UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

DEPARTAMENTO ACADÉMICO DE CIENCIAS EN INFORMÁTICA Y SISTEMAS

CONTROLES DE SEGURIDAD SEGÚN LA NORMA ISO/IEC 27002:2013 PARA EL MEJORAMIENTO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

Tesis

Para optar el título de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

EINSTEIN ARNOLD ORTIZ MORALES

Asesor:

MG. WILLIAM ROGELIO MARCHAND NIÑO

Promoción 2013

Tingo María – Perú

2018

Universidad Nacional Agraria de la Selva Facultad de Ingeniería en Informática y Sistemas	**ACTA DE SUSTENTACIÓN DE TESIS N.° 03-2018**	COMISION DE GRADOS Y TITULOS **Fecha:** 28/09/2018

PARTE 3. CONFORMIDAD

PARTE 1. FASE INICIAL

Siendo las 18:15 horas del día 28 de SETIEMBRE de 2018; en la Sala de Grados de la UNAS, se instala el jurado calificador conformado por:

Jurado 1. Dr. WALTER RUBEN BERNUY BLANCO (Presidente)

Jurado 2. Ms.C. NILTON CHUCOS BAQUERIZO

Jurado 3. Ing. EDWIN JESUS VEGA VENTOCILLA

Oficializado mediante **Resolución N.° 101-2018-D-FIIS-UNAS** del 22 de agosto de 2018, para el proceso de sustentación del informe final de Tesis del bachiller **Einstein Arnold ORTIZ MORALES,** titulado: **"CONTROLES DE SEGURIDAD SEGÚN LA NORMA ISO/IEC 27002:2013 PARA EL MEJORAMIENTO DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA".** ASESOR**: Mg. William Rogelio MARCHAND NIÑO.**

Se manifiesta que el bachiller cumple con los requisitos exigidos de Ley y se le invita a disertar su Tesis por espacio de 30 minutos, asimismo se dispondrá de igual tiempo para la absolver preguntas y sugerencias.

PARTE 2. FASE DE PREGUNTAS Y RESULTADO

Culminada la exposición se inicia la fase de preguntas por parte del jurado calificador; también se invita a los asistentes a formular preguntas sobre el tema de Tesis.

Absueltas todas las peticiones, el jurado calificador procede a deliberar en privado la calificación y resultado.

Concluida la deliberación y en presencia del público asistente, el jurado calificador anuncia que el resultado de la Sustentación de Tesis es: APROBADO POR UNANIMIDAD

(NOTA: consignar una de la siguientes: DESAPROBADO, APROBADO POR MAYORIA o APROBADO POR UNANIMIDAD)

Con calificativo de: MUY BUENO

(NOTA: consignar una de la siguientes: EXCELENTE, MUY BUENO, BUENO, DEFICIENTE, MUY DEFICIENTE)

Por lo que se comunicará a las instancias correspondientes para el trámite respectivo.

De todo lo mencionado se firma al pie en señal de conformidad, siendo las 19:50 horas.

Firma:	Firma:	Firma:
Jurado 1: Walter Bernuy B.	Jurado 2: NILTON CHUCOS B.	Jurado 3: EDWIN J. VEGA V
Firma:		
Sustentante: EINSTEIN ARNOLD ORTIZ MORALES		

DEDICATORIA

A mis queridos padres, Fausto Ortiz López y Nilda Morales Roque, por su infinito amor y dedicación en cada etapa de mi formación personal y profesional.

A mis adorados hermanos, Elkin Ortiz Morales y Jackeline Ortiz Morales por la confianza que me brindan en cada momento de mi vida.

A Hallel Del Rosario, por llegar a nuestras vidas y enseñarnos el maravilloso valor que tiene una familia.

AGRADECIMIENTO

A Dios, nuestro creador, quien nos ama y bendice siempre.

A la Universidad Nacional Agraria de la Selva - Facultad de Ingeniería en Informática y Sistemas por haberme acogido y brindado los medios necesarios para mi formación profesional y a los docentes de la facultad por contribuir en mi formación académica.

A mi asesor Mg. William R. Marchand Niño, por haberme brindado la confianza de integrarme al equipo del CTIC, por su apoyo constante en la elaboración de la tesis y compartir siempre sus vastos conocimientos y experiencias académicas.

A los miembros del jurado, Dr. Walter Bernuy Blanco, Mg. Nilthon Chucos Baquerizo e Ing. Edwin Vega Ventocilla por los consejos y recomendaciones en la redacción final de esta tesis.

A Luz Cristina Rojas Ramírez y Cayle, por estar siempre a mi lado, brindarme mucho amor, cariño, alegría y motivarme siempre a la superación en cada etapa de mi vida personal y profesional.

A mis amigos, Eder, Johnny, Roy, Ruth, Jeraldine, Xiomara, Yovi, Leidy, Valery, Stephanie, Jennifer, Edgar, Milko, Fitzgeral, Vladimir, Samuel, Norris, Chalks, Arnaldo y a todos mis amigos y compañeros, por su apoyo incondicional y buenos deseos para cumplir este objetivo.

ÍNDICE

Página

ÍNDICE DE CUADROS

Cuadro Página

ÍNDICE DE FIGURAS

Figura Página

RESUMEN

La finalidad de esta investigación es implementar controles de seguridad de la información establecidos en la Norma ISO/IEC 27002:2013 para mejorar la gestión de la seguridad de la información en la Universidad Nacional Agraria de la Selva. La determinación de estos controles a implementar, se inicia con el diagnóstico situacional de la universidad en el contexto de la seguridad de la información, a fin de efectuar el análisis y gestión de riesgos de acuerdo con la Metodología de Análisis y Gestión de Riesgos (MAGERIT), en ese sentido, conocer el estado inicial del nivel de protección de los activos de información, determinar las amenazas, la probabilidad de que éstas se materialicen y las vulnerabilidades existentes en los activos, para finalmente estimar el nivel de riesgo asociado a los activos. Por otra parte, se realizaron pruebas de intrusión en los sistemas informáticos y uso de la Norma NTP-ISO/IEC 27005 para complementar la identificación de vulnerabilidades y riesgos asociados a los activos de información en estudio. En efecto, el propósito de esta investigación fue definir e implementar los controles de seguridad estratégicos y operativos que establece la Norma ISO/IEC 27002:2013, controles que se implementaron de manera incremental, por lo tanto, se consiguió mejorar la gestión de la seguridad de la información en la universidad. Finalmente, esta investigación servirá para alinear las bases en una futura implementación del sistema de gestión de seguridad de la información establecida en la Norma Técnica Peruana NTP-ISO/EIC 27001 que el Estado Peruano exige a toda institución pública.

Palabras clave: *seguridad de la información, gestión de la seguridad de la información, controles de seguridad, ISO/IEC 27002, activos de información.*

ABSTRACT

The purpose of this research is to implement security measures from the information established in the norm, ISO/IEC 27002:2013, for the improvement of the management of the information security at the Universidad Nacional Agraria de la Selva. The determination of the implementation of the controls begins with a situational diagnosis of the university within the context of the security of information with the purpose of bringing about the analysis and management of the risks according to the Analysis and Management of Risk Methodology (MAGERIT – acronym in Spanish), in this sense, to find the initial state of the protection levels of the information assets, to determine the threats, the probability that they materialize and the existing vulnerabilities in the assets, to, in the end, estimate the level of risk associated with the assets. On the other hand, intrusion tests were done on the information systems and the use of the NTP-ISO/IEC 27005 norm to complement the identification of vulnerabilities and risks associated with the information assets in study. In effect, the purpose of this research was to definite and implement the strategical and operational security controls established in the ISO/IEC 27002:2013 norm, controls that will be implemented in an increasing manner, thus, improving the security management of the information at the university. Finally, the research serves to align the bases for the future implementation of the information security management system established in the Peruvian Technical Norm, NTP-ISO/EIC 27001, which the Peruvian government requires of every public institution.

Keywords: *information security, information security management, security controls, ISO/IEC 27002, information assets*

INTRODUCCIÓN

La seguridad de información se ha vuelto crucial en las organizaciones de nuestra era, en tal sentido surge la necesidad de conocer el grado de seguridad a la cual se encuentran asociado los activos de información en la Universidad Nacional Agraria de la Selva (UNAS), y si éstos requieren la implementación de controles de seguridad que permitan preservar su integridad, confidencialidad y disponibilidad, de ese modo contar con herramientas que permitan mejorar la Gestión de la Seguridad de la Información.

Según últimas investigaciones sobre costos de las brechas de seguridad PONEMON INSTITUTE (2017), indica que la pérdida o robo de información sigue siendo uno de los eventos más costosos para las organizaciones, entonces para el caso de la UNAS, nos planteamos la interrogante ¿Cómo mejorar la gestión de la seguridad de la información? ya que al ser una institución en proceso de licenciamiento institucional es fundamental garantizar la mejora continua a través del tiempo respecto a la seguridad de la información.

El contenido de la presente tesis consta de siete capítulos: en el CAPÍTULO I, se especifica la formulación del problema, la justificación de la investigación, los objetivos e hipótesis que se debe validar. El CAPÍTULO II hace referencia al marco teórico en el que se detallan las teorías en el contexto de la seguridad de la información que fueron utilizados en el desarrollo de la tesis. En el CAPÍTULO III se evidencia el diagnóstico situacional respecto a incidentes de seguridad, la gestión de incidencias, los procesos institucionales y las políticas de gestión de seguridad que inicialmente se pudo contrastar. EL CAPÍTULO IV

uno de los más importantes capítulos, presenta los resultados del Análisis y Gestión de Riesgos que se utilizan en el siguiente capítulo. En el CAPÍTULO V se realiza el mapeo de los controles de seguridad sugeridos por la ISO/IEC 27002:2013 para finalmente realizar una propuesta a la oficina responsable de canalizar temas relacionados con la seguridad de la información. Para el caso del CAPÍTULO VI se detallan los materiales y métodos utilizados en esta investigación. En el CAPÍTULO VII se describe los resultados alcanzados, en el CAPÍTULO VII se discute los resultados contrastando con las teorías y demás revisión bibliográfica. Además, se incluye las conclusiones, recomendaciones bibliografía y anexos utilizados en el desarrollo de la tesis.

I. ASPECTOS GENERALES

1.1 Formulación del problema

1.1.1 Problema general

¿De qué manera mejora la gestión de la seguridad de la información en la Universidad Nacional Agraria de la Selva con la implementación incremental de controles de seguridad según la ISO/IEC 27002:2013?

