REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

MARCO DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO COBIT 2019 PARA GARANTIZAR LOS ATRIBUTOS CID DEL PROCESO DE TITULACIÓN DE LA UNIVERSIDAD YACHAY TECH.

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR: Manuel Agustín Narváez Revelo

DIRECTOR: Msc. Luis Rolando Aguilar Buitrón

IBARRA - ECUADOR

2024

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

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

1. IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0401390109		
APELLIDOS Y NOMBRES:	Narváez Revelo Manuel Agustín		
DIRECCIÓN:	Guayas 1-427 y 13 de Abril		
EMAIL:	manarvaezr@utn.edu.ec		
TELÉFONO FIJO:	062545291	**TELÉFONO MÓVIL:**	0980336543

DATOS DE LA OBRA	
TÍTULO:	Marco de Seguridad de la Información utilizando COBIT 2019 para garantizar los atributos CID del proceso de Titulación de la Universidad YACHAY TECH
AUTOR (ES):	Narváez Revelo Manuel Agustín
FECHA: DD/MM/AAAA	16/05/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TÍTULO POR EL QUE OPTA:	Magister en computación con mención en seguridad informática
ASESOR /DIRECTOR:	Phd. Marco Pusdá, Msc. Luis Aguilar

CONSTANCIAS

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

Ibarra, a los 10 días del mes de junio de 2024

EL AUTOR:

Nombre: Narváez Revelo Manuel Agustín
CI: 0401390109

Ibarra, 17 de mayo de 2024

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado "MARCO DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO COBIT 2019 PARA GARANTIZAR LOS ATRIBUTOS CID DEL PROCESO DE TITULACIÓN DE LA UNIVERSIDAD YACHAYTECH" del maestrante Narváez Revelo Manuel Agustín, de la Maestría de Computación con mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	Firma
Tutor/a	Msc. Aguilar Buitrón Luis	Firmado electrónicamente por: LUIS ROLANDO AGUILAR BUITRON
Asesor/a	Phd. Marco Pusdá Chulde	0401200951 MARCO REMIGIO PUSDA CHULDE Firmado digitalmente por 0401200951 MARCO REMIGIO PUSDA CHULDE Fecha: 2024.05.17 16:48:40 -05'00'

DEDICATORIA

Este trabajo de maestría es un logro que no habría sido posible sin el amor incondicional de mis amadas hijas Doménica, Karen y Alison. Cada una de ustedes ha sido una fuente de inspiración y motivación en mi vida.

Verito, mi amada esposa, su amor y apoyo incondicional han sido mi mayor motivación en el camino hacia la maestría. Su presencia a mi lado ha convertido cada desafío en una oportunidad de crecimiento y éxito. Gracias por ser mi compañera de vida y mi mayor inspiración.

Mis queridos padres, Manuel y Rosa, su sacrificio y dedicación han sido el cimiento de mi educación. Su amor incondicional y su confianza en mí han sido el motor que me impulsó a perseguir mis metas. Su ejemplo de trabajo duro y constancia siempre estará presente en cada logro que alcance. Les debo todo lo que soy y todo lo que logro.

A cada uno de ustedes, les dedico este trabajo de maestría con profundo agradecimiento y amor. Sin su presencia en mi vida, este logro no tendría el mismo significado. Gracias por su amor, apoyo y creer en mí.

Con amor y gratitud,
Manuel Agustín Narváez Revelo

AGRADECIMIENTO

A través de estas líneas, quiero expresar mi profundo agradecimiento a los miembros de la Universidad Técnica del Norte y del Instituto de Postgrados por brindarme la oportunidad de cursar mi maestría en tan prestigiosa institución. Ha sido un honor formar parte de esta comunidad académica y completar mi investigación bajo su guía y apoyo.

Quiero agradecer especialmente a mi tutor, Msc. Luis Aguilar Buitrón, por su dedicación, paciencia y orientación a lo largo de este proceso. Su profundo conocimiento en el campo de estudio y su compromiso con mi crecimiento académico han sido invaluables. Gracias por su apoyo constante, por sus comentarios constructivos y por desafiarme a alcanzar mis metas más altas.

También quiero expresar mi gratitud hacia mi asesor de tesis, Msc. Marco Pusdá por su valiosa contribución y orientación en el desarrollo de mi investigación. Sus conocimientos expertos y su perspectiva crítica han sido fundamentales para dar forma y mejorar mi trabajo. Agradezco sinceramente su disponibilidad y compromiso durante todo el proceso.

No puedo dejar de mencionar el apoyo recibido de todo el personal docente del Instituto de Postgrado. Sus esfuerzos para garantizar un entorno de aprendizaje enriquecedor y su disposición para resolver cualquier duda o dificultad son verdaderamente apreciados. Gracias por su dedicación y por proporcionar los recursos necesarios para mi crecimiento académico.

Por último, pero no menos importante, quiero expresar mi gratitud a todos los participantes y colaboradores que se involucraron en mi investigación. Sus aportes y tiempo dedicado fueron fundamentales para el éxito de este trabajo.

Con gratitud sincera,

Manuel Agustín Narváez Revelo

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

ACRÓNIMOS

CID: Confidencialidad, Integridad y Disponibilidad.

COBIT: Control Objectives for Information Systems and related Technology (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas).

EGIT: Gobierno Empresarial de la Tecnología y la Información.

ISACA: Information Systems Audit and Control Association.

ISO: Organización Internacional de Estandarización.

LOPDP: Ley Orgánica de Protección de Datos Personales.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones.

MINTEL: El Ministerio de Telecomunicaciones y de la Sociedad de la Información.

SIGA: Sistema de Gestión Académica.

TI: Tecnologías de la Información.

UITEY: Universidad de Investigación de Tecnología Experimental Yachay.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

MARCO DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO COBIT 2019 PARA GARANTIZAR LOS ATRIBUTOS CID DEL PROCESO DE TITULACIÓN DE LA UNIVERSIDAD YACHAY TECH.

Autor: Manuel Agustín Narváez Revelo

Director: Msc. Aguilar Buitrón Luis

Año: 2024

RESUMEN

La ciberseguridad se ha convertido en un aspecto crítico para las instituciones de educación superior, especialmente en el contexto del proceso de titulación interna. La Universidad de Investigación de Tecnología Experimental Yachay reconoce la importancia de establecer un marco de seguridad sólido para proteger la integridad, confidencialidad y disponibilidad de la información durante este proceso.

En este sentido, esta tesis se centra en el diseño para la implementación de un marco de seguridad basado en COBIT 2019, con un enfoque específico en el objetivo de gestión APO12. Este objetivo busca garantizar que se establezcan y mantengan políticas, estándares y procedimientos de seguridad de la información alineados con los objetivos estratégicos de la institución.

A través de un enfoque metodológico estructurado, que incluye la identificación de activos de información, la evaluación de riesgos, la implementación de controles de seguridad y el monitoreo continuo, se busca fortalecer la postura de seguridad de la Universidad Yachay Tech y mitigar las amenazas potenciales que puedan surgir durante el proceso de titulación. La adopción de un marco de seguridad basado en COBIT 2019 permitirá a la institución gestionar de manera efectiva los riesgos de seguridad de la

información y garantizar la protección de los datos sensibles y la continuidad de las operaciones académicas, además los resultados se han sintetizado en una guía de implementación del marco de seguridad para el proceso de titulación de la UITEY.

Además, se llevó a cabo una encuesta entre los usuarios académicos y administrativos para evaluar la percepción sobre un marco de seguridad del proceso de titulación de la UITEY, además de la eficacia y la idoneidad de las medidas propuestas, e identificar posibles áreas de mejora. Los resultados obtenidos proporcionaron una valiosa retroalimentación que se integró en el diseño final del marco de seguridad, asegurando así su relevancia y utilidad para proteger adecuadamente los activos de información crítica.

ABSTRACT

The cybersecurity has become a critical aspect for higher education institutions, especially in the context of internal graduation processes. The Universidad de Investigación de Tecnología Experimental Yachay recognizes the importance of establishing a robust security framework to protect the integrity, confidentiality, and availability of information during this process.

In this regard, this thesis focuses on designing the implementation of a security framework based on COBIT 2019, with a specific focus on management objective APO12. This objective aims to ensure that information security policies, standards, and procedures aligned with the institution's strategic objectives are established and maintained.

Through a structured methodological approach, including the identification of information assets, risk assessment, implementation of security controls, and continuous monitoring, the goal is to strengthen Yachay Tech University's security posture and mitigate potential threats that may arise during the graduation process. The adoption of a security framework based on COBIT 2019 will enable the institution to effectively manage information security risks and ensure the protection of sensitive data and continuity of academic operations. Furthermore, the results have been synthesized into a security framework implementation guide for the UITEY graduation process.

Additionally, a survey was conducted among academic and administrative users to assess the perception of a security framework for the UITEY graduation process, as well as the effectiveness and suitability of the proposed measures, and identify possible areas for improvement. The obtained results provided valuable feedback that was integrated into the final design of the security framework, thus ensuring its relevance and usefulness in adequately protecting critical information assets.

CAPITULO I

1. EL PROBLEMA

1.1. Problema de Investigación

Chang (2020) indica que el ciberataque es uno de los delitos informáticos que más ha crecido desde el 2005, el robo de información y la afectación a instituciones públicas y privadas son las principales consecuencias de los ataques cibernéticos. Mundialmente, las organizaciones y compañías de seguridad establecen medidas para prevenir estos ataques.

Redacción CyberWar (2022) establece que en Ecuador hubo más de 51 mil registros relacionados con cryptominers (malware utilizado para la minería de criptomonedas), alrededor de 140 mil detecciones de exploits (código utilizado para aprovechar vulnerabilidades en software), cerca de seis mil detecciones de ransomware (malware para el secuestro de información) y casi ocho mil detecciones de spyware (software espía), como datos de algunos tipos de software malicioso.

En el ámbito de la seguridad informática, la creciente complejidad y sofisticación de las amenazas cibernéticas plantea un desafío significativo para las organizaciones. A medida que evolucionan las técnicas de ataque, los sistemas de seguridad tradicionales a menudo resultan insuficientes para proteger los activos digitales de manera efectiva. Además, las organizaciones suelen enfrentarse a problemas de coherencia y gestión de políticas de seguridad en entornos heterogéneos, donde diferentes tecnologías y plataformas están interconectadas. Esta falta de estandarización y la dificultad para implementar políticas de seguridad coherentes pueden conducir a vulnerabilidades y brechas de seguridad.

Para abordar estos desafíos, es fundamental desarrollar un framework de seguridad sólido y adaptable que proporcione un enfoque integral para la protección de los sistemas y datos. Un framework de seguridad eficaz debe ser capaz de proporcionar una arquitectura de seguridad coherente, estrategias de defensa en capas y mecanismos de detección y alerta temprana. Además, debe ser lo suficientemente flexible como para adaptarse a diferentes entornos tecnológicos y requisitos empresariales específicos.

Sin embargo, a pesar de la importancia de contar con un framework de seguridad integral, existe una falta de investigación y desarrollo de frameworks que satisfagan todas

estas necesidades. Actualmente, muchos de los frameworks disponibles se centran en aspectos específicos de la seguridad, como el control de acceso o la detección de intrusiones, pero carecen de una visión global y coherente de la seguridad de la información. Además, la mayoría de estos frameworks no cuentan con un respaldo documental ni han sido validados en entornos reales.

Por lo tanto, se requiere una investigación íntegra para desarrollar un framework de seguridad que aborde los desafíos mencionados y proporcione una solución confiable para la protección de los sistemas y datos en el contexto actual de amenazas cibernéticas. Esta investigación se basa en la revisión y análisis de frameworks existentes, así como en la identificación de las mejores prácticas de seguridad y cumplimiento de estándares.

1.2. Interrogantes de la Investigación

Las interrogantes planteadas en esta investigación están directamente relacionadas con los objetivos específicos.

¿Existe un análisis de los atributos de Confidencialidad, Integridad y Disponibilidad (CID) para el proceso de titulación de la Universidad Yachay Tech en base al marco de seguridad de la información de COBIT 2019?

¿Cuáles son los principales riesgos y amenazas que pueden afectar la seguridad de la información en el proceso de titulación de la Universidad Yachay Tech?

¿Cuáles son las mejores prácticas y recomendaciones para la implementación efectiva de un Marco de Seguridad de la Información utilizando COBIT 2019 en el proceso de titulación de la Universidad Yachay Tech?

¿En qué medida es necesaria la implementación de un Marco de Seguridad de la Información basado en COBIT 2019 aplicando los atributos CID en el proceso de titulación de la Universidad Yachay Tech?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

Diseñar un marco de seguridad de la información basado en COBIT 2019 para garantizar la confidencialidad, integridad, y disponibilidad de la información crítica del proceso académico de titulación frente a las amenazas internas y externas de la Universidad de Investigación de Tecnología Experimental Yachay.

1.3.2. Objetivos Específicos

- Analizar los atributos de Confidencialidad, Integridad y Disponibilidad (CID) del proceso de titulación de la Universidad Yachay Tech en el contexto del Marco de Seguridad de la Información de COBIT 2019.
- Valorar los principales riesgos de la seguridad de la información del proceso de titulación de la Universidad de Investigación de Tecnología Experimental Yachay Tech mediante el dominio APO 12 de COBIT 2019.
- Diseñar un plan de implementación del Marco de Seguridad de la Información utilizando COBIT 2019 para el proceso de titulación de la Universidad Yachay Tech.
- Evaluar la percepción sobre la existencia de un Marco de Seguridad de la Información en el proceso de Titulación de la Universidad Yachay Tech y la necesidad de su implementación, en los actores involucrados.

1.4. Justificación

El desarrollo y la implementación de un Marco de Seguridad de la Información es de vital importancia en el entorno académico, especialmente en instituciones de educación superior como la Universidad Yachay Tech. La protección de la información sensible y confidencial, así como la garantía de los atributos CID (Confidencialidad, Integridad y Disponibilidad), son elementos cruciales para asegurar la calidad y la integridad de los procesos académicos, como el proceso de titulación.

El presente proyecto tiene como objetivo investigar y proponer la implementación de un Marco de Seguridad de la Información utilizando COBIT 2019 para garantizar los atributos CID en el proceso de titulación de la Universidad Yachay Tech. Es importante destacar los siguientes aspectos:

Relevancia académica: La seguridad de la información es un campo en constante evolución y de gran importancia en la actualidad. La aplicación de un marco reconocido como COBIT 2019 en el contexto específico de la Universidad Yachay Tech brinda una oportunidad para contribuir al conocimiento y las mejores prácticas en el campo de la seguridad de la información en el ámbito académico.

Protección de datos sensibles: En el proceso de titulación de una institución educativa, se manejan datos sensibles de estudiantes, como calificaciones, registros académicos y datos personales. La implementación de un marco de seguridad de la

información busca salvaguardar la confidencialidad de estos datos, garantizar su integridad y asegurar su disponibilidad de manera oportuna.

Cumplimiento normativo y regulatorio: La implementación de un marco de seguridad de la información basado en COBIT 2019 en el proceso de titulación permite a la Universidad Yachay Tech cumplir con las regulaciones y normativas pertinentes en cuanto a la protección de datos y la seguridad de la información. Esto incluye leyes de privacidad, protección de datos personales y regulaciones internas de la institución.

Mejora de la calidad y la confianza: Al garantizar los atributos CID en el proceso de titulación, la Universidad Yachay Tech fortalece la calidad de sus servicios académicos y genera confianza tanto en los estudiantes como en los actores externos, como empleadores y otras instituciones educativas. Un proceso de titulación seguro y confiable refuerza la reputación y el prestigio de la institución.

Contribución a la ciberseguridad: La implementación de un marco de seguridad de la información basado en COBIT 2019 no solo beneficia el proceso de titulación de la Universidad Yachay Tech, sino que también contribuye al desarrollo de la ciberseguridad en el ámbito académico en general. Los resultados de esta investigación podrían ser utilizados por otras instituciones educativas para mejorar sus prácticas de seguridad de la información.

CAPITULO II

2. MARCO REFERENCIAL

2.1. Antecedentes

La evolución tecnológica constante hace que la información sensible de personas, organizaciones e instituciones se tornen vulnerables ante potenciales ataques cibernéticos que conlleve pérdidas de índole personal, económico y empresarial; ante ello adoptar buenas prácticas tecnológicas para garantizar la seguridad de la información es de vital importancia.

La Universidad de Investigación de Tecnología Experimental Yachay fue creada mediante Ley, publicada en el Registro Oficial número 144 de 16 de diciembre de 2013, como una institución de educación superior de derecho público, sin fines de lucro, con personería jurídica propia, con autonomía académica, administrativa, financiera y orgánica. Esta institución cuenta con una política de aseguramiento de la calidad cuyo objeto es "Establecer los procesos académicos y administrativos ejecutados en la Universidad de Investigación de Tecnología Experimental Yachay (UITEY), relacionados con las funciones sustantivas de la educación superior y las condiciones institucionales, bajo estándares de calidad que serán de estricto cumplimiento para toda la comunidad universitaria" (Política de aseguramiento de la calidad UITEY, 2022).

En la UITEY el proceso de titulación es uno de los procesos claves en la gestión académica, este proceso es el que cierra el macroproceso de formación profesional, por lo tanto, articula la intervención de varios actores, entre ellos: estudiantes, tutores de trabajos de integración curricular, autoridades y personal administrativo, con interacciones que buscan generar productos para la obtención del título profesional y su registro en el SNIESE – Plataforma de registro de títulos.

La intervención de varios actores para la generación de varios productos requiere contar con herramientas que faciliten dicha intervención articulada para mitigar el error y producir información exacta y confiable en tiempos mínimos que produzcan servicios eficientes.

COBIT (Control Objectives for Information and related Technology) es un marco de trabajo para el buen gobierno y la gestión de las tecnologías de la información (TI) y la tecnología de la empresa (EGIT). COBIT 2019 es la versión más reciente de este framework creado por ISACA (Information Systems Audit and Control Association), entidad enfocada en el desarrollo de metodologías y certificaciones para la ejecución de actividades de auditoría y control de sistemas de la información.

De esta manera es oportuno analizar en el marco de la normativa referencial nacional e internacional, acorde una metodología estandarizada como es COBIT 2019 la información que se relaciona con el proceso de titulación y sus atributos CID, al ser fundamental la gestión de este proceso cuya información es confidencial y sensible, para verificar su estado actual y proponer un marco de seguridad de la información que responda a las necesidades de la institución.

2.2. Marco Teórico

Este apartado es importante ya que amplía y enriquece el horizonte del estudio al aportar información científica existente a partir de la bibliografía revisada.

2.2.1. Introducción

La seguridad de la información es un tema crucial para las instituciones de educación superior, ya que estas manejan grandes cantidades de información confidencial y sensible, como datos personales de estudiantes y profesores, información financiera e intelectual. Un marco de seguridad basado en COBIT 2019 puede ayudar a estas instituciones a proteger sus activos de información y garantizar sus atributos de confidencialidad, integridad y disponibilidad.

Este campo de estudio se enfoca en la protección de la confidencialidad, integridad y disponibilidad de los datos. Según ISO/IEC 27000, 2021, la seguridad de la información se define como “la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un enfoque de gestión de riesgos y proporcionando confianza a las partes interesadas”.

Según García (2018), COBIT 2019 se centra en la gobernanza y gestión de la información y tecnología, y proporciona un conjunto de principios y procesos que permiten a las organizaciones garantizar la confidencialidad, integridad y disponibilidad de la información.

Según Disterer (2019), la confidencialidad se refiere a la protección de la información contra el acceso no autorizado, la integridad se relaciona con la precisión y

completitud de la información, asegurando que no se hayan realizado modificaciones no autorizadas y la disponibilidad se refiere a la accesibilidad y utilización de la información cuando sea necesario, por tanto estos atributos son los pilares fundamentales de la seguridad de la información que deben estar inmersos en los procesos institucionales.

2.2.2. Tecnologías de la Información (TIC)

Son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, etc). Las TIC se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones de manera interactiva para conseguir nuevas realidades comunicativas (Ortí, 2012).

2.2.2.1. Gobierno Empresarial de la Tecnología y la Información (EGIT).

Según ISACA (2018) el EGIT procura la entrega de valor proveniente de la transformación digital y la mitigación del riesgo de; el Gobierno se asegura de evaluar las necesidades de las partes interesadas para cumplir los objetivos empresariales, priorizando y balanceando entre desempeño y cumplimiento, pudiendo obtener 3 resultados principales:

- Realización de beneficios,
- Optimización del riesgo,
- Optimización de recursos.

2.2.3. Seguridad de la Información

Es un concepto que se involucra cada vez más en muchos aspectos de nuestra sociedad hiperconectada, y se define 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 (Vega Briceño, 2021).

"La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados" (ISOTools Excellence, 2017).

2.2.3.1. Atributos de Seguridad de la Información.

Se identifican tres propiedades principales de seguridad de la información, mismas que se analizan para identificar, valorar y tratar los riesgos a los cuales están expuestos los activos de un proceso, según la metodología Magerit 3.0 (2012) se define de la siguiente manera:

Confidencialidad, Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Integridad, Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Disponibilidad, Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

En algunos casos las propiedades de autenticidad y trazabilidad de la información también deben ser evaluadas para fines de identificación de riesgos.

Figura 1. ***Atributos de Seguridad de la Información***

Fuente: (Fandom, 2021)

Nota: Este gráfico indica la triada CID y su relación con la información como eje central.

2.2.3.2. Valoración de Riesgos.

Consiste en evaluar o medir el coste de la ocurrencia de una amenaza; la Dirección Nacional de Interoperabilidad, Seguridad de la Información e Infraestructura de la Administración Pública Nacional – (Gobierno Electrónico, 2020) sugiere los siguientes conceptos como base dentro del proceso de valoración de riesgos:

Riesgo, posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Amenaza, causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Vulnerabilidad, debilidad de un activo o control que puede ser explotada por una o más amenazas.

Impacto, es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Riesgo inherente, es el riesgo existente y propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual, el riesgo que permanece tras el tratamiento del riesgo.

2.2.3.3. Gestión de Riesgos.

La gestión de riesgos de ciberseguridad es un proceso que tiene como objetivo identificar, analizar, medir y encargarse de los riesgos asociados a la seguridad de la información. Establece controles de forma preventiva contra las amenazas que se puedan encontrar y consigue reducirlas (Parra, 2012).

Figura 2. ***Marco de trabajo en la gestión de riesgos***

Fuente: (ISACA, 2017)

2.2.3.4. Marco de Seguridad Informática.

Los marcos de ciberseguridad son políticas y procedimientos diseñados para ayudar a reducir el riesgo de seguridad de manera más efectiva. Fueron concebidos con la premisa de identificar normas y directrices de seguridad aplicables en diferentes sectores de infraestructura crítica, facilitando un enfoque flexible y repetible, que permite

la priorización de actividades y busca obtener un buen rendimiento de las infraestructuras tecnológicas (Organización de los Estados Americanos (OEA), 2019).

Los marcos de seguridad permiten la innovación tecnológica y se ajusta a cualquier tipo de organización basándose en estándares ya aceptados por la industria para la ciberseguridad.

2.2.4. COBIT 2019 (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas)

COBIT 2019 (Control Objectives for Information and Related Technologies) es un marco de gobierno y gestión de tecnología de la información que proporciona una estructura para la implementación de controles y mejores prácticas en la seguridad de la información. Este marco de referencia para la gestión y el gobierno de la información y la tecnología (IT) reporta un conjunto de principios, procesos y herramientas que ayudan a las organizaciones a alinear la IT con las necesidades del negocio, proteger los activos de información y optimizar la gestión de la IT (Introduction and Methodology, 2018).

Ha sido desarrollado por ISACA (Information Systems Audit and Control Association) desde su primera versión en 1996 y actualmente se encuentra disponible la versión COBIT 2019. En la primera versión del marco de trabajo COBIT su público objetivo eran los auditores de TI. La versión actual considera no solamente la función de TI de una empresa, sino a otros interesados como juntas directivas, direcciones ejecutivas, entre otras, buscando abordar los desafíos actuales de la tecnología y la seguridad de la información. (Global Suite, 2023)

2.2.4.1. Beneficios de un Marco de Seguridad basado en COBIT 2019.

Los beneficios del uso de esta herramienta son variados, para una mejor comprensión se enlistan (ISACA, 2020):

Mejora la seguridad de la información: Un marco de seguridad basado en COBIT 2019 ayuda a las instituciones a identificar, evaluar y mitigar los riesgos de seguridad de la información.

