad de la información, a la cual se tiene que alinear la gestión de la seguridad de la información.

Proceso

El enfoque metodológico de la etapa de evaluación riesgos de seguridad de la información, se despliega a través de las siguientes etapas:

Análisis de Riesgos

El análisis de los riesgos de seguridad de la información se inicia con el cuestionamiento de lo que puede fallar a causa de las amenazas que pueden explotar las vulnerabilidades de los activos o los controles y cuáles serían las consecuencias de la falla. Los pasos del análisis de riesgos son:

Identificar amenazas

Esta actividad se centra en la identificación de amenazas que tienen el potencial de dañar a los activos de información, a través de la explotación de las vulnerabilidades propias del activo de información o de los controles relacionados. Para cada uno de los activos de información, se realiza la identificación de las amenazas.

Identificar vulnerabilidades

Luego de la actividad de identificación de amenazas, se identifican las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos de información. Asimismo, un control implementado de manera incorrecta, que funciona mal, o que se utiliza de modo incorrecto puede constituir una vulnerabilidad. Para la identificación de vulnerabilidades es importante entender que

la sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios.

Identificar riesgos

Los riesgos de seguridad de la información se definen en función a las pérdidas que se podrían ocasionar sobre los procesos cuando una amenaza explota una vulnerabilidad ocasionando un daño en los activos de información.

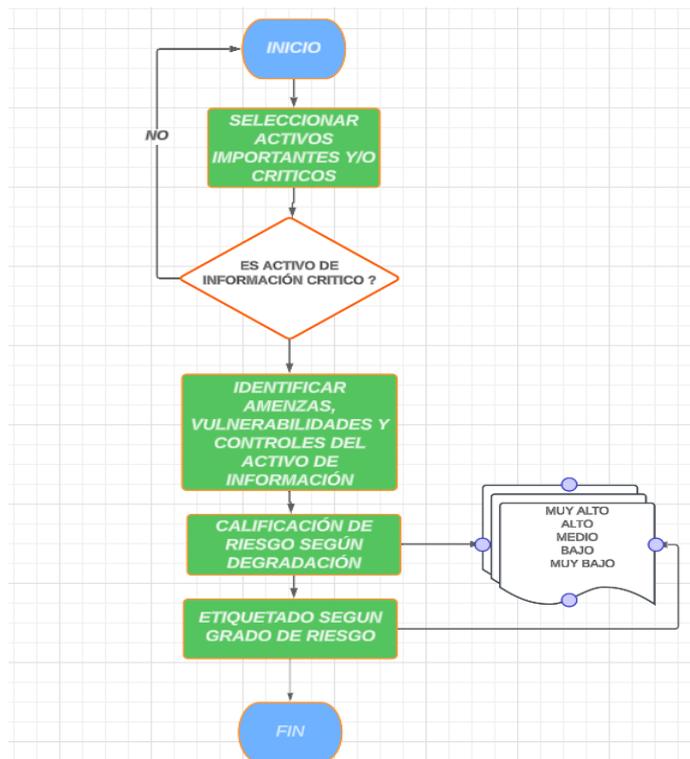
Por lo tanto, para cada amenaza identificada se deben determinar las consecuencias que podría ocasionar sobre los activos de información teniendo en cuenta las vulnerabilidades a las que están expuestos. El riesgo debe estar escrito en un lenguaje común y comprensible para toda la institución.

Por lo tanto, la nomenclatura para cada riesgo será basada en la siguiente expresión: “Posibilidad de pérdida (de confidencialidad/ de integridad/ de disponibilidad) sobre (activo de información) ocasionada por (amenaza) debido a (vulnerabilidad).”



A continuación, se ilustra el flujo a seguir para el proceso de análisis de riesgos de activos de información:

Figura 23
Proceso de análisis de riesgos de activos de información



Elaboración: Fuente propia

3.3.3. Proponer controles de seguridad

El principal fin es establecer directrices generales relacionadas a los dominios de seguridad de la información a fin de reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o se use de forma indebida los activos de información, garantizando así la confidencialidad, autenticidad y/o integridad de la información.

Esta política aplica a todos los trabajadores (directores, jefes, funcionarios y empleados académicos y administrativos), contratistas, consultores, proveedores y personal temporal que tengan acceso a recursos de información de propiedad de la Universidad Nacional San Antonio Abad del Cusco.

Prueba de Efectividad de Controles

El objetivo de evaluar el control es determinar su efectividad en la reducción de la exposición del riesgo residual con respecto al riesgo inherente. La evaluación de la efectividad del control se realiza bajo las dimensiones de diseño y ejecución, para determinar su grado de efectividad en la mitigación de probabilidad e impacto del riesgo. A continuación, se muestran los criterios de diseño y ejecución:

Controles

Son aquellos controles que se encuentran implementados por la organización, al momento del Análisis de Riesgos que son identificados para realizar el cálculo de los Riesgos Residuales.

Tipos De Control.

Controles Preventivos: Sirven para que la amenaza no cumpla con su objetivo de atentar contra la seguridad del activo.

Controles Detectivos: Son aquellos que sirven para descubrir amenazas o vulnerabilidades de la seguridad de la información.

Controles Correctivos: Son aquellos que se ejecutan después de un ataque contra la seguridad de la información y sirven para corregir el daño en la seguridad que ha sufrido el activo.

Calificación De Controles. - Utilizando criterios establecidos se califican los controles asociados al riesgo y según su resultado los controles tendrán un efecto sobre los riesgos inherentes y se calculará el riesgo residual.

a) Definición de Control: Política, dispositivo o acción que actúa para eliminar o minimizar los riesgos adversos, puede tener efecto sobre uno o varios riesgos y proveen una seguridad razonable relativa al logro de los objetivos.

b) Consideraciones para la Calificación del Control:

- Iniciar el proceso en orden descendente, comenzando por el riesgo de mayor severidad absoluta, teniendo en cuenta cada una de las causas asociadas al riesgo.
- No omitir ningún control existente dentro del proceso, para obviar duplicidades y superposiciones con los tratamientos (controles planeados).
- Identificar primero los controles de mayor cobertura (que mitigan las causas de mayor probabilidad o reducen significativamente las consecuencias) y que a su vez sean los de mayor efectividad.
- En los riesgos subsiguientes, antes de incluir nuevos controles, identificar y evaluar controles ya descritos y vinculados a los riesgos de mayor severidad.

- Calificar únicamente los controles existentes, no incluir controles que no existen. Si en el momento de la calificación se plantea la creación de un control que debería tener el riesgo, este debe registrarse en la columna de Planes de Tratamiento.