1.1.2 Problemas específicos

A. ¿Cómo determinar los riesgos a la que se encuentran expuestos los activos de información?

B. ¿De qué manera se identifica las vulnerabilidades existentes en los activos de información?

C. ¿Qué controles de seguridad son necesarios para mejorar la seguridad de la información?

1.2 Justificación

El Plan Estratégico Institucional 2018 – 2021 de la universidad señala que, dentro de los principales problemas se ha identificado el incumplimiento de reglamentos y normatividad, haciendo que cada vez la información se encuentre expuesta a grandes riesgos.

La Universidad Nacional Agraria de la Selva, así como cualquier otra institución de nuestra era se encuentra interconectado a redes internas y

externas, por lo tanto, la información, los procesos, los sistemas, y personal que participan en la operación, manejo y protección de activos; se encuentran vulnerables a ataques, robos, alteración, sabotaje y otros delitos existentes; que de ocurrir repercutiría drásticamente en las actividades del personal administrativo, estudiantil y usuarios de cualquier sistema de información.

Actualmente las diferentes áreas de la universidad realizan flujos de datos que dependen de un sistema, de una red para conducir diariamente procesos, transacciones organizacionales y acceso crucial a la información; la información, así como otros activos tienen un valor muy significativo y demanda estar muy bien protegido.

La sociedad de la información, la normatividad peruana y las nuevas tecnologías de la información y comunicación, exigen la necesidad de mantener los aspectos básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad).

Por lo tanto, se decide realizar el análisis e implementación incremental de controles de seguridad de la norma ISO/IEC 27002:2013, del mismo modo definir políticas, procedimientos y herramientas que sirvan como base para implementación y certificación futura de la ISO/IEC 27001 en la universidad y aportar en el proceso de licenciamiento institucional de la UNAS.

A continuación, se considera algunos aspectos específicos que justifican la investigación:

A **nivel normativo**, la PCM mediante la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), actualmente denominada Secretaría de Gobierno Digital (SeGDi), establece el uso obligatorio de un

Sistema de Gestión de la Seguridad de la Información mediante un plan de seguridad de la información basada en la NTP-ISO/IEC 17799:2007 la misma que es análoga y cuyo origen se desprende de la Norma Internacional ISO/IEC 27002:2013. De esta manera poder cumplir con la legislación sobre la protección de los datos personales de todo el personal involucrado en la universidad, los registros críticos de la institución (registro de notas, base de datos del pabellón central, caja, biblioteca, entre otros) y los de Propiedad Intelectual.

A **nivel técnico**, la implementación de los controles de seguridad mencionados en la Norma Internacional ISO/IEC 27002:2013 nos permitirá manejar de manera más eficiente los sistemas informáticos actuales, infraestructura tecnológica; así como, definir e implementar herramientas de TI para mitigar los constantes problemas que afectan a los servicios tecnológicos de la institución y garantizar la confidencialidad, integridad y disponibilidad de la información en la UNAS.

A **nivel social**, generar confianza en la población estudiantil, administrativa y usuarios externos de la universidad demostrando el compromiso de la institución hacia la Seguridad de la Información proporcionando los elementos requeridos para gestionar de manera eficiente los riesgos que puedan atentar con la seguridad de su información, lo cual genera confianza en sus partes interesadas que es fundamental para el crecimiento y la sostenibilidad de la institución lo que permitirá garantizar su mejora continua a través del tiempo.

Lo expuesto anteriormente, nos indica la importancia que tiene la presente investigación pues nos permitirá abordar a un amplio conocimiento en el marco de la seguridad de la información dentro de la universidad y llegar a las

conclusiones y recomendaciones luego de la implementación de la Norma ISO/IEC 27002:2013, así dar cumplimiento de las resoluciones emanadas de la Presidencia del Consejo de Ministros en relación con la gestión de la seguridad de la información en las entidades públicas.

En resumen, se pretende realizar un análisis e implementación incremental de controles de seguridad de la Norma ISO/IEC 27002:2013 con el fin de establecer las bases para la posterior implementación de un sistema de gestión de seguridad de la información en la Universidad y cumplir con la normatividad nacional vigente y buscar una certificación a futuro.

1.3 Objetivos

1.3.1 Objetivo general

Implementar de forma incremental la Norma Internacional ISO/IEC 27002:2013 para mejorar la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva.

1.3.2 Objetivos específicos

A. Aplicar una metodología de Análisis y Gestión de Riesgos para determinar los riesgos a la que se encuentran expuestos los activos de información, en el contexto de la gestión de la seguridad de la información.

B. Identificar las vulnerabilidades de los activos de información en la UNAS, con la aplicación de herramientas de pruebas de intrusión, metodologías y estándares vigentes.

C. Determinar los controles de seguridad de la información a implementar según la norma ISO/IEC 27002:2013.

1.4 Hipótesis

1.4.1 Hipótesis general

Con la implementación de los controles de seguridad de la información de la Norma ISO/IEC-27002:2013 existe una mejora de al menos un 5% en la gestión de la seguridad de la información en la Universidad Nacional Agraria de la Selva.

1.4.2 Hipótesis específicas

A. La aplicación de una metodología de Análisis y Gestión de Riesgos permite determinar los valores cualitativos del riesgo (alto, medio, bajo) asociados a los activos de información.

B. La aplicación de herramientas y técnicas de prueba de intrusión, metodologías y estándares vigentes permite determinar vulnerabilidades técnicas de los activos de información.

C. Los controles de seguridad de la norma ISO/IEC 27002:2013 necesarios a implementar para mejorar la gestión de la seguridad de la información son los controles estratégicos (A.5.1.1, A.9.1.1, A.9.1.2, A.18.1.1) y operativos (A.7.2.2, A.12.2.1, A.13.1.1, 14.2.1).

1.4.3 Variables y dimensiones

a) Variable independiente (VI): Implementación de controles de seguridad.

Dimensiones:

- Controles operativos

Indicador:

- Nivel de implementación de controles operativos

- Controles estratégicos

Indicador:

- Nivel de implementación de controles estratégicos

b) Variable dependiente (VD): Gestión seguridad de la información en la UNAS.

Dimensiones:

- Eficiencia

Indicador:

- Capacidad de respuesta a incidentes.
- Costos de recuperación de incidentes respecto al presupuesto.
- Tiempo de recuperación de un incidente.

- Eficacia

Indicador:

- Nivel de riesgo en procesos institucionales.
- Nivel de riesgo en datos e información.
- Nivel de riesgo en sistemas y software.
- Nivel de riesgo infraestructura de TI y hardware.
- Nivel de riesgo en equipamiento auxiliar.
- Nivel de riesgo en personal.
- Nivel de riesgo en Infraestructura Física.

II. REVISIÓN DE LITERATURA

2.1 Antecedentes

Citamos algunos trabajos relacionados con el tema como son:

Lamilla Rubio, E. 2009. Desarrollo de políticas de seguridad informática e implementación de cuatro dominios en base a la Norma ISO/IEC 27002 para el Área de Hardware en la empresa UNIPLEX SYSTEMS S.A. en Guayaquil. Tesis de grado. Guayaquil, Ecuador, Escuela Superior Politécnica del Litoral.

Resultados Obtenidos:

El trabajo tiene como objetivo fundamental, diseñar e implementar políticas de seguridad informática en base a la norma ISO/EIC27002:2007 para la empresa UNIPLEX S.A. En la cual se proporcionan lineamientos básicos de la seguridad de la información, gestión de riesgos y diferentes alternativas para el tratamiento de los mismos. Se presenta un plan de tratamiento de riesgos en donde se identifican las acciones apropiadas, así como los responsables para minimizar los riesgos identificados, para posteriormente realizar la implementación del Proyecto de Gestión de Seguridad de la Información (PGSI) en base a los controles seleccionados y finalmente obtener como resultado el manual de procedimientos para la implementación del PGSI. Para la implementación del sistema se basan en única y exclusivamente en la norma de seguridad de la información ISO/EIC27002:2007. Para la realización se creó un

sumario que involucra los pasos para aplicar la seguridad en la empresa UNIPLEX SYSTEMS S.A. en Guayaquil. Se realizó además una auditoría para determinar las fortalezas y debilidades de la empresa UNIPLEX Guayaquil referente a las políticas de seguridad de Informática. Se establecieron propuestas de procesos y procedimientos de seguridad que incorporan una serie de medidas sobre los activos de información, conociendo, asumiendo y gestionando los posibles riesgos de forma documentada, estructurada, eficiente y adaptable a futuros cambios.

Aguirre Mollehuanca DA. 2014. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Tesis de grado. Lima, Perú, Pontificia Universidad Católica del Perú Facultad de Ciencias e Ingeniería.

Resultados Obtenidos:

En esta investigación trabajaron con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo. En consecuencia, se realizaron varias reuniones con la alta dirección que permitieran definir el alcance y las políticas del SGSI en la organización enfocándose en los procesos institucionales críticos de dicha entidad, posteriormente se realizó una serie de entrevistas que permitieran identificar y valorar los activos críticos de la organización, así como identificar y evaluar los riesgos a los cuales estos estaban sometidos.

Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 (norma análoga a la ISO/IEC 27002:2013 que es la versión actualizada) se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

Ampuero Chang, CE. 2011. Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Tesis de grado. Lima, Perú, Pontificia Universidad Católica del Perú.

Resultados Obtenidos:

El autor explica que para llegar a la implementación del SGSI es necesario obedecer el marco legal y regulatorio al que está ligado una organización y el uso obligatorio de algunas normas y estándares tales como la ISO/IEC 27002. De la misma manera indica que un adecuado análisis de riesgos es muy importante para el análisis de la seguridad de la información ya que de ella dependen los controles que serán necesarios implementar para el tratamiento de riesgos.

El incremento de los incidentes de seguridad a nivel empresarial, que afectan la operativa y continuidad del negocio de las organizaciones, con impactos a nivel económico, legal y de imagen, hacen que sea necesario la implementación de mecanismos de seguridad de la información, que contribuyan a establecer políticas, guiar en las mejores prácticas de seguridad y gestionar los riesgos asociados. Se suma a esto la creciente adopción a nivel mundial de

estándares de seguridad, algunos de los cuales ya han sido homologados a nivel nacional.

Por tanto, mejorar su situación frente a la seguridad de la información, mantener una ventaja competitiva en el mercado o proveer seguridad a sus clientes o socios, son algunos de los motivos por los cuales las organizaciones deciden adoptar estándares de seguridad.