Reduce los costos: Un marco de seguridad efectivo puede ayudar a las instituciones a evitar los costos asociados a los incidentes de seguridad, como la pérdida de datos, el robo de identidad y el daño a la reputación.

Mejora la eficiencia: Un marco de seguridad bien diseñado puede ayudar a las instituciones a optimizar sus procesos de gestión de la IT y mejorar la eficiencia.

Aumenta la confianza: Un marco de seguridad sólido puede ayudar a las instituciones a aumentar la confianza de sus stakeholders, como estudiantes, profesores, padres y autoridades.

2.2.4.2. Estudios de Caso – Uso de COBIT 2019.

En el estudio realizado por Gunawan, Wang & Kalensun, Engelina & Fajar, Ahmad & Sfenrianto, Sfenrianto. (2018). Applying COBIT 5 in Higher Education. IOP Conference Series: Materials Science and Engineering. 420. 012108. 10.1088/1757-899X/420/1/012108. titulado " Applying COBIT 5 in Higher Education ", se analiza la implementación del marco de referencia COBIT 2019 en instituciones de educación superior para la gestión de la seguridad de la información. El objetivo principal del estudio fue evaluar la efectividad de COBIT 2019 en el contexto académico y su aplicación en procesos clave, como el proceso de titulación.

Los resultados de la investigación mostraron que la adopción de COBIT 2019 permitió a las instituciones de educación superior mejorar la gestión de la seguridad de la información y garantizar los atributos CID en sus procesos académicos. Mediante el uso de los procesos definidos en COBIT 2019, las instituciones lograron identificar los riesgos asociados a la seguridad de la información y establecer controles adecuados para mitigarlos.

Además, el estudio resalta que COBIT 2019 proporciona una estructura clara y bien definida para la gestión de la seguridad de la información, lo que facilita la implementación de controles de manera sistemática y coherente. Asimismo, se destaca la importancia de la alineación de COBIT 2019 con otros marcos y estándares de seguridad de la información, lo que permite una integración efectiva con las políticas y regulaciones existentes.

En el estudio realizado por Smith et al. (2020), se destaca la implementación de COBIT 2019 como marco de referencia en instituciones de educación superior para la gestión de la seguridad de la información. El estudio muestra que COBIT 2019 ha demostrado ser efectivo para mejorar la gestión de la seguridad de la información y garantizar los atributos CID en los procesos académicos, como el proceso de titulación.

Según los resultados del estudio, la aplicación de COBIT 2019 permitió a las instituciones identificar riesgos, establecer controles adecuados y mejorar la eficiencia en la gestión de la seguridad de la información.

Otro antecedente relevante es el estudio de (Merchan-Lima, 2021) titulado "Information security management frameworks and strategies in higher education institutions: a systematic review ". En este trabajo, se lleva a cabo una revisión sistemática de la literatura para analizar las prácticas de gestión de seguridad de la información en instituciones de educación superior.

El estudio resalta la necesidad de implementar marcos de referencia, como COBIT 2019, para abordar los desafíos de seguridad de la información en el ámbito académico. Se concluyó que COBIT 2019 permite a las instituciones establecer un enfoque integral para la gestión de la seguridad de la información, cubriendo aspectos como la planificación, implementación, monitoreo y mejora continua.

Además, se identificó que COBIT 2019 proporciona una estructura para la asignación de responsabilidades claras y la definición de procesos y controles específicos. Esto permite una mayor eficiencia en la gestión de la seguridad de la información y la garantía de los atributos CID en los procesos académicos, como el proceso de titulación.

Estos antecedentes de investigación respaldan la implementación del marco de seguridad de la información COBIT 2019 en el proceso de titulación de la Universidad Yachay Tech. A través de estos estudios, se evidencia la efectividad de COBIT 2019 en la gestión de la seguridad de la información en instituciones de educación superior, así como su capacidad para garantizar los atributos CID y fortalecer la protección de la información sensible en los procesos académicos.

2.2.5. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administración)

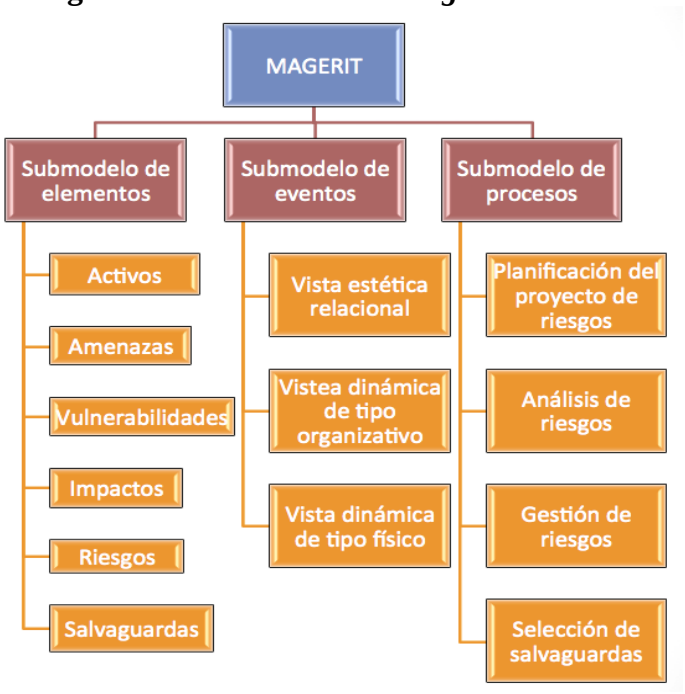
Es una herramienta gratuita y de código abierto desarrollada por el gobierno español para la gestión de riesgos de seguridad de la información. Se puede utilizar para identificar los activos de una institución de educación superior y clasificarlos según su criticidad (Ministerio de hacienda y administración pública, 2012).

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina “Proceso de Gestión de los Riesgos”, dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

MAGERIT es un instrumento alienado con estándares y que facilitan a una empresa enfocarse en implementar herramientas y metodologías que satisfagan los requerimientos básicos de la administración de riesgos en sus sistemas de información,

cuenta con una guía detallada en tres áreas: métodos, catálogo de elementos y guía de técnicas (Gutiérrez, 2016).

Figura 3. ***Estructura metodología MAGERIT***



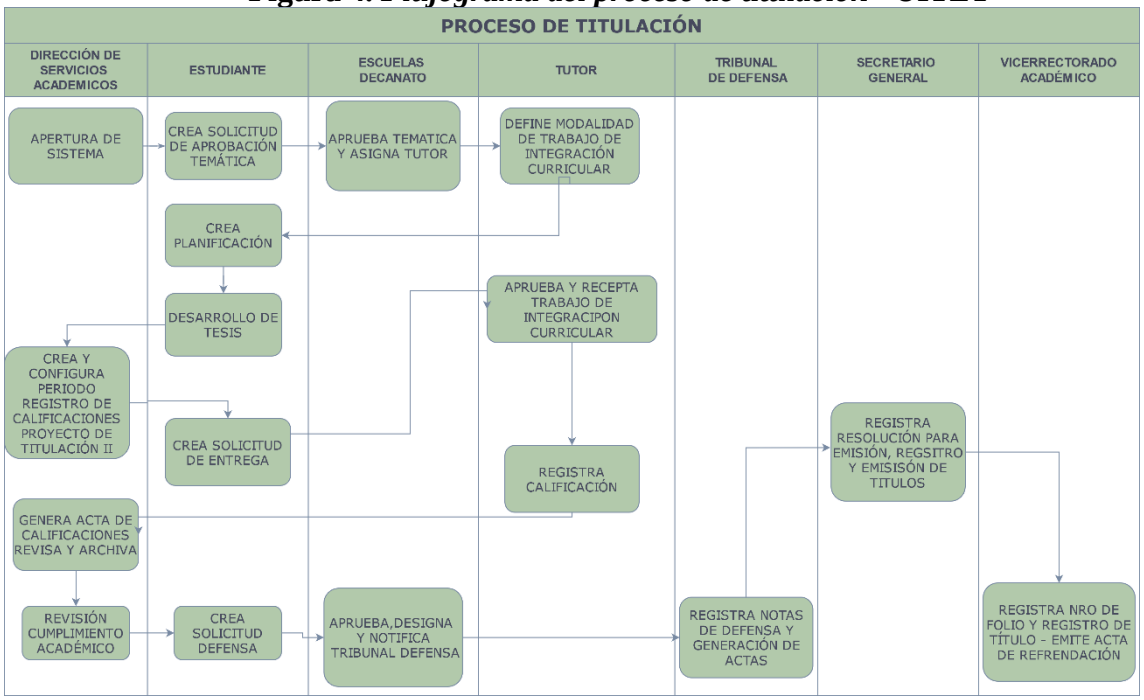
Fuente: (Amaya, 2016)

2.2.6. Proceso de Titulación de la Universidad de Investigación de Tecnología Experimental Yachay

El proceso de Titulación abarca varias actividades que se han automatizado a través del Sistema de Gestión Académica (SIGA) – Módulo de Gestión de la Titulación; la parametrización permite insertar al sistema la información inicial sobre la cual se sustentan todas las actividades del proceso, se puede crear y modificar parámetros como: fecha de creación de solicitudes de ingreso a titulación, tipos de titulación disponibles, número máximo de participantes por trabajo de integración curricular, modalidades de titulación, listado de posibles tutores, mínimo establecido para la calificación de la defensa, rutas de archivos donde se cargarán los trabajos de integración curricular, porcentajes para la calificación final del estudiante.

Este módulo tecnológico cuenta con accesos para distintos roles asignados a diferentes usuarios del área administrativa, docente y estudiantes.

Figura 4. ***Flujograma del proceso de titulación - UITEY***



Fuente: (UITEY, 2024).

Nota: El gráfico muestra las actividades por responsable que demanda el proceso de titulación,

2.3.Marco Legal

El marco de seguridad para una institución de educación superior basado en COBIT 2019 se fundamenta en los principios de gobernabilidad, gestión y aseguramiento de la información. Este marco busca proteger la información confidencial, sensible y crítica de la institución, así como los sistemas y recursos informáticos que la soportan.

2.3.1. Constitución de la República del Ecuador (Registro Oficial 449 de 20 de octubre de 2008)

La Constitución de la República del Ecuador, es la Norma Suprema, a la que está sometida toda la legislación ecuatoriana, donde se establecen las normas fundamentales que amparan los derechos, libertades y obligaciones de todos los ciudadanos, así como las del estado y las instituciones de este.

La carta magna cita en su título II sobre derechos, capítulo segundo, sección tercera el articulado referente a comunicación e información, donde se detalla el derecho de acceso universal a las tecnologías de información y comunicación (Constitución de la República del Ecuador, 2008).

2.3.2. Ley Orgánica de Protección de Datos Personales (Registro Oficial 459 de 26 de mayo de 2021)

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) y su reglamento establecen el marco legal para la protección de la información personal. Esta ley se aplica a toda persona natural o jurídica que trate datos personales, tanto en el sector público como privado (Ley orgánica de Protección de Datos Personales, 2021).

La LOPDP define los principios que deben regir el tratamiento de datos personales, como la licitud, lealtad y transparencia, el consentimiento, la finalidad, la exactitud, la proporcionalidad y la responsabilidad. Además, establece los derechos de los titulares de los datos, como el derecho de acceso, rectificación, cancelación, oposición, portabilidad y limitación del tratamiento.

COBIT 2019 es un marco de referencia internacional para la gestión y el gobierno de la información y las tecnologías de la información. Este marco puede ser utilizado para implementar un marco de seguridad para la protección de datos personales que cumpla con los requisitos de la LOPDP.

La LOPDP exige la implementación de medidas de seguridad para proteger los datos personales. Estas medidas deben ser técnicas, organizativas y adecuadas al riesgo que representa el tratamiento de los datos.

COBIT 2019 proporciona una guía completa para la implementación de medidas de seguridad. Esta guía incluye la identificación de los riesgos, la selección de las medidas de control adecuadas y la evaluación de la eficacia de las medidas de seguridad.

La implementación de un marco de seguridad basado en COBIT 2019 puede ayudar a las organizaciones a cumplir con la LOPDP y a proteger la información personal de sus stakeholders.

2.3.3. Ley Orgánica de Educación Superior (Registro Oficial 298 del 12 de octubre de 2010)

Establece los principios generales que rigen el sistema de educación superior en Ecuador, definiendo las políticas, lineamientos y regulación de la calidad para la gestión de las universidades.

La Ley Orgánica de Educación Superior (LOES) mantiene inmersa en su articulado la importancia de la calidad de la educación superior, basada en la pertinencia, inclusión, democratización, e integralidad; para lo cual es necesario el mejoramiento,

aseguramiento y construcción colectiva de la cultura de la calidad educativa superior con la participación de todos los estamentos de las instituciones de educación superior y el Sistema de Educación Superior (Ley Orgánica de Educación Superior, 2010).

2.3.3.1. Reglamento General a la Ley Orgánica de Educación Superior (Registro Oficial 526 del 02 de septiembre de 2011).

Complementa la Ley Orgánica de Educación Superior, estableciendo normas específicas para la organización y funcionamiento de las universidades. Es importante destacar el artículo 9 "De la evaluación de la calidad. - La evaluación de la calidad se realizará de manera periódica de conformidad con la normativa que expida el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior, CEAACES", lo que denota la relevancia que tienen los procesos de evaluación en la educación superior.

2.3.4. Ley de Creación de la Universidad de Investigación de Tecnología Experimental Yachay (Registro Oficial 144 del 16 de diciembre de 2013)

Define la naturaleza jurídica; autonomía académica, administrativa, financiera y orgánica; sede, patrimonio y fuentes de financiamiento de la universidad (Ley de Creación de la Universidad de Investigación Experimental Yachay, 2013). Con el tiempo esta ley se ha tornado operativa mediante la expedición de normativa específica mediante, reglamentos y resoluciones.

2.3.4.1. Estatuto de la Universidad de Investigación de Tecnología Experimental Yachay (Resolución RCG-SE-01 No. 002-2014 de fecha 22 de abril de 2014).

Desarrolla la ley de creación de la universidad, define los derechos y deberes de los miembros de la comunidad universitaria, regula los procesos académicos, administrativos y financieros de la universidad. Es importante destacar que uno de los principios que rigen es el de calidad, mismo que promueve la adopción de máximos estándares de excelencia en sus actividades y programas académicos, a fin de asegurar el mejoramiento continuo en todos sus niveles de formación, capacitación e investigación.

Adicionalmente como parte de los objetivos se establece el brindar una alta calidad educativa y de excelencia, mediante una permanente evaluación de las actividades académicas; apoyar los procesos de innovación social a fin de alcanzar los objetivos

nacionales establecidos en la Constitución de la República, el Plan Nacional de Desarrollo; mantener niveles altos de autoevaluación con rigurosidad técnica y académica (UITEY, 2014). Consejo Superior Universitario es el máximo órgano colegiado de cogobierno académico y administrativo.

2.3.4.2. Plan Estratégico de Desarrollo Institucional UITEY (2022).

El cual detalla la planificación institucional como una herramienta que permite establecer el camino a seguir en la universidad y determina 4 ejes y objetivos estratégicos; el presente estudio se relaciona con el eje estratégico 4 – Eficiencia Institucional y Transparencia, así como el objetivo estratégico 4 - Fortalecer la gestión institucional enfocados en la calidad, eficiencia y la transparencia (UITEY , 2022).

Esta investigación responde al plan estratégico de desarrollo institucional ya que mediante el uso de la metodología propuesta se promoverá la implementación de mejoras en uno de los procesos de gran importancia para la Universidad mediante el cual se canaliza el proceso de titulación buscando la mejora continua, procesos de calidad y eficientes.

2.3.4.3. Política de Aseguramiento de la Calidad de la Universidad de Investigación de Tecnología Experimental Yachay (2022).

Esta política menciona dentro del capítulo de condiciones institucionales como una prioridad la gestión interna de la calidad, destacando la importancia de ejecutar procesos de autoevaluación institucional, como también el seguimiento oportuno para la formulación y aplicación de Planes de Mejora de las áreas administrativas y académicas (UITEY, 2022).

2.3.4.4. Resoluciones Universitarias (2020).

Mediante resolución No. RCA-SE-020 No. 046-2020 de fecha 13 de agosto de 2020 el Consejo Académico de la Universidad de Investigación de Tecnología Experimental Yachay aprueba el Instructivo para la Presentación y Sustentación del Trabajo de Integración Curricular y Obtención de Título de Grado (UITEY, 2020).

Mediante resolución Nro. UITEY-REC-2020-0044-R de fecha 14 de octubre de 2020 la Universidad de Investigación de Tecnología Experimental Yachay resuelve actualizar el “Instructivo para la Presentación y Sustentación del Trabajo de Integración Curricular y Obtención de Título de Grado – Estudiantes” (UITEY, 2020).

2.3.5. Plan Nacional de Desarrollo del Ecuador (2024)

El Plan Nacional de Desarrollo es un instrumento al que se ajustan las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto ecuatoriano, además de la inversión y asignación de recursos públicos; coordinando las competencias exclusivas para el estado central y los gobiernos autónomos descentralizados.

Este instrumento nacional establece 4 ejes estratégicos y 9 objetivos nacionales, en el eje Institucional se cita el artículo 9 “Propender la construcción de un Estado eficiente, transparente y orientado al bienestar social” el cual se fundamenta en la consolidación de una institucionalidad robusta que dinamice los servicios públicos en favor de la sociedad; el presente estudio se aliena a este objetivo nacional y sus políticas ya que se busca mejorar la eficiencia de un proceso crucial dentro de la razón de ser las instituciones de educación superior como es el proceso de titulación de los estudiantes (Secretaría Nacional de Planificación, 2024).

2.3.6. Normas de calidad ISO

Las Normas ISO son un conjunto de estándares reconocidos internacionalmente, creados por la Organización Internacional de Estandarización (ISO) con el objetivo de garantizar que las empresas alcancen criterios homogéneos en la gestión de su actividad, estableciendo niveles reconocidos de cumplimiento de calidad, eficiencia y seguridad en relación con las áreas y actividades concretas que desarrolla cada norma procurando la mejora continua. (Global Suite, 2023).

2.3.6.1. Norma ISO 27000.

Las normas que forman la serie ISO/IEC-27000 son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). En la actualidad, la información es uno de los activos más importantes en una organización, por lo que se requiere que se encuentre correctamente protegida. Las normas de la familia de ISO 27000 tratan la gestión de la seguridad de la información y contienen un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.

Esta norma y sus procesos tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la

información, con una fuerte orientación a la mejora continua y la mitigación de riesgos, siendo aplicables a cualquier tipo de organización pública o privada (Global Suite, 2023).

2.3.6.2. Norma ISO 31000.

La norma ISO 31000 es un conjunto de directrices y principios internacionales que suministran un enfoque sistemático y estructurado para la identificación, evaluación, tratamiento y monitoreo de riesgos en cualquier organización, publicada por primera vez en el año 2009 y su última actualización se llevó a cabo en 2018. Su objetivo principal es ayudar a las organizaciones a proteger sus activos, cumplir con sus objetivos y mejorar la toma de decisiones (Global Suite, 2023).

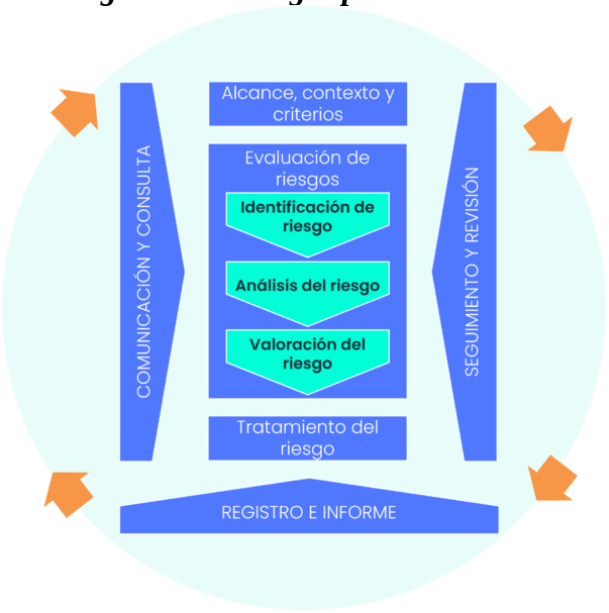
Esta norma se basa en tres componentes principales: los principios, el marco y el proceso de gestión de riesgos. Estos componentes relacionan y refuerzan mutuamente para facilitar un enfoque coherente y eficaz para la gestión de riesgos.

Figura 5. ***Marco de gestión del riesgo según ISO 31000***

Fuente*:* (Global Suite, 2023)

ISO 31000 plantea un Proceso de gestión de riesgos que consta de varias etapas, desde las generalidades, comunicación y consulta, alcance, evaluación del riesgo, tratamiento del riesgo, seguimiento y revisión, registro e informe.

Figura 6. ***Proceso de gestión de riesgos planteado en la norma ISO 31000***



Fuente: (Global Suite, 2023)

2.3.7. Normas de Control Interno de la Contraloría General del Estado (Acuerdo Ministerial 39, Registro Oficial 87 del 14 de diciembre de 2009)

Las normas de control interno cuentan con una clasificación, la norma 410 se relaciona con la Tecnología de la Información, en esta norma se desarrollan diferentes enunciados para las entidades y organismos del sector público que deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control. Se responsabiliza a las Unidades de Tecnología de Información en el enunciado 410-10 sobre seguridad de tecnología de información, el establecimiento de mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos y el enunciado 410-11 sobre plan de contingencias señala la responsabilidad de la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado (Contraloría General del Estado, 2009).

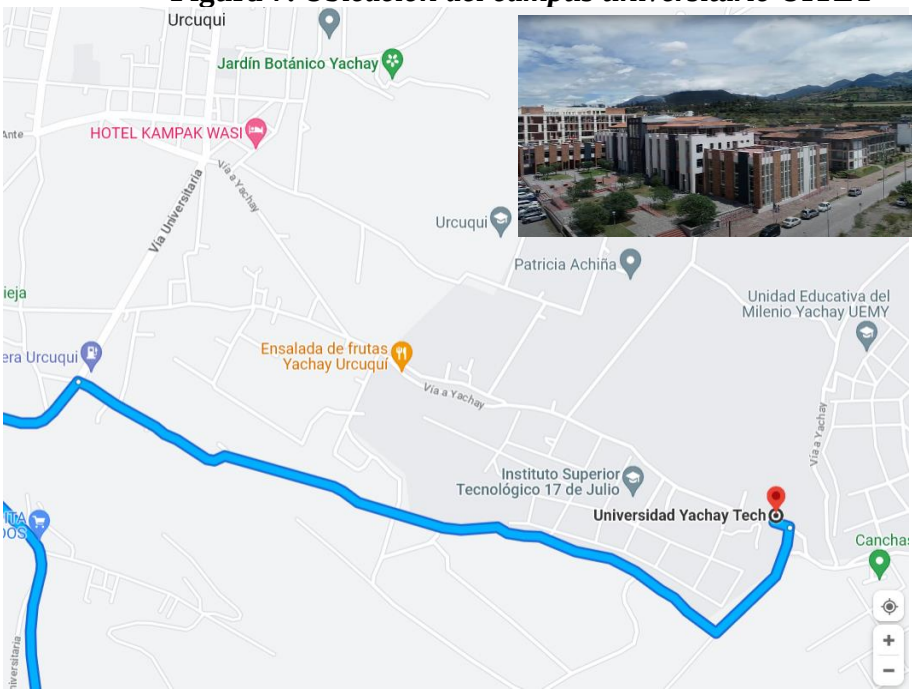
CAPITULO III

MARCO METODOLÓGICO

3.1. Descripción del Área de Estudio

La Universidad de Investigación de Tecnología Experimental Yachay, también conocida como Universidad Yachay o Yachay Tech es una universidad pública del Ecuador, situada en Ciudad del Conocimiento Yachay, cantón San Miguel de Urcuquí, provincia de Imbabura a una altitud de 2035 m.s.n.m. En la actualidad, Yachay Tech, cuenta con 1153 estudiantes de carrera, y 332 estudiantes de nivelación distribuidos en 6 escuelas, 10 carreras de pregrado y 7 programas de posgrado en áreas como ciencias físicas, matemáticas, ingeniería, ciencias biológicas y ciencias de la computación.