La documentación mínima del control considera los siguientes factores

Tabla 17
Efectividad de controles

Factores	Peso Considerado Porcentual
Tipo	50%
Implementación	10%
Frecuencia	15%
Complejidad	5%
Documentación	10%
Responsabilidad	10%

Fuente: Elaboración propia

Tipos de Control (Preventivo, Detectivo, Correctivo)

Preventivo: Su objetivo es evitar que ocurran incidentes de seguridad. Ejemplos incluyen la autenticación multifactor, las políticas de contraseñas y las restricciones de acceso. La efectividad de estos controles se evalúa según su capacidad para bloquear amenazas antes de que se materialicen.

Detectivo: Estos controles identifican y notifican incidentes de seguridad después de que ocurren, como los sistemas de detección de intrusos (IDS) y las auditorías de logs. La efectividad se mide en su capacidad para alertar rápidamente sobre actividades sospechosas.

Correctivo: Diseñados para corregir o mitigar los efectos de un incidente de seguridad, como los procedimientos de recuperación y los planes de contingencia. La efectividad se mide en términos de rapidez y capacidad de restauración de servicios.

Implementación

Se refiere a la calidad y completitud de la implementación del control. Para un control efectivo, la implementación debe ser exhaustiva y sin brechas. Y la forma de evaluación: Se examina si el control ha sido completamente implementado y está operando en todas las áreas relevantes. Se valoran

aspectos como la conformidad con los procedimientos y si se han cumplido los requisitos técnicos y operativos de cada control.

Frecuencia

Se refiere a cuán frecuentemente se aplica o revisa el control. Algunos controles, como las auditorías de seguridad, pueden aplicarse trimestralmente, mientras que otros, como los monitoreos de acceso, se ejecutan en tiempo real. La forma de evaluar la efectividad de un control puede depender de su frecuencia; un control aplicado muy ocasionalmente podría no ser suficiente para mitigar ciertos riesgos. La frecuencia debe ajustarse al nivel de riesgo y al tipo de actividad protegida.

Complejidad

Descripción: Evalúa el nivel de dificultad para implementar y mantener el control. Los controles demasiado complejos pueden ser más costosos y difíciles de operar de forma consistente. La forma de realizar una evaluación se realiza analizando si la complejidad del control puede afectar su efectividad, ya que un control que es difícil de entender o de operar puede ser aplicado incorrectamente. Los controles deben ser lo suficientemente sencillos como para que el personal los aplique correctamente sin comprometer la seguridad.

Documentación

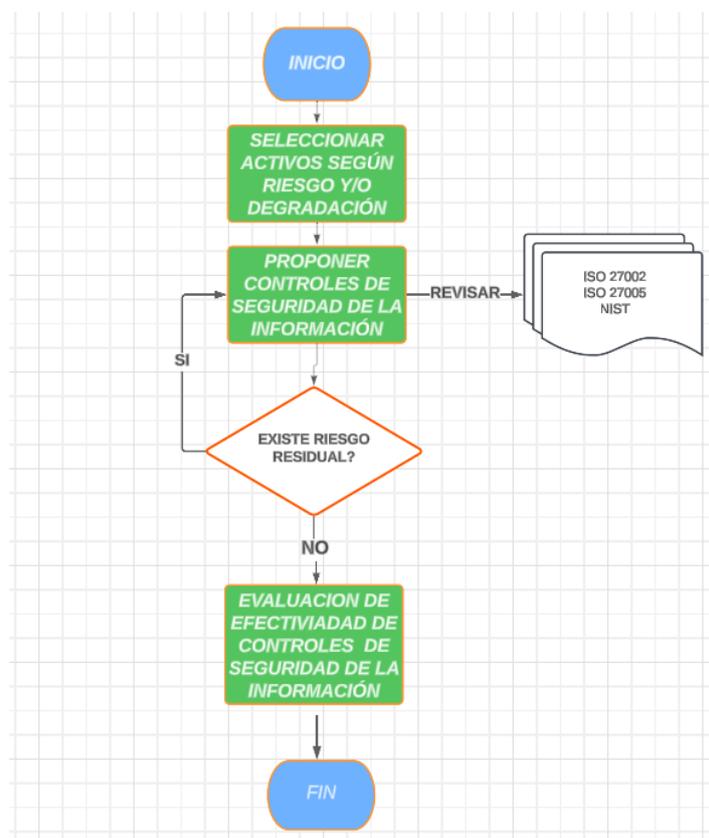
Descripción: La documentación es crucial para la efectividad del control, ya que establece directrices claras sobre cómo debe implementarse, mantenerse y revisarse. La forma de realizar una evaluación mediante la efectividad de los controles se evalúa en función de la calidad de la documentación, que debe ser clara, accesible y completa. La documentación adecuada también facilita la auditoría y el cumplimiento normativo.

Responsabilidad

Descripción: Se refiere a la asignación clara de roles y responsabilidades para cada control, asegurando que alguien esté encargado de su operación y monitoreo. La forma de realizar una evaluación sería identificando la efectividad del control la cual depende de que haya personal designado y capacitado que asuma responsabilidad directa sobre su funcionamiento y revisión. Esto incluye un seguimiento

constante para asegurar que los controles se mantengan operativos y se adapten a cambios en el entorno de riesgo.

Figura 24
Proceso de propuesta de controles de seguridad de la información



Fuente: Elaboración propia

3.3.4. Plantear un procedimiento para Cumplimiento normativo

Con el objetivo de Establecer un conjunto de políticas y directivas de seguridad de la información que permitan proteger la confidencialidad, integridad y disponibilidad de la información dentro de la organización. Esto incluye definir lineamientos claros que guíen el comportamiento de los usuarios, administradores y todos los actores involucrados en el tratamiento de la información, de manera que se minimicen los riesgos de seguridad y se asegure el cumplimiento normativo y legal aplicable. La propuesta busca también apoyar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Con el alcance garantizaríamos que todos los aspectos críticos en la gestión de la seguridad de la

información estén cubiertos, y que las políticas y directivas propuestas se puedan implementar de manera integral y efectiva en la organización.

Estas Propuesta se ha desarrollado según algunos marcos regulatorios y normativos, como ISO/IEC 27001, 27003 entre otras para la guía de la elaboración de las políticas y directivas, la cual servirá como una guía estructurada para proteger los recursos de información de manera proactiva, fomentando la cultura de seguridad en toda la Universidad. A continuación, se muestran los Títulos desarrollados propuestos en el ANEXO 01: POLÍTICAS Y DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN:

Tabla 18
Propuestas para las políticas y directivas de seguridad de la información