Por otro lado, según las últimas investigaciones, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual INDECOPI (2013) muestra que hasta el 2014 se manejaba escasa información sobre la gestión de seguridad de la información en entidades públicas del Perú. Cabe mencionar que, hasta el momento, solo hay ocho empresas que tienen certificada la ISO/IEC 27001; las mismas que previamente tuvieron que implementar controles de seguridad basados en la ISO/EIC 27002 de las cuales, tres pertenecen al sector público, INDECOPI, la Oficina de Normalización Previsional (ONP) y La oficina Nacional de Procesos Electorales (ONPE), siendo este último la entidad más reciente en conseguirla, aunque al año 2016, solo tiene certificado 3 procesos:

1. Verificación y control de la información financiera de partidos políticos.
2. Trámite documentario.
3. Generación de expediente electrónico electoral y la línea de producción de microformas.

2.2 Marco teórico

2.2.1 Controles de seguridad de la información

Según Laudon (2012), los controles de seguridad de la información son métodos, políticas y procedimientos organizacionales que refuerzan la seguridad de los activos de la organización; la precisión y confiabilidad de sus registros, y la adherencia operacional a los estándares gerenciales.

Areitio (2008:24) expresa textualmente lo siguiente:

"Los controles también denominado salvaguardas o contramedidas, son procedimientos o dispositivos, físicos o lógicos que pueden proteger contra una amenaza, reducir la vulnerabilidad, limitar el impacto de un incidente no deseado y facilitar la recuperación".

También indica que las medidas que se adoptan frente a una amenaza pueden ser proactivas que son utilizadas para prevenir un problema y reactivas que se emplean cuando el daño se produce, para minimizar sus efectos. Asimismo, los controles de seguridad de la información se pueden clasificar en:

- ✓ **Controles Operativos:** que a su vez se dividen en preventivos (mecanismos de control de acceso, antivirus, mecanismos de identificación y autenticación, cortafuegos y mecanismos de cifrado) y detectivos (detección de intrusos, registros y pistas de auditorías)
- ✓ **Controles Estratégicos:** que también se dividen en preventivos (formación y concienciación en seguridad, planes de emergencia, contingencia

y recuperación ante desastres y planes de continuidad del negocio) y detectivos (revisiones y auditorias).

Por otra parte, autores como Fernández (2013), afirman textualmente lo siguiente:

"Los controles de seguridad representan todas las acciones que deben implementarse en una organización y tienen el objetivo de prevenir, contrarrestar o minimizar los riesgos sobre la seguridad y mejorar la protección ante las amenazas".

De igual modo, señala que los controles que deben implementarse en una organización pueden ser tanto soluciones técnicas como medidas de concienciación y capacitación por parte de los de usuarios de los activos de información de las reglas de seguridad definidas.

De acuerdo con su naturaleza los controles pueden ser:

✓ **Controles procedimentales o administrativos:** Políticas, procedimientos, leyes, regulaciones, políticas, guías, estándares, etc.

✓ **Controles físicos:** Puertas, cierres, detectores de incendios, extintores. etc.

✓ **Controles técnicos o lógicos:** Mecanismos de autenticación y control de acceso, antivirus, firewalls, etc.

Los controles al respecto de su aplicación ante la ocurrencia de un incidente de seguridad pueden ser:

✓ **Controles preventivos:** Previenen la posibilidad de ocurrencia de un incidente de seguridad antes de que se materialice, los controles disuasorios son un tipo especial de controles preventivos diseñados para hacer desistir a un potencial atacante antes de que se produzca el ataque.

✓ **Controles detectivos:** Identifican que se está produciendo un incidente de seguridad en la organización y aportar toda información posible relativa al mismo. En algunos casos este tipo de controles también aplican medidas correctivas.

✓ **Controles correctivos:** Limitan y en ciertos casos corrigen la extensión del daño producido por el incidente de seguridad, los controles mitigantes son un tipo de controles correctivos que además puede cubrir las deficiencias de otros controles.

Gómez y Andrés (2012), afirman que la selección de controles es un punto crítico del Sistema de Gestión de la Seguridad de la Información, a la hora de seleccionar o rechazar un control se debe considerar hasta qué punto ese control va a ayudar a reducir el riesgo que hay y cual va ser el coste de su implementación y mantenimiento; cabe la posibilidad de que un control que se estime oportuno implementar, sea demasiado costoso o difícil de implementar para una organización, ya sea por resistencia al cambio o por falta de formación, y que haya que excluirlo de la selección por esos y otros motivos justificados. De igual forma, mencionan que el coste de implementación y mantenimiento de un control no debe superar al costo del activo que se desea proteger.

Sin embargo, Gonzales (2015), afirma que el estándar ISO/IEC 27002:2013 proporciona directrices para las normas de seguridad de la información de la organización y las buenas prácticas de gestión de la seguridad de la información, incluyendo la selección, implementación y gestión de controles de seguridad de la información. También señala que en la ISO/IEC 27002: 2013 se detallan los controles de la seguridad de la información que pueden ser seleccionados dependiendo de las decisiones organizacionales basadas en los criterios para la aceptación del riesgo, las opciones para el tratamiento de riesgos y el acercamiento a la gestión general del riesgo aplicado a la organización, y debería también estar conforme a la legislación y regulaciones nacionales e internacionales relevantes.

Los controles serán seleccionados e implementados de acuerdo con los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo, por lo que la implementación es lo que permite garantizar que cada aspecto que se valoró con un cierto riesgo queda cubierto, es decir se tratará de minimizar lo más que pueda el riesgo previamente identificado, manifiesta Corletti (2011).

De los párrafos anteriores, se puede concluir que los controles de seguridad representan todas las acciones preventivas y/o correctivas en caso se detecten eventos que escapan a la naturaleza de un proceso; estas acciones incluyen políticas, procedimientos, estructuras organizacionales, entre otras y que pueden ser de naturaleza administrativa, técnica, gerencial o legal. Además, los controles de seguridad se pueden aplicar a los datos, los usuarios, las operaciones y a todos los activos que tengan valor para una organización.

Puesto que aún con las mejores herramientas de seguridad, los sistemas de información no serán confiables y seguros a menos que se conozca cómo y en dónde implementarlos, por tanto, se necesitará saber en dónde está el riesgo y qué controles se debe establecer para proteger la información.

Finalmente, para el caso de esta investigación se tomará la norma ISO/IEC 27002:2013, es en esencia una guía que permite conocer qué se puede hacer para mejorar la seguridad de la información, describe los objetivos de control y los controles recomendables que deben ser implementados en las organizaciones que se deseen mejorar la seguridad de la información o se encuentren en proceso de implementación de un Sistema de Gestión de la Seguridad de la Información. Asimismo, expone en distintos campos, una serie de apartados a tratar con relación a la seguridad de la información, los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de sugerencias para cada uno de esos controles. Sin embargo, la propia norma ya indica que no existe ningún tipo de priorización entre controles, y que las sugerencias pueden variar de acuerdo con las necesidades de las organizaciones.

2.2.2 Gestión de la seguridad de la información

Antes de referirnos a Gestión de Seguridad de la Información, se debe tener claro el significado de “seguridad”, “información” y “gestión”.

La seguridad viene a ser la protección de los activos frente a acciones o situaciones no deseadas, mediante la implementación de controles o salvaguardas, lo que suele suponer una inversión y un esfuerzo, todo ello para

proteger los intereses de los usuarios, empleados, clientes, proveedores y a toda la organización. (Peso, 2004)

Es preciso acotar, que la seguridad no es ningún hito, por el contrario, representa un proceso continuo que se debe gestionar conociendo siempre las vulnerabilidades y las amenazas existentes sobre cualquier activo de información, teniendo siempre en cuenta las causas de riesgo y la probabilidad que ocurran, así como el impacto que se puede tener. Una vez conocidos todos estos puntos, y nunca antes, se deben tomar medidas de seguridad oportunas.

Con respecto a la información, se define como todo aquel elemento que contenga datos organizados y procesados, que se encuentran almacenados en cualquier tipo de soporte sea físico o digital y que son de utilidad para la toma de decisiones como, por ejemplo, documentos, libros, correspondencia, patentes, estudios de mercado, datos de los empleados, manuales de usuario, base de datos, copias de seguridad, etc. Por lo tanto, la información se cataloga como el activo más importante para una organización y requiere una protección adecuada, manifiesta Escrivá, et al. (2013).

Escrivá, et al. (2013), también define la seguridad de la información como un conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información.

Seguridad de la información es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo,

medio de almacenamiento y forma en que se transmita. La seguridad de la información debe ser prioridad de la dirección ejecutiva; por lo tanto, debe comenzar como una gran responsabilidad de gestión corporativa (Von-Solms, 2006).

La seguridad de la información protege a la información, propiamente dicha, de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios (INDECOPI, 2004).

De lo mencionado se puede definir en primera instancia como seguridad de la información a todas aquellas medidas preventivas y reactivas de la persona, las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma.

Arjonilla y Medina (2013), indican que el concepto de gestión seguridad de la información suele ser percibido de forma sesgada en muchas organizaciones, al confundir la parte con el todo, en demasiadas ocasiones se restringen el ámbito de dicha seguridad a uno de sus componentes, la “seguridad informática”, que no es más que el conjunto de procedimientos orientados a evitar la destrucción, modificación, utilización y difusión no autorizada de datos y la información de una organización. En cambio, la gestión de seguridad de la información contempla que además de la seguridad informática, la organización debe cuidar la seguridad del entorno del que depende el sistema, de los procesos y procedimientos, y de las actuaciones de las personas que interactúan con el

sistema de información. De este modo la gestión de la seguridad de la información puede representarse en una pirámide que conforman los elementos de seguridad de la información tal como se muestra en la Figura 1.