Figura 7. ***Ubicación del campus universitario UITEY***



Fuente: (Google Maps, 2024)

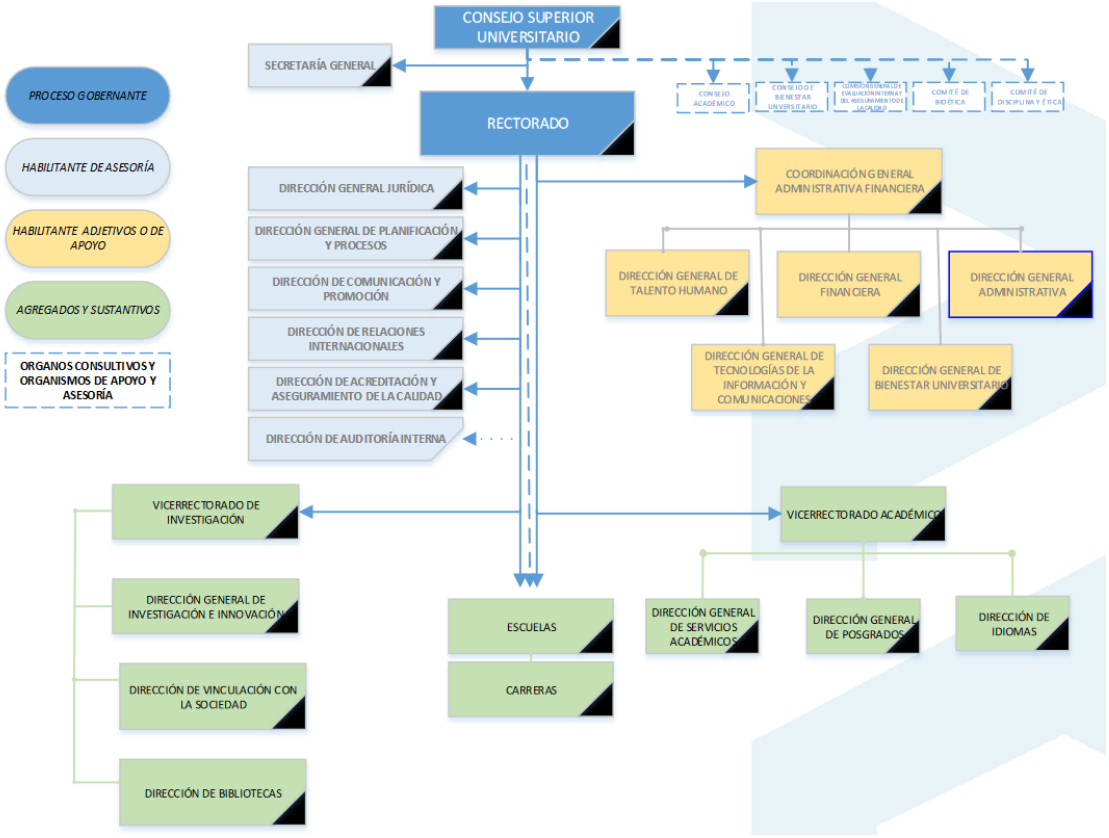
Nota: Ubicación Campus universitario UITEY

Uno de los aspectos distintivos de Yachay Tech es su enfoque en la investigación científica y tecnológica de alta calidad. La universidad cuenta con laboratorios e instalaciones de vanguardia para apoyar la investigación en diversas disciplinas. Además,

fomenta la colaboración entre estudiantes, profesores e investigadores para promover la generación de conocimiento y la innovación.

Yachay Tech también tiene una fuerte orientación hacia el emprendimiento y la transferencia de tecnología. Busca formar profesionales capaces de aplicar sus conocimientos en la creación de empresas y proyectos innovadores que contribuyan al desarrollo económico y social del país. La siguiente figura muestra la estructura organizacional de la Universidad de Investigación de Tecnología Experimental Yachay.

Figura 8. ***Organigrama estructural UITEY***



Fuente: (UITEY, 2014)

Nota: Tomado de la página web de Yachay Tech, https://www.yachaytech.edu.ec/

3.2. Método y Enfoque de la Investigación

El presente estudio emplea un método analítico-sintético e inductivo, ya que con la finalidad de lograr un objetivo general se parte del estudio individual de diferentes parámetros, en este caso sobre los activos del proceso de titulación de la UITEY y la valoración de sus tributos CID, de lo cual se parte para realizar un análisis de riesgos y

posteriormente se fusionan parámetros para definir su tratamiento en relación a la seguridad de la información (Arispe, y otros, 2020).

El tipo de investigación corresponde a aplicada, ya que se enfoca en identificar a través del conocimiento científico los medios por los cuales se puede contribuir a solucionar una necesidad delimitada, particularizando soluciones a través del uso de la tecnología, se identifica un problema actual y su solución se basa en estrategias actuales específicas para el caso estudiado.

Así también se ha identificado el enfoque de la investigación definido como cualitativo, ya que examina los hechos, revisando estudios existentes, de tal manera que se genera una teoría relacionada con lo que se está observando; este es un proceso "circular" donde no hay una secuencia definida y su proceso puede ser flexible. Sin embargo, en ciertos momentos de la investigación se emplea un enfoque mixto, ya que se realizan cálculos cuantitativos para el análisis de riesgos y sobre esto se sustentan las decisiones adoptadas para el plan de acción dentro del marco de seguridad propuesto.

En el análisis de datos cualitativos se explica la perspectiva analítica que se adopta, sus fundamentos y características. En general, los datos pueden ser trabajados a través de análisis de contenido que responde a la pregunta de investigación y objetivos. Los componentes de la metodología en la investigación cualitativa son los siguientes: diseño de investigación, muestra, técnicas de producción de datos, análisis, criterios de rigor y aspectos éticos. En el diseño de investigación se explican los fundamentos de la metodología cualitativa, con respaldo de bibliografía actualizada y congruente con el problema y perspectiva de investigación (Universidad Norbert Wiener, 2020).

3.3. Consideraciones Bioéticas

Las consideraciones bioéticas están relacionadas con los principios éticos y los aspectos morales que involucran el uso de la tecnología y la gestión de la información. A continuación, se presentan algunas consideraciones bioéticas relevantes para este tema:

Privacidad y confidencialidad: Es fundamental respetar la privacidad y confidencialidad de los datos e información personal de los estudiantes y participantes en el proceso de titulación. Se deben implementar medidas de seguridad apropiadas para proteger la información y garantizar que solo las personas autorizadas tengan acceso a ella.

Consentimiento informado: Si se recolecta información personal de los estudiantes como parte del proceso de titulación, es necesario obtener su consentimiento

informado de manera clara y transparente. Los estudiantes deben ser informados sobre el propósito de la recopilación de datos, cómo se utilizarán y qué medidas se tomarán para proteger su privacidad.

Acceso equitativo: Es importante garantizar que todos los estudiantes tengan acceso equitativo a los recursos y servicios relacionados con el marco de seguridad de la información. No se deben establecer barreras injustas o discriminatorias que limiten la participación o el acceso a oportunidades académicas debido a cuestiones de seguridad de la información.

Responsabilidad y rendición de cuentas: La implementación del marco de seguridad de la información debe ir acompañada de una clara asignación de responsabilidades y rendición de cuentas. Las personas y entidades involucradas en el proceso de titulación deben ser responsables de garantizar la seguridad de la información y de tomar medidas adecuadas para prevenir incidentes de seguridad.

Transparencia y comunicación: La comunicación transparente es esencial para mantener la confianza de los estudiantes y demás partes interesadas. Debe existir una comunicación clara sobre las políticas y prácticas de seguridad de la información, así como sobre cualquier cambio o incidente relevante que pueda afectar la privacidad o seguridad de los datos.

Estas consideraciones bioéticas son fundamentales para asegurar que el marco de seguridad de la información utilizado en el proceso de titulación de la Universidad Yachay Tech sea ético, respete los derechos de los estudiantes y promueva la confianza en el uso responsable de la tecnología y la gestión de la información.

3.4. Población y Muestra

Con fines de cálculos, se establecerá una muestra de la población vinculada con el proceso de titulación, la cual se define como un subgrupo de la población en el cual se recolectan los datos. El trabajar con muestra permite: ahorrar tiempo, reduce costos y si está bien seleccionada puede ayudar con la precisión y exactitud de los datos. Otro aspecto por considerar es que la población y muestra deben estar en relación con la pregunta de investigación y objetivos, al igual que debe tener representatividad estadística (Arispe, y otros, 2020).

La población engloba el conjunto de personas que se relacionan con el proceso de titulación, en este caso se refiere a estudiantes de octavo, noveno y décimo semestre que

se encuentran cursando materias de titulación; personal administrativo y académico vinculado con roles de administración y seguimiento del proceso de titulación.

3.4.1. Cálculo del Tamaño de la Muestra

El tamaño de muestra depende del grado de precisión que se busca en los resultados. Para calcular el tamaño de la muestra se puede utilizar fórmulas estadísticas, donde se consideran los siguientes parámetros:

- Tamaño de la población
- Nivel de confianza: generalmente se trabaja con un 95% de confianza
- Proporción (p,q): cuando se conoce se trabaja con 50%
- Error máximo: se aconseja utilizar máximo un 5%

La fórmula que se utiliza es de Krejcie y Morgan:

$$n = \frac{Z^2 N p(1-q)}{e^2(N-1) + Z^2 p(1-p)}$$

Dónde:

n = tamaño de muestra

Z = nivel de confianza (correspondiente a la tabla de valores Z= 1,96)

p = porcentaje de la población que tiene el atributo deseado

q = porcentaje complementario (1-p)

N = tamaño de la población (162 personas)

e = error máximo permitido (5%)

Para desarrollar el presente estudio se identifica como usuarios del proceso de titulación a personal responsable de TI, personal administrativo y académico. Por lo que la muestra será calculada a partir de dicha población.

Sustituyendo los valores:

$$n = \frac{1.96^2 \; x \; 162 \; x \; (0{,}5 \; x \; (1 - 0{,}5))}{0{,}05^2 \; x \; (162 - 1) + [1.96^2 \; x \; (0{,}5 \; x \; (1 - 0{,}5))]}$$

Calculando:

- n ≈ 114.15

Redondeando al siguiente número entero:

Tamaño de muestra mínimo: 114 personas

Interpretación:

Para lograr un nivel de confianza del 95% y un margen de error del 5% en una encuesta a una población de 162 personas, se recomienda una muestra mínima de **114 individuos**.

3.5. Diseño del Marco de Seguridad de la Información para el Proceso de Titulación de la Universidad Yachay Tech

El Marco de Seguridad de la Información se ha diseñado según la matriz guía para la Implementación de Buenas prácticas Basadas en COBIT 2019, según el dominio APO 12 (Alinear, Planificar y Organizar) – Gestión de Riesgos Tecnológicos adoptando criterios metodológicos para la gestión de riesgos de seguridad de la información expedido por el MINTEL en el 2020.

Gestión de Riesgos Prácticas de Manejo de Riesgos

APO12 es un proceso dentro del marco de referencia COBIT 5 (Control Objectives for Information and Related Technologies), que se enfoca en la **Gestión de Riesgos**. Este proceso está diseñado para identificar, evaluar, responder, monitorear y comunicar los riesgos que pueden afectar el logro de los objetivos de la organización. (FOURMATT, 2022)

Tabla 1 ***Actividades Esenciales Proceso APO12***

Código de Práctica	Práctica Clave	Descripción
APO12.01	Recopilación de Datos	Desarrollar y mantener un enfoque estructurado para la gestión de riesgos, alineado con los objetivos de la organización y sus estrategias.
APO12.02	Análisis de Riegos	Definir el contexto interno y externo en el que opera la organización, identificando y evaluando factores que influyen en la gestión de riesgos.
APO12.03	Mantener un Perfil de Riesgos	Realizar actividades sistemáticas para identificar riesgos, utilizando técnicas como análisis de escenarios y revisión de incidentes anteriores.

Código de Práctica	Práctica Clave	Descripción
APO12.04	Articulación del Riesgo	Analizar la probabilidad y el impacto de los riesgos identificados, priorizando en función de su relevancia para la organización.
APO12.05	Portafolio de Acciones Gestión de Riesgos	Desarrollar e implementar respuestas adecuadas a los riesgos, eligiendo entre opciones como evitar, mitigar, transferir o aceptar el riesgo.
APO12.06	Responder al Riesgo	Asegurar una comunicación continua y efectiva con las partes interesadas sobre los riesgos, consultando a expertos y partes relevantes para obtener insights y feedback.
APO12.07	Monitorear y revisar la gestión de riesgos	Evaluar continuamente la eficacia del proceso de gestión de riesgos, realizando auditorías y revisiones para asegurar que los controles de riesgos sean adecuados.

Fuente: Elaboración Propia

3.5.1. Actividad Esencial APO 12.01 Recopilación de Datos

El proceso de recopilación de datos es la primera práctica planteada en la matriz guía para la Implementación de Buenas prácticas Basadas en COBIT 2019, según el dominio APO 12 (Alinear, Planificar y Organizar) – Gestión de Riesgos Tecnológicos. Las actividades propuestas por la metodología COBIT 2019 son:

- Establecer y mantener un método para la recolección, clasificación y análisis de datos relacionados con el riesgo de I&T.
- Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.
- Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.
- Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.
- Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles,

homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.

- Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.
- Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.
- Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.

En función de las actividades planteadas en la primera práctica, los indicadores asociados son:

- Número de eventos de pérdida con características clave capturados en repositorios.
- Porcentaje de auditorías, eventos y tendencias capturados en repositorios.
- Porcentaje de sistemas críticos con problemas conocidos.

Adicionalmente se presentará un análisis del contexto interno y externo en base a la situación actual del proceso de titulación al iniciar el estudio.

3.5.2. Actividad Esencial APO 12.02 Análisis de Riesgos

El análisis de riesgos es la segunda práctica dentro de la guía para la Implementación de Buenas prácticas Basadas en COBIT 2019, según el dominio APO 12. Las actividades planteadas en esta práctica son:

- Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.
- Crear y actualizar regularmente los escenarios de riesgo de I&T; las exposiciones a pérdidas relacionadas con I&T; y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Desarrollar previsiones para actividades de control específicas y capacidades de detección.

- Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.
- Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado.
- Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.
- Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionadas. Identificar los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de mitigación de riesgos.
- Validar el análisis de riesgo y los resultados del análisis de impacto del negocio (BIA) antes de usarlos en la toma de decisiones. Confirmar que el análisis se corresponde con los requisitos empresariales y comprobar que los sesgos de las estimaciones se calibraron y analizaron de forma adecuada.
- Analizar el coste/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/aprovechar. Confirmar la respuesta óptima al riesgo.

Los indicadores relacionados con esta segunda práctica son:

- Número de escenarios de riesgo de I&T identificados.
- Tiempo transcurrido desde la última actualización de los escenarios de riesgos de I&T.

El proceso de análisis se basa en la guía para la gestión de riesgos de seguridad de la información expedido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información en el año 2020, el cual parte de conceptos básicos enmarcados en el proceso para la gestión del riesgo de la seguridad de la información; así también se han adaptado criterios de valoración de la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT 3.0) expedida por el Ministerio de Hacienda y Administraciones Públicas del Gobierno de España. Las dos metodologías cuentan con la validez y reconocimiento gubernamental a nivel nacional e internacional.

Los riesgos se deben identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la

institución. Un riesgo es una combinación de las consecuencias presentadas después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los propietarios de los activos priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

La valoración del riesgo consta de cuatro actividades básicas:

- Análisis del riesgo
    - Identificación de los activos
    - Identificación de las amenazas
    - Identificación de vulnerabilidades
    - Identificación de la existencia de controles
- Identificación del riesgo
- Estimación del riesgo
- Evaluación del riesgo

3.5.2.1. Identificación de los activos.

Inicia con la identificación de activos, considerando que un activo es todo aquello que tiene valor para la organización y que requiere de protección. Para realizar la valoración de los activos, es necesario que la institución identifique primero sus activos (con un grado adecuado de detalles). La guía propone dos clases de activos:

Activos primarios:

- Actividades y procesos del negocio.
- Información.

Activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:

- Hardware.
- Software.
- Redes.
- Personal.
- Ubicación.
- Estructura de la organización.

Una vez identificados los activos se realiza la valoración o ponderación de la criticidad de activos en términos de “alto, medio o bajo” donde se asigna un valor

cuantitativo a cada valor cualitativo de los atributos de confidencialidad, integridad y disponibilidad, la metodología adoptada plantea las siguientes ponderaciones:

Tabla 2 ***Valoración del impacto en términos de la perdida de la confidencialidad***

CONFIDENCIALIDAD	CRITERIO
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución. Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución. Ej. Divulgación de información de uso interno.
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución. Ej. Divulgación de información pública.

Fuente: (Gobierno Electrónico, 2020)

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

Tabla 3 ***Valoración del impacto en términos de la perdida de la integridad***

INTEGRIDAD	CRITERIO
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución.
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución.
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Fuente: (Gobierno Electrónico, 2020)

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

Tabla 4 ***Valoración del impacto en términos de la perdida de la disponibilidad***

DISPONIBILIDAD	CRITERIO
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución.
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución.

Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución.

Fuente: (Gobierno Electrónico, 2020)

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

Con referencia a las tablas mencionadas, la valoración se la realiza respecto a la confidencialidad, integridad y disponibilidad ya que estas son las dimensiones en que se basa la seguridad de la información (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020).

La valoración detallará el número y nombre del activo, tipo de soporte, ubicación, ponderaciones CID y valoración calculada acorde la siguiente formula.

$$VA = \frac{C + I + D}{3}$$

Dónde:

VA = Valoración de los activos

C = Confidencialidad

I = Integridad

D = Disponibilidad

3 = No. de atributos

3.5.2.2. Identificación de amenazas.

Para la identificación de amenazas se ha adoptado el catálogo de amenazas posibles sobre los activos de un sistema de información propuesto en la metodología MAGERIT 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, la cual presenta la siguiente clasificación:

- Desastres naturales
    - Fuego
    - Daños por agua
    - Desastres naturales: contaminación, siniestro mayor, fenómeno climático, fenómeno sísmico, fenómeno de origen volcánico, fenómeno meteorológico, inundación, etc.
- De origen industrial
    - Fuego
    - Daños por agua

  - Desastres industriales
  - Contaminación mecánica
  - Contaminación electromagnética
  - Avería de origen físico o lógico
  - Corte del suministro eléctrico
  - Condiciones inadecuadas de temperatura o humedad
  - Fallo de servicios de comunicaciones
  - Interrupción de otros servicios y suministros esenciales
  - Degradación de los soportes de almacenamiento de la información
  - Emanaciones electromagnéticas
- Errores y fallos no intencionados
  - Errores de los usuarios
  - Errores del administrador
  - Errores de monitorización (log)
  - Errores de configuración
  - Deficiencias en la organización
  - Difusión de software dañino
  - Errores de [re-]encaminamiento
  - Errores de secuencia
  - Escapes de información
  - Alteración accidental de la información
  - Destrucción de información
  - Fugas de información
  - Vulnerabilidades de los programas (software)
  - Errores de mantenimiento / actualización de programas (software)
  - Errores de mantenimiento / actualización de equipos (hardware)
  - Caída del sistema por agotamiento de recursos
  - Pérdida de equipos
  - Indisponibilidad del personal
- Ataques intencionados
  - Manipulación de los registros de actividad (log)
  - Manipulación de la configuración
  - Suplantación de la identidad del usuario

    - Abuso de privilegios de acceso
    - Uso no previsto
    - Difusión de software dañino
    - [Re-]encaminamiento de mensajes
    - Alteración de secuencia
    - Acceso no autorizado
    - Análisis de tráfico
    - Repudio
    - Interceptación de información (escucha)
    - Modificación deliberada de la información
    - Destrucción de información
    - Divulgación de información
    - Manipulación de programas
    - Manipulación de los equipos
    - Denegación de servicio
    - Robo
    - Ataque destructivo
    - Ocupación enemiga
    - Indisponibilidad del personal
    - Extorsión
    - Ingeniería social (picaresca)
- Correlación de errores y ataques
    - Amenazas que sólo pueden ser errores, nunca ataques deliberados
    - Amenazas que nunca son errores: siempre son ataques deliberados
    - Amenazas que pueden producirse tanto por error como deliberadamente
- Nuevas amenazas: XML
    - Sintaxis BNF
    - Esquema XSD

3.5.2.3. Identificación de vulnerabilidades.

Se identifican las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución. La presencia de una vulnerabilidad no causa daño por sí misma, puesto 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. Es importante considerar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad.

Las vulnerabilidades se han adoptado del catálogo del esquema gubernamental de seguridad de la información de la subsecretaría de gobierno electrónico y registro civil con referencia de la norma ISO 27005.

3.5.2.4. Identificación de la existencia de controles.

Es necesario identificar los controles existentes y los planificados; se debe realizar la identificación de los controles existentes para evitar la duplicidad. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente y en caso de identificar que no existen o resultan insuficientes o inadecuados se deberán identificar controles necesarios a implementar.

Los controles deben brindar protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos en cumplimiento de las normas, estándares, procedimientos y disposiciones legales establecidas. Los controles corresponden a políticas y procedimientos auditables establecidos por una empresa para ayudar a garantizar la confidencialidad, la integridad y la disponibilidad de sus sistemas y datos de TI.

Figura 9 ***Ejemplos de controles generales aplicados a las tecnologías de la información***

Fuente: (EnterpriseIT, 2021)

3.5.2.4. Evaluación del riesgo.

La guía plantea la evaluación como una comparación de los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto. El grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad. Para lo cual se han adoptado los siguientes criterios:

3.5.2.4.1. Criterios de probabilidad de ocurrencia de amenazas.

La guía para la gestión de riesgos de seguridad de la información (2020) detalla los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explotar alguna vulnerabilidad existente.

Tabla 5 ***Criterios de probabilidad de ocurrencia de amenazas***

Nivel de amenaza	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%).	Bajo circunstancias normales.	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable

Medio (2)	La ocurrencia probable (probabilidad = 50%).	Por errores descuidos.	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable.
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%).	En rara ocasión.	El atacante no se beneficia del ataque.

Fuente: (Gobierno Electrónico, 2020)

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

Tabla 6 ***Criterios de probabilidad de ocurrencia de vulnerabilidades***

Nivel de vulnerabilidad	**Criterio**	**Ejemplo**
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza.	No se utilizan contraseñas para que los usuarios ingresen a los sistemas.
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable.	Existen normas para la utilización de contraseñas, pero no se implementa.
Bajo (1)	La medida de seguridad es adecuada.	Existen normas para la utilización de contraseñas y es aplicada.

Fuente: (Gobierno Electrónico, 2020)

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

3.5.2.4.2. Criterio de la Evaluación de Riesgos.

El nivel de riesgo de cada activo es el resultado del producto de la probabilidad de ocurrencia de una amenaza, la probabilidad de ocurrencia de vulnerabilidades y el valor del impacto del activo de la información (CID).

Nivel de riesgo=VA(CID) x Nivel de amenaza x Nivel de vulnerabilidad

Tabla 7 ***Nivel de riesgo***

Valoración	Nivel de riesgo
1 - 3	El riesgo es BAJO
4 - 8	El riesgo es MEDIO
9 - 27	El riesgo es ALTO

Fuente: (Gobierno Electrónico, 2020)

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

3.5.3. Actividad Esencial APO 12.03 Mantener un Perfil de Riesgo

La tercera práctica planteada en la matriz guía para la Implementación de Buenas prácticas Basadas en COBIT 2019 se denomina “Mantener un perfil de riesgo”, según el dominio APO 12 (Alinear, Planificar y Organizar) – Gestión de Riesgos Tecnológicos. Las actividades propuestas por la metodología COBIT 2019 son:

- Actualizar regularmente la evaluación de riesgos de TI para reflejar cambios en el entorno empresarial, tecnológico y regulatorio.
- Revisar y validar los criterios de evaluación de riesgos para garantizar su relevancia y aplicabilidad.
- Analizar y clasificar los riesgos identificados según su impacto potencial y probabilidad de ocurrencia.