Títulos Propuestos para las Políticas y Directivas de Seguridad de la Información	
5.	DEL DOMINIO DE ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN
5.1.	Del alcance del dominio
5.2.	Declaración de la política
5.3.	De las políticas de los controles del dominio
5.3.1.	De la organización interna
5.3.2.	De los dispositivos móviles
6.	DEL DOMINIO DE SEGURIDAD DE LOS RECURSOS HUMANOS
6.1.	Del alcance del dominio
6.2.	Declaración de la política
6.3.	De las políticas de los controles de recurso humanos
6.3.1.	Antes del empleo
6.3.2.	Durante el empleo
6.3.3.	Terminación y cambio de empleo
7.	DEL DOMINIO DE GESTIÓN DE ACTIVOS
7.1.	Del alcance del dominio
7.2.	Declaración de la política
7.3.	De las políticas de los controles del dominio
7.3.1.	De la responsabilidad por los activos
7.3.1.2.	De la propiedad de los activos:
7.3.1.3.	Del uso aceptable de los activos:
7.3.2.	De la clasificación de la información
7.3.3.	Del manejo de los medios
8.	DEL DOMINIO DE CONTROL DE ACCESO
8.1.	Del alcance del dominio
8.2.	Declaración de la política
8.3.	De las políticas de los controles del dominio
8.3.1.	De los requisitos para el control de acceso
8.3.2.	De la gestión de acceso de usuario
8.3.3.	De las responsabilidades de los usuarios
8.3.4.	Del control de acceso a sistemas y aplicaciones
9.	DEL DOMINIO DE CRIPTOGRAFÍA

Títulos Propuestos para las Políticas y Directivas de Seguridad de la Información

- 9.1. Del alcance del dominio
 - 9.2. Declaración de la política
 - 10. DEL DOMINIO DE SEGURIDAD FÍSICA Y AMBIENTAL
 - 10.1. Del alcance del dominio
 - 10.2. Declaración de la política
 - 10.3. De las políticas de los controles del dominio
 - 10.3.1. De las áreas seguras
 - 10.3.2. De los equipos
 - 11. DEL DOMINIO DE SEGURIDAD DE LAS OPERACIONES
 - 11.1. Del alcance del dominio
 - 11.2. Declaración de la política
 - 11.3. De las políticas de los controles del dominio
 - 11.3.1. De los procedimientos y responsabilidades operativas
 - 11.3.2. De la protección contra código malicioso
 - 11.3.3. Del respaldo
 - 11.3.4. De los registros y monitoreo
 - 11.3.5. De la gestión de vulnerabilidad técnica
 - 11.3.6. De las consideraciones para la auditoría de los sistemas de información
 - 12. DEL DOMINIO DE SEGURIDAD DE LAS COMUNICACIONES
 - 12.1. Del alcance del dominio
 - 12.2. Declaración de la política
 - 12.3. De las políticas de los controles del dominio
 - 12.3.1. De la gestión de seguridad de la red
 - 12.3.2. De la transferencia de información
 - 13. DEL DOMINIO DE RELACIONES CON PROVEEDORES
 - 13.1. Del alcance del dominio
 - 13.2. De las políticas de los controles
 - 13.2.1. De la seguridad de la información en las relaciones con los proveedores
 - 13.2.2. De la gestión de entrega de servicios del proveedor
 - 14. DEL DOMINIO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
 - 14.1. Del alcance del dominio
 - 14.2. Declaración de la política
 - 14.3. De las políticas de los controles del dominio
 - 14.3.1. De las responsabilidades y procedimientos
 - 14.3.2. Del reporte de eventos de seguridad de información
 - 14.3.3. Del reporte de debilidades de seguridad de información
 - 14.3.4. De la evaluación y decisión sobre eventos de seguridad de la información
 - 14.3.5. De la respuesta a incidentes de seguridad de la información
 - 14.3.6. Del aprendizaje de los incidentes de seguridad de la información
 - 14.3.7. De la recolección y resguardo de la evidencia
 - 14.3.8. De la comunicación a los usuarios y/o usuarios
 - 15. DEL DOMINIO DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO
 - 15.1. Del alcance del dominio
 - 15.2. Declaración de la política
 - 15.3. De las políticas de los controles
 - 15.3.1. De la continuidad de seguridad de la información
 - 15.3.2. De las redundancias
 - 16. DEL DOMINIO DE CUMPLIMIENTO
-

Títulos Propuestos para las Políticas y Directivas de Seguridad de la Información

- 16.1. Del alcance del dominio
 - 16.2. Declaración de la política
 - 16.3. De las políticas de los controles del dominio
 - 16.3.1. Del cumplimiento con requisitos legales y contractuales
 - 16.3.2. De las revisiones de seguridad de la información
 - 17. RESPONSABILIDADES
 - 17.1. Asamblea universitaria
 - 17.2. Consejo universitario
 - 17.3. Órgano de control institucional
 - 17.4. Oficina de tecnologías de la información
 - 17.5. Rectorado
 - 17.6. Jefatura de direcciones o unidad organizacional
 - 17.6.1. Del dominio de Gestión de activos
 - 17.6.2. Del dominio de Seguridad Física y Ambiental
 - 17.6.3. Del dominio de Control de Acceso
 - 17.6.4. Del dominio de Cumplimiento
 - 17.6.5. Del dominio de Organización de la seguridad de la información
 - 17.7. UNIDAD DE RECURSOS HUMANOS
 - 17.8. ESPECIALISTA DE SEGURIDAD DE LA INFORMACIÓN
 - 17.8.1. Respecto a todos los dominios
 - 17.8.2. Del dominio de gestión de activos.
 - 17.8.3. Del dominio de la organización de la seguridad de la información
 - 17.8.4. Del dominio de control de acceso
 - 17.8.5. Del dominio de criptografía
 - 17.8.6. Del dominio de la seguridad en las operaciones
 - 17.9. ESTABLECER, DOCUMENTAR Y COORDINAR LA DISPOSICIÓN DE LOS PROCEDIMIENTOS RELACIONADOS AL ESCALAMIENTO Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD.
 - 17.9.1. Del dominio de incidentes de seguridad
 - 17.10. UNIDAD DE SERVICIOS GENERALES
 - 17.10.1 Del dominio de la seguridad de la información
 - 17.10.2 De dominio de Seguridad Física y Ambiental:
 - 17.11. JEFE DE OFICINA DE ASESORÍA JURÍDICA
 - 17.12. JEFE DE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
 - 17.12.1 Respecto a todos los dominios
 - 17.12.2 Del dominio de la organización de la seguridad de la información
 - 17.12.3 Del dominio de control de acceso
 - 17.12.4 Del dominio de seguridad en las operaciones
 - 17.12.5 Del dominio de seguridad física y ambiental
 - 17.12.6 Del dominio de la seguridad de las comunicaciones
 - 17.12.7 Del dominio de adquisición, desarrollo y mantenimiento de sistemas
 - 17.12.8 Del dominio de gestión de incidentes de seguridad de la información
 - 17.12.9 Del dominio de aspecto de seguridad de la información en continuidad del negocio
 - 17.13. JEFE DE PROYECTOS Y MEJORA DE PROCESOS
 - 17.13.1 Del dominio de gestión de activos
 - 17.13.2 Del dominio de seguridad de los recursos humanos
 - 17.13.3 Del dominio de la organización de la seguridad de la información
 - 17.14. TRABAJADORES
 - 17.14.1 Del dominio de la organización de la seguridad de la información
-

Títulos Propuestos para las Políticas y Directivas de Seguridad de la Información

- 17.14.2 Del dominio de la seguridad de los recursos humanos
 - 17.14.3 Del dominio de gestión de activos
 - 17.14.4 Del dominio de gestión de incidentes de seguridad de información
 - 17.14.5 Del dominio de gestión de activos
 - 18. DISPOSICIONES COMPLEMENTARIAS
-

Fuente: Elaboración propia

3.3.5. Proponer Estrategias de Concienciación y capacitación

Se desarrolló una propuesta de un plan estratégico de concientización en seguridad de la información orientado a fortalecer la cultura de seguridad en todos los niveles de la organización. Su objetivo es informar, sensibilizar y capacitar a los trabajadores en la importancia de la seguridad de la información, los riesgos asociados al manejo inadecuado de datos, protocolos y buenas prácticas que deben seguirse. La iniciativa busca reducir incidentes de seguridad, garantizar el cumplimiento de políticas internas, regulaciones externas y promover conductas proactivas hacia la protección.