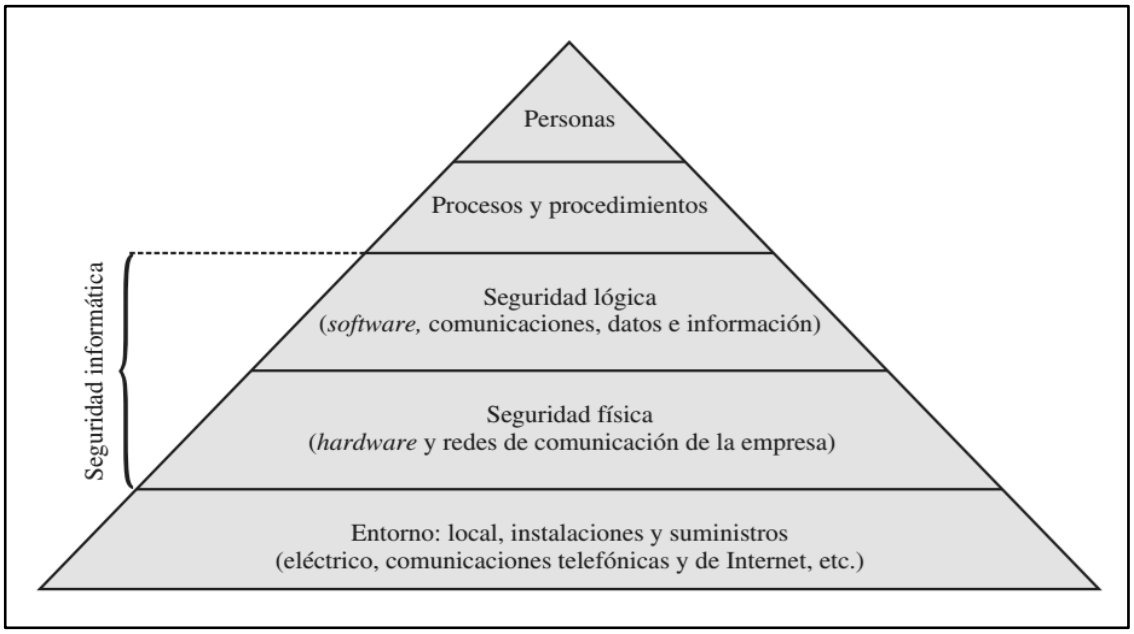


Figura 1. Elementos de la seguridad de la información
Fuente: Arjonilla y Medina (2013)

Areitio (2008), manifiesta lo siguiente:

"La gestión de la seguridad de la información necesita medidas de seguridad técnicas, de procedimientos, físicas, lógicas, de personal y de gestión; la gestión de la seguridad de la información engloba todas las actividades relacionadas con la dirección y control de la seguridad de los activos de información, estas actividades consisten en la valoración de las amenazas y del estado actual en el que se encuentra la seguridad de la información en la organización, el diseño y la implementación de controles de seguridad administrativos, como son las reglas de seguridad de la información para los empleados o los controles técnicos, como los sistemas de control de acceso y la

operación de los esfuerzos del día a día para preservar la seguridad de la información, mediante documentación y respuesta a incidentes, la información, la formación y concienciación de los empleados"

Bajo este concepto la gestión de la seguridad de la información es el modo en la que se emplean medidas de seguridad a nivel estratégico y operativo que permite evaluar el estado actual y asegurar a los activos de información frente a las amenazas que se puedan presentar.

Por otra parte, Ampuero (2011), manifiesta que para llegar gestionar de manera eficiente la seguridad de la información, es necesario obedecer el marco legal y regulatorio al que está ligado una organización y el uso obligatorio de algunas normas y estándares tales como la ISO/IEC 27002. También indica que un adecuado análisis de riesgos es muy importante para el análisis de la seguridad de la información ya que de ella dependen los controles que serán necesarios implementar para el tratamiento de riesgos.

En otro sentido, INCIBE (2015), indica que, existen varias maneras de clasificar métricas de gestión de la seguridad de la información, La Guía de Medición del Desempeño para la Seguridad de la Información (NIST SP 800-55) divide las métricas de seguridad en tres categorías y enlaza cada una con los niveles de madurez de seguridad, las categorías son:

- ✓ **Implementación:** métricas utilizadas para mostrar progresos en la implementación de políticas y procedimientos y controles de seguridad individuales
- ✓ **Eficacia / eficiencia:** métricas utilizadas para monitorear los resultados de la implementación del control de seguridad para un solo control a través de varios controles
- ✓ **Medidas de impacto:** utilizadas para transmitir el impacto del programa de seguridad de la información en la misión de la institución, a menudo mediante la cuantificación de la evitación de costos o la reducción del riesgo producido por el programa de seguridad general

En resumen, la gestión de la seguridad de la información consiste en garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías; ya que el incremento de los incidentes de seguridad a nivel empresarial, que afectan la operatividad y continuidad del negocio de las organizaciones, con impactos a nivel económico, legal y de imagen, hacen que sea necesario la implementación de mecanismos que ayuden a mejorar la gestión de seguridad de la información, a esto se suma la creciente adopción a nivel mundial de estándares de seguridad, algunos de los cuales ya han sido homologados a nivel nacional.

Por consiguiente, las métricas que se utilizan en la gestión de la seguridad de la información son a nivel estratégico y operativo, las métricas

realmente útiles indican el grado en el que se están cumpliendo las metas de seguridad y conducen las acciones tomadas para mejorar la seguridad de la información de una organización.

2.2.3 Análisis y gestión de riesgos

Areitio (2008), manifiesta lo siguiente:

"El análisis de riesgos es un proceso consistente en identificar los peligros que afectan la seguridad, determinar su magnitud e identificar qué áreas necesitan salvaguardas. La valoración de riesgos es el resultado del proceso del análisis de riesgos."

En otro sentido, indica que para tratar de minimizar los efectos de un problema de seguridad se realiza el denominado análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas de la seguridad en una organización, que es saber qué se quiere proteger, contra quién o qué se quiere proteger y cómo se va a proteger, para lo cual existen dos enfoques básicos para realizar el análisis de riesgos, uno cualitativo y otro cuantitativo.

Desde otro punto de vista, en España, el Ministerio para las Administraciones Públicas (MAP, 2012) afirma lo siguiente:

"Si el sistema aspira a una certificación en temas de seguridad de la información, el análisis de riesgos es un requisito previo que exigirá el evaluador. Es la fuente de información para determinar la relación de controles pertinentes para el sistema y que por tanto deben ser inspeccionados".

Por lo tanto, para una adecuada implementación de controles de seguridad de la información en función de los riesgos identificados y el nivel de criticidad; se propondrán una serie de controles que permitan asumir el riesgo si la probabilidad de ocurrencia es muy baja o reducir el riesgo a través de la implementación de controles de seguridad según sea necesario.

Pero también se debe tener en cuenta la explicación que presenta MINHAFP (2012), que expresa lo siguiente:

"El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra). El resultado del análisis es sólo un análisis. A partir de ello disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados), de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo".

Del concepto anterior se puede afirmar que para el análisis de riesgos se tiene que considerar aspectos fundamentales como son: probabilidad, amenaza, riesgo e impacto; factores clave que se deben tener en cuenta al momento de realizar un análisis de riesgos.

Por otra parte, la Gestión de Riesgo de la seguridad de la información es el proceso de identificar, medir, controlar y minimizar los riesgos de seguridad en sistemas de información a un nivel proporcional al valor de los activos protegidos. La identificación y la gestión del riesgo están en funcionen de tres variables: criticidad, vulnerabilidad y amenaza. Areitio (2008).

Bajo este concepto, en la Gestión de Riesgos se seleccionan posibles soluciones para cada riesgo para lo cual primero se debe estimar el riesgo, definido como la criticidad del impacto ponderado con la tasa de ocurrencia de la amenaza e implementar las salvaguardas necesarias para lo cual se requiere la participación de todo el personal involucrado con los sistemas de información.

En conclusión, el análisis de riesgos consiste en no solo una observación detallada y sistemática, sino que principalmente es una propuesta metodológica, que permite la comprensión de los riesgos, sus orígenes, las consecuencias potenciales, residuales y la probabilidad de que esto se materialice.

El análisis de riesgos también es un proceso de mejora continua, que busca estimar las probabilidades de que ocurran eventos indeseables que permitan medir la magnitud de los impactos negativos en el transcurso de intervalos determinados de tiempo, mediante el análisis de riesgos se deben alcanzar los siguientes objetivos: determinar los activos más significativos, establecer las amenazas a las que están expuestos cada activo, estimar el

impacto si se materializa alguna amenaza y escoger salvaguardas apropiadas para los activos

Por último, la Gestión de Riesgos es un proceso independiente pero que utiliza los resultados del análisis de riesgos que nos ayuda a seleccionar y establecer los controles de seguridad apropiados para mitigar los riesgos identificados. La gestión de riesgos implica que se deben dar tratamiento a los riesgos identificados mediante el uso de controles o salvaguardas de seguridad adecuados.

2.3 Marco conceptual

2.3.1 Controles de seguridad

Son los procedimientos o mecanismos estratégicos u operativos que al implementarse permiten reducir el riesgo y por consiguiente que los activos de información estén mejor protegidos, los controles pueden actuar disminuyendo el impacto o la probabilidad de un incidente de seguridad de la información (Fernández, 2013).

Areitio (2008) afirma que, los controles de seguridad de la información son denominados también salvaguardas cuyo objetivo es proteger a los activos contra una amenaza, reducir la vulnerabilidad, limitar el impacto de un incidente no deseado y facilitar la recuperación. Los procesos para determinar los controles de seguridad más apropiados y rentables son a menudo bastante complejos y a veces se convierte en una cuestión subjetiva, no obstante, una de

las funciones primarias del análisis de riesgos es hacer que este proceso sea más objetivo.

El control estratégico requiere del monitoreo sistemático en puntos de control estratégicos, así como de modificar la estrategia de la organización con base en esa evaluación. Planear y controlar se relacionan estrechamente; por tanto, los planes estratégicos requieren control estratégico ya que el control facilita la comparación de las metas propuestas con el desempeño real, también permite oportunidades de aprendizaje, que a su vez son la base del cambio organizacional. Mediante el control estratégico se logra el entendimiento, no sólo del desempeño organizacional, sino también del siempre variable ambiente, al monitorearlo.

Por otra parte, los controles operativos corresponden a la asignación de actividades puntuales que se debe realizar en la organización, se desarrolla a partir de los lineamientos proporcionadas por los niveles de planeación estratégicos. La función de estos controles es que las actividades rutinarias de la organización se realicen en forma eficaz.

Por lo tanto, los controles de seguridad representan todas las acciones que deben implementarse en una organización y tienen el objetivo de prevenir, contrarrestar o minimizar los riesgos sobre la seguridad y mejorar la protección ante las amenazas. Los controles que deben implementarse en una organización pueden ser de nivel estratégico y operativo, la norma ISO/IEC 27002:2013 contempla dominios de control que abarcan desde los aspectos estratégicos de un sistema de gestión de seguridad de la información hasta los operativos.

2.3.2 Gestión de la seguridad de la información

La gestión, en el contexto de la seguridad de la información son aquellas actividades relacionadas con la dirección y control de la seguridad de los activos de información, estas actividades consisten en la valoración de las amenazas y del estado actual en el que se encuentra la seguridad de la información en la organización y gestionar los riesgos identificados proporcionando información adecuada para la toma de decisiones.

Areitio (2008) manifiesta que hablar de gestión hace referencia al compromiso de la dirección de una organización y consiste en un conjunto de políticas y controles internos por los cuales se dirigen y gestionan las organizaciones, sin importar su tamaño. La gestión de la seguridad de la información puede ser medida mediante indicadores de eficiencia y eficacia.