Esta práctica busca una gestión efectiva de los riesgos de TI y ayuda a garantizar que la institución esté al tanto de los riesgos actuales y potenciales que enfrenta en su entorno operativo.

La práctica "Mantener un perfil de riesgo" implica la actualización regular y el mantenimiento de un registro detallado de los riesgos de TI que enfrenta la institución, así como sus impactos y probabilidades asociadas. Este perfil de riesgo sirve para la toma de decisiones informadas sobre la asignación de recursos, la priorización de los esfuerzos de mitigación de riesgos y la evaluación del rendimiento en la gestión de riesgos.

3.5.4. Actividad Esencial APO 12.04 Articulación del Riesgo

Como cuarta práctica planteada en la matriz guía para la Implementación de Buenas prácticas Basadas en COBIT 2019 “Articulación del riesgo”, según el dominio APO 12 (Alinear, Planificar y Organizar) – Gestión de Riesgos Tecnológicos se centra en la comunicación efectiva de los riesgos de seguridad de la información dentro de la organización. Esta práctica es esencial para garantizar que todas las partes interesadas

estén al tanto de los riesgos identificados, comprendan su impacto potencial en los objetivos del negocio y participen en la toma de decisiones relacionadas con la gestión de riesgos. A continuación, se detallan las actividades propuestas por la metodología COBIT 2019:

- Identificación de partes interesadas relevantes dentro de la institución que debe estar involucrada en la gestión de riesgos de seguridad de la información.
- Realizar una evaluación minuciosa de los riesgos de seguridad de la información utilizando métodos de análisis de riesgos, evaluación de vulnerabilidades, revisión de controles existente para identificar y documentar los riesgos claves que pueden afectar a los activos de información de la institución.
- Clasificar y priorizar los riesgos identificados con su respectivo impacto potencial en la confidencialidad, integridad y disponibilidad de la información.
- Desarrollar un plan de comunicaciones de riesgo que detalle cómo se comunicarán los riesgos identificados a las partes interesadas relevantes, que puede incluir reuniones periódicas, informes de estado, presentaciones ejecutivas entre otros.
- Proporcionar formación y concienciación sobre los riesgos de seguridad de la información a las partes involucradas, asegurando la comprensión de la importancia de la gestión de riesgos y como se puede contribuir a mitigar los riesgos en las áreas respectivas.
- Fomentar la colaboración y participación de las partes interesadas en la toma de decisiones que incluya aprobación de estrategias de mitigación de riesgos y asignación de recursos para la implementación de controles de seguridad.

Esta práctica es importante para una gestión efectiva de los riesgos de TI y ayuda a garantizar que la institución esté al tanto de los riesgos actuales y potenciales que enfrenta en su entorno operativo.

La articulación del riesgo corresponde al tratamiento, es decir tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la institución, para lo cual se debe definir un plan para el tratamiento. Existen cuatro tipos de opciones para el tratamiento del riesgo:

3.5.4.1. Reducción del Riesgo.

El riesgo se debe reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable. Se debe seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo. En esta selección se deberían tener en cuenta los criterios de aceptación del riesgo, así como requisitos legales, reglamentarios, contractuales, aspectos técnicos, ambientales y culturales. Con frecuencia es posible disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

3.5.4.2. Evitación del Riesgo.

Se debe evitar la actividad o la acción que da origen al riesgo particular. Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

Por ejemplo, para los riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control.

3.5.4.3. Transferencia del Riesgo.

Implica que el riesgo se debe transferir a otra parte o dependencia de la institución que pueda gestionarlo de manera más eficaz dependiendo de su evaluación.

3.5.4.4. Retención/Aceptación del Riesgo.

La decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo. Es posible aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la institución para la aceptación de los riesgos.

Esta opción se toma cuando los costos de implementación de un control de seguridad sobrepasan el valor del activo de información que se desea proteger o cuando el nivel del riesgo es muy bajo, en ambos casos la organización asume los daños provocados por la materialización del riesgo.

3.5.5. Actividad Esencial APO 12.05 Portafolio de Acciones para la Gestión de Riesgos

La quinta práctica planteada en la matriz guía para la Implementación de Buenas prácticas Basadas en COBIT 2019, según el dominio APO 12 (Alinear, Planificar y Organizar) – Gestión de Riesgos Tecnológicos se centra en:

- Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados.
- Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.
- Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.

3.5.5.1. Comunicación del Riesgo.

Para conocer sobre las acciones propuestas dentro del portafolio de riesgos es importante un enfoque especial en el área de comunicación, ya que la información acerca de los riesgos se debe intercambiar y/o compartir entre quienes toman las decisiones y las partes involucradas.

La comunicación del riesgo busca lograr un acuerdo sobre la forma de gestionar los riesgos al intercambiar y/o compartir la información. La información incluye datos de la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos y otros que sean pertinentes. La comunicación del riesgo busca:

- Proporcionar seguridad del resultado de la gestión del riesgo de la institución.
- Recolectar información del riesgo.
- Compartir los resultados de la valoración del riesgo y presentar el plan para el tratamiento del riesgo.

- Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas de seguridad de la información debido a la falta de entendimiento entre quienes toman las decisiones y las partes involucradas.
- Brindar soporte para la toma de decisiones.
- Obtener conocimientos nuevos sobre la seguridad de la información.
- Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente.
- Dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos.
- Mejorar la toma de conciencia.

La coordinación para la toma de decisiones se puede lograr a través de una Comité de Seguridad de la Información (CSI) en el cual pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación.

3.5.5.2. Monitoreo y Revisión del Riesgo.

Para este apartado es importante considerar que los riesgos no son estáticos. Las amenazas, vulnerabilidades, probabilidad o consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar estos cambios, la institución debe garantizar el monitoreo continuo de los siguientes aspectos:

- Activos nuevos que se han incluido en el alcance de la gestión del riesgo.
- Modificaciones necesarias de los valores de los activos, por ejemplo, debido a cambios en los requisitos del negocio.
- Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no se han valorado.
- Probabilidad de que nuevas vulnerabilidades o el incremento en las vulnerabilidades existentes permitan que las amenazas las exploten.
- Vulnerabilidades identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a surgir.
- El incremento en el impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo.
- Incidentes de la seguridad de la información.

El monitoreo y revisión del riesgo se aborda en el plan de seguimiento y monitoreo propuesto en el presente estudio.

3.5.6. Actividad Esencial APO 12.06 Responder al Riesgo

Finalmente la matriz guía para la Implementación de Buenas prácticas Basadas en COBIT 2019 según el dominio APO 12 (Alinear, Planificar y Organizar) – Gestión de Riesgos Tecnológicos considera la práctica de "*Responder al riesgo*", se considera un componente crucial del marco de seguridad ya que luego del análisis del riesgo se enfoca en establecer un proceso efectivo respuesta de incidentes de la seguridad de la información que permita proteger los activos de información de la institución y minimizar el impacto de las brechas de seguridad. A continuación, se detallan las actividades propuestas por la metodología COBIT 2019:

- Establecer un equipo de respuesta a incidentes que debe estar compuesto por personal con habilidades y experiencias en el manejo de incidentes de seguridad que tenga roles y responsabilidades definidas con la asignación de recursos necesarios para llevar dichas funciones.
- Definición del proceso de incidentes debidamente documentados que incluya pasos para la detección, análisis contención, erradicación y recuperación de incidentes.
- Implementar controles de seguridad técnicos y organizativos para prevenir, detectar incidentes de seguridad.
- Revisión de controles de seguridad periódica y pruebas para garantizar la eficiencia.
- Capacitación y sensibilización al personal sobre seguridad de la información, importancia de reportar incidentes de seguridad de la información y la realización de simulacros para probar la eficacia del proceso de respuesta frente al incidente.
- Finalmente, la revisión y actualización constante sobre las últimas amenazas y vulnerabilidades de la seguridad de la información.

3.5.7. Actividad Esencial APO 12.07 Plan de Implementación del Marco de Seguridad

Una vez construido el Marco de Seguridad para el proceso de titulación de la UITEY, el plan de implementación considerará estrategias de implementación, tiempos, responsables y presupuestos considerando el primer año de ejecución.

3.6. Evaluación de la Percepción sobre la Existencia de un Marco de Seguridad de la Información en el proceso de Titulación de la UITEY.

La evaluación propuesta busca recabar información de la percepción de los actores involucrados en el proceso de titulación, sobre la existencia de un marco de seguridad de la información y/o la necesidad de su implementación.

Para esta evaluación se propone la aplicación de una encuesta dirigida a un grupo muestra de los actores involucrados, conformado por el personal docente y administrativo vinculado con el proceso de titulación de la UITEY.

3.6.1. Validación del Instrumento de Investigación por el Juicio de Expertos

La validación del instrumento de investigación determina la capacidad de los cuestionarios para medir las cualidades para lo cual fueron construidos, esta validación se realizó mediante la revisión y observaciones de dos expertos en seguridad de la información, a través de un formulario, donde se plasmó cada uno de sus criterios los cuales se incluyen en la sección de anexos.

CAPITULO IV

RESULTADOS

La presente investigación plantea un enfoque cualitativo, emplea un método analítico-sintético e inductivo, y es de tipo aplicada; los resultados obtenidos se presentan en este capítulo.

4.1 Marco de Seguridad de la Información para el proceso de titulación de la Universidad Yachay Tech

El Marco de Seguridad propuesto está basado en el Dominio APO12 de COBIT 2019, el cual determinan las siguientes prácticas:

4.1.1. Recopilación de Datos

Para establecer la situación actual en la seguridad de la información del proceso de titulación de la UITEY fue necesario recolectar toda la documentación relevante relacionada, como: políticas de seguridad, procedimientos, informes de auditoría previos, registros de incidentes, y acercamientos con personal clave de las áreas de tecnologías, infraestructura, dirección académica y planificación.

De la información recopilada se logra determinar que el proceso de titulación de la UITEY no cuenta con un marco de seguridad de la información, pero si cuenta con algunos controles implementados.

4.1.1.1. Contexto Interno.

Actualmente, la Universidad de Investigación Experimental Yachay carece de un marco formal de seguridad de la información. A pesar de la importancia crucial de proteger los activos de información críticos, no existe una estructura organizativa dedicada específicamente a la gestión de la seguridad de la información. La falta de un marco de seguridad documentado expone a la institución a diversas amenazas y vulnerabilidades que podrían comprometer la confidencialidad, integridad y disponibilidad de los datos.

Además, la universidad no cuenta con un comité de seguridad de la información que supervise y coordine las actividades relacionadas con la seguridad de la información, lo que dificulta la identificación y respuesta efectiva a los riesgos de seguridad, así como la implementación de controles y mejores prácticas para proteger los activos de información.

A pesar de las falencias encontradas en la estructura de seguridad de la información, la UITEY ha implementado algunos controles. Estos controles incluyen medidas básicas, como el acceso restringido a los sistemas de información que contienen datos de los estudiantes, la implementación de contraseñas seguras y la realización de copias de seguridad periódicas de los datos. Con estas medidas se busca responder a la normativa interna de la Universidad, como sus políticas, reglamento y directrices que abordan aspectos relacionados con la calidad y de manera implícita con la seguridad de la información.

Sin embargo, estos controles no son suficientes para abordar de manera integral los riesgos de seguridad asociados con el proceso de titulación. La falta de un marco de seguridad formal y un comité de seguridad de la información dificulta la evaluación y mejora continua de los controles de seguridad existentes, así como la implementación de nuevos controles que sean necesarios para proteger los activos de información de manera efectiva.

4.1.1.2. Contexto Externo.

La Universidad de Investigación y Tecnología Experimental Yachay presenta desafíos en materia de seguridad de la información, especialmente en relación con la protección de datos personales y el cumplimiento de la normativa interna y externa.

La presente investigación busca responder al mandato constitucional que reconoce el derecho fundamental a la privacidad y a la protección de datos personales; por lo que la universidad es legalmente responsable de garantizar la confidencialidad y seguridad de la información personal de sus estudiantes, docentes y personal administrativo. Para ello también se considera la Ley de Protección de Datos Personales, la cual establece obligaciones y requisitos específicos para el tratamiento de datos personales, incluyendo la necesidad de obtener el consentimiento de los titulares de los datos, implementar medidas de seguridad adecuadas y notificar las brechas de seguridad en caso de que ocurran.

También, la Universidad responde a los lineamientos de gestión normativos establecidos en la Ley Orgánica de Educación Superior (Ley Orgánica de Educación Superior, 2010) . En el contexto de seguridad de la información, la LOES exige a las universidades implementar medidas de protección adecuadas para salvaguardar la calidad e integridad de la información institucional.

Además, para el desarrollo de la propuesta se consideran Buenas Prácticas de Seguridad de la Información catalogadas en estándares internacionales y nacionales como ISO/IEC 27000, 31000 y norma 410-10 de la Contraloría General del Estado.

4.1.2. Análisis de Riesgos

Dentro del análisis de riesgos considerado para el proceso de titulación se han considerado las siguientes actividades.

4.1.2.1. Identificación de Activos.

Se realizó la identificación de los principales activos que intervienen en el proceso de titulación, obteniendo un total de 10, de los cuales uno es primario y nueve de soporte; además se determina su ubicación y el responsable según se indica en la siguiente tabla.

Tabla 8 ***Identificación de Activos de Información***

Nro. Activo	Clase de Activo	Tipo Activo	Nombre del Activo	Descripción del activo	Ubicación	Responsable
A1	**Soporte**	**Hardware**	Controladora Wireless, puntos de acceso	Puntos de acceso inalámbrico en toda la institución	Campus Universitario	Dirección TIC Infraestructura
A2	**Soporte**	**Hardware**	Firewall	Control de acceso y permisos de seguridad perimetral para la red institucional	Data Center	Dirección TIC Infraestructura
A3	**Soporte**	**Redes**	Infraestructura de Red y Comunicaciones	Servidores de correo electrónico. Servidores de almacenamiento de archivos. Redes locales y acceso a internet	Data Center	Dirección TIC Infraestructura
A4	**Soporte**	**Redes**	Switchs de Acceso	Procesamiento de trafico de red de acceso en cada piso del edificio	Data Center	Dirección TIC Infraestructura
A5	**Soporte**	**Software**	Sistemas de Gestión Académica	Plataformas de gestión de estudiantes y programas académicos. Sistema de registro de tesis y trabajos de investigación.	Data Center	Dirección TIC Desarrollo
A6	**Soporte**	**Software**	Plataformas de Aprendizaje en Línea	Entorno Virtual de Aprendizaje EVA	Data Center	Dirección TIC Soporte
A7	**Soporte**	**Localidad**	Data center	Centro de Datos Institucional	Campus Universitario	Infraestructura
A8	**Soporte**	**Personal**	Personal Académico y Administrativo	Profesores, tutores y personal docente. Personal administrativo y de apoyo.	Campus Universitario	Rectorado UITEY

Nro. Activo	Clase de Activo	Tipo Activo	Nombre del Activo	Descripción del activo	Ubicación	Responsable
A9	**Soporte**	**Personal**	Personal de desarrollo de sistemas	Personal técnico que desarrolla aplicaciones o automatiza procesos	Campus Universitario	Dirección TIC
A10	**Primario**	**Información**	Bases de información personal y académica	Datos Personales Datos Académicos	Data Center	Dirección TIC

Fuente: Elaboración Propia

Cada uno de los activos ha sido valorado en términos de confidencialidad, integridad y disponibilidad, las ponderaciones obtenidas se detallan en la siguiente tabla.

Tabla 9 ***Valoración de Activos de Información***

Nro. Activo	Clase de Activo	Tipo Activo	Nombre de Activo	Valoración impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	**I**	**D**	**VA**
A1	Soporte	Hardware	Controladora Wireless, puntos de acceso	1	1	3	1,67
A2	Soporte	Hardware	Firewall	2	2	3	2,33
A3	Soporte	Redes	Infraestructura de Red y Comunicaciones	1	1	3	1,67
A4	Soporte	Redes	Switchs de Acceso	2	2	2	2,00
A5	Soporte	Software	Sistemas de Gestión Académica	1	2	3	2,00
A6	Soporte	Software	Plataformas de Aprendizaje en Línea	1	1	3	1,67
A7	Soporte	Localidad	Datacenter	1	1	3	1,67
A8	Soporte	Personal	Personal Académico y Administrativo	1	1	3	1,67

Nro. Activo	Clase de Activo	Tipo Activo	Nombre de Activo	Valoración impacto (pérdida) C: Confidencialidad I: Integridad D: Disponibilidad			
				C	I	D	VA
A9	Soporte	Personal	Personal de desarrollo de sistemas	1	1	3	1,67
A10	Primario	Información	Bases de información personal y académica	3	2	3	2,67

Fuente: Elaboración Propia

4.1.2.2. Identificación de Amenazas y Vulnerabilidades.

Una vez identificados y valorados los activos, se han detallado las tres principales amenazas y vulnerabilidades que podrían afectar la seguridad de la información de los activos del proceso de titulación de la UITEY, estas amenazas podrían comprometer la seguridad de los activos de información y poner en riesgo la reputación y la operación del proceso. Del análisis se han identificado un total de 30 amenazas y 30 vulnerabilidades que serán parte del estudio.

Tabla 10 ***Identificación de Amenazas y Vulnerabilidades***

Nro. Activo	Nombre de Activo	Amenaza	Vulnerabilidad	Responsable
A1	Controladora Wireless, puntos de acceso	Abuso de privilegios de acceso	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	DTIC Unidad Infraestructura
		Daños por agua	Ubicación en un área susceptible de inundación	DTIC Unidad Redes y Comunicaciones
		Condiciones inadecuadas de temperatura o humedad	Susceptibilidad a las variaciones de temperatura	
A2	Firewall	Fuego	Susceptibilidad a las variaciones de temperatura	DTIC Unidad Infraestructura
		Contaminación electromagnética	Susceptibilidad a las variaciones de voltaje	DTIC Unidad Redes y Comunicaciones
		Contaminación mecánica	Susceptibilidad a la humedad, el polvo y la suciedad.	

Nro. Activo	Nombre de Activo	Amenaza	Vulnerabilidad	Responsable
A3	Infraestructura de Red y Comunicaciones	Manipulación de la configuración	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	DTIC Unidad Infraestructura
		Fallo de servicios de comunicaciones	Arquitectura insegura de la red	DTIC Unidad Redes y Comunicaciones
		Errores del administrador	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	
A4	Switchs de Acceso	Errores de [re-]encaminamiento	Falta de capacitación al personal	DTIC Unidad Redes y Comunicaciones
		Denegación de servicio	Líneas de comunicación sin protección	
		Fugas de información	Tráfico sensible sin protección	
A5	Sistemas de Gestión Académica	Divulgación de información	Habilitación de servicios innecesarios	DTIC Unidad Desarrollo
		Errores de los usuarios	Descarga y usos no controlados de software	
		Avería de origen físico o lógico	Defectos bien conocidos en el software	
A6	Plataformas de Aprendizaje en Línea	Errores de los usuarios	Uso de contraseñas débiles o reutilizadas:	DTIC Unidad Soporte
		Avería de origen físico o lógico	Configuración incorrecta de parámetros	
		Manipulación de programas	Descarga y usos no controlados de software	
A7	Data Center	Fuego	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	DTIC Unidad Infraestructura
		Daños por agua	Ubicación en un área susceptible de inundación	
		Fenómeno sísmico	Ausencia de procedimiento de control de cambios	
A8	Personal Académico y Administrativo	Ingeniería social (picaresca)	Uso incorrecto de software y hardware	Rectorado UITEY

Nro. Activo	Nombre de Activo	Amenaza	Vulnerabilidad	Responsable
		Deficiencias en la organización	Ausencia de reportes de fallas en los registros de administradores y operadores	
		Indisponibilidad del personal	Ausencia del personal	
A9	Personal de desarrollo de sistemas	Fugas de información	Ausencia de protección física de la edificación, puertas y ventanas	DTIC Unidad Desarrollo
		Indisponibilidad del personal	Ausencia del personal	
		Extorsión	Habilitación de servicios innecesarios	
A10	Bases de información personal y académica	Errores del administrador	Procedimientos inadecuados de contratación	DTIC Unidad Infraestructura
		Alteración accidental de la información	Falta de conciencia acerca de la seguridad	
		Destrucción de información	Uso incorrecto de software y hardware	

Fuente: Elaboración Propia

4.1.2.3. Identificación de la Existencia de Controles.

Como parte de la evaluación interna del estado de la seguridad de la información en el proceso de titulación se identificó la existencia de controles sobre los activos de la información para cada una de las amenazas y vulnerabilidades identificadas en el análisis, estos datos se obtuvieron a través de métodos como la observación y revisión de documentación.

Así también en base de la metodología se ha dado una ponderación de entre bajo (1), medio (2) y alto (3) al nivel de amenaza y vulnerabilidad en función de su probabilidad de ocurrencia; estos datos serán insumos básicos para el cálculo de evaluación del riesgo.

Se verifica que actualmente existen controles implementados para cada amenaza y vulnerabilidad identificadas para los activos del proceso de titulación, sin embargo, estos controles no responden a en su totalidad a los requerimientos de seguridad de la información del proceso.

Tabla 11 ***Identificación de Controles Existentes***

Nro. Activo	Tipo Activo	Amenaza	Vulnerabilidad	Nivel Am.	Nivel Vul.	Controles implementados existentes
A1	**Hardware**	Abuso de privilegios de acceso	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	2	3	Segregación de Funciones
		Daños por agua	Ubicación en un área susceptible de inundación	1	1	Monitoreo de Infraestructura Física
		Condiciones inadecuadas de temperatura o humedad	Susceptibilidad a las variaciones de temperatura	1	2	Sistemas de Control de Climatización Redundantes
A2	**Hardware**	Fuego	Susceptibilidad a las variaciones de temperatura	2	1	Sistemas de Detección y Extinción de Incendios
		Contaminación electromagnética	Susceptibilidad a las variaciones de voltaje	2	1	NA
		Contaminación mecánica	Susceptibilidad a la humedad, el polvo y la suciedad.	1	1	Mantenimiento regular
A3	**Redes**	Manipulación de la configuración	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	3	3	Restricción de acceso
		Fallo de servicios de comunicaciones	Arquitectura insegura de la red	2	3	Monitoreo de red
		Errores del administrador	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	2	3	Separación de funciones
A4	**Redes**	Errores de [re-]encaminamiento	Falta de capacitación al personal	2	3	Monitoreo continuo de la red
		Denegación de servicio	Líneas de comunicación sin protección	2	2	Firewalls y sistemas de filtrado de paquetes
		Fugas de información	Tráfico sensible sin protección	2	2	Control de Accesos
A5	**Software**	Divulgación de información	Habilitación de servicios innecesarios	2	2	Control de acceso
		Errores de los usuarios	Descarga y usos no controlados de software	2	2	Actualizaciones y parches automáticos

Nro. Activo	Tipo Activo	Amenaza	Vulnerabilidad	Nivel Am.	Nivel Vul.	Controles implementados existentes
		Avería de origen físico o lógico	Defectos bien conocidos en el software	1	2	Seguimiento y actualizaciones de proveedores
A6	**Software**	Errores de los usuarios	Uso de contraseñas débiles o reutilizadas:	1	2	Entrenamiento y concientización del usuario
		Avería de origen físico o lógico	Configuración incorrecta de parámetros	2	2	Control de acceso a la configuración
		Manipulación de programas	Descarga y usos no controlados de software	1	3	Documentación detallada
A7	**Localidad**	Fuego	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	1	2	Sistemas de detección y extinción de incendios
		Daños por agua	Ubicación en un área susceptible de inundación	1	1	Respaldo de datos fuera del sitio
		Fenómeno sísmico	Ausencia de procedimiento de control de cambios	1	3	Seguro de propiedad
A8	**Personal**	Ingeniería social (picaresca)	Uso incorrecto de software y hardware	1	2	Control de acceso basado en roles
		Deficiencias en la organización	Ausencia de reportes de fallas en los registros de administradores y operadores	2	3	Asignación adecuada de recursos
		Indisponibilidad del personal	Ausencia del personal	2	3	Cruzamiento de habilidades y conocimientos
A9	**Personal**	Fugas de información	Ausencia de protección física de la edificación, puertas y ventanas	1	2	Cifrado de datos
		Indisponibilidad del personal	Ausencia del personal	2	3	Rotación de tareas
		Extorsión	Habilitación de servicios innecesarios	1	2	Análisis de necesidades
A10	**Información**	Errores del administrador	Procedimientos inadecuados de contratación	1	2	Segregación de funciones
		Alteración accidental de la información	Falta de conciencia acerca de la seguridad	1	3	Controles de acceso y permisos
		Destrucción de información	Uso incorrecto de software y hardware	1	3	Restricción de privilegios de administrado

Fuente: Elaboración Propia

4.1.2.4. Evaluación del Riesgo.

En los ítems anteriores se han obtenido los insumos básicos para el cálculo de la evaluación de riesgos, en la siguiente tabla se indican los datos obtenidos para el cálculo del nivel de riesgo, que corresponde al producto entre la valoración CID de los activos, nivel de amenaza y nivel de vulnerabilidad.