Establecer una cultura organizacional de seguridad de la información mediante la concientización y la capacitación continua, para que todos los miembros de la comunidad universitaria comprendan su rol y responsabilidades en la protección de los activos de información.

Marco del NIST (Instituto Nacional de Estándares y Tecnología)

El *NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program* proporciona una guía estructurada para desarrollar y mantener programas de concienciación y capacitación.

Marco de ISO 27001:2014 y 27002:2014

La norma ISO/IEC 27001, en combinación con ISO/IEC 27002, recomienda acciones específicas para la concienciación y capacitación en seguridad de la información como parte de un SGSI.

Enfoque basado en el Ciclo de Vida de la Seguridad de la Información

Un enfoque práctico es estructurar la estrategia en fases, como las propuestas en el ciclo de vida de la seguridad.

El Plan propuesto está desarrollado en el ANEXO 03: PLAN DE CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN 2024.

3.4. Planes propuestos de Monitoreo y Control

3.4.1. *Planificación de Supervisión del Rendimiento del SGSI.*

Para el cumplimiento de la Supervisión del Rendimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en el proyecto de tesis de la UNSAAC, se recomienda implementar un conjunto de prácticas y herramientas que permitan medir y mejorar continuamente el desempeño del SGSI.

Algunas recomendaciones clave serían:

Capacitar al personal en los procedimientos del SGSI, así como en la importancia de la supervisión del rendimiento y el cumplimiento de las normas de seguridad.

Evalúa el nivel de comprensión y adherencia del personal a las políticas de seguridad mediante pruebas periódicas o cuestionarios.

Establece un ciclo de revisión de políticas y procedimientos de seguridad para adaptarlos a los cambios en el entorno y a los resultados del monitoreo y auditorías.

Asegúrate de que los procedimientos de supervisión se actualicen en función de las necesidades y riesgos detectados.

3.5. Cierre del Proyecto

3.5.1. *Resultado del análisis de la situación actual en base a la NTP ISO 27001:2014*

El tesista designado como analista de Seguridad de la Información, Marco Emerson Solís Cano, informa sobre el objetivo del taller, Inventario y Tasación de Activos de Información y Generar matrices de análisis de riesgos seguridad de la información de la Unidad de Trámite Documentario de la Universidad Nacional San Antonio Abad del Cusco, identificando los controles existentes, validar su efectividad y proponer planes de acción y oportunidades de mejora en el proceso, considerando que al finalizar el taller se deberá de establecer planes de tratamiento, en caso corresponda, a los riesgos identificados y considerados.

El despliegue de la metodología de análisis y evaluación de riesgos de seguridad de la información se desarrolló conforme a los lineamientos metodológicos y procedimientos definidos en la metodología en mención y por lo cual se desarrollaron las siguientes fases:

- ✓ Capacitación y transmisión de entendimiento de la metodología.
- ✓ Identificación de amenazas
- ✓ Identificación de vulnerabilidades
- ✓ Identificación y evaluación de riesgos
- ✓ Identificación de controles existentes
- ✓ Evaluación de la efectividad de los controles

La Actividad se inició con la revisión de los documentos de referencia como son la “Manual de Procedimientos” brindados por el Dueño del Proceso Posteriormente se procedió con valorar a todos los activos de información en base al CID (Confidencialidad, Integridad y Disponibilidad), obteniendo el siguiente resultado:

Tabla 19
Resultado de valorización a activos de información de la UTD

	Bajo	Medio	Alto	Muy Alto	Totales
Activos de información del proceso de Trámite Documentario	10	6	12	3	31

Fuente: Elaboración propia

La etapa se inició tomando en consideración a los activos y recursos con un valor de “ALTO” y “MUY ALTO”, identificados previamente.

La actividad se llevó a cabo según lo establecido la metodología MAGERIT “Análisis de Riesgos de Seguridad de la Información”. La actividad se inició con la identificación de riesgos de los activos de información y recursos que pudieran degradar la Confidencialidad, Integridad y/o Disponibilidad (impacto) y estableciendo una probabilidad de ocurrencia del riesgo, obteniendo así el valor de “RIESGO INHERENTE”. Seguidamente, a los riesgos inherentes con una valoración de “ALTO” y “EXTREMO”, se procedió con establecer con los controles existentes que pudieran mitigar el impacto (controles defectivos y/o correctivos) y la probabilidad (preventivos y/o disuasivos), obteniendo así el valor de “RIESGO RESIDUAL”. A los riesgos con un valor de riesgo residual de “ALTO” y “EXTREMO”, se procedió con establecer planes de acción (fecha inicio, fecha fin, responsable) que al ser implementados puedan convertirse en controles que mitiguen el Impacto o la Probabilidad del riesgo.

Adicionalmente y a fin de reforzar algunos controles se procedió con establecer oportunidades de mejora. El resultado de la actividad es el siguiente:

- Resultados Autoevaluación de riesgos desde Seguridad de la Información:

Tabla 20
Resultados de autoevaluación de riesgos de seguridad de la información para la UTD

	SEVERIDAD DE LOS RIESGOS IDENTIFICADOS				TOTALES
	BAJO	MEDIO	ALTO	EXTREMO	
RIESGOS INHERENTES	2	3	11	11	27
RIESGO RESIDUAL	10	8	6	3	27

Fuente: Elaboración propia

Tabla 21
Cantidad de Controles y Planes de tratamiento identificados

Número de Controles Identificados	21
Número de Planes de Tratamiento y Oportunidades de Mejora	18

Fuente: Elaboración propia

Se manifiesta para tener en cuenta la importancia de la evaluación de riesgos sobre los activos de información bajo su custodia y/o propiedad a fin de preservar la confidencialidad, integridad y disponibilidad de dichos activos.

Siendo el lunes 14/08/2024 a las 10:00 a.m. se da por finalizado el taller.