Los indicadores de eficiencia miden el logro de un objetivo utilizando la cantidad mínima necesaria de recurso, es decir se busca un uso óptimo de los recursos disponibles para lograr los objetivos deseados. Aportan información al proceso sobre el mejor o peor funcionamiento de los mecanismos de control ya implantados. El conjunto de controles para mitigar el riesgo debe tener un impacto sustancial en el riesgo percibido, atenuando el riesgo por debajo de algún nivel umbral.

Los indicadores de eficacia se relacionan con la comparación entre lo alcanzado y lo esperado, los niveles de eficacia corresponden a porcentajes de ejecución muy altos cuya calificación cada vez es más difícil de obtener.

Normalmente niveles superiores de cumplimiento exigen mayores esfuerzos e imponen mayor grado de dificultad.

Por lo tanto, eficacia es el grado en que se logran los objetivos y metas de un plan, es decir cuánto de los resultados esperados se alcanzó.

El concepto de gestión de la seguridad de la información implica identificar activos, establecer políticas y procedimientos en relación con los objetivos de una organización con la finalidad de mantener una exposición menor al riesgo que la propia organización decide asumir. (Cárdenas, 2008)

Gestionar la seguridad de la información es una tarea integral y que involucra actividades como conocer el estado de riesgo de los activos, asumir, minimizar o transferir el riesgo identificado mediante un sistema de gestión definido, documentado y conocido por toda la organización, y que se revisa y mejora constantemente. Finalmente, la gestión, describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización.

Teniendo en cuenta lo anterior, se puede definir que la gestión de la seguridad de la información es coordinar y dirigir una serie de actividades con recursos disponibles para proteger los activos de información. Estas actividades requieren de una estrategia alineada a la organización y sus objetivos, también del uso de recursos y un conjunto de actividades dirigidas y coordinadas que se extienda a través de toda la organización, desde la alta dirección hasta los usuarios finales.

2.4 Marco normativo

2.4.1 Estándares de seguridad de la información

A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Por otra parte, se tiene a ISACA acrónimo de *Information Systems Audit and Control Association* (Asociación de Auditoría y Control de Sistemas de Información), ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase. Establecida en 1969, ISACA es una asociación global sin ánimo de lucro de 140 000 profesionales en 180 países. ISACA también ofrece *Cybersecurity Nexus*™ (CSX), un recurso integral y global en ciberseguridad, y COBIT®, un marco de negocio para gobernar la tecnología de la empresa. ISACA adicionalmente promueve el avance y certificación de habilidades y conocimientos críticos para el negocio, a través de las certificaciones globalmente respetadas: *Certified Information Systems Auditor* (CISA), *Certified Information Security Manager* (CISM), *Certified in the Governance of Enterprise IT* (CGEIT®) y *Certified in Risk and Information Systems Control* (CRISC).

a) ISO/IEC 27001:2013

Publicada el 25 de Setiembre de 2013, es la norma principal de la familia de la ISO 27000, y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del ciclo PLAN – DO – CHECK – ACT para el diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Un SGSI como el que se especifica en la ISO/IEC 27001:2013 tiene una visión holística y coordinada de los riesgos de seguridad de la información de la organización a fin de implementar un conjunto completo de controles de seguridad de la información en el marco global de un sistema de información.

b) ISO/IEC 27002:2013

Denominado *"Tecnología de la Información, Técnicas de Seguridad, Código de Buenas Prácticas para Controles de Seguridad de la Información";* se trata de la segunda edición de la norma, la cual reemplaza y cancela el ISO/IEC 27002:2005. Esta norma contiene el código para la práctica de la gestión de la seguridad de la información (anteriormente denominados BS 7799 Parte 1 y también, norma ISO/IEC 17799).

Este estándar internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en

este estándar proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

La norma ISO/IEC 27002:2013 se encuentra distribuido en 14 dominios, 35 objetivos de control y 114 controles, que abarcan de una forma integral todos los aspectos estratégicos y operativos que han de ser tenidos en cuenta por las organizaciones. Esta norma se diseñó para ser utilizado por las organizaciones que pretenden:

- ✓ Seleccionar los controles dentro del proceso de implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001;
- ✓ Implementar controles de seguridad de la información generalmente aceptadas.
- ✓ Desarrollar sus propias directrices de gestión de seguridad de información.

La norma ISO/IEC 27002:2013 contiene las mejores prácticas de los objetivos de control y controles en los siguientes dominios de gestión de seguridad de la información:

1. Política de la seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad de los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía
7. Seguridad física y ambiental.

8. Seguridad de las operaciones.
9. Seguridad de las comunicaciones.
10. Adquisición, desarrollo y mantenimiento de sistemas.
11. Relaciones con los proveedores.
12. Gestión de incidentes de seguridad de la información.
13. Aspectos de seguridad de la información de la gestión de la continuidad de negocio.
14. Cumplimiento.

Figura 2. Dominios de control ISO/IEC 27002:2013
Fuente: http://www.unit.org.uy/normalizacion/sistema/27000/

Los 14 dominios también pueden ser agrupados en función a los tipos de seguridad, entre ellos se tiene a la seguridad organizativa, seguridad lógica, seguridad física y seguridad legal.

Los objetivos de control están destinados a ejecutarse para satisfacer los requisitos identificados por una evaluación de riesgos. Además, el ISO/IEC 27002:2013 pretende ser una base común y guía práctica para el

desarrollo de estándares de seguridad de la organización y las prácticas eficaces de gestión de la seguridad, y para ayudar a construir la confianza en las actividades interinstitucionales.

Los controles generales que este documento contiene se procederán a seleccionar aquellos que aplican según el análisis de riesgos previo que se realizará. Cabe mencionar que todos los controles y objetivos de control que se detallen en este documento deben estar acompañados por la justificación correspondiente de su elección o exclusión.

2.4.2 Ley Nº 29733 - Ley de protección de datos personales

El año 2011, se promulgó la ley de protección de datos personales, que tiene como objetivo garantizar el derecho fundamental a la protección de los datos personales, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconoce.

En el 2013, se aprobó esta ley y entró en vigencia en mayo del mismo año. Consta de 7 títulos y 40 artículos que describen los principios, el tratamiento de datos personales, los derechos del titular, obligaciones del titular y el encargado del banco de datos, la autoridad nacional de cumplimiento de la ley y finalmente, las infracciones y sanciones administrativas ante la presunta comisión de actos contrarios a lo dispuesta a ley. Toda información relativa a una persona se le conoce como dato personal. La norma se aplica a los datos personales contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realice en el territorio nacional.

El sentido de esta ley es que toda información personal no sea usada indiscriminadamente sin el consentimiento de la persona, salvo se establezcan determinadas excepciones como la investigación de un delito. El ente regulador de esta ley es la Dirección General de Protección de Datos Personales o Autoridad Nacional de Protección de Datos Personales cuya función es la de cumplir y hacer cumplir la normatividad vigente en materia de protección de datos personales. Sus funciones son administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.

2.4.3 Decreto Supremo N° 031-2006-PCM

Mediante la el cual se aprueba el "Plan de Desarrollo de la Sociedad de la información en el Perú - La Agenda Digital Peruana".

La Agenda 2.0 define una visión del desarrollo de la Sociedad de la Información y el Conocimiento en el Perú, a ser desarrollada a través de ocho objetivos, con sus respectivas estrategias, las que deben ser complementadas con acciones, proyectos y actividades por parte de las instituciones públicas, entidades privadas, universidades y agentes de la sociedad civil comprometidas en lograr un país con mayor grado social y económico donde las TIC se hayan convertido en un aspecto central para ello, no como fin en sí mismo sino como las herramientas transversales que apoyarán a lograr objetivos institucionales, locales, regionales y nacionales.

2.4.4 Resolución Ministerial Nº 246-2007-PCM

Mediante esta resolución se aprueba el uso obligatorio de la "NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas

para la gestión de la seguridad de la información” en todas las entidades públicas que pertenecen al Sistema Nacional de Informática. Esto significaba el reemplazo de la NTP-ISO/IEC 17799:2004 que en ese tiempo era de uso obligatorio.

2.4.5 Resolución Ministerial Nº 197-2011-PCM

Mediante esta resolución se establece como fecha límite para la implementación de la “NTP ISO/IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información” el día 31 de diciembre del 2012 para todas aquellas empresas que pertenecen al Sistema Nacional de Informática.

Valga aclarar que a la fecha las normas técnicas peruanas no han sido actualizadas, y la norma análoga a la NTP ISO/IEC 17799:2007 es el estándar internacional ISO/IEC 27002:2013, en su última versión actualizada.

2.4.6 Resolución Ministerial Nº 004-2016-PCM

Se define que se debe implementar de manera obligatoria la “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición” y da nuevas fechas límites para desarrollar la implementación para todas las empresas públicas.

La norma fue emitida el 8 de enero de 2016, y establece que las entidades integrantes del Sistema Nacional de Informática tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma. Asimismo, las entidades públicas tendrán un plazo de 60 días contados

a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), actualmente denominada Secretaría de Gobierno Digital (SeGDi) de la Presidencia del Consejo de Ministros (PCM).

III. DIAGNÓSTICO SITUACIONAL

3.1 Incidentes de seguridad de la información

La UNAS, en los últimos años ha sufrido múltiples incidentes, dado que, según los reportes emitidos por el CTIC el año 2015, 2016 y 2017 se ha producido incidentes que afectan a los sistemas de información y sistemas informáticos, tales como: Pérdida de datos, pérdida u olvido de contraseñas, ataques de denegación de servicios, ataques de SQLi, ataques de *dafecement* de página web, infección por virus o *malware* e instalación de programas crackeados, siendo éstos los incidentes más comunes. A continuación, el Cuadro 1, resume los incidentes ocurridos en la UNAS en el periodo del año 2015 al 2017:

Cuadro 1. Registro histórico de incidentes de seguridad en la UNAS

Incidentes	Año		
	2015	2016	2017
Infección por virus o *malware*	10	7	4
Instalación de programas crackeados	970	1000	985
Pérdida de datos	6	4	5
Pérdida u olvido de contraseñas	10	7	8
Conexión de dispositivos no autorizados	6	3	3
Ataques de DDoS	2	1	0
***Defacement* de página web**	2	2	0
Ataques de SQLi	4	0	0

Fuente: Centro de Tecnologías de la Información y Comunicación - UNAS

Por otro lado, se ha observado que, en aspectos relacionados a la preservación de la seguridad de la información, no existe oficialmente un sistema de gestión de seguridad de la informacion, definido y aprobado mentiante una resolución institucional, las políticas y procedimientos no se encuentran documentadas; además no se tiene definido los riesgos y amenazas a la cual se exponen la información, los servicios de TI, infraestructura tecnológica y demás recursos.