Del cálculo de la evaluación de riesgo se obtiene el nivel de riesgo, definido como bajo cuando el producto de las variables es de 1 a 3, medio cuando el producto de las variables es de 4 a 8 y alto cuando el producto de las variables es de 9 a 27.

Una vez realizado el cálculo de riesgo se determina que ningún riesgo es de nivel alto, 15 riesgos son de nivel medio y 15 riesgos son de nivel bajo; con estos datos se podrá definir el método de tratamiento de los riesgos identificados.

Tabla 12 ***Evaluación de riesgos***

Análisis de Riesgos				**Evaluación del Riesgo**				
Nro. Activo	**Amenaza**	**Vulnerabilidad**	**VA CID**	**Nivel Am.**	**Nivel Vul.**	**Controles implementados existentes**	**Cálculo de Riesgo**	**Nivel de Riesgo**
A1	Abuso de privilegios de acceso	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	1,7	2	3	Segregación de Funciones	10	MEDIO
	Daños por agua	Ubicación en un área susceptible de inundación		1	1	Monitoreo de Infraestructura Física	1,7	BAJO
	Condiciones inadecuadas de temperatura o humedad	Susceptibilidad a las variaciones de temperatura		1	1	Sistemas de Control de Climatización Redundantes	3.3	BAJO
A2	Fuego	Susceptibilidad a las variaciones de temperatura	2,3	2	1	Sistemas de Detección y Extinción de Incendios	4,7	MEDIO
	Contaminación electromagnética	Susceptibilidad a las variaciones de voltaje		2	1	Protección de equipos críticos	4,7	MEDIO
	Contaminación mecánica	Susceptibilidad a la humedad, el polvo y la suciedad.		1	1	Mantenimiento regular	2,3	BAJO
A3	Manipulación de la configuración	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	1,7	3	3	Restricción de acceso	18	MEDIO
	Fallo de servicios de	Arquitectura insegura de la red		2	3	Monitoreo de red	12	MEDIO

Análisis de Riesgos				Evaluación del Riesgo				
Nro. Activo	**Amenaza**	**Vulnerabilidad**	**VA CID**	**Nivel Am.**	**Nivel Vul.**	**Controles implementados existentes**	**Cálculo de Riesgo**	**Nivel de Riesgo**
	comunicaciones							
	Errores del administrador	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)		2	3	Separación de funciones	12	MEDIO
A4	Errores de [re-]encaminamiento	Falta de capacitación al personal	2,0	2	3	Monitoreo continuo de la red	12	MEDIO
	Denegación de servicio	Líneas de comunicación sin protección		2	2	Firewalls y sistemas de filtrado de paquetes	8	MEDIO
	Fugas de información	Tráfico sensible sin protección		2	2	Control de Accesos	8	MEDIO
A5	Divulgación de información	Habilitación de servicios innecesarios	2,0	2	3	Control de acceso	12	MEDIO
	Errores de los usuarios	Descarga y uso no controlado de software		2	3	Actualizaciones y parches automáticos	12	MEDIO
	Avería de origen físico o lógico	Defectos bien conocidos en el software		1	2	Seguimiento y actualizaciones de proveedores	4	MEDIO
A6	Errores de los usuarios	Uso de contraseñas débiles o reutilizadas:	1,7	1	2	Entrenamiento y concientización del usuario	3.3	BAJO
	Avería de origen físico o lógico	Configuración incorrecta de parámetros		2	2	Control de acceso a la configuración	6,7	MEDIO
	Manipulación de programas	Descarga y usos no controlados de software		1	3	Documentación detallada	5	BAJO
A7	Fuego	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	1,7	1	2	Sistemas de detección y extinción de incendios	4	BAJO
	Daños por agua	Ubicación en un área susceptible de inundación		1	1	Respaldo de datos fuera del sitio	2	BAJO
	Fenómeno sísmico	Ausencia de procedimiento de control de cambios		1	3	Seguro de propiedad	6	BAJO
A8	Ingeniería social (picaresca)	Uso incorrecto de software y hardware	1,7	1	2	Control de acceso basado en roles	3,3	BAJO

Análisis de Riesgos				Evaluación del Riesgo				
Nro. Activo	**Amenaza**	**Vulnerabilidad**	**VA CID**	**Nivel Am.**	**Nivel Vul.**	**Controles implementados existentes**	**Cálculo de Riesgo**	**Nivel de Riesgo**
	Deficiencias en la organización	Ausencia de reportes de fallas en los registros de administradores y operadores		2	3	Asignación adecuada de recursos	10	MEDIO
	Indisponibilidad del personal	Ausencia del personal		2	3	Cruzamiento de habilidades y conocimientos	10	MEDIO
A9	Fugas de información	Ausencia de protección física de la edificación, puertas y ventanas	1,7	1	2	Cifrado de datos	3,3	BAJO
	Indisponibilidad del personal	Ausencia del personal		2	3	Rotación de tareas	3.3	BAJO
	Extorsión	Habilitación de servicios innecesarios		1	2	Análisis de necesidades	3,3	BAJO
A10	Errores del administrador	Procedimientos inadecuados de contratación	2,7	1	2	Segregación de funciones	5,3	BAJO
	Alteración accidental de la información	Falta de conciencia acerca de la seguridad		1	3	Controles de acceso y permisos	8	BAJO
	Destrucción de información	Uso incorrecto de software y hardware		1	3	Restricción de privilegios de administrado	8	BAJO

Fuente: Elaboración Propia

4.1.3. Mantener Perfil del Riesgo

Mantener el riesgo dentro del marco de seguridad propuesto para la Universidad de Investigación Experimental Yachay (UITEY) en el proceso de titulación podría tener varias implicaciones y resultados:

- Identificación y Evaluación Controlada: Al optar por mantener ciertos riesgos dentro del marco de seguridad, la UITEY puede decidir no implementar controles adicionales o medidas de mitigación para abordar esos riesgos específicos. En su lugar, la institución puede optar por monitorear estos riesgos de cerca y evaluar su impacto de manera regular para tomar decisiones informadas sobre cómo manejarlos en el futuro.
- Reducción de Costos y Recursos: Mantener ciertos riesgos puede ayudar a evitar la inversión de recursos significativos en la implementación de controles

adicionales. Esto puede ser especialmente beneficioso si la evaluación de riesgos determina que el costo de mitigar el riesgo supera los posibles daños o pérdidas que podrían resultar de su materialización.

- Gestión de Riesgos Aceptable: La decisión de mantener ciertos riesgos puede reflejar una evaluación cuidadosa de los riesgos en relación con los objetivos y las capacidades de la UITEY. Si los riesgos son considerados aceptables y consistentes con la tolerancia al riesgo de la institución, mantenerlos puede ser una estrategia viable para gestionarlos.
- Foco en Mitigación Selectiva: Al mantener ciertos riesgos, la UITEY puede optar por enfocar sus recursos en la mitigación de riesgos que son considerados de mayor prioridad o que tienen un impacto potencial más significativo en el proceso de titulación. Esto puede ayudar a optimizar el uso de recursos y a garantizar que los esfuerzos de seguridad estén dirigidos a áreas donde son más necesarios.
- Transparencia y Responsabilidad: Es importante que la UITEY sea transparente acerca de los riesgos que ha decidido mantener y las razones detrás de esa decisión. Esto ayuda a garantizar la responsabilidad y la rendición de cuentas en la gestión de riesgos y permite a todas las partes interesadas comprender mejor los riesgos asociados con el proceso de titulación.

En resumen, mantener el riesgo dentro del marco de seguridad propuesto para la UITEY en el proceso de titulación puede ser una estrategia válida dependiendo de la evaluación de riesgos y los objetivos de la institución. Sin embargo, es importante realizar un seguimiento continuo de estos riesgos y estar preparado para revisar y ajustar la estrategia de gestión de riesgos según sea necesario en el futuro.

4.1.4. Articulación del Riesgo

Para poder desarrollar la práctica de gestión de articulación de riesgo fue necesario realizar las siguientes actividades:

Identificación de partes interesadas relevantes dentro de la institución que debe estar involucrada en la gestión de riesgos de seguridad de la información.

En la siguiente tabla se proporciona una visión general de las partes interesadas relevantes y sus roles/responsabilidades en la gestión de riesgos de seguridad de la información para el proceso de titulación. Es importante involucrar a todas estas partes

interesadas en el proceso para garantizar una gestión integral y efectiva de los riesgos de seguridad de la información y a su vez contribuir con la toma de decisiones.

Tabla 13 ***Identificación de partes interesadas roles y responsabilidades***

Identificación de partes interesadas con sus roles y responsabilidades

Partes Interesadas	Descripción del Rol/Responsabilidades
Dirección Ejecutiva (Rectorado)	Proporcionar dirección estratégica y apoyo financiero para la gestión de riesgos de seguridad de la información.
Equipo de TI (Departamento TIC´s)	Responsable de implementar y mantener controles de seguridad de la información, y de monitorear la infraestructura tecnológica.
Personal de Administración (Escuelas y Decanatos)	Encargado de la gestión y administración de los sistemas de información utilizados en el proceso de titulación.
Personal Académico (Dirección General de Servicios Académicos)	Responsable de la administración y seguridad de los datos académicos y de titulación de los estudiantes.
Personal de Recursos Humanos (Dirección General de Talento Humano)	Encargado de gestionar el acceso y la seguridad de la información del personal involucrado en el proceso de titulación.
Estudiantes (Estudiantes que ingresan a la Unidad Organizacional de Titulación)	Usuarios finales cuya información personal y académica está sujeta a protección y seguridad durante el proceso de titulación.
Personal de Seguridad (Comité de Seguridad de la Información)	Equipo encargado de supervisar y aplicar políticas de seguridad de la información, así como de coordinar actividades de respuesta a incidentes.
Auditores Internos (Departamento de Aseguramiento de la Calidad)	Encargados de realizar auditorías regulares de seguridad para evaluar el cumplimiento de políticas y controles de seguridad.
Proveedores de Servicios Externos	Entidades externas que prestan servicios relacionados con el proceso de titulación y

Identificación de partes interesadas con sus roles y responsabilidades	
Partes Interesadas	**Descripción del Rol/Responsabilidades**
	cuyos sistemas y datos pueden representar riesgos de seguridad.
Reguladores y Organismos de Conformidad	Entidades externas que establecen normativas y estándares de seguridad de la información a los que la institución debe cumplir.

Fuente: Elaboración Propia

Determinado las partes interesadas e identificados el rol y las responsabilidades se puede definir la evaluación de los riesgos en función de la valoración de la vulnerabilidad que permita generar un plan de comunicación efectiva con cada una de las actividades de la gestión de riesgos para el proceso de titulación.

Para lograr una completa articulación de riesgos se diseñó un plan de tratamiento de acuerdo con la estrategia institucional, para lo cual se determinan cuatro opciones acordes a la Norma ISO 27005 de tratamiento del riesgo.

Tabla 14 ***Tratamiento del Riesgo***

ANÁLISIS DE RIESGOS			TRATAMIENTO DE RIESGOS							
Nro. Activo	**Amenazas**	**Vulnerabilidades (Vuln.)**	**Método de Tratamiento de Riesgo**	**Tipo de Control**	**Controles Por Implementar**	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálculo de Evaluación Riesgo con el Control Implementado**	**Nivel de Riesgo con el Control Implementado**	**Riesgo Residual**
	Abuso de privilegios de acceso	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Monitoreo de actividades de usuario	1	2	3,3	MEDIO	MITIGAR/EVITAR/TRANSFERIR
A1	Daños por agua	Ubicación en un área susceptible de inundación	ACEPTAR	CONTROL PREVENTIVO	Ubicación de Equipos y Respaldo de Datos	1	2	3,3	MEDIO	MITIGAR/EVITAR/TRANSFERIR
	Condiciones inadecuadas de temperatura o humedad	Susceptibilidad a las variaciones de temperatura	ACEPTAR	CONTROL PREVENTIVO	Respaldo y Recuperación de Datos	1	1	1,7	BAJO	ACEPTABLE
	Fuego	Susceptibilidad a las variaciones de temperatura	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Respaldo y Recuperación de Datos	1	2	4,7	MEDIO	MITIGAR/EVITAR/TRANSFERIR
A2	Contaminación electromagnética	Susceptibilidad a las variaciones de voltaje	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Pruebas y evaluaciones	1	1	2,3	BAJO	ACEPTABLE
	Contaminación mecánica	Susceptibilidad a la humedad, el polvo y la suciedad.	ACEPTAR	CONTROL PREVENTIVO	Formación y concienciación del personal	1	1	2,3	BAJO	ACEPTABLE

ANÁLISIS DE RIESGOS				TRATAMIENTO DE RIESGOS						
Nro. Activo	**Amenazas**	**Vulnerabilidades (Vuln.)**	**Método de Tratamiento de Riesgo**	**Tipo de Control**	**Controles Por Implementar**	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálculo de Evaluación Riesgo con el Control Implementado**	**Nivel de Riesgo con el Control Implementado**	**Riesgo Residual**
	Manipulación de la configuración	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Formación y concienciación del personal	1	2	4	MEDIO	MITIGAR/EVITAR/TRANSFERIR
A3	Fallo de servicios de comunicaciones	Arquitectura insegura de la red	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Redundancia de servicios	1	1	2	BAJO	ACEPTABLE
	Errores del administrador	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Pruebas y simulacros	1	2	4	MEDIO	MITIGAR/EVITAR/TRANSFERIR
	Errores de [re-]encaminamiento	Falta de capacitación al personal	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Pruebas de redundancia y conmutación por error	1	1	2	BAJO	ACEPTABLE
A4	Denegación de servicio	Líneas de comunicación sin protección	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Plan de respuesta a incidentes	1	1	2	BAJO	ACEPTABLE
	Fugas de información	Tráfico sensible sin protección	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Clasificación de datos	1	1	2	BAJO	ACEPTABLE

ANÁLISIS DE RIESGOS				TRATAMIENTO DE RIESGOS						
Nro. Activo	**Amenazas**	**Vulnerabilidades (Vuln.)**	**Método de Tratamiento de Riesgo**	**Tipo de Control**	**Controles Por Implementar**	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálculo de Evaluación Riesgo con el Control Implementado**	**Nivel de Riesgo con el Control Implementado**	**Riesgo Residual**
	Divulgación de información	Habilitación de servicios innecesarios	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Respuesta ante incidentes	1	1	2	BAJO	ACEPTABLE
A5	Errores de los usuarios	Descarga y usos no controlados de software	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Supervisión y auditoría de actividades de usuario	1	2	4	MEDIO	MITIGAR/EVITAR/TRANSFERIR
	Avería de origen físico o lógico	Defectos bien conocidos en el software	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Control de acceso y privilegios	1	1	2	BAJO	ACEPTABLE
	Errores de los usuarios	Uso de contraseñas débiles o reutilizadas:	ACEPTAR	CONTROL PREVENTIVO	Autenticación multifactorial	1	1	1,7	BAJO	ACEPTABLE
A6	Avería de origen físico o lógico	Configuración incorrecta de parámetros	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Auditorías de configuración	1	1	1,7	BAJO	ACEPTABLE
	Manipulación de programas	Descarga y uso no controlados de software	ACEPTAR	CONTROL PREVENTIVO	Pruebas de penetración	1	1	1,7	BAJO	ACEPTABLE
A7	Fuego	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	ACEPTAR	CONTROL PREVENTIVO	Plan de evacuación y entrenamiento	1	1	2	BAJO	ACEPTABLE

	ANÁLISIS DE RIESGOS			TRATAMIENTO DE RIESGOS						
Nro. Activo	**Amenazas**	**Vulnerabilidades (Vuln.)**	**Método de Tratamiento de Riesgo**	**Tipo de Control**	**Controles Por Implementar**	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálculo de Evaluación Riesgo con el Control Implementado**	**Nivel de Riesgo con el Control Implementado**	**Riesgo Residual**
	Daños por agua	Ubicación en un área susceptible de inundación	ACEPTAR	CONTROL PREVENTIVO	Elevación de equipos críticos	1	1	2	BAJO	ACEPTABLE
	Fenómeno sísmico	Ausencia de procedimiento de control de cambios	ACEPTAR	CONTROL PREVENTIVO	Respaldo de datos fuera del sitio	1	1	2	BAJO	ACEPTABLE
	Ingeniería social (picaresca)	Uso incorrecto de software y hardware	ACEPTAR	CONTROL PREVENTIVO	Monitorización de la actividad de usuario	1	1	2	MEDIO	MITIGAR/EVITAR/TRANSFERIR
A8	Deficiencias en la organización	Ausencia de reportes de fallas en los registros de administradores y operadores	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Gobierno de seguridad de la información	1	2	3,3	MEDIO	MITIGAR/EVITAR/TRANSFERIR
	Indisponibilidad del personal	Ausencia del personal	MITIGAR/EVITAR/ TRASNFERIR	CONTROL PREVENTIVO	Documentación detallada de procedimientos	1	2	3,3	MEDIO	MITIGAR/EVITAR/TRANSFERIR
	Fugas de información	Ausencia de protección física de la edificación, puertas y ventanas	ACEPTAR	CONTROL PREVENTIVO	Concientización y capacitación del personal	1	1	1,7	BAJO	ACEPTABLE
A9	Indisponibilidad del personal	Ausencia del personal	ACEPTAR	CONTROL PREVENTIVO	Capacitación continua	1	1	1,7	BAJO	ACEPTABLE
	Extorsión	Habilitación de servicios innecesarios	ACEPTAR	CONTROL PREVENTIVO	Auditorías de seguridad regulares	1	1	1,7	BAJO	ACEPTABLE

	ANÁLISIS DE RIESGOS			TRATAMIENTO DE RIESGOS						
Nro. Activo	**Amenazas**	**Vulnerabilidades (Vuln.)**	**Método de Tratamiento de Riesgo**	**Tipo de Control**	**Controles Por Implementar**	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálculo de Evaluación Riesgo con el Control Implementado**	**Nivel de Riesgo con el Control Implementado**	**Riesgo Residual**
A10	Errores del administrador	Procedimientos inadecuados de contratación	ACEPTAR	CONTROL PREVENTIVO	Auditorías y revisiones regulares	1	1	2,7	BAJO	ACEPTABLE
	Alteración accidental de la información	Falta de conciencia acerca de la seguridad	ACEPTAR	CONTROL PREVENTIVO	Copias de seguridad regulares	1	2	5,3	MEDIO	MITIGAR/EVITAR/TRANSFERIR
	Destrucción de información	Uso incorrecto de software y hardware	ACEPTAR	CONTROL PREVENTIVO	Monitoreo de la actividad de usuario	1	1	2,7	BAJO	ACEPTABLE

Fuente: Elaboración Propia

4.1.5. Mantener un Portafolio de Acciones para la Gestión del Riesgo

Mantener un portafolio de acciones nos permite definir de mejor manera los controles sobre los activos de información a implementar lo que permitirá clasificar de mejor manera las medidas y estrategias que permitan mitigar, controlar o gestionar los riesgos de la seguridad de la información de manera efectiva. A continuación, se detallan las acciones definidas para el presente marco de seguridad.

Tabla 15 ***Portafolio acciones gestión del riesgo***

Acción	Descripción
Análisis y Evaluación de Riesgos	Realizar evaluaciones periódicas de riesgos para identificar amenazas y vulnerabilidades.
Pruebas y evaluaciones	Garantizar la eficacia de los controles de seguridad, identificar vulnerabilidades y evaluar el cumplimiento de los requisitos de seguridad.
Formación y concienciación del personal	Proporcionar entrenamiento regular sobre seguridad de la información a empleados y usuarios.
Planificación de la Continuidad del Negocio	Desarrollar planes para garantizar la continuidad de las operaciones en caso de interrupciones.
Gestión de Proveedores	Evaluar y gestionar los riesgos asociados con proveedores externos de servicios y productos.
Monitoreo y Detección de Amenazas	Implementar sistemas de monitoreo para detectar y responder a actividades sospechosas.
Respuesta y Gestión de Incidentes	Establecer un proceso formal para responder y gestionar incidentes de seguridad de la información.
Auditorías de seguridad regulares	Realizar auditorías internas y externas para evaluar el cumplimiento de políticas de seguridad.
Actualización y Mantenimiento	Mantener actualizados los sistemas y controles de seguridad, incluyendo parches y actualizaciones.
Gobierno de seguridad de la información	Establecer/Revisar un marco de políticas, procesos, procedimientos y controles que una organización implementa para gestionar y proteger sus activos de información de manera efectiva.
Monitoreo de actividades de usuario	Registrar acciones realizadas por usuarios en redes y sistemas de información.
Respaldo y Recuperación de Datos	Gestionar copias de seguridad regular de los datos importantes y la implementación de medidas para restaurarlos en caso de pérdida o corrupción

Fuente: Elaboración Propia

4.1.6. Responder al Riesgo

Responder al riesgo dentro del marco de seguridad propuesto para la Universidad de Investigación Experimental Yachay (UITEY) en el proceso de titulación implica implementar medidas específicas para mitigar o reducir los riesgos identificados. Aquí hay algunos resultados potenciales de responder al riesgo:

Mejora de la Seguridad del Proceso de Titulación: Al responder proactivamente a los riesgos identificados, la UITEY puede fortalecer la seguridad del proceso de titulación. Esto puede incluir la implementación de controles técnicos, la mejora de las políticas y procedimientos, y la capacitación del personal para mitigar las amenazas y reducir la probabilidad de incidentes de seguridad.

Reducción del Impacto de los Riesgos: La implementación de medidas de respuesta al riesgo puede ayudar a reducir el impacto potencial de los riesgos en el proceso de titulación. Por ejemplo, la encriptación de datos sensibles puede reducir el riesgo de divulgación de información confidencial en caso de acceso no autorizado.

Cumplimiento Normativo y Legal: Responder al riesgo puede ayudar a la UITEY a cumplir con los requisitos legales y normativos relacionados con la seguridad de la información y la protección de datos. Esto puede incluir el cumplimiento de leyes y regulaciones locales e internacionales, así como estándares y mejores prácticas de la industria.

Aumento de la Confianza y la Reputación: La implementación de medidas de seguridad sólidas puede aumentar la confianza de los estudiantes, profesores y otras partes interesadas en la seguridad y la integridad del proceso de titulación de la UITEY. Esto puede contribuir a mejorar la reputación de la institución y fortalecer las relaciones con la comunidad académica y el público en general.

Reducción de Pérdidas Financieras y Reputacionales: Responder de manera efectiva a los riesgos puede ayudar a prevenir o minimizar posibles pérdidas financieras y daños a la reputación que podrían resultar de incidentes de seguridad. Esto puede incluir la prevención de fraudes, el robo de datos o la interrupción del proceso de titulación debido a problemas de seguridad.