Según el NIST SP 800-30 y la ISO/IEC 27001, el informe de vulnerabilidades identifica puntos débiles en los sistemas y aplicaciones que pueden ser explotados. Divulgarlo incrementa el riesgo de ataques, ya que proporciona información detallada sobre áreas susceptibles a amenazas específicas. De acuerdo con el NIST SP 800-39 y la ISO/IEC 27005 (Gestión de Riesgos de Seguridad de la Información), las matrices de análisis de riesgos contienen evaluaciones detalladas de los activos críticos, sus amenazas, y la probabilidad de ocurrencia de incidentes de seguridad. Según el NIST SP 800-50 (*Building an Information Technology Security Awareness and Training Program*) y la ISO/IEC 27001, las políticas y los planes de concientización contienen detalles sobre el enfoque de la organización para educar a los empleados en prácticas seguras. En conclusión, Las normativas de seguridad como ISO/IEC 27001, 27005, y las guías del NIST insisten en la confidencialidad de estos documentos para

evitar el uso indebido de la información sensible y proteger la infraestructura de seguridad organizacional. Limitar el acceso a estos documentos a personal autorizado es una práctica que refuerza la postura de seguridad y ayuda a cumplir con los estándares internacionales en gestión de la seguridad de la información.

Acuerdos: Se transmite a través de un dispositivo de almacenamiento externo (usb) todos los anexos considerados en el producto y resultado del análisis de la situación actual en base a la NTP ISO 27001:2014 al dueño del proceso crítico, en este caso al jefe de la Unidad de Tramite Documentario de la Universidad Nacional San Antonio Abad del Cusco.

3.5.2. Propuesta de políticas, procedimientos y controles de seguridad de información

Basándonos en el análisis de riesgos realizado previamente conforme a la NTP ISO/IEC 27001:2014, se clasificarán los riesgos según su probabilidad de ocurrencia e impacto sobre los activos críticos de la UNSAAC, como datos académicos, administrativos e investigativos. Este ejercicio permitirá establecer un ranking de acciones que prioricen la mitigación de los riesgos más significativos, como la protección de datos sensibles de estudiantes y docentes frente a ciberataques o accesos no autorizados.

Los controles seleccionados estarán alineados con las mejores prácticas y estándares internacionales, considerando las necesidades específicas de la universidad.

Con este enfoque, la UNSAAC estará en capacidad de establecer un entorno de seguridad robusto que no solo proteja sus activos de información, sino que también promueva una cultura de seguridad dentro de la comunidad universitaria en base al cumplimiento de los requisitos establecidos por la NTP ISO/IEC 27001:2014.

Los controles propuestos que vienen dados desde un plan de acción y Oportunidades de Mejora están descritos de forma amplia en las hojas de trabajo denominada ANEXO 07: PLAN DE TRATAMIENTO DE RIESGOS y en el ANEXO 08: EVALUACIÓN PLANES Y OPORTUNIDADES DE MEJORA.

3.5.3. Planteamiento de Políticas y propuesta de procedimiento para Cumplimiento normativo

Establecer directrices generales relacionadas a los dominios de seguridad de la información a fin de reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o se use

de forma indebida los activos de información, garantizando así la confidencialidad, autenticidad y/o integridad de la información.

Esta política aplica a todos los trabajadores (directores, jefes, funcionarios y empleados académicos, estudiantes y administrativos), contratistas, consultores, proveedores y personal temporal que tengan acceso a recursos de información de propiedad de la Universidad Nacional San Antonio Abad del Cusco.

El alcance y el desarrollo del plan como proyecto esta descrito acorde un marco metodológico en el “ANEXO 02: POLÍTICAS Y DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN”

3.5.4. Propuesta de Estrategias de Concienciación y capacitación

Un plan efectivo de concientización y entrenamiento en seguridad de la información debe explicar de la manera más apropiada las reglas de comportamiento para el uso de los sistemas de informáticos como el de Tramite Documentario de la Universidad Nacional San Antonio Abad del Cusco, y los demás sistemas que deben estar plasmadas generalmente en las políticas y procedimiento de Seguridad de la Información de la organización que requiere que sean cumplidos y acatados por parte de todos los usuarios del sistema.

Teniendo en cuenta lo anterior, en la elaboración de un plan de concientización y entrenamiento sobre seguridad de la información, la NIST *Special Publication* SP-800-50 “Construcción de un Programa de Concientización y Entrenamiento de Seguridad de Tecnologías de Información”, nos proporciona una guía para la elaboración de dicho programa.

- **Concientización:** Su propósito es enfocar la atención en seguridad de la información para posibilitar que el público objetivo reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar. Por ejemplo, mantener el escritorio limpio, usar de forma adecuada las contraseñas, elaborar copias de respaldo, usar el correo responsablemente, entre otros.
- **Entrenamiento:** Se centra en producir habilidades y competencias en seguridad de la información relevantes y requeridas con el fin de que el público objetivo las aprenda y aplique en el día a día.

- Educación: Integra habilidades de seguridad y competencias de las diferentes especialidades funcionales dentro de un cuerpo común de conocimientos, enfocándose en producir especialistas en seguridad.

El alcance y el desarrollo del plan como proyecto esta descrito acorde un marco metodológico en el “ANEXO 03: PLAN DE CONCIENTIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN 2024”.

CONCLUSIONES

1. La Unidad de Trámite Documentario de la Universidad Nacional de San Antonio Abad del Cusco presenta vulnerabilidades significativas en la gestión de la seguridad de la información, comprometiendo la confidencialidad, integridad y disponibilidad de documentos y activos de información. Esta situación es resultado de la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014.

2. Luego de realizar un análisis de la situación actual se logró evidenciar una comprensión limitada de los riesgos reales que enfrentan los puntos críticos de la unidad de Trámite Documentario. La falta de evaluaciones basadas en datos concretos, obtenidas mediante entrevistas y encuestas al personal, impide la identificación adecuada de vulnerabilidades y entendimiento del nivel de exposición de los activos de información.

3. La falta de políticas, procedimientos y controles de seguridad de información compromete la capacidad de la Unidad de Trámite Documentario para prevenir y mitigar riesgos. Esto incrementa la exposición a incidentes de seguridad, como accesos no autorizados, pérdidas de datos y alteraciones de información crítica, que podrían prevenirse mediante un sistema de control efectivo.

4. Actualmente, la Universidad no cumple con las normativas y regulaciones aplicables en materia de seguridad de la información basada en la Norma Técnica Peruana NTP ISO/IEC 27001:2014. Esto incrementa el riesgo de sanciones legales y administrativas, además de posibles incidentes que podrían afectar su operatividad y reputación institucional.

5. La ausencia de un plan estratégico de capacitación y concientización limita el desarrollo de una cultura sólida de seguridad de la información dentro de la universidad. La implementación de estrategias de capacitación, evaluación continua y difusión de información es fundamental para garantizar que la comunidad universitaria comprenda la importancia de la seguridad de la información y participe activamente en la protección de los activos de la institución.