3.2 Gestión de incidencias en la atención al usuario.

El Centro de Tecnología de la Información y Comunicación no tiene establecido un procedimiento formal para la gestión de incidencias, cada usuario realiza solicitudes de solución de incidencias de la siguiente manera:

Vía telefónica: Mediante llamadas directamente a las extensiones de la oficina del CTIC o llamando a los teléfonos celulares del personal.

Vía correo electrónico: Mediante el envío de correo electrónico al personal del CTIC.

Presencial: Realizando la visita a la oficina o puesto de trabajo del personal especializado para buscar solución a las incidencias reportadas.

En ninguno de los casos se tiene clara la forma en la que se deben registrar las incidencias y en la mayoría de las ocasiones no queda un documento del incidente ni de la solución que se dio al mismo; todas las incidencias son atendidas de acuerdo al orden de reporte o de acuerdo al criterio que toma el personal encargado de su diagnóstico.

3.3 Procesos institucionales

En el mapa de procesos de la UNAS que se muestra en la Figura 5, se identifican 3 procesos fundamentales: **Procesos Estratégicos**, que involucran actividades de Planeamiento Estratégico, Gestión por Procesos, Gestión de la Calidad y Bienestar Estudiantil; **Procesos Misionales**, Responsabilidad Social Universitaria, Formación Profesional e Innovadora e Investigación Formativa y Científica como bases para impulsar el desarrollo y fortalecimiento institucional los cuales son soportados por los **Procesos de Apoyo** Gestión de Capital Humano, Gestión de Recursos Financieros, Gestión de la Infraestructura Equipamiento y Mantenimiento y por último la Gestión de la Información y Grupos de Interés.

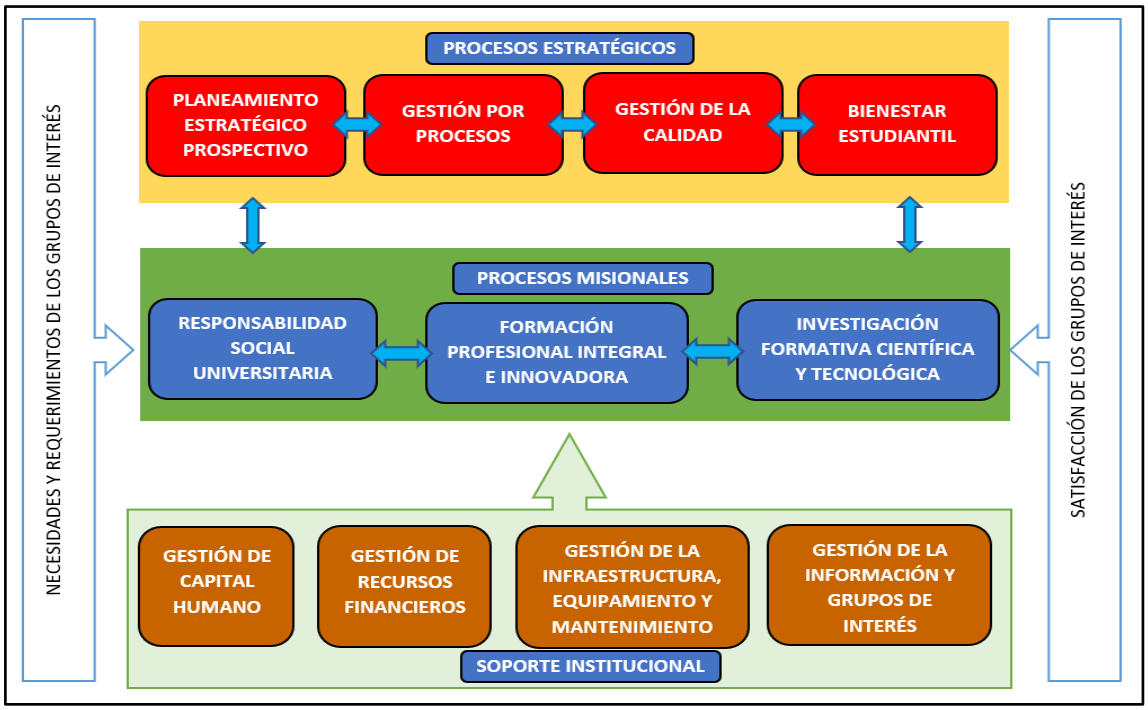


Figura 3. Mapa de procesos de la UNAS
Fuente: PEI 2018-2020

3.4 Políticas de gestión de la seguridad de la información

Según la VIII Encuesta Nacional de Recursos Informáticos en la Administración (ENRIAP) del año 2010, de 552 entidades públicas, 182 (33%) habían iniciado la implementación de la norma ISO/IEC 17799, mientras que las que no implementaron fueron 370 entidades públicas (67%), lo cual representa un avance muy lento respecto a la implementación mecanismos que permitan mejorar la Gestión de Seguridad de la Información en las instituciones públicas.

La universidad se encuentra incluido dentro del 67% de entidades que hasta el momento no tienen implementado un Sistema de Gestión de Seguridad de la Información, lo que representa que estamos incumpliendo la Resolución Ministerial N.º 129-2012-PCM, normativa que el estado peruano exige a toda institución pública, ante ello la institución, los procesos y sus sistemas de información están expuestas a un número cada vez más elevado de amenazas que aprovechando cualquier vulnerabilidad existente, pueden someter a los activos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Por otra parte, también se percibe que a nivel de políticas integrales aún no se cuenta con un documento formal que permita gestionar la seguridad de la información de forma adecuada, esto se debe a la falta de compromiso y apoyo de la alta dirección, que es la que debe establecer y hacer cumplir la política de seguridad de la información.

Tal como se puede evidenciar en la Figura 4 se aprecia que, dentro de los problemas fundamentales de la UNAS, existe una carencia de políticas de

gestión y esto incluye políticas de seguridad de la información, asimismo otro de los problemas que más resalta es el incumplimiento de los reglamentos y normatividad.

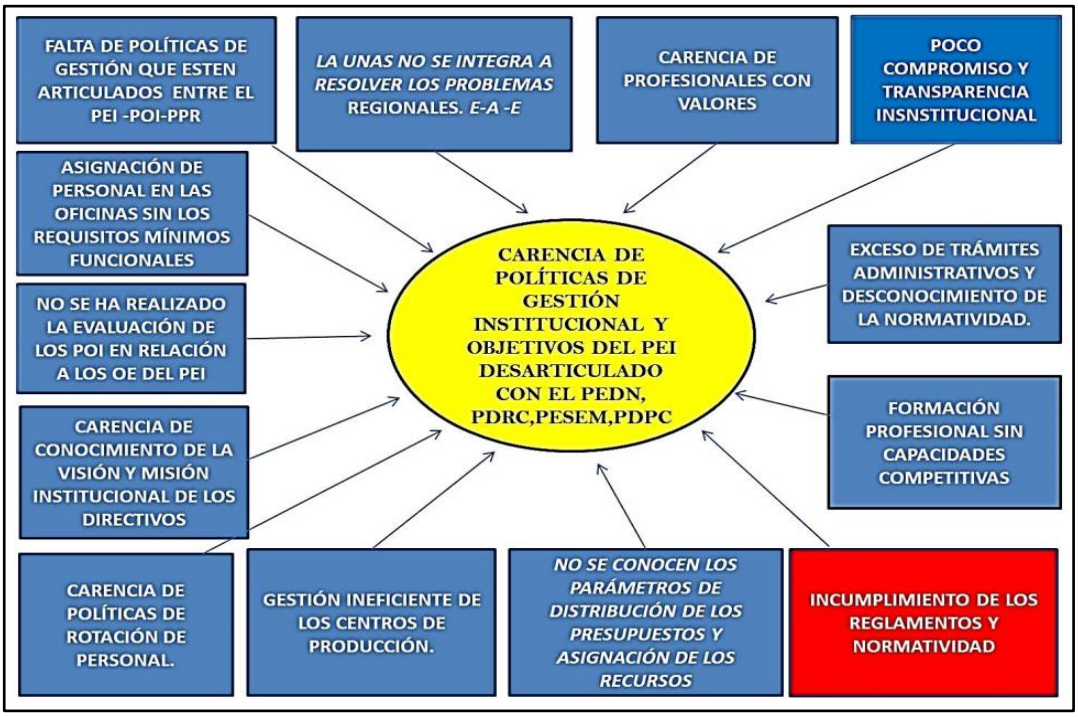


Figura 4. Problemas recurrentes de la UNAS
Fuente: PEI 2018-2020

3.5 Tecnologías de la información

3.5.1 Plataforma de tecnologías de la información

Con el paso de los años e incremento de los procesos en la universidad, existe la necesidad de incorporar nuevos sistemas de información optimizados mediante aplicaciones que permitan mejorar el servicio que se brinda.

Actualmente se dispone de la plataforma de tecnologías tal como se aprecia en el Cuadro 2, que permiten el uso sistematizado de la información y que se encuentra a cargo del Centro de Tecnología de la Información y Comunicación.

Cuadro 2. Componentes de la plataforma de TI de la UNAS

Plataforma de TI de la UNAS		
Servicios de red	**Sistemas de escritorio**	**Sistemas web**
Proxy	SIAF	Sistema Académico (OCDA)
Firewall	SIMI	Sistema Virtual de Acreditación (Sysva)
Antivirus	SIGA	Sistema de Aula virtual (CAMPUS)
Dominio	Módulo administrativo	Revista de Investigación UNAS (rEVIA)
Archivos		Sistema de Racionalización Docente
Web		Sistema de convalidación académico – FIIA
Base de datos		Sistema de convalidación académico – Economía
Glasfish		Sistema de convalidación académico – FIIS
		Sistema de Prácticas Pre Profesionales – FIIS – SPPP
		Sistema de Escuela de PostGrado – EPG
		Sistema de Centro de Idiomas
		Sistema de biblioteca – BOOK

Fuente: Centro de Tecnología de la Información y Comunicación – UNAS, 2017

Del Cuadro 2 se observa que existe gran cantidad de servicios de TI que en total son 24 implementados y funcionando, cabe mencionar que también existen otros en proceso de desarrollo e implementación motivo por el cual no han sido considerados.

Una de las mayores preocupaciones dentro de los sistemas es el Módulo Administrativo (Sistema de escritorio); ya que es un sistema obsoleto desarrollado en lenguaje de programación Visual Fox Pro. Todo el proceso administrativo es canalizado por este sistema, y por lo tanto se debe tener un sistema que pueda ser escalable en el tiempo, además de permitir la compatibilidad con software y hardware de última generación; pero en la actualidad esto no sucede ya que, este sistema implementado solo permite operar bajo sistemas operativos Windows Xp y Windows 7, presentando en este último algunos problemas de compatibilidad y múltiples amenazas de seguridad

que pueden ser explotadas fácilmente . Estos sistemas operativos actualmente se encuentran desfasados y no presentan soporte, haciendo que la información procesada en estos sistemas se encuentre expuesto frente a graves riesgos de disponibilidad, confidencialidad e integridad.