En resumen, responder al riesgo dentro del marco de seguridad propuesto para la UITEY en el proceso de titulación puede tener una serie de beneficios, incluida la mejora de la seguridad, la integridad del proceso, el cumplimiento normativo, el aumento de la confianza y la reducción de pérdidas financieras y reputacionales. Es importante

implementar medidas de respuesta al riesgo de manera efectiva y continua para garantizar la protección adecuada de los activos de información y la continuidad de las operaciones.

4.2 Balance de Riesgo Inicial y Posterior a la Implementación del Marco de Seguridad.

Antes de la implementación del marco de seguridad, la infraestructura estaba expuesta a riesgos potenciales que podrían comprometer la confidencialidad, integridad y disponibilidad de los activos de la información. Sin embargo, al implementar el marco de seguridad se fortalecen las defensas, reduciendo la vulnerabilidad y asegurando la protección de los activos y la continuidad de las operaciones. En la siguiente tabla se realiza un análisis numérico comparativo del porcentaje de riesgo en la situación inicial y el porcentaje de riesgo una vez implementado el marco de seguridad.

Los valores descritos en la columna de Situación Inicial corresponden a los calculados en la Tabla 7 y 8 de la identificación de riesgos con su respectiva valoración en términos de los atributos de CID y la valoración de la amenaza y la vulnerabilidad-

Los valores indicados en la columna de Aplicación de Marco de Seguridad corresponden a la valoración de los activos que intervienen en el proceso de titulación con su valoración en términos de los atributos CID y la valoración del nivel de amenaza y vulnerabilidad, pero una vez implementados los controles.

Tabla 16 ***Porcentajes de Riesgo: Situación Inicial, Controles implementados y con Marco de seguridad.***

	SITUACIÓN INICIAL			APLICACIÓN MARCO SEGURIDAD			PORCENTAJES EVALUACIÓN DE RIESGOS	
COD	Nivel de Amenaza	Nivel de Vuln.	Cálc de Eval. Riesgo con el Control Implem.	Nivel de Amenaza	Nivel de Vuln.	Cálc de Eval. Riesgo con Marc. Seg	CONTROLES EXISTENTES	MARCO DE SEGURIDAD
A4.4.	2	3	10	1	2	3,3	67%	22%
N1.2.	1	1	2	1	2	2,8	11%	22%
I2.8.	1	2	3	1	1	5,6	22%	11%
I2.1.	2	1	5	1	2	10,9	22%	22%
I2.5.	2	1	5	1	1	10,9	22%	11%
I2.4.	1	1	2	1	1	5,4	11%	11%
A4.2.	3	3	18	1	2	36,0	100%	22%
I2.9.	2	3	12	1	1	24,0	67%	11%
E3.2.	2	3	12	1	2	24,0	67%	22%
E3.7.	2	3	12	1	2	24,0	67%	22%
A4.18.	2	2	8	1	1	16,0	44%	11%
E3.12.	2	2	8	1	1	16,0	44%	11%
A4.15.	2	3	12	1	1	24,0	67%	11%

SITUACIÓN INICIAL				APLICACIÓN MARCO SEGURIDAD			PORCENTAJES EVALUACIÓN DE RIESGOS	
COD	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálc de Eval. Riesgo con el Control Implem.**	**Nivel de Amenaza**	**Nivel de Vuln.**	**Cálc de Eval. Riesgo con Marc. Seg**	**CONTROLES EXISTENTES**	**MARCO DE SEGURIDAD**
E3.1.	2	3	12	1	2	24,0	67%	22%
I2.6.	1	2	4	1	1	8,0	22%	11%
E3.1.	1	2	3	1	1	5,6	22%	11%
I2.6.	2	2	7	1	1	11,1	44%	11%
4.16.	1	3	5	1	1	8,3	33%	11%
I2.1.	1	2	4	1	1	8,0	22%	11%
N1.2.	1	1	2	1	1	4,0	11%	11%
N1.3.4.	1	3	6	1	1	12,0	33%	11%
A4.24.	1	2	3	1	2	5,6	22%	22%
E3.5.	2	3	10	1	2	16,7	67%	22%
E3.18.	2	3	10	1	1	16,7	67%	11%
E3.12.	1	2	3	1	1	5,6	22%	11%
E3.18.	2	3	3	1	1	5,6	67%	11%
A4.23.	1	2	3	1	1	5,6	22%	11%
E3.2.	1	2	5	1	1	14,2	22%	11%
E3.10.	1	3	8	1	2	21,3	33%	22%
A4.14.	1	3	8	1	1	21,3	33%	11%
				Totales			41%	15%

Fuente: Elaboración Propia

El análisis comparativo de la situación inicial de la evaluación de riesgos, que arroja un riesgo del 41%, frente a la perspectiva potencial tras la implementación de un marco de seguridad, reduciendo el riesgo al 15%, evidencia un cambio significativo en la gestión de riesgos. Este contraste subraya la importancia y el impacto sustancial que puede tener la adopción de medidas de seguridad adecuadas. La reducción del riesgo del 46% al 15% sugiere una mejora considerable en la protección de los activos y la mitigación de posibles amenazas, lo que fortalecería la resiliencia y la estabilidad de la institución ante diversos escenarios.

4.1.7. Aplicación de la Encuesta

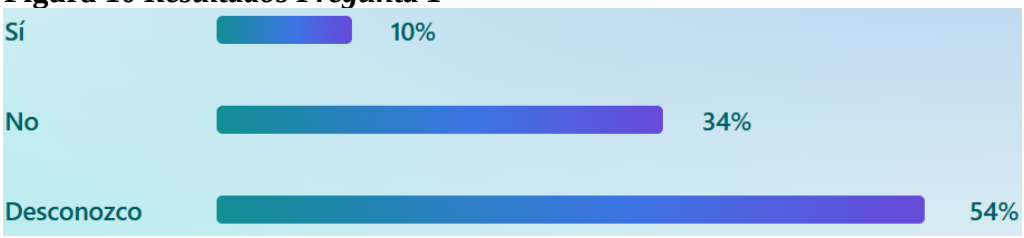
Para obtener una comprensión exhaustiva de la percepción y la eficacia de la implementación de un marco de seguridad de la información, se llevó a cabo una encuesta detallada dirigida al personal académico, administrativo y de TI relacionado con el proceso de titulación. Esta encuesta está diseñada para evaluar diversos aspectos del marco de seguridad, desde la conciencia y el cumplimiento de las políticas hasta la efectividad de los controles implementados. Sus respuestas son fundamentales para

identificar áreas de mejora y fortalecer nuestro enfoque hacia la protección de datos y la mitigación de riesgos.

4.1.7.1. Pregunta 1.

¿Conoce si la institución cuenta con un procedimiento documentado que permita la gestión de los riesgos de seguridad de la información en el proceso de titulación?

Figura 10 ***Resultados Pregunta 1***



Fuente*:* Elaboración Propia

Análisis

Los resultados indican una falta de claridad sobre si la institución cuenta con un procedimiento documentado para gestionar los riesgos de seguridad de la información en el proceso de titulación:

- **Sí (10%):** Un pequeño porcentaje de los encuestados está seguro de que la institución cuenta con un procedimiento documentado para gestionar los riesgos de seguridad de la información en el proceso de titulación. Esto sugiere que algunos están familiarizados con los procesos de seguridad de la información dentro de la institución.
- **No (34%):** Un porcentaje significativo de los encuestados afirma que la institución no cuenta con un procedimiento documentado para gestionar los riesgos de seguridad de la información en el proceso de titulación. Esto puede ser preocupante ya que indica una falta de estructura formal para abordar los riesgos de seguridad de la información en un momento crítico como el proceso de titulación.
- **Desconozco (54%):** La mayoría de los encuestados indican que desconocen si la institución cuenta con un procedimiento documentado para gestionar los riesgos de seguridad de la información en el proceso de titulación. Esto podría ser

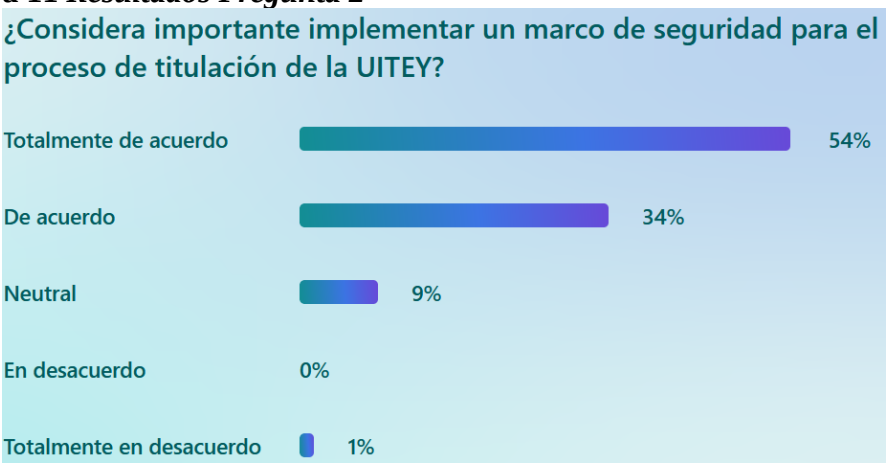
indicativo de una falta de comunicación o transparencia por parte de la institución en cuanto a sus prácticas de seguridad de la información.

En resumen, los resultados sugieren una necesidad de mayor claridad y transparencia por parte de la institución en lo que respecta a sus procedimientos de gestión de riesgos de seguridad de la información en el proceso de titulación. Además, destaca la importancia de establecer procedimientos documentados para garantizar la protección de la información sensible durante este proceso académico importante.

4.1.7.2. Pregunta 2.

¿Considera importante implementar un marco de seguridad para el proceso de titulación de la UITEY?

Figura 11 ***Resultados Pregunta 2***



Fuente: Elaboración Propia

Análisis

Los resultados muestran un fuerte consenso sobre la importancia de implementar un marco de seguridad para el proceso de titulación de la UITEY:

- **Totalmente de acuerdo (54%):** Más de la mitad de los encuestados están totalmente de acuerdo en que es importante implementar un marco de seguridad para el proceso de titulación de la UITEY. Este grupo reconoce claramente la necesidad y la importancia de contar con medidas de seguridad adecuadas para proteger la información sensible durante este proceso académico crucial.
- **De acuerdo (34%):** Un porcentaje significativo de los encuestados está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer

grupo. Esto sugiere que, si bien algunos pueden tener algunas reservas o dudas, en general reconocen la importancia de implementar un marco de seguridad para el proceso de titulación.

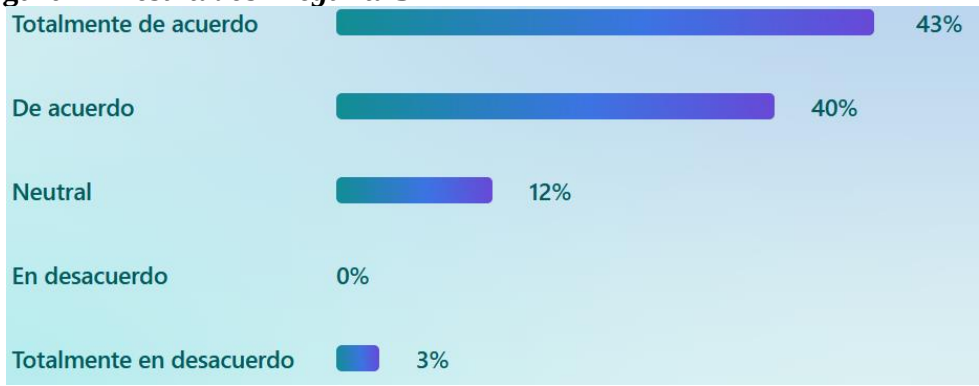
- **Neutral (9%):** Un número relativamente pequeño de encuestados permanece neutral. Esto podría indicar una falta de opinión formada o información insuficiente sobre los beneficios y la necesidad de implementar un marco de seguridad para el proceso de titulación.
- **En desacuerdo (0%) / Totalmente en desacuerdo (1%):** Es notable que solo un pequeño porcentaje de encuestados esté en desacuerdo con la importancia de implementar un marco de seguridad para el proceso de titulación. Esto sugiere un fuerte consenso en la importancia percibida de esta medida.

En resumen, la mayoría de los encuestados reconocen la importancia de implementar un marco de seguridad para el proceso de titulación de la UITEY, lo que subraya la necesidad percibida de proteger la información durante este proceso académico crucial.

4.1.7.3. Pregunta 3.

¿Cree que la adopción de un marco de seguridad mejoraría la confidencialidad integridad y disponibilidad de la información en el proceso de titulación?

Figura 12 ***Resultados Pregunta 3***



Fuente*:* Elaboración Propia

Análisis

Los resultados muestran una tendencia clara hacia la percepción positiva sobre los beneficios de la adopción de un marco de seguridad en el proceso de titulación:

- **Totalmente de acuerdo (43%):** Casi la mitad de los encuestados está totalmente de acuerdo en que la adopción de un marco de seguridad mejoraría la

confidencialidad, integridad y disponibilidad de la información en el proceso de titulación. Este grupo reconoce claramente el valor que un marco estructurado puede aportar para proteger la información sensible y garantizar su integridad y disponibilidad durante este proceso crucial.

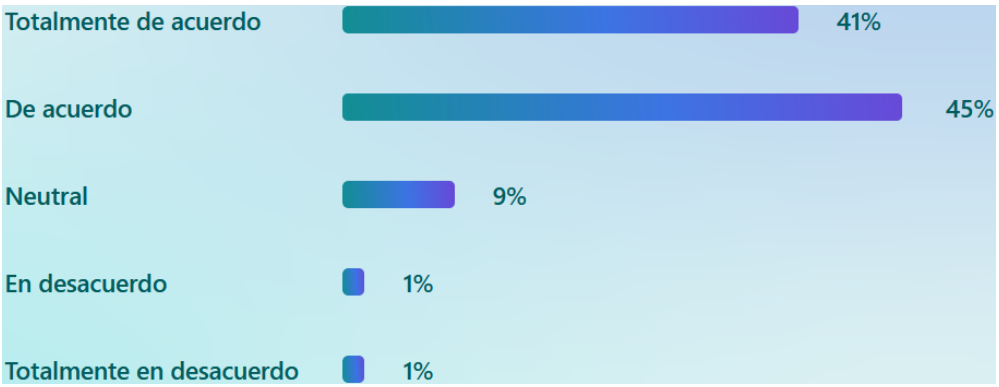
- **De acuerdo (40%):** Un porcentaje significativo de los encuestados está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto sugiere que, si bien algunos pueden tener algunas reservas o dudas, en general reconocen los beneficios potenciales que la adopción de un marco de seguridad podría ofrecer en términos de confidencialidad, integridad y disponibilidad de la información.
- **Neutral (12%):** Un número considerable de encuestados permanece neutral. Esto podría reflejar una falta de opinión formada o información insuficiente sobre los beneficios específicos de la adopción del marco de seguridad para mejorar la confidencialidad, integridad y disponibilidad de la información durante el proceso de titulación.
- **En desacuerdo (0%) / Totalmente en desacuerdo (3%):** Es notable que solo un pequeño porcentaje de encuestados esté en desacuerdo con la idea de que la adopción de un marco de seguridad mejoraría la confidencialidad, integridad y disponibilidad de la información. Esto sugiere un fuerte consenso en la importancia percibida de la adopción del marco de seguridad en este contexto.

En resumen, la mayoría de los encuestados reconocen los beneficios de la adopción de un marco de seguridad para mejorar la confidencialidad, integridad y disponibilidad de la información en el proceso de titulación. Esto subraya la importancia percibida de implementar medidas de seguridad adecuadas para proteger los datos sensibles durante este proceso académico crucial.

4.1.7.4. Pregunta 4.

¿Considera que la implementación del marco de seguridad debería adaptarse a las necesidades y especificidades del proceso de titulación de la institución?

Figura 13 ***Resultados Pregunta 4***



Fuente*:* Elaboración Propia

Análisis

Los resultados reflejan una fuerte inclinación hacia la adaptación del marco de seguridad a las necesidades y especificidades del proceso de titulación de la institución:

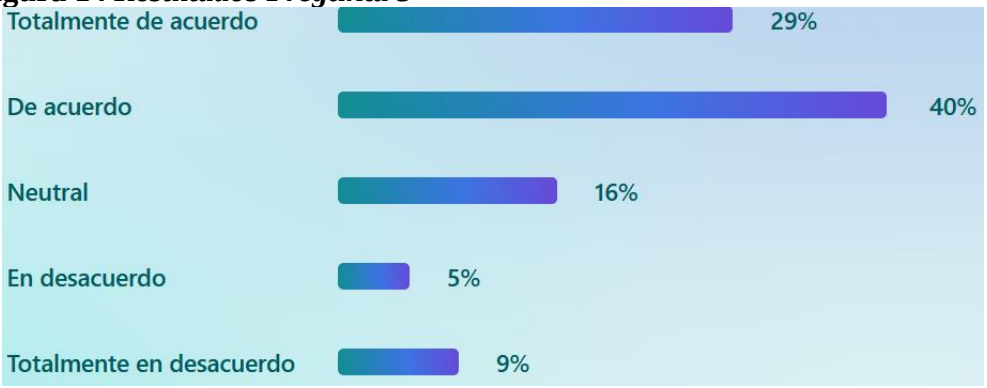
- **Totalmente de acuerdo (41%):** Un porcentaje considerable de los encuestados está totalmente de acuerdo en que la implementación del marco de seguridad debería adaptarse a las necesidades y especificidades del proceso de titulación de la institución. Este grupo reconoce la importancia de personalizar el marco de seguridad para garantizar que sea efectivo y adecuado para abordar los desafíos y requisitos específicos del proceso de titulación de la institución.
- **De acuerdo (45%):** Un porcentaje aún mayor de los encuestados está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto sugiere que hay un consenso generalizado sobre la importancia de la adaptación del marco de seguridad, aunque algunos pueden tener algunas reservas o dudas sobre la flexibilidad necesaria para lograr esta adaptación.
- **Neutral (9%):** Un número relativamente pequeño de encuestados permanece neutral. Esto podría indicar una falta de opinión formada o una necesidad de más información sobre cómo exactamente la adaptación del marco de seguridad podría beneficiar al proceso de titulación de la institución.
- **En desacuerdo (1%) / Totalmente en desacuerdo (1%):** Solo un pequeño porcentaje de los encuestados está en desacuerdo con la idea de que la implementación del marco de seguridad debería adaptarse a las necesidades y especificidades del proceso de titulación. Esto sugiere un fuerte consenso en la importancia percibida de la adaptación del marco de seguridad.

En resumen, la mayoría de los encuestados respaldan la idea de adaptar el marco de seguridad a las necesidades específicas del proceso de titulación de la institución, lo que destaca la importancia percibida de personalizar las medidas de seguridad para abordar los requisitos únicos de cada contexto institucional.

4.1.7.5. Pregunta 5.

¿Considera que la implementación de un marco de seguridad facilitaría la evaluación y mejora continua del proceso de titulación?

Figura 14 ***Resultados Pregunta 5***



Fuente*:* Elaboración Propia

Análisis

Estos resultados revelan una diversidad de opiniones sobre cómo la implementación de un marco de seguridad podría facilitar la evaluación y mejora continua del proceso de titulación:

- **Totalmente de acuerdo (29%):** Casi un tercio de los encuestados está totalmente de acuerdo en que la implementación de un marco de seguridad facilitaría la evaluación y mejora continua del proceso de titulación. Este grupo reconoce claramente el valor de tener un marco estructurado que permita identificar áreas de mejora y establecer procesos de evaluación regulares para garantizar la eficiencia y seguridad del proceso.
- **De acuerdo (40%):** Un porcentaje aún mayor de los encuestados está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto sugiere que hay un consenso generalizado sobre la utilidad de un marco de seguridad para facilitar la evaluación y mejora continua, aunque algunos pueden tener algunas reservas o dudas sobre su impacto exacto.
- **Neutral (16%):** Un número considerable de encuestados permanece neutral. Esto podría indicar una falta de opinión formada o una necesidad de más información sobre cómo exactamente la implementación del marco de seguridad contribuiría a la evaluación y mejora continua del proceso de titulación.
- **En desacuerdo (5%) / Totalmente en desacuerdo (9%):** Un pequeño pero notable porcentaje de los encuestados está en desacuerdo con la idea de que la implementación de un marco de seguridad facilitaría la evaluación y mejora continua del proceso de titulación. Estos individuos pueden tener dudas sobre la

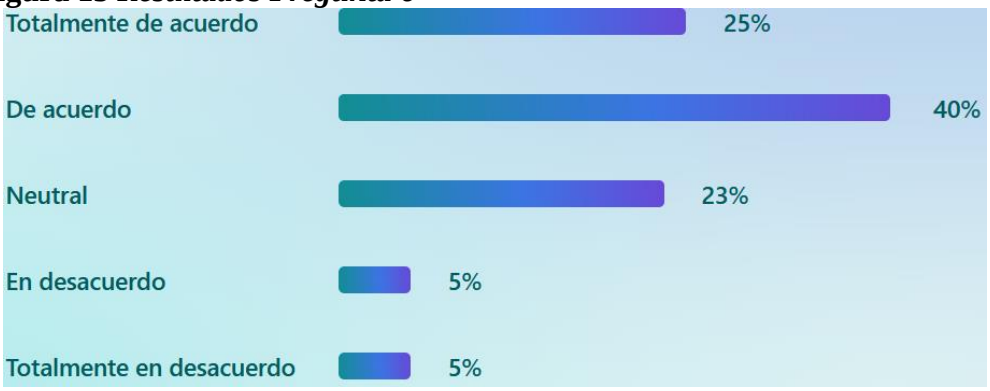
efectividad del marco o su capacidad para abordar adecuadamente las necesidades de mejora del proceso.

En resumen, mientras que la mayoría de los encuestados ven positivamente el impacto de un marco de seguridad en la evaluación y mejora continua del proceso de titulación, también hay una parte significativa que permanece neutral o tiene opiniones divergentes sobre este tema. Esto destaca la necesidad de una comunicación clara y una comprensión compartida sobre los beneficios potenciales de la implementación del marco de seguridad.

4.1.7.6. Pregunta 6.

¿Considera importante la asignación de recursos (económicos y administrativos) suficientes para la implementación efectiva del marco de seguridad en el proceso de titulación?

Figura 15 ***Resultados Pregunta 6***



Fuente: Elaboración Propia

Análisis

Estos resultados reflejan una diversidad de opiniones sobre la asignación de recursos para la implementación efectiva del marco de seguridad en el proceso de titulación:

- **Totalmente de acuerdo (25%):** Un cuarto de los encuestados está totalmente de acuerdo en que es importante asignar recursos suficientes, tanto económicos como administrativos, para la implementación efectiva del marco de seguridad en el proceso de titulación. Esto sugiere un reconocimiento claro de la necesidad de recursos adecuados para garantizar que el marco de seguridad pueda implementarse de manera eficiente y completa.

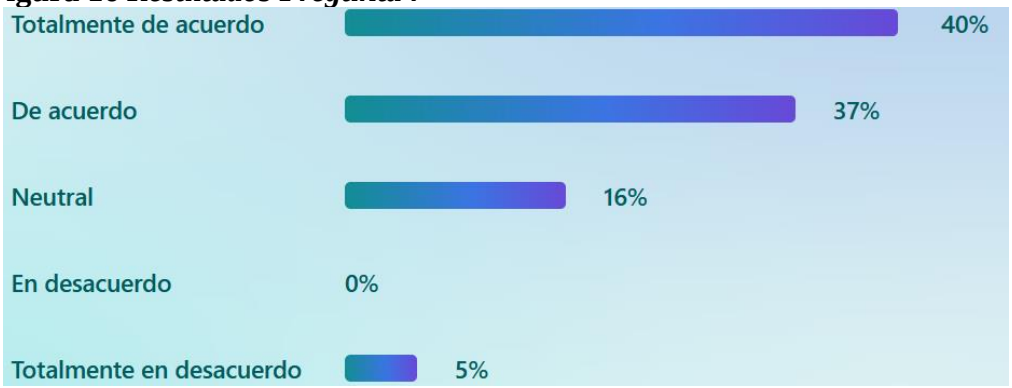
- **De acuerdo (40%):** Un porcentaje aún mayor de los encuestados está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto indica que hay un consenso generalizado sobre la importancia de asignar recursos adecuados, aunque algunos pueden tener algunas reservas o dudas sobre la cantidad exacta de recursos necesarios.
- **Neutral (23%):** Un número considerable de encuestados permanece neutral. Esto podría indicar una falta de opinión formada o una necesidad de más información sobre los recursos requeridos y su impacto en la implementación del marco de seguridad.
- **En desacuerdo (5%) / Totalmente en desacuerdo (5%):** Un pequeño pero notable porcentaje de los encuestados está en desacuerdo con la importancia de asignar recursos suficientes para la implementación efectiva del marco de seguridad en el proceso de titulación. Estos individuos pueden tener preocupaciones sobre los costos asociados con la asignación de recursos o tener opiniones divergentes sobre su necesidad.