6. La falta de una gestión adecuada de la seguridad de la información y la ausencia de un profesional especializado en la Universidad Nacional de San Antonio Abad del Cusco puede generar

vulnerabilidades que comprometan la confidencialidad, integridad y disponibilidad de los activos de información. Esta deficiencia impide implementar el Sistema de gestión de Seguridad de la Información SGSI, exponiendo a la universidad a riesgos de seguridad cibernética, pérdida de datos y sanciones legales. La asignación de un experto es crucial para asegurar el cumplimiento normativo, establecer políticas efectivas y proteger los recursos institucionales de amenazas internas y externas.

RECOMENDACIONES

1. Se recomienda tomar en cuenta el diseño e implementar un SGSI basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 para mitigar las vulnerabilidades identificadas en la Unidad de Trámite Documental. Este sistema debe incluir un enfoque estructurado para garantizar la confidencialidad, integridad y disponibilidad de los documentos y activos de información, y establecer controles efectivos para prevenir incidentes de seguridad de la información.

2. Se recomienda que según la base del análisis de riesgos realizados en esta investigación, se debe de institucionalizar evaluaciones periódicas para identificar, evaluar y priorizar riesgos asociados a los activos de información. Estas evaluaciones deben ser dinámicas, incorporando herramientas de análisis que permitan un entendimiento claro de las amenazas y vulnerabilidades existentes.

3. Se recomienda tomar en cuenta que a partir del análisis GAP y diagnóstico realizado, se propone tomar en cuenta las políticas, procedimientos y controles de seguridad de información propuestos. Estos documentos detallan las medidas necesarias para proteger la información, definir roles y responsabilidades, estructurar comités de seguridad de la información y establecer protocolos específicos para la prevención, detección y respuesta a incidentes de seguridad.

4. Se recomienda que en concordancia con la norma NTP ISO/IEC 27001:2014 desarrollada en la investigación, se debe establecer un proceso formal para garantizar el cumplimiento normativo. Este proceso debe incluir revisiones periódicas de las leyes y regulaciones aplicables, así como auditorías o controles internos que permitan evaluar el nivel de conformidad con los estándares de seguridad. Tener en cuenta que la actualización o desestimación de cualquier punto de la norma es adaptable al Sistema de Gestión de Seguridad de la Información diseñado teniendo una característica de elasticidad impuesta.

5. Con base en los resultados obtenidos sobre la falta de una cultura de seguridad, se recomienda evaluar e implementar el programa estratégico propuesto para fomentar la concientización y capacitación continua en seguridad de la información. Este programa incluye

actividades prácticas, simulaciones de riesgos reales y la difusión de buenas prácticas para todos los niveles de la organización.

6. Se recomienda contar con un especialista en Seguridad de la Información y en elaboración de proyectos, quien deberá hacer el acompañamiento en la implementación del sistema. La participación de un especialista permite garantizar que los requisitos de seguridad sean considerados desde las primeras etapas del proyecto, previniendo riesgos de vulnerabilidades, pérdidas de información, y garantizando el cumplimiento de normativas (como ISO/IEC 27001, ISO/IEC 31000 y/o la Ley de Protección de Datos 29733).

ANEXOS

Según el NIST SP 800-30 y la ISO/IEC 27001, el informe de vulnerabilidades identifica puntos débiles en los sistemas y aplicaciones que pueden ser explotados. Divulgarlo incrementa el riesgo de ataques, ya que proporciona información detallada sobre áreas susceptibles a amenazas específicas. De acuerdo con el NIST SP 800-39 y la ISO/IEC 27005 (Gestión de Riesgos de Seguridad de la Información), las matrices de análisis de riesgos contienen evaluaciones detalladas de los activos críticos, sus amenazas, y la probabilidad de ocurrencia de incidentes de seguridad. Según el NIST SP 800-50 (*Building an Information Technology Security Awareness and Training Program*) y la ISO/IEC 27001, las políticas y los planes de concientización contienen detalles sobre el enfoque de la organización para educar a los empleados en prácticas seguras. En conclusión, Las normativas de seguridad como ISO/IEC 27001, 27005, y las guías del NIST insisten en la confidencialidad de estos documentos para evitar el uso indebido de la información sensible y proteger la infraestructura de seguridad organizacional. Limitar el acceso a estos documentos a personal autorizado es una práctica que refuerza la postura de seguridad y ayuda a cumplir con los estándares internacionales en gestión de la seguridad de la información.

Por lo antes indicado los anexos descritos fueron entregados al dueño del proceso, jefe de la Unidad de trámite documentario – UTD; Información en un archivo digital cifrado y siguiendo las recomendaciones según la norma ISO/IEC 27001:2013.

BIBLIOGRAFÍA

Referencias y Citas Bibliográficas

- Fressia Lisset Ariasca Suma, Sheny Katerine Quispe Borda. (2017). *Repositorio Universidad Nacional de San Antonio Abad del Cusco*. Obtenido de https://alicia.concytec.gob.pe/vufind/Record/RUNS_cb3a7217503fec45539050345de71d76/Details
- International Organization for Standardization. (2022). *International Organization for Standardization*. Obtenido de <https://www.iso.org/standard/27001>
- Alberto G. Alexander. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información*. Marcombo.
- Alejandro Riveros. (26 de 07 de 2023). *Matriz de riesgos*. Obtenido de <https://www.ealde.es/como-elaborar-matriz-de-riesgos/>
- Alejandro Riveros. (07 de julio de 2023). *Matriz de riesgos: Guía completa sobre qué es, cómo crear una y herramientas complementarias*. Obtenido de <https://www.ealde.es/como-elaborar-matriz-de-riesgos/>
- Anderson, D. J. (2010). *Kanban: Successful Evolutionary Change for Your Technology Business*. Blue Hole Press.
- Anita Guerra. (17 de 01 de 2024). *LA IMPORTANCIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL MUNDO ACTUAL*. Obtenido de <https://www.linkedin.com/pulse/la-importancia-del-sistema-de-gesti%C3%B3n-seguridad-sgsi-en-guerra-mba-qzcx/?originalSubdomain=es>
- Arturo Díaz Garcia . (5 de 10 de 2020). *Qué es la metodología PRINCE2*. Obtenido de <https://openwebinars.net/blog/que-es-la-metodologia-prince2/>
- Bentley, C. (2010). *PRINCE2 for Beginners: An Introduction to PRINCE2 Project Management*. Routledge.
- Carlos Arturo Avenía. (2017). Fundamentos de seguridad. En C. A. Avenía, *Fundamentos de seguridad* (pág. 98). Bogotá D.C: Fondo editorial Areandino.
- Castro, Martha Irene Romero. (Octubre de 2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA*. Obtenido de <https://www.biblioinfo.com.ar/wp-content/uploads/2024/07/Seguridad-informatica.pdf>
- Daniel Elías Santos Llanos. (01 de 02 de 2017). *Repositorio Pontificia Universidad Católica del Perú*. Obtenido de <https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7616>
- Digital Learning. (2021). *Aprendizaje Digital*. Obtenido de <https://www.digitallearning.es/plan-social-media-mejora-continua.html>
- Docuware. (21 de 6 de 2024). Obtenido de <https://start.docuware.com/>
- Edgar Vega Briceño. (2021). *SEGURIDAD DE LA INFORMACIÓN*. Alicante: Área de Innovación y Desarrollo,S.L. Obtenido de <https://3ciencias.com/wp-content/uploads/2021/03/LIBRO->