Los otros sistemas tales como el SIMI, SIGA y SIAF son provistos por el estado peruano para el uso exclusivo en entidades públicas, motivo por el cual, es necesario adecuarse al uso de estos sistemas.

Por otro lado, se tiene 12 sistemas web, que se han ido implementando a lo largo del tiempo y de acuerdo a las necesidades generadas por el personal de la universidad para desarrollar sus actividades, pero al ser sistemas con un grado de madurez baja, se encuentran en constante actualización técnica, y según se ha podido comprobar por parte del CTIC, la mayoría de estos sistemas han presentado más de una incidencia técnica y también se evidencian vulnerabilidades al no utilizar protocolos de transmisión seguros (SSL, TSL) motivo por el cual toda la información procesada por estos sistemas es susceptible a sufrir daños de consideración. El sistema web más crítico y en el que se debe poner más énfasis es el Sistema de Coordinación Académica, ya que se almacena y procesa toda la información de la población estudiantil y docentes de todas las facultades.

En resumen, la universidad cuenta con diversidad de aplicaciones que muchas de ellas se encuentran aisladas y en diferentes plataformas de desarrollo. Este escenario ha llevado a múltiples problemas de compatibilidad, seguridad y confiabilidad de los datos; además de la duplicidad de información y esfuerzos.

3.5.2 Red de datos

La distribución de red de la UNAS es de tipo estrella, el cual consiste en un nodo central, del cual parten todos los enlaces hacia los demás nodos a través de fibra óptica.

La red actual se encuentra bajo una sola subred de clase B (172.16.0.0/22). Entonces, al existir 29 *Switches*, y ninguna VLAN, se genera demasiado tráfico de Broadcast cuando un *Switch* recibe una trama con una dirección broadcast de destino entonces inundan esa trama a todos causando una reducción del rendimiento de la red e incluso puede llegar a interrumpir el servicio. Así mismo, el servicio de internet con el que se cuenta es una línea dedicadas 20 Mb.

Los servicios de red son administrados exclusivamente por el CTIC, pero para ello solo se dispone de 2 (dos) profesionales (Administrador de red y Administrador Web) que no es suficiente para poder gestionar y dar soporte a la gran demanda por parte de los usuarios finales, además se cuenta con una oficina de soporte técnico encargado exclusivamente de solucionar problemas de hardware de computadoras e impresoras a nivel de usuario final.

Para dar soporte a todos estos servicios de red antes mencionados, el CTIC cuenta con equipos modernos tales como 19 *switches*, 1 *router*, 12 servidores, entre otros que se detallarán más adelante. Pero debido a la creciente demanda de los sistemas informáticos que se están implementando, el uso de la infraestructura disponible se encuentre al límite de sus capacidades; sin embargo, hasta el momento no se cuenta con un sistema de almacenamiento y *backup* (*Storage*), servidores con mayor capacidad y un adecuado ancho de

banda del internet para poder brindar un buen servicio, todos estos factores y entre otros ponen en alerta la seguridad de la información en la institución.

3.6 Recursos humanos

Según el Plan Estratégico Institucional (PEI) 2018 - 2020, la UNAS al 2016 cuenta con 3210 estudiantes de pregrado, 230 docentes, 344 administrativos, distribuidos en 6 facultades y 10 especialidades en funcionamiento (no se considera la facultad de Ingeniería Mecánica y Eléctrica), por lo que se evidencia que existe gran cantidad de usuarios de los sistemas de información de la universidad.

Por otra parte, en los resultados de la encuesta realizada en febrero del 2017 a la corporación universitaria el principal valor que se está perdiendo es la honestidad, respeto y ética moral respectivamente tal como se puede apreciar en Figura 5.

Valores	Corporación universitaria	%
- Honestidad	26	14,4
- Responsabilidad	17	9,4
- Respeto	24	13,3
- Ética y moral	21	11,7
- Honestidad y responsabilidad	11	6,1
- Honestidad, responsabilidad y puntualidad	36	20,0
- Respeto, tolerancia y humildad	13	7,2
- Otros	13	7,2
Total responden	161	89,4
Total no responden	19	10,6
Total	**180**	**100,0**

Figura 5. Valores que se están perdiendo en la UNAS
Fuente: Plan Estratégico Institucional (PEI) 2018-2020

Estos aspectos si lo relacionamos con la seguridad de la información entonces se puede evidenciar por ejemplo la materialización de incidentes de como por ejemplo instalación de programas crackeados, accesos no autorizados a la red de datos, olvido de contraseñas y estar susceptible a ataques de ingeniería social, puesto que los recursos humanos son los encargados de gestionar, procesar, almacenar, modificar, transmitir y eliminar la información ya que son el engranaje principal para el buen funcionamiento institucional, tal como se puede evidenciar en el Cuadro 1, Anexo 10 y Anexo 11.

3.7 Identificación de controles según la ISO/IEC 27002:2013

De acuerdo con lo especificado en la ISO/IEC 27002:2013 la selección de controles debe estar sujeta a la actividad de la organización, a las leyes y regulaciones nacionales vigentes. Para el caso de esta investigación primero se debe identificar y valorar los controles que nos presenta la ISO/IEC 27002:2013 en sus 14 dominios, éstos controles pueden estar implementados de manera informal, por lo tanto, se realizó el diagnóstico actual de controles de seguridad de la información existentes en la UNAS.

A continuación, en la Figura 6, se puede ver los resultados de la evaluación de los aspectos normativos y regulatorios de la UNAS tomando como referencia la norma ISO/IEC 27002:2013. En este caso, la línea roja representa el grado de cumplimiento actual, la línea amarilla un posible objetivo de cumplimiento a medio/largo plazo y, por último, la línea verde representa el nivel de cumplimiento óptimo hacia la cual se debe estar encaminados.

Los valores que se muestran en la gráfica hacen referencia a los diferentes dominios contemplados en la ISO/IEC 27002:2013. Para mayor detalle ver el Anexo 1

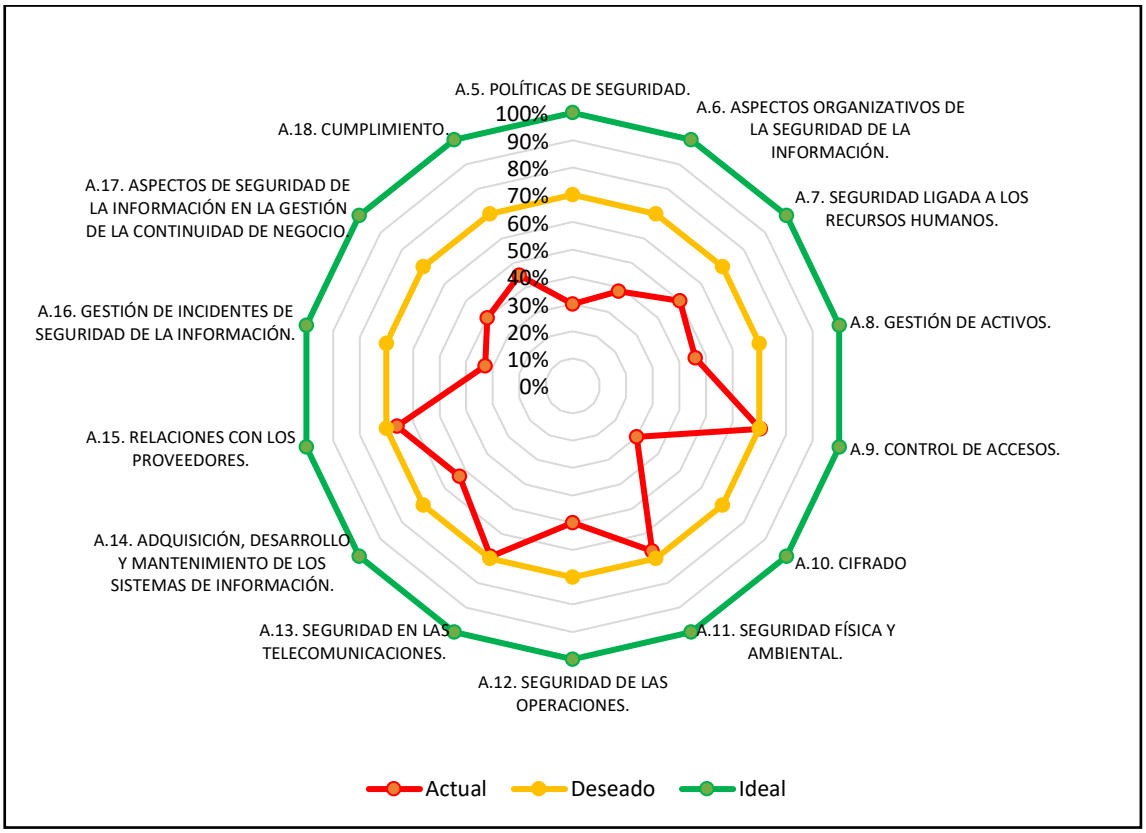


Figura 6. Nivel de madurez de dominios de control ISO/IEC 27002:2013
Fuente: Elaboración propia

Para la obtención del estado de los controles existentes se pondera cada control en función del nivel de madurez, luego se consolida por cada dominio, por ejemplo, si un control tiene nivel inicial se le asigna 10%, repetible 50%, definido 90%, gestionado 95% y optimizado 100%. De modo que al final se consolida el total de controles de cada dominio obteniendo así el nivel de madurez global por cada dominio de la norma ISO/IEC 27002:2013.

La herramienta PILAR que se utiliza en la metodología MAGERIT para el Análisis y Gestión de Riesgos calcula el nivel de madurez en base a estos

valores. Por lo tanto, en el Cuadro 3 se puede apreciar un resumen del nivel de madurez de los controles de seguridad que existe en la universidad.