En resumen, aunque la mayoría de los encuestados reconocen la importancia de asignar recursos adecuados para la implementación del marco de seguridad en el proceso de titulación, también hay una parte significativa que permanece neutral o tiene opiniones divergentes sobre este tema. Esto resalta la importancia de considerar cuidadosamente la asignación de recursos en el contexto de la seguridad de la información.

4.1.7.7. Pregunta 7.

¿Cree que la capacitación del personal involucrado en el proceso de titulación sobre las medidas de seguridad sería beneficiosa para la implementación del marco de seguridad?

Figura 16 ***Resultados Pregunta 7***



Fuente: Elaboración Propia

Análisis

Los resultados de esta pregunta sugieren una percepción general positiva sobre la importancia de capacitar al personal involucrado en el proceso de titulación en medidas de seguridad:

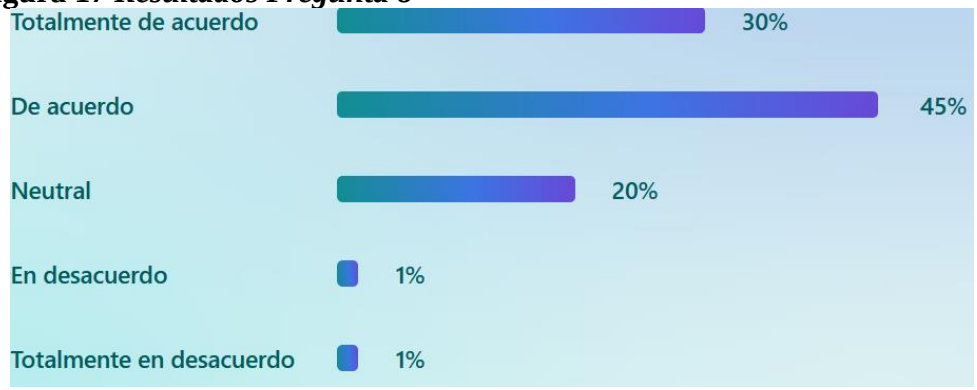
- **Totalmente de acuerdo (40%):** Una parte significativa de los encuestados está totalmente de acuerdo en que la capacitación del personal involucrado en el proceso de titulación sobre medidas de seguridad sería beneficiosa para la implementación del marco de seguridad. Esto indica un reconocimiento claro de la importancia de la capacitación para garantizar que el personal esté preparado para implementar y mantener eficazmente las medidas de seguridad.
- **De acuerdo (37%):** Casi el mismo porcentaje de encuestados está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto sugiere que hay un consenso generalizado sobre la utilidad de la capacitación, aunque algunos pueden tener algunas reservas o dudas sobre su impacto exacto.
- **Neutral (16%):** Un porcentaje considerable de encuestados permanece neutral. Esto podría indicar una falta de opinión formada o una necesidad de más información sobre los beneficios específicos de la capacitación en medidas de seguridad para el personal involucrado en el proceso de titulación.
- **En desacuerdo (0%) / Totalmente en desacuerdo (5%):** Es notable que no haya encuestados que estén en desacuerdo con la idea de que la capacitación del personal sería beneficiosa para la implementación del marco de seguridad. Esto sugiere un fuerte consenso en la importancia percibida de la capacitación en este contexto.

En resumen, la mayoría de los encuestados reconocen la importancia de capacitar al personal involucrado en el proceso de titulación en medidas de seguridad, lo que indica un apoyo generalizado hacia esta medida como parte de la implementación del marco de seguridad.

4.1.7.8. Pregunta 8.

¿Está de acuerdo en que la implementación del marco de seguridad en el proceso de titulación debería ser supervisada por personal especializado en seguridad de la información?

Figura 17 ***Resultados Pregunta 8***



Fuente*:* Elaboración Propia

Análisis

Estos resultados indican una tendencia general positiva hacia la supervisión del proceso de implementación del marco de seguridad por parte de personal especializado en seguridad de la información:

- **Totalmente de acuerdo (30%):** Un porcentaje significativo de los encuestados está totalmente de acuerdo en que la implementación del marco de seguridad en el proceso de titulación debería ser supervisada por personal especializado en seguridad de la información. Esto sugiere un reconocimiento claro de la importancia de contar con expertos en seguridad para garantizar que el proceso se realice de manera efectiva y conforme a los estándares de seguridad.
- **De acuerdo (45%):** La mayoría de los encuestados están de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto indica que hay un consenso generalizado sobre la necesidad de involucrar a personal especializado en seguridad de la información en el proceso de implementación del marco de seguridad, pero algunos pueden tener algunas reservas o dudas sobre la medida.
- **Neutral (20%):** Un porcentaje considerable de encuestados permanece neutral. Esto podría reflejar una falta de opinión formada o información

insuficiente sobre la importancia de la supervisión especializada en seguridad de la información en este contexto.

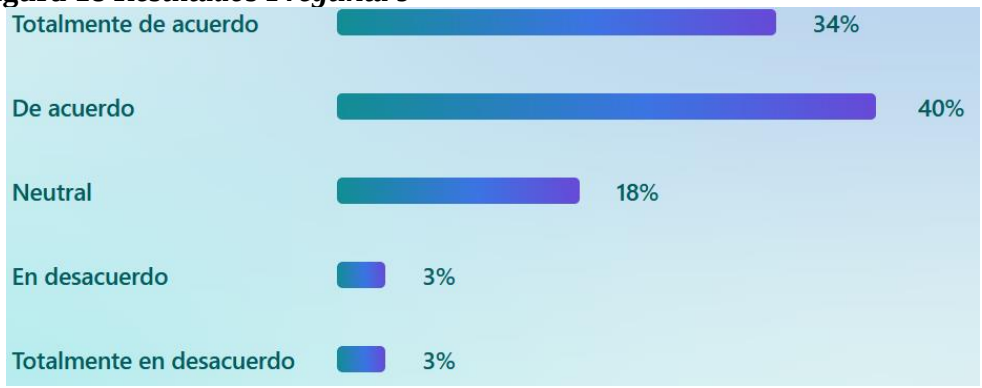
- **En desacuerdo (1%) / Totalmente en desacuerdo (1%):** Solo un pequeño porcentaje de los encuestados está en desacuerdo con la idea de que la implementación del marco de seguridad debería ser supervisada por personal especializado en seguridad de la información. Esto sugiere que la mayoría reconoce la importancia de la supervisión especializada en este proceso.

En resumen, la mayoría de los encuestados están de acuerdo en que la implementación del marco de seguridad en el proceso de titulación debería ser supervisada por personal especializado en seguridad de la información, lo que subraya la importancia percibida de contar con experiencia técnica en seguridad durante este proceso crítico.

4.1.7.9. Pregunta 9.

¿Cree que la implementación del marco de seguridad en el proceso de titulación aumentaría la confianza de los estudiantes en la seguridad de sus datos?

Figura 18 ***Resultados Pregunta 9***



Fuente*:* Elaboración Propia

Análisis

Estos resultados muestran una percepción general positiva sobre cómo la implementación del marco de seguridad en el proceso de titulación podría afectar la confianza de los estudiantes en la seguridad de sus datos:

- **Totalmente de acuerdo (34%):** Un porcentaje considerable de los encuestados está totalmente de acuerdo en que la implementación del marco de seguridad aumentaría la confianza de los estudiantes en la seguridad de sus datos durante el proceso de titulación. Esto sugiere una fuerte creencia en el

papel que juega un marco de seguridad en la mejora de la confianza y la protección de los datos.

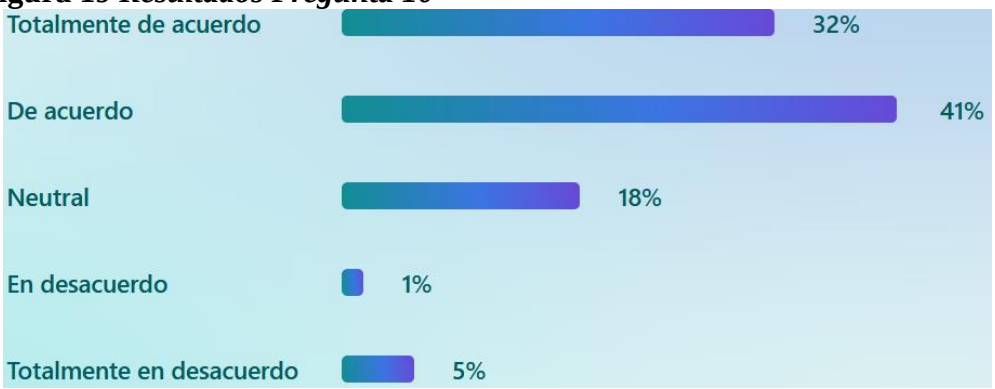
- **De acuerdo (40%):** Otro segmento importante está de acuerdo con la afirmación, aunque no de manera tan enfática como el primer grupo. Esto indica que, si bien algunos pueden tener algunas reservas o dudas, en general reconocen el impacto positivo que la implementación del marco de seguridad podría tener en la confianza de los estudiantes.
- **Neutral (18%):** Un número considerable de encuestados permanece neutral. Esto podría reflejar una falta de información o comprensión completa sobre cómo la implementación del marco de seguridad influiría en la confianza de los estudiantes en la seguridad de sus datos durante el proceso de titulación.
- **En desacuerdo (3%) / Totalmente en desacuerdo (3%):** Solo un pequeño porcentaje de los encuestados está en desacuerdo con la idea de que la implementación del marco de seguridad aumentaría la confianza de los estudiantes en la seguridad de sus datos. Estos individuos pueden tener opiniones divergentes sobre el impacto que tendría la implementación del marco de seguridad.

En resumen, la mayoría de los encuestados muestran una percepción positiva sobre cómo la implementación del marco de seguridad podría mejorar la confianza de los estudiantes en la seguridad de sus datos durante el proceso de titulación, aunque hay una parte significativa que permanece neutral sobre el tema.

4.1.7.10. Pregunta 10.

¿Considera que la implementación del marco de seguridad debería ser un requisito obligatorio en todos los procesos de la institución?

Figura 19 ***Resultados Pregunta 10***



Fuente: Elaboración Propia

Análisis

Estos resultados muestran una diversidad de opiniones sobre si la implementación del marco de seguridad debería ser un requisito obligatorio en todos los procesos de la institución:

- **Totalmente de acuerdo (32%):** Un poco menos de un tercio de los encuestados están totalmente de acuerdo en que la implementación del marco de seguridad debería ser obligatoria en todos los procesos de la institución. Este grupo percibe claramente la importancia y la necesidad de una seguridad integral en todos los aspectos de las operaciones institucionales.
- **De acuerdo (41%):** Un porcentaje significativo de encuestados está de acuerdo con que el marco de seguridad debería ser un requisito obligatorio, aunque no de manera tan enfática como el primer grupo. Esto sugiere que muchos reconocen la importancia de la seguridad, pero pueden tener algunas reservas sobre la imposición obligatoria de un marco específico.
- **Neutral (18%):** Un número considerable de encuestados permanece neutral. Esto podría indicar una falta de opinión formada o un equilibrio entre las ventajas y desventajas percibidas de hacer obligatoria la implementación del marco de seguridad.
- **En desacuerdo (1%) / Totalmente en desacuerdo (5%):** Solo un pequeño porcentaje de los encuestados está en desacuerdo con la idea de hacer obligatoria la implementación del marco de seguridad en todos los procesos de la institución. Estos individuos pueden tener preocupaciones sobre la flexibilidad o los costos asociados con dicha medida.

En resumen, mientras que hay un respaldo general hacia la idea de hacer obligatoria la implementación del marco de seguridad, también hay un segmento significativo de encuestados que tienen opiniones más reservadas o neutralidad sobre este tema.

4.1.7.11. Interpretación de resultados de la encuesta

Después de analizar las respuestas a estas preguntas, es evidente que existe una diversidad de opiniones y percepciones con respecto a la implementación de un marco de seguridad en el proceso de titulación de la UITEY. Si bien algunos encuestados están completamente de acuerdo con la necesidad e importancia de implementar dicho marco, otros muestran neutralidad hacia esta propuesta. Sin embargo, una gran mayoría reconoce

la importancia de adaptar el marco de seguridad a las necesidades específicas del proceso de titulación de la institución y asignar los recursos adecuados para su implementación efectiva.

Además, existe consenso en la importancia de la capacitación al personal involucrado en el proceso de titulación sobre las medidas de seguridad, así como en la supervisión por parte de personal especializado en seguridad de la información. Estas medidas son vistas como fundamentales para garantizar el éxito y la eficacia del marco de seguridad.

En última instancia, la implementación del marco de seguridad no solo se percibe como una medida para mejorar la confidencialidad, integridad y disponibilidad de la información en el proceso de titulación, sino también como un elemento que podría aumentar la confianza de los estudiantes en la seguridad de sus datos. Sin embargo, aún queda por definir si esta implementación debe ser un requisito obligatorio en todos los procesos de la institución, lo que podría generar más debate y análisis en futuras discusiones.

CAPITULO V

5.1 CONCLUSIONES

- **Análisis de los atributos CID**: Se han analizado los atributos de Confidencialidad, Integridad y Disponibilidad (CID) del proceso de titulación de la Universidad Yachay Tech para los 10 activos de la información identificados en el proceso obteniendo una valoración promedio de 1,9 en una escala máxima de 3, lo que evidencia que la pérdida de los atributos CID del proceso tendría un efecto negativo considerable en la institución.
- **Valoración de los principales riesgos de seguridad de la información**: A través de la aplicación del dominio APO12 de COBIT 2019, se han identificado y evaluado los principales riesgos de seguridad de la información asociados con el proceso de titulación de la Universidad Yachay Tech. En este proceso se ha evaluado y valorado el nivel de riesgo en función de la valoración de las amenazas, vulnerabilidades y ponderación de los atributos CID de los activos, obteniendo una valoración de riesgo en nivel medio para el 50% de las amenazas y vulnerabilidades, mientras que el 50% restante presenta un nivel de riesgo bajo.
- **Diseño de un plan de implementación del Marco de Seguridad de la Información**: Se ha desarrollado una guía para la implementación del Marco de Seguridad de la Información utilizando COBIT 2019 en el proceso de titulación de la Universidad Yachay Tech. Este plan aborda el proceso a seguir para la identificación, evaluación y tratamiento del riesgo; con lo cual se puede comparar el nivel de riesgo en la situación inicial y en un escenario potencial al implementar el Marco de Seguridad propuesto.
- **Evaluación de la percepción sobre la existencia de un Marco de Seguridad de la Información**: mediante una encuesta aplicada al personal docente y administrativo involucrado en el proceso de titulación de la Universidad Yachay Tech se ha evaluado su percepción respecto a la existencia y necesidad de implementar un Marco de Seguridad de la Información, los datos recopilados permiten identificar en la mayoría de actores el desconocimiento sobre la existencia de un procedimiento que permita la gestión de riesgos en el proceso de titulación de la UITEY y a su vez destacan la importancia y necesidad de contar con un Marco de Seguridad de la Información.

- **Cumplimiento normativo:** La implementación del Marco de Seguridad propuesto permite que la institución cumpla con las normas de control interno establecidas por la Contraloría General del Estado, como la norma 410-10; además de estándares internacionales como las normas ISO 27005 e ISO 31000, lo cual evita implicaciones legales negativas para la institución.
- **Satisfacción de stakeholders:** La implementación del Marco de Seguridad propuesto contribuye a generar confianza en el proceso de titulación de la Universidad Yachay Tech, con lo que la institución se posiciona al cumplir con sus políticas de calidad en la educación superior.
- **Oportunidades de mejora:** La implementación del Marco de Seguridad brinda la posibilidad de mantener activo un portafolio de acciones para gestionar los riesgos identificados, evaluar y valorar periódicamente la aparición de nuevos riesgos y establecer opciones para su tratamiento, de manera que se garantice la seguridad de los activos de la información y sus atributos CID.

5.2 RECOMENDACIONES

- **Implementar un Marco de Seguridad de la Información formal**, basado en el dominio APO12 de COBIT 2019, para establecer políticas, procedimientos y acciones estructuradas.
- **Establecer un Comité de Seguridad de la Información** que coordine y supervise las actividades relacionadas con la seguridad de los activos de la información del proceso de titulación de la UITEY.
- **Realizar evaluaciones periódicas de la seguridad de la información** y medir la mejora continua mediante métricas de rendimiento y resultados.
- **Capacitar al personal en las mejores prácticas de seguridad de la información** y promover una cultura de conciencia y responsabilidad en toda la universidad.
- **La ciberseguridad no es un desafío estático**; evoluciona constantemente. Por lo tanto, es crucial mantenerse actualizado con las últimas amenazas y mejores prácticas de seguridad. Implementar un marco como APO12 ayuda a adaptarse y proteger a la institución contra las crecientes amenazas cibernéticas en el panorama actual.

Referencias

Amaya, H. C. (2016). Obtenido de https://chmasiunal20161912041.wordpress.com/magerit/

Arispe, C., Yangali, J., Guerrero, M., Lozada, O., Acuña, L., & Arellano., C. (2020). *La investigación científica, uns aproximación para los estudios de posgrado.* Guayaquil: Universidad Internacional del Ecuador.

CHANG, J. E. (1 de Mayo de 2020). Obtenido de https://revistacientificaistjba.edu.ec

Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador*. Montecristi: Asamblea Nacional.

Contraloría General del Estado. (2009). *Normas de control interno de la Contraloría general del Estado.* Quito: Contraloría General del Estado.

Contreras Abad, R. X. (2020). *Análisis comparativo de la norma 410 de control interno de la Contraloría General del Estado con COBIT5.* Cuenca: Universidad católica de Cuenca. Obtenido de https://dspace.ucacue.edu.ec/handle/ucacue/10284

El Comercio. (01 de Enero de 2023). *La ciberseguridad cobrará más importancia en 2023*. Obtenido de https://www.elcomercio.com/tendencias/tecnologia/ciberseguridad-empresas-plataformas-paginas-informacion.html

EnterpriseIT. (2021). *Controles Generales de Tecnología de la Información*. Obtenido de https://enterpriseit.cl/controles-generales-de-tecnologias-de-informacion/

Fabara López, F. B. (2020). *Implementación de los procesos de Gobierno de COBIT 2019 en la Dirección de Tecnologías de la Información y Comunicaciones del Ejército del Ecuador.* Universidad de las Fuerzas Armadas ESPE.

Fandom. (2021). *Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información*. Obtenido de https://ticsalborada1.fandom.com/es/wiki/1._Principios_de_la_seguridad_inform%C3%A1tica:_Confidencialidad,_Integridad_y_Disponibilidad_de_la_informaci%C3%B3n

FOURMATT. (27 de 06 de 2022). *COBIT 2019: Gestión de riesgos (APO12)*. Obtenido de https://4matt.com.br/es-mx/cobit-2019-gestao-de-riscos-apo12/

Global Suite. (25 de 09 de 2023). *¿Qué es COBIT y para qué sirve?* Obtenido de https://www.globalsuitesolutions.com/es/que-es-cobit/

Global Suite. (28 de septiembre de 2023). *Global Suite*. Obtenido de Global Suite: https://www.globalsuitesolutions.com/es/que-son-normas-iso/

Global Suite. (27 de 09 de 2023). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. Obtenido de ISO 27000 y el conjunto de estándares de Seguridad de la Información: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Global Suite. (19 de octubre de 2023). *ISO 31000: La norma que te ayuda a gestionar los riesgos*. Obtenido de ISO 31000: La norma que te ayuda a gestionar los riesgos: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-31000-y-para-que-sirve/

Gobierno Electrónico. (2020). *Guía para la gestión de riesgos de seguridad de la información*. Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Google Maps. (2024). *Ubicación Campus universitario UITEY*. Obtenido de https://www.google.com/maps/place/Universidad+Yachay+Tech/@0.4056559,-78.1777783,17.62z/data=!4m6!3m5!1s0x8e2a3a4b5d36ad37:0x29804a25cc7029fb!8m2!3d0.4043154!4d-78.1756221!16s%2Fm%2F010fbl7l?entry=ttu

Gutiérrez, H. C. (01 de abril de 2016). *Gobierno y Gestión de TI*. Obtenido de Gobierno y Gestión de TI: https://chmasiunal20161912041.wordpress.com/magerit/

ISACA. (2017). Obtenido de https://www.isaca.org/es-es/resources/isaca-journal/issues/2016/volume-6/assessing-security-controls-keystone-of-the-risk-management-framework

ISACA. (2020). *COBIT ® 2019 FRAMEWORK: INTRODUCTION & METHODOLOGY*. Obtenido de https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

Lance Dubsky, C. C. (2017). *La evaluación de los controles de seguridad: Las claves del marco de la gestión de riesgos.* ISACA.

Ley de Creación de la Universidad de Investigación Experimental Yachay. (2013). *Ley de Creación de la Universidad de Investigación Experimental Yachay.* Quito : Presidencia de la República.

Ley Orgánica de Educación Superior. (2010). *Ley Orgánica de Educación Superior*. Quito: Asamblea Nacional.

Ley orgánica de Protección de Datos Personales. (2021). *Ley orgánica de Protección de Datos Personales.* Quito: Asamblea Nacional .

Merchan-Lima, J. A.-S.-O. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review.

Ministerio de hacienda y administración pública. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de hacienda y administración pública.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). *Guía para la gestión de riesgos de seguridad de la información.* Quito: Gobierno Electrónico.

Organización de los Estados Americanos (OEA). (2019). *CIBERSEGURIDAD - MARCO NIST.* Washington D. C.: White paper series.

Ortí, C. B. (2012). *LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (T.I.C.).* Valencia, España: Universidad de Valencia.

Parra, D. A. (2012). *Gestión del riesgo en la seguridad informática: "Cultura de la Auto-Seguridad Informática".* Bogotá, Colombia: Universidad Militar Nueva Granada.

Ritegno, E. O. (2019). *Cobit 2019.* ISACA.

Secretaría Nacional de Planificación. (2024). *Plan Nacional de Desarrollo.* Quito: SENPLADES.

UITEY . (2022). *Plan Estratégico de Desarrollo Institucional* . Urcuquí: Yachay Tech.

UITEY. (2014). *Estatuto de la Universidad de Investigación de Tecnología Experimental Yachay*. Obtenido de https://www.yachaytech.edu.ec/normativa/

UITEY. (2020). *RESOLUCION No. RCA-SE-020 No. 046-2020.* Urcuquí: Yachay Tech.

UITEY. (2020). *Resolución Nro. UITEY-REC-2020-0044-R.* Urcuquí: Yachay Tech.

UITEY. (2022). *Política de Aseguramiento de la Calidad de la Universidad de Investigación de Tecnología Experimental Yachay* . Urcuquí: Yachay Tech.

Universidad Norbert Wiener. (2020). *Guía de enfoque de investigación cualitativa.* Lima: Vicerrectorado de Investigación .

Vega Briceño, E. (2021). *SEGURIDAD DE LA INFORMACIÓN*. Alicante, España: Área de Innovación y Desarrollo,S.L.

ANEXOS

Guía de Validación de instrumentos N°. 01
Figura 20 ***Instrumento de Validación Experto 01***

UNIVERSIDAD TÉCNICA DEL NORTE
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

Instrumento de Validación

Instrucciones:

En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere para mejorar el instrumento. Al final encontrará un espacio para agregar observaciones generales.