SEGURIDAD-INFORMACIO%CC%81N.pdf

- Eduardo Amable Samaniego Mena. (2021). Fundamentos de seguridad informática. En E. A. Mena, *Fundamentos de seguridad informática* (pág. 110). Guayaquil: Grupo Compás.
- Escuela Europea de Excelencia. (16 de 05 de 2018). *Cómo realizar la evaluación de riesgos según ISO 31000:2018*. Obtenido de <https://www.escuelaeuropeaexcelencia.com/2018/05/como-realizar-la-evaluacion-de-riesgos-segun-iso-310002018/>
- Escuela Superior de Administración Pública. (2020). *Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Información*. Obtenido de *Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Información*: https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf
- ESG Innova Group. (21 de 02 de 2014). *BLOG ESPECIALIZADO EN CIBERSEGURIDAD*. Obtenido de <https://www.pmg-ssi.com/2014/02/isoiec-27008-controles-de-seguridad-de-informacion/>
- ESG Innova Group. (2022). *BLOG ESPECIALIZADO EN CIBERSEGURIDAD*. Obtenido de <https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/>
- Exact. (2021). *Exact.com.pe*. Obtenido de <https://www.exact.com.pe/noticias/gestion-tramite-documentario>
- Excelencia, E. E. (2022). <https://www.escuelaeuropeaexcelencia.com/2022/02/evaluacion-de-riesgos-de-seguridad-de-la-informacion-7-pasos-para-asegurar-el-cumplimiento-de-iso-27001/>. Obtenido de <https://www.escuelaeuropeaexcelencia.com/2022/02/evaluacion-de-riesgos-de-seguridad-de-la-informacion-7-pasos-para-asegurar-el-cumplimiento-de-iso-27001/>: <https://www.escuelaeuropeaexcelencia.com/2022/02/evaluacion-de-riesgos-de-seguridad-de-la-informacion-7-pasos-para-asegurar-el-cumplimiento-de-iso-27001/>
- Gobierno del Perú. (30 de Noviembre de 2023). *Normas Técnicas Peruanas sobre seguridad de la información*. Obtenido de https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n_Ministerial_N_004-2016-PCM20190902-25578-19siyuu.pdf
- GROUP, Q. (2023). *Implementa la Norma ISO 9001*. Obtenido de <https://quama.pe/iso-9001-gestion-calidad/>
- GRUPO ACS. (28 de 07 de 2022). *Política de Seguridad de la Información*. Obtenido de https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf
- <https://es.wikipedia.org/>. (3 de 9 de 2024). <https://es.wikipedia.org/>. Obtenido de [https://es.wikipedia.org/wiki/Magerit_\(metodolog%C3%ADa\)#:~:text=Magerit%20\(Metodolog%C3%ADa%20de%20An%C3%A1lisis%20y,enfocada%20a%20las%20Administraciones%20P%C3%ABlicas.](https://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa)#:~:text=Magerit%20(Metodolog%C3%ADa%20de%20An%C3%A1lisis%20y,enfocada%20a%20las%20Administraciones%20P%C3%ABlicas.)
- I&T Solutions. (10 de Agosto de 2022). Fundamentos ISO 27001.
- IBM Corporation. (Octubre de 2024). *IBM Corporation*. Obtenido de IBM Corporation: <https://www.ibm.com/mx-es/topics/nist>
- Ikusi Redes de Telecomunicaciones, S. (Octubre de 2024). *¿Qué es el marco de ciberseguridad NIST?*

- Obtenido de <https://www.ikusi.com/mx/blog/nist/>
- Institute., P. M. (2017). *Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®)*. . Project Management Institute.
- International Organization for Standardization. (2017). *International Organization for Standardization*. Obtenido de <https://www.iso.org/standard/63417.html>
- International Organization for Standardization. (2022). *International Organization for Standardization*. Obtenido de <https://www.iso.org/standard/75652.html>
- interpolados.wordpress.com. (7 de 10 de 2020). *interpolados.wordpress.com*. Obtenido de <https://interpolados.wordpress.com/2020/10/07/magerit-3-0-vision-de-conjunto/>
- ISO 31000:2018. (s.f.). Obtenido de <https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486>
- ISO 31000:2018. (2018). *SCRIBD*. Obtenido de <https://es.scribd.com/document/612938238/ISO-31000-2018>
- ISO, N. (s.f.). <https://normasiso.org/norma-iso-27006/>. Obtenido de <https://normasiso.org/norma-iso-27006/>
- Jaima Andrés Bello Vieda. (04 de 2015). *Norma ISO/IEC Generalidades y Cambios 2005 a 2013*. Obtenido de <https://es.slideshare.net/JaimeAndrsBelloVieda/iso-27001-cambios-2005-a-2013#18>
- Jaime Andrés Bello Vieda. (20 de 03 de 2017). *ISO 27001 cambios 2005 a 2013*. Obtenido de <https://es.slideshare.net/JaimeAndrsBelloVieda/iso-27001-cambios-2005-a-2013#18>
- Jeffrey K. Pinto. (2021). *Guide to the Project Management Body of Knowledge* . Project Management Institute.
- Jorge García Martínez. (29 de 10 de 2024). *¿Qué es la norma ISO 27001?* Obtenido de <https://www.deltaprotect.com/blog/que-es-iso-27001>
- José Luis Arias Gonzales. (06 de 2021). *DISEÑO Y METODOLOGÍA DE LA INVESTIGACIÓN*. Obtenido de https://gc.scalahed.com/recursos/files/r161r/w26022w/Arias_S2.pdf
- Kaspersky Lab. (2024). *Kaspersky Lab*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOorEXXR9vk4gvn9sJB4q0RMDIw7DGVLY7I8--vAL32LJYUYkk_OC
- Licencia Creative Commons. (18 de 7 de 2024). *Glosario TI*. Obtenido de <https://www.glosarioit.com/Procedimiento>
- Martín Frias. (28 de Junio de 2021). *Openwebinars*. Obtenido de <https://openwebinars.net/blog/ciberseguridad-metodos-preventivos-y-concienciacion-del-usuario/#:~:text=La%20concienciaci%C3%B3n%20es%20una%20actividad,a%20trav%C3%A9s%20de%20un%20dispositivo.>
- Michael Quinn Patton. (2010). *Developmental Evaluation Applying Complexity Concepts to Enhance Innovation and Use*.