Item Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	E	
2	E	E	E	
3	E	E	E	
4	E	E	E	
5	E	E	E	
6	E	E	E	
7	E	E	E	
8	E	E	E	
9	E	E	E	
10	E	E	E	

Observaciones generales:

_____
_____
_____
_____
_____

UNIVERSIDAD TÉCNICA DEL NORTE
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

Datos del Validador	
Nombres y Apellidos:	**EDISON ORLANDO TUQUERRES CANCAN**
Teléfono:	**0999655086**
Correo electrónico:	**etuquerres@atuntaqui.fin.ec**
Título de formación de Posgrado:	**MAGISTER EN COMPUTACION MENCION EN SEGURIDAD INFORMATICA**
Cargo que ejerce/ Institución:	**AUDITOR INFORMATICO**
Fecha de validación:	**29/04/2024**

EDISON ORLANDO TUQUERRES CANCAN
Firmado digitalmente por EDISON ORLANDO TUQUERRES CANCAN
Fecha: 2024.04.29 10:40:30 -05'00'

Firma

Guía de Validación de instrumentos N°. 02
Figura 21 ***Instrumento de Validación Experto 02***

UNIVERSIDAD TÉCNICA DEL NORTE
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

Instrumento de Validación

Instrucciones:

En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere para mejorar el instrumento. Al final encontrará un espacio para agregar observaciones generales.

Item Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	M	Analizar las opciones de respuesta ya que considero que la opción b y c son redundantes.
2	E	E	E	
3	E	E	M	Analizar la relación del verbo de la pregunta con las opciones de respuesta, podría mejorar su consistencia para usuarios inexpertos.
4	E	E	E	
5	E	E	E	
6	E	E	E	
7	E	E	M	Analizar la relación del verbo de la pregunta con las opciones de respuesta, podría mejorar su consistencia para usuarios inexpertos.
8	E	E	M	Analizar la redacción de la pregunta se sugiere usar (de acuerdo con).
9	E	E	E	Analizar la relación del verbo de la pregunta con las opciones de respuesta, podría mejorar su

UNIVERSIDAD TÉCNICA DEL NORTE
Resolución No. 001-073 CEAACES-2013-13
INSTITUTO DE POSGRADO

				consistencia para usuarios inexpertos.
10	E	E	E	

Observaciones generales:

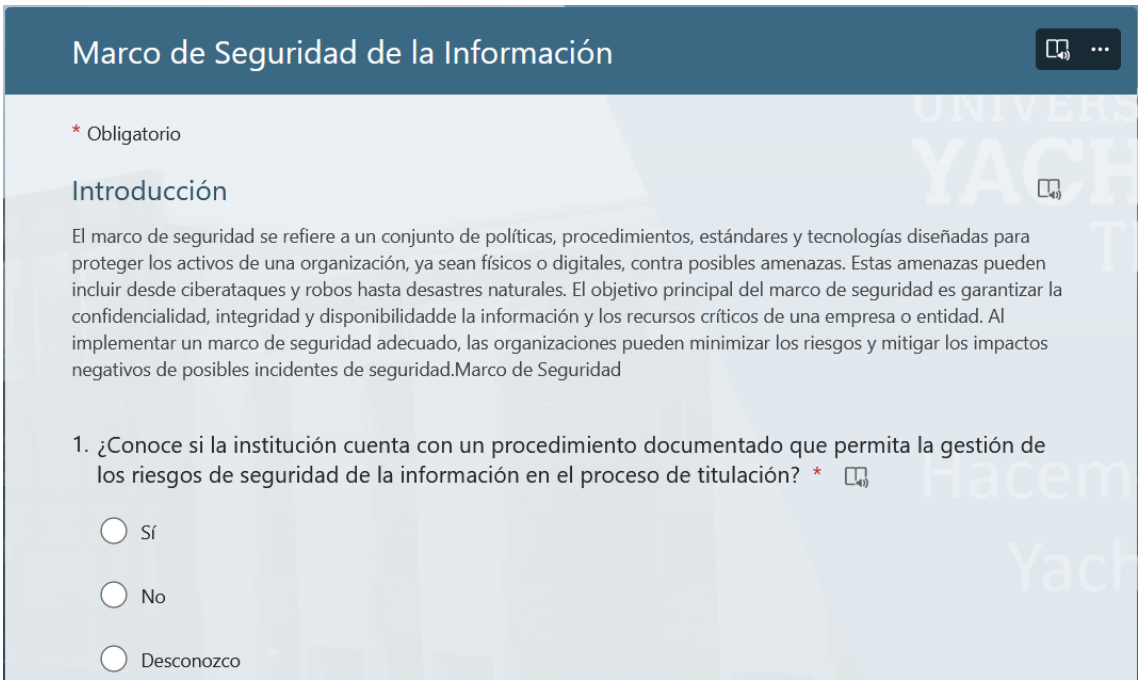
Una vez revisadas cada una de las preguntas se concluye que se ha construido un instrumento bastante completo y útil para la investigación que se ha propuesto, excepto por algunas deficiencias sencillas en la redacción de ciertas preguntas que sin embargo no desvían del objetivo de la interrogante.

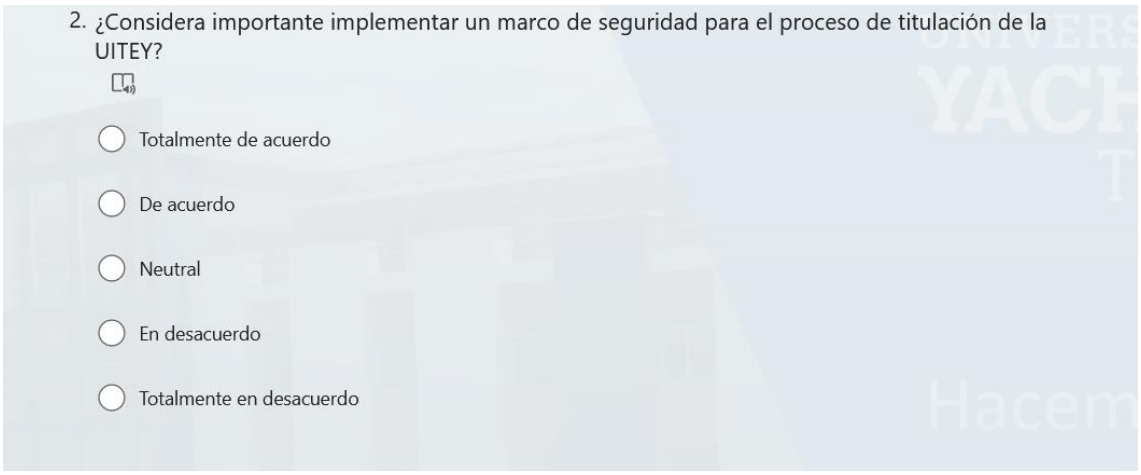
Datos del Validador	
Nombres y Apellidos:	Evelin Guadalupe Enríquez Huaca
Teléfono:	0982955533
Correo electrónico:	evelinehg@gmail.com
Título de formación de Posgrado:	MÁSTER EN INGENIERIA DE SOFTWARE Y SISTEMAS INFORMATICOS
Cargo que ejerce/ Institución:	Analista de sistemas 2 /UTN
Fecha de validación:	07/05/2024

Firma

Captura Encuesta Digital Aplicada

Figura 22 ***Encuesta Digital***





3. ¿Cree que la adopción de un marco de seguridad mejoraría la confidencialidad integridad y disponibilidad de la información en el proceso de titulación?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

4. ¿Considera que la implementación del marco de seguridad debería adaptarse a las necesidades y especificidades del proceso de titulación de la institución?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

5. ¿Considera que la implementación de un marco de seguridad facilitaría la evaluación y mejora continua del proceso de titulación?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

6. ¿Considera importante la asignación de recursos (económicos y administrativos) suficientes para la implementación efectiva del marco de seguridad en el proceso de titulación?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

7. ¿Cree que la capacitación del personal involucrado en el proceso de titulación sobre las medidas de seguridad sería beneficiosa para la implementación del marco de seguridad?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

¿Está de acuerdo en que la implementación del marco de seguridad en el proceso de titulación debería ser supervisada por personal especializado en seguridad de la información?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

9. ¿Cree que la implementación del marco de seguridad en el proceso de titulación aumentaría la confianza de los estudiantes en la seguridad de sus datos?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

10. ¿Considera que la implementación del marco de seguridad debería ser un requisito obligatorio en todos los procesos de la institución?

- ◯ Totalmente de acuerdo
- ◯ De acuerdo
- ◯ Neutral
- ◯ En desacuerdo
- ◯ Totalmente en desacuerdo

Guía Implementación Marco de Seguridad

GUIA IMPLEMENTACIÓN MARCO DE SEGURIDAD DE LA INFORMACIÓN
PROCESO DE TITULACIÓN
Versión 1.0
Producido por:
Dirección General de Tecnologías de Información y Comunicaciones
Universidad de Investigación de Tecnología Experimental Yachay

HISTORIAL DE CAMBIOS			
Versión	**DETALLE / ACCIÓN**	**Responsable**	**Fecha**
Versión 1.1	Creación del documento	Manuel Narváez R.	01/04/2024

UNIVERSIDAD YACHAY TECH

Tabla de Contenido

UNIVERSIDAD YACHAY TECH

INTRODUCCIÓN

Este manual tiene como objetivo proporcionar una guía paso a paso para la implementación del marco de seguridad de la información en nuestra institución para el proceso de titulación. El marco de seguridad establece los procesos, controles y mejores prácticas necesarias para proteger los activos de información.

1. Planificación de la Implementación

1.1. Definición de Objetivos y Alcance

- Identificar los objetivos de seguridad de la información de la organización.
- Determinar el alcance de la implementación, incluyendo los activos y procesos que se verán afectados.

1.2. Asignación de Recursos

- Designar un equipo de implementación encargado de liderar el proceso.
- Asignar recursos humanos, financieros y tecnológicos necesarios para la implementación.

2. Evaluación de la Situación Actual

2.1. Análisis de Riesgos

- Realizar una evaluación de riesgos para identificar amenazas, vulnerabilidades y activos críticos.
- Priorizar los riesgos identificados según su impacto y probabilidad de ocurrencia.

2.1.1. Identificación de activos

Para realizar la valoración de los activos, es necesario que la institución identifique primero sus activos (con un grado adecuado de detalles). La guía propone dos clases de activos en base a la metodología de MAGETIR V3.0:

Activos primarios:

- Actividades y procesos del negocio.
- Información.

Activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:

- Hardware.
- Software.

- Redes.
- Personal.
- Ubicación.
- Estructura de la organización.

Además, es necesario registrar dentro del levantamiento de la información de identificación de activos a los responsables y ubicación de cada uno de los mismo para que en el proceso de gestión de riesgos de la seguridad de la información facilite las actividades siguientes de evaluación y tratamiento del riesgo.

Identificados los activos se realiza la valoración o ponderación de la criticidad de activos en términos de "alto, medio o bajo" donde se asigna un valor cuantitativo a cada valor cualitativo de los atributos de confidencialidad, integridad y disponibilidad, la metodología adoptada plantea las siguientes ponderaciones:

Tabla 1 ***Valoración del impacto en términos de la perdida de la confidencialidad***

CONFIDENCIALIDAD	CRITERIO
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución. Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución. Ej. Divulgación de información de uso interno.
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución. Ej. Divulgación de información pública.

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

Tabla 2 ***Valoración del impacto en términos de la perdida de la integridad***

INTEGRIDAD	CRITERIO
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución.

Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución.
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

Tabla 3 ***Valoración del impacto en términos de la perdida de la disponibilidad***

DISPONIBILIDAD	CRITERIO
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución.
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución.
Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución.

Nota: Información tomada de la guía para la gestión de riesgos de seguridad de la información expedido por el MINTEL, 2020

En base a las tablas mencionadas, la valoración se la realiza respecto a la confidencialidad, integridad y disponibilidad ya que estas son las dimensiones en que se basa la seguridad de la información (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020).

La valoración detallará el número y nombre del activo, tipo de soporte, ubicación, ponderaciones CID y valoración calculada acorde la siguiente formula.

$$VA = \frac{C + I + D}{3}$$

Dónde:
VA = Valoración de los activos
C = Confidencialidad
I = Integridad
D = Disponibilidad
3 = No. de atributos

2.1.2. Identificación de amenazas y vulnerabilidades

Posterior a la identificación de los activos de la información es necesario determinar las principales amenazas tomando en cuenta el nivel del riesgo y su posible afectación que no permitiría garantizar la seguridad de la información, basado en la información propuesta en la metodología de MAGERIT V3.0 se establece la siguiente clasificación:

- Desastres naturales
  - Fuego
  - Daños por agua
  - Desastres naturales: contaminación, siniestro mayor, fenómeno climático, fenómeno sísmico, fenómeno de origen volcánico, fenómeno meteorológico, inundación, etc.
- De origen industrial
  - Fuego
  - Daños por agua
  - Desastres industriales
  - Contaminación mecánica
  - Contaminación electromagnética
  - Avería de origen físico o lógico
  - Corte del suministro eléctrico
  - Condiciones inadecuadas de temperatura o humedad
  - Fallo de servicios de comunicaciones
  - Interrupción de otros servicios y suministros esenciales
  - Degradación de los soportes de almacenamiento de la información
  - Emanaciones electromagnéticas
- Errores y fallos no intencionados
  - Errores de los usuarios
  - Errores del administrador
  - Errores de monitorización (log)
  - Errores de configuración
  - Deficiencias en la organización
  - Difusión de software dañino
  - Errores de [re-]encaminamiento
  - Errores de secuencia
  - Escapes de información

- Alteración accidental de la información
- Destrucción de información
- Fugas de información
- Vulnerabilidades de los programas (software)
- Errores de mantenimiento / actualización de programas (software)
- Errores de mantenimiento / actualización de equipos (hardware)
- Caída del sistema por agotamiento de recursos
- Pérdida de equipos
- Indisponibilidad del personal

- Ataques intencionados
  - Manipulación de los registros de actividad (log)
  - Manipulación de la configuración
  - Suplantación de la identidad del usuario
  - Abuso de privilegios de acceso
  - Uso no previsto
  - Difusión de software dañino
  - [Re-]encaminamiento de mensajes
  - Alteración de secuencia
  - Acceso no autorizado
  - Análisis de tráfico
  - Repudio
  - Interceptación de información (escucha)
  - Modificación deliberada de la información
  - Destrucción de información
  - Divulgación de información
  - Manipulación de programas
  - Manipulación de los equipos
  - Denegación de servicio
  - Robo
  - Ataque destructivo
  - Ocupación enemiga
  - Indisponibilidad del personal
  - Extorsión
  - Ingeniería social (picaresca)

- Correlación de errores y ataques

- Amenazas que sólo pueden ser errores, nunca ataques deliberados
- Amenazas que nunca son errores: siempre son ataques deliberados
- Amenazas que pueden producirse tanto por error como deliberadamente

- Nuevas amenazas: XML
  - Sintaxis BNF
  - Esquema XSD

2.1.3. Identificación de controles existentes

La identificación de controles existentes es clave para evitar el trabajo y costos innecesarios a la implementación de duplicidad en los mismo, a la vez se recomienda realizar la verificación del correcto funcionamiento del control.

2.1.4. Evaluación del Riesgo

Para la evaluación del riesgo determinados los datos en los pasos anteriores se proceden a comparar los riesgos estimados con los criterios de evaluación y aceptación de riesgos. A continuación, se presentan en la tabla siguiente la valoración de la probabilidad de ocurrencia de la amenaza que podría explotar una determinada vulnerabilidad.

Tabla 4 *Criterios de probabilidad de ocurrencia de amenazas*

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	En rara ocasión	El atacante no se beneficia del ataque.	Desastres naturales

Tabla 5 *Criterios de probabilidad de ocurrencia de vulnerabilidades*

NIVEL DE VULNERABILIDAD	CRITERIO	EJEMPLO
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

El proceso de comparación del riesgo estimado con el criterio de riesgo calculado permite determinar la importancia del riesgo, el grado del riesgo se expresa de manera numérica en función de lo determinado en la valoración de la importancia del activo en terminados de Confidencialidad, Integridad y Disponibilidad, el valor del impacto de la amenaza y el valor del impacto de la vulnerabilidad, el producto de estos valores permite determinar el nivel del riesgo tal como se detalla a continuación.

Tabla 6 *Niveles de Riesgos*

Nivel de Riesgo	
1-3	El riesgo es BAJO
4-8	El riesgo es MEDIO
9-27	El riesgo es ALTO

Nivel de riesgo **= VA(CID) ∗ Nivel de amenaza ∗ Nivel de vulnerabilidad**

3. Mantener un perfil de riesgo

La gestión efectiva de los riesgos de TI ayuda a garantizar mantener al tanto a la institución de los riesgos actuales y potenciales en el entorno mediante la práctica de perfil de riesgo. Para ello se deben de considerar las actividades propuestas por la práctica de gestión de COBIT 2019 de su dominio de APO12 de Gestión de Riesgos que se detallan a continuación.

- Actualizar regularmente la evaluación de riesgos de TI para reflejar cambios en el entorno empresarial, tecnológico y regulatorio.
- Revisar y validar los criterios de evaluación de riesgos para garantizar su relevancia y aplicabilidad.
- Analizar y clasificar los riesgos identificados según su impacto potencial y probabilidad de ocurrencia.

4. Articulación del Riesgo

Es importante mantener una conexión y relación entre diferentes riesgos identificados dentro de la institución porque los riesgos no existen de forma aislada; están interrelacionados y pueden tener efectos secundarios o consecuencias en cascada que impactan en múltiples áreas de la institución. Aquí hay algunas formas en que se puede abordar la articulación de riesgos

4.1. Identificación de Interdependencias

Identificar y comprender cómo los diferentes riesgos están interconectados y pueden influirse mutuamente. Por ejemplo, un fallo en la seguridad de la red puede exponer datos sensibles, lo que a su vez aumenta el riesgo de violación de la privacidad del personal de la institución.

4.2. Evaluación de Riesgos Compuestos

Evaluar los riesgos compuestos que resultan de la interacción de varios riesgos individuales. Esto implica analizar cómo la materialización de un riesgo puede agravar o mitigar otros riesgos en la institución.

4.3. Priorización Estratégica

Priorizar los riesgos en función de su articulación y su potencial impacto en los objetivos estratégicos de la institución. Esto implica considerar no solo la probabilidad y el

impacto de cada riesgo individual, sino también su relación con otros riesgos y la capacidad de la institución para gestionarlos.

4.4. Planificación de Respuesta Integrada

Desarrollar planes de respuesta a riesgos que aborden de manera integral las interdependencias y articulaciones entre diferentes riesgos. Esto implica coordinar las acciones y recursos necesarios para abordar los riesgos de manera efectiva y minimizar el impacto en la institución.

4.5. Comunicación y Coordinación

Fomentar una comunicación abierta y una coordinación efectiva entre los equipos y partes interesadas involucradas en la gestión de riesgos. Esto ayuda a garantizar una comprensión común de las interrelaciones entre los riesgos y facilita la toma de decisiones informadas sobre cómo mitigarlos.

5. Portafolio de acciones para la gestión de riesgos

Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de TI específicos y escenarios de riesgos de TI agregados.

- Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de TI específicos y escenarios de riesgos de TI agregados.
- Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.
- Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.

En base de la valoración del riesgo se deben de seleccionar las opciones para el tratamiento del riesgo tal cual se especifica a continuación.

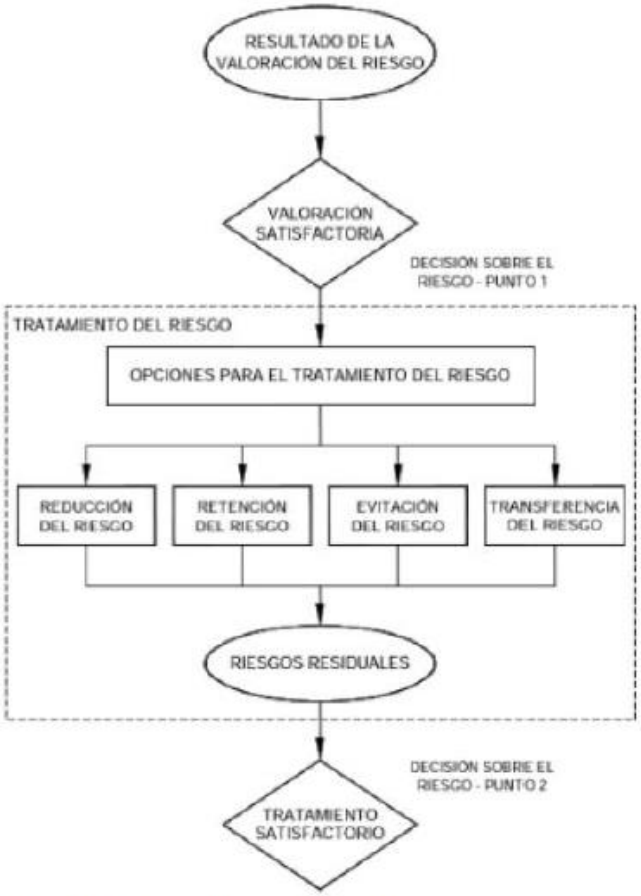


Figura 1: Actividades propuestas para el tratamiento del riesgo

Fuente 27005

Reducir, mantener, evitar y transferir riesgos son estrategias comunes en la gestión de riesgos que pueden aplicarse en el contexto de la seguridad de la información. A continuación, se detalla de cada una:

5.1. Reducir el Riesgo:

- Consiste en implementar medidas y controles para disminuir la probabilidad de ocurrencia o el impacto de un riesgo. Esto podría incluir la implementación de

controles de seguridad adicionales, la mejora de procesos o la inversión en tecnologías más seguras. Por ejemplo, el cifrado de datos puede reducir el riesgo de divulgación de información confidencial en caso de robo o pérdida de dispositivos.

5.2. Mantener el Riesgo:

- En algunos casos, puede ser aceptable o incluso deseable mantener ciertos riesgos si los costos asociados con la mitigación son prohibitivos o si los beneficios de la actividad superan los posibles impactos negativos. Sin embargo, es importante asegurarse de que la organización esté consciente y dispuesta a asumir estos riesgos. Por ejemplo, una empresa puede optar por mantener el riesgo de una interrupción del servicio en su sitio web durante picos de tráfico si los costos de implementar redundancias son demasiado altos en comparación con el beneficio esperado.

5.3. Evitar el Riesgo:

- Esta estrategia implica eliminar completamente la exposición a un riesgo, ya sea eliminando la actividad que lo genera o cambiando el enfoque de la organización. Por ejemplo, una empresa podría optar por evitar el riesgo de una brecha de seguridad al dejar de almacenar ciertos datos sensibles o externalizando ciertos procesos a proveedores de servicios especializados.

5.4. Transferir el Riesgo:

- Esta estrategia implica transferir la responsabilidad del riesgo a otra parte, como una compañía de seguros o un proveedor de servicios externo. Por ejemplo, una organización puede transferir el riesgo de pérdida de datos a través de un seguro cibernético o externalizar ciertas funciones de seguridad de la información a un proveedor de servicios de seguridad gestionada.

Al combinar estas estrategias de manera efectiva, la institución puede gestionar de manera proactiva los riesgos de seguridad de la información y minimizar su impacto. Es importante evaluar cuidadosamente cada riesgo y seleccionar la estrategia más apropiada en función de los objetivos y las necesidades específicas de la organización.

CONCLUSIONES

Este manual proporciona una guía para la implementación del marco de seguridad de la información en nuestra institución. Al seguir estos pasos y procesos, podemos garantizar la protección efectiva de nuestros activos de información y mantener la integridad, disponibilidad y confidencialidad de los datos en todo momento.

SOPORTE

La Dirección General de Tecnologías de la Información, proporciona asesoría y soporte directo, para ello puede escribir a nuestra mesa de ayuda, contactarnos telefónicamente o visitarnos en nuestra oficina:

Mesa de ayuda:	helpdesk@yachaytech.edu.ec
Teléfono:	06 2999 500 extensión 2600
Dirección:	Hacienda San José s/n y Proyecto Yachay Sector Sala Capitular