- Miguel Angel Amutio Gómez. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid: Ministerio de Hacienda y Administraciones Públicas.
- Ministros, P. d. (Enero de 2024). *Gobierno del Perú*. Obtenido de Gobierno del Perú: <https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion>
- Nathal Dawson. (04 de 27 de 2024). <https://es.linkedin.com/>. Obtenido de <https://es.linkedin.com/pulse/el-origen-del-modelo-cascada-y-su-importancia-en-la-industria-dawson-bsp4e>
- Neira, A. L. (Octubre de 2005). *ISO27000*. Obtenido de <https://www.iso27000.es/sgsi.html>
- NELSON ALEJANDRO YAÑEZ CACERES. (2017). *Repositorio Universidad de Chile*. Obtenido de <https://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y>
- Normas ISO. (s.f.). <https://normasiso.org/norma-iso-27004/>. Obtenido de <https://normasiso.org/norma-iso-27004/>
- Novasec. (2024). *Planes de Tratamiento de Riesgos*. Obtenido de <https://www.novasec.co/blog/69-planes-tratamiento-riesgos>
- Phd Harold Kerzner. (s.f.). *Project Management: A Systems Approach to Planning, Scheduling, And Control*. John Wiley & Sons, Inc.
- Pirani Risk. (2024). *Guía para implementar la gestión de riesgos según ISO 31000*. Obtenido de <https://www.piranirisk.com/es/academia/especiales/guia-del-sistema-de-gestion-de-riesgos-iso-31000#:~:text=Es%20el%20proceso%20que%20se,una%20estrategia%20que%20permita%20reducir>
- Presidencia de Consejo de Ministros. (8 de 1 de 2016). *Gobierno del Perú*. Obtenido de https://cdn.www.gob.pe/uploads/document/file/357224/Resoluci%C3%B3n_Ministerial_N_004-2016-PCM20190902-25578-19siyuu.pdf?v=1720460433
- Presidencia del Consejo de Ministros. (Octubre de 2024). *Gobierno del Perú*. Obtenido de <https://www.gob.pe/74247-que-es-la-ingenieria-social>
- RAMÓN ROBLES, ÁLVARO RODRÍGUEZ DE ROA. (06 de 2026). *¿Cómo crear e implementar su. Sistema de Gestión de Seguridad de la Información?* Obtenido de https://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128
- Robert R. Sherman, Rodman B. Webb. (1988). *Qualitative Research in Education: Focus and Methods*. Psychology Press.
- Roberto Carlos Fuentes Serrate. (2020). *Repositorio Universidad Nacional Pedro Ruiz Gallo*. Obtenido de <https://repositorio.unprg.edu.pe/handle/20.500.12893/9097>
- Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio. (2014). *Tesis de Investigación*. España: McGraw Hill España. Obtenido de <https://tesisdeinvestig.blogspot.com/2012/12/disenos-no-experimentales-segun.html>

- Royce Winston. W. (1970). *Managing the development of large software systems*. Estados Unidos.
- SegWeb Blog Spot. (24 de 04 de 2012). *ISO/IEC 27005 Gestion de riesgos de seguridad de la Información*. Obtenido de <https://segweb.blogspot.com/2012/04/27005.html>
- Sophie Danby. (9 de junio de 2023). *La ISO 27001 y la Gestión de Activos: ¿Qué dice el anexo A.8.1?* Obtenido de <https://blog.invgate.com/es/iso-27001-gestion-activos>
- Soraya Jiménez Beamud. (2016). *Elaboración de un plan de implementación de la ISO/IEC 27001:2013*. Universitat Oberta de Catalunya.
- SPRINTO. (2024). *What is the ISO/IEC 27004 standard?* Obtenido de <https://sprinto.com/blog/iso-27004-standard/>
- The Power MBA. (2024). *La metodología Kanban, esencial para mejorar el flujo de trabajo de tu proyecto*. Obtenido de <https://www.thepowermba.com/es/blog/metodologia-kanban>
- Thomas R. Peltier. (2001). *Information Security Risk Analysis*. Boca Ratón, Flórida: Taylor & Francis Group. Obtenido de <https://www.revistaespacios.com/a10v31n01/10310152.html>
- TI, C. y. (2019). *FIRMA-E*. Obtenido de FIRMA-E: <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>
- Universidad Nacional De San Antonio Abad del Cusco. (1 de 09 de 2021). *REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES – ROF DE LA UNIVERSIDAD*. Obtenido de <https://cdn.www.gob.pe/uploads/document/file/4028741/CU-265APROBACION-ROFUNSAAC.pdf.pdf?v=1673241955>
- UNSAAC. (2021). *Universidad Nacional de San Antonio Abad del Cusco*. Obtenido de <http://transparencia.unsaac.edu.pe/links/datosgenerales/documentos/OrganigramaUNSAAC2021.pdf?s=2&p=a>
- UNSAAC. (03 de 04 de 2021). *UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO*. Obtenido de http://transparencia.unsaac.edu.pe/links/planeamiento/documentos/TUPAUNSAAC_NuevoFormato2021.pdf
- UNSAAC. (01 de 09 de 2021). *www.unsaac.edu.pe*. Obtenido de [www.unsaac.edu.pe](http://transparencia.unsaac.edu.pe/links/planeamiento/documentos/CU-265APROBACION-ROFUNSAAC.pdf): <http://transparencia.unsaac.edu.pe/links/planeamiento/documentos/CU-265APROBACION-ROFUNSAAC.pdf>
- Valmi D. Sousa, Martha Driessnack, Isabel Amélia Costa Mendes. (05 de 2007). *REVISIÓN DE DISEÑOS DE INVESTIGACIÓN RESALTANTES PARA*. Obtenido de <https://www.scielo.br/j/rlae/a/7zMf8XypC67vGPrXVrVFGdx/?format=pdf&lang=es>
- Varios. (2021). *Implementación Del Sistema De Gestión De Ciberseguridad*.
- William Edwards Deming. (s.f.). *ENVIRA*. Obtenido de <https://envira.es/es/el-ciclo-deming-que-consiste-y-como-ayuda-gestion-procesos/>
- William Stallings. (2005). *Sistemas operativos: aspectos internos y principios de diseño*. Madrid: Pearson Prentice Hall.
- Willian Jhoel Murillo Hernandez. (18 de 4 de 2008). *La investigación científica*. Obtenido de <https://www.monografias.com/trabajos15/invest-cientifica/invest-cientifica>

Yangaly, A. M. (s.f.). https://issuu.com/angelacamposyangaly/docs/tipos_de_iso_1_/s/28505073.
Obtenido de https://issuu.com/angelacamposyangaly/docs/tipos_de_iso_1_/s/28505073

Yuan, Y. T. (2014). *Critical Success Factors Analysis on Effective*. Obtenido de
<http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1158&context=amcis2014>