Cuadro 3. Nivel de madurez de controles de seguridad en la UNAS

Dominio	Actual	Deseado	Ideal
A.5	30%	70%	100%
A.6	39%	70%	100%
A.7	50%	70%	100%
A.8	46%	70%	100%
A.9	70%	70%	100%
A.10	30%	70%	100%
A.11	67%	70%	100%
A.12	50%	70%	100%
A.13	69%	70%	100%
A.14	53%	70%	100%
A.15	66%	70%	100%
A.16	33%	70%	100%
A.17	40%	70%	100%
A.18	45%	70%	100%

Fuente: Elaboración propia

Como pudo apreciar en la Figura 6 se evidencia que controles sobre políticas de seguridad de la información aún se encuentran en un estado de implementación no formal, siendo éste un factor primordial para poder encaminar los procesos de la universidad. Del mismo modo referente a criptografía aún se encuentra en un nivel de madurez L2 (repetible) en la que los procesos siguen un patrón regular en base a la experiencia, como por ejemplo cifrado hash de contraseñas. Es importante hace un énfasis en aquellos dominios que presentan un porcentaje menor a 50%, para poder realizar las mejoras necesarias.

En la Figura 7 se tiene un resumen del estado de implementación de controles de seguridad según el nivel de madurez: Inicial, repetible, definido, gestionado y optimizado.

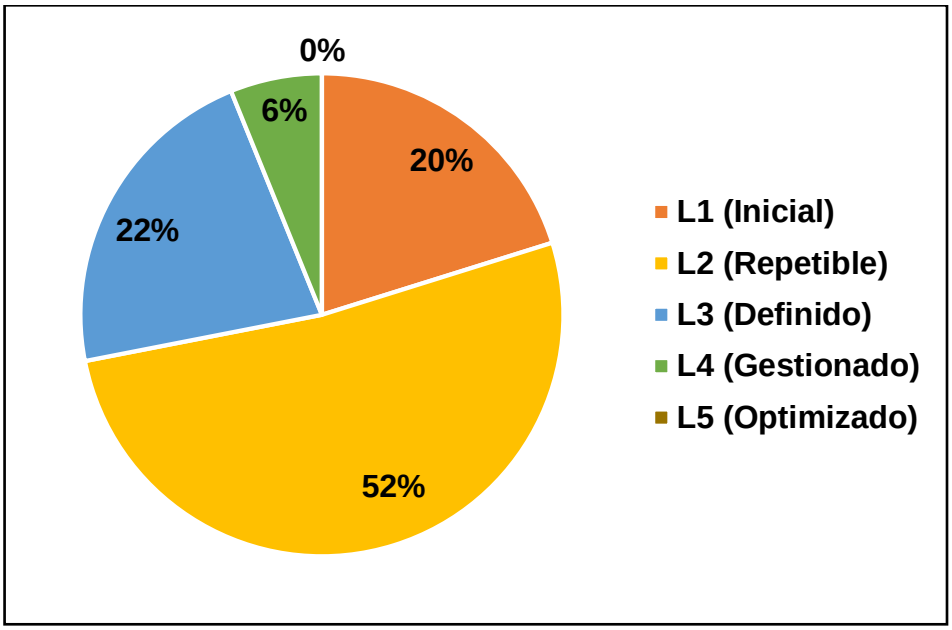


Figura 7. Controles de seguridad de la información en la UNAS
Fuente: Elaboración propia

Cuadro 4. Leyenda del nivel de madurez

Leyenda		
CMM	**Detalle**	**Detalle**
L5	Optimizado	En base a resultados cuantitativos, se optimizan los procesos.
L4	Gestionado	Los procesos se monitorean y se miden.
L3	Documentado	Los procesos definidos se documentan y comunican.
L2	Repetible	Se normalizan las buenas prácticas en base a la experiencia.
L1	Inicial	Inexistente o informal localizado en áreas concretas.

Fuente: Elaboración propia

IV. ANÁLISIS DE RIESGOS

4.1 Identificación de los activos

El primer paso será identificar todo el conjunto de activos de la universidad y elaborar un inventario de estos. Luego de identificar los activos, se valorarán en cada una de las dimensiones de confidencialidad, integridad y disponibilidad, de acuerdo con la importancia que tengan para la institución. El valor de cada activo será uno de los parámetros que intervendrán en el cálculo de los valores de riesgo: cuanto más valor tengan los activos para la institución, mayor riesgo tendrá; esta actividad se puede resumir en la expresión “conócete a ti mismo”.

Las consideraciones importantes que se tienen en cuenta en la metodología MAGERIT para identificar activos críticos en la universidad se puede resumir en las siguientes preguntas:

- ✓ ¿Qué información es necesaria para prestar un servicio?
- ✓ ¿Con qué aplicaciones se gestiona esa información?
- ✓ ¿Dónde se almacenan la información y las aplicaciones?
- ✓ ¿Se han subcontratado servicios o productos de los que dependan los activos de información?
- ✓ ¿Por qué medios se transmite la información?
- ✓ ¿De qué personas depende el servicio?

Para iniciar con el análisis de riesgos, se identifican los activos de la universidad agrupándolos de la siguiente manera:

4.1.1 Activos esenciales o primarios

Aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente al correcto funcionamiento de la institución.

- ✓ Procesos institucionales
- ✓ Datos e información

Cuadro 5. Grupo de activos – Procesos institucionales

Grupo de Activo	Activos	Total
[PI] Procesos	– Procesos estratégicos – Procesos misionales – Procesos de soporte institucional	03

Fuente: Elaboración propia

Cuadro 6. Grupo de activos – Datos e Información

Grupo de Activo	Activos	Total
[DI] Datos e información	– Base de datos de aplicaciones web – Base de datos de páginas web – Bases de datos administrativa – Código fuente de aplicaciones – Copias de respaldo de sistemas de TI – Correo electrónico corporativo – Credenciales de acceso a los sistemas informáticos – Datos de configuración de sistemas de TI – Directorio institucional – Documentos estratégicos – Documentos normativos académicos – Documentos normativos administrativos – Documentos normativos de investigación	26

	– Documentos operativos – Información académica – Información de página web institucional – Información de transparencia institucional – Información financiera – Legajo de personal – Otros documentos administrativos – Producción intelectual y patentes – Registro académico de estudiante – Registro de actividad – Resoluciones institucionales – Transacciones bancarias – Informes, planes y proyectos

Fuente: Elaboración propia

4.1.2 Activos de apoyo o secundarios

Encargados de dar soporte de almacenamiento, procesamiento y transmisión de los activos esenciales.

- ✓ Sistemas y software
- ✓ Infraestructura de TI y Hardware
- ✓ Equipamiento auxiliar
- ✓ Personal
- ✓ Infraestructura Física

Cuadro 7. Grupo de activos – Sistemas y software

Grupo de Activo	Activos	Total
[SI] Sistemas y software	– Active Directory – Antivirus corporativo – Internet corporativo – Internet Speedy – Intranet biblioteca – BOOK – Modulo administrativo – Páginas web – Revista de Investigación (RevIA) – Seguridad perimetral (Proxy/Firewall)	32

	– Servicio de aplicaciones – Servicio de Base de Datos – Servicio de transferencia de Archivos – Servicio web – Sistema de aula virtual – Sistema de Centro de Idiomas – Sistema de convalidación académica – FIIA – Sistema de convalidación académico – Economía – Sistema de convalidación académico – FIIS – Sistema de escuela de PostGrado – EPG – Sistema de gestión académica – Sistema de prácticas pre profesionales FIIS – Sistema de repositorio digital – Sistema de seguimiento a egresados – Sistema Integrado de Administración Financiera (SIAF) – Sistema Integrado de Gestión Administrativa (SIGA) – Sistema operativo de usuario final – Sistema operativo para servidores – Sistema presupuestal (UNASPOI) – Sistema Virtual de Autoevaluación (SVA) – Software especializado académico y de investigación – Software Inventario Mobiliario Institucional (SIMI) – Software utilitario

Fuente: Elaboración propia

Cuadro 8. Grupo de activos – Infraestructura de TI y hardware

Grupo de Activo	Activos	Total
[IH] Infraestructura de TI y Hardware	– Cableado estructurado – Dispositivos periféricos – Equipamiento de respaldo – Equipo biométrico – Equipos de red – Pc de escritorio – Pc portátil – Red eléctrica – Servidor – Soportes de información electrónicos – Soportes de información no electrónicos	11

Fuente: Elaboración propia

Cuadro 9. Grupo de activos – Equipamiento auxiliar

Grupo de Activo	Activos	Total
[EA] Equipamiento Auxiliar	– Fuentes de alimentación – Gabinetes – Generador eléctrico – Mobiliario – Transformador eléctrico – UPS	06

Fuente: Elaboración propia

Cuadro 10. Grupo de activos – Personal

Grupo de Activo	Activos	Total
[PE] Personal	– Administrador de aplicaciones – Administrador de red – Alta dirección – Asamblea Universitaria – Consejo Universitario – Decanos y directores – Director del CTIC – Personal de limpieza de planta – Personal de vigilancia – Proveedor de servicio de Internet y telefonía – Soporte técnico informático – Usuarios finales externos – Usuarios finales internos	13

Fuente: Elaboración propia

Cuadro 11. Grupo de activos – Infraestructura física

Grupo de Activo	Activos	Total
[IF] Infraestructura física	– Campus universitario – Laboratorios de cómputo – Laboratorios especializados – Modulo universitario – Sala de servidores – Sedes o locales	06

Fuente: Elaboración propia

4.2 Descripción de los activos

4.2.1 Procesos institucionales

Conjunto de actividades planificadas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir el objetivo de la universidad. Según el Plan Estratégico Institucional (PEI) 2018 - 2020 se tiene los siguientes procesos:

- ✓ **Procesos estratégicos:** son los que impulsan el desarrollo y fortalecimiento institucional, previa identificación de las necesidades y requisitos de Stakeholders o Grupos de Interés, entre los procesos estratégicos se tiene al Planeamiento Estratégico Prospectivo, Gestión por Procesos, Gestión de la Calidad y Bienestar Estudiantil.
- ✓ **Procesos misionales:** permiten asegurar los recursos necesarios para alcanzar los objetivos y se encuentran a cargo de la Alta Dirección, entre ellos se tiene identificado a 3 procesos: Responsabilidad Social Universitaria, Formación Profesional Integral e Innovadora y por último Investigación Formativa Científica y Tecnológica.
- ✓ **Procesos de soporte institucional:** gestionan los recursos institucionales (tangibles e intangibles) y soportan el desarrollo de la institución. La universidad tiene identificado 4 procesos: Gestión del Capital Humano, Gestión de Recursos Financieros, Gestión de la Infraestructura y Mantenimiento, Gestión de la Información y Grupos de Interés.

4.2.2 Datos e información

Los datos son el conjunto básico de hechos referentes a una persona, cosa o transacción; incluyen cosas como: tamaño, cantidad, descripción, volumen, tasa, nombre o lugar, los datos son la parte fundamental de toda institución para poder prestar sus servicios.

La información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno; es un activo abstracto que será almacenado en equipos o soportes de información (en su mayoría como archivos o base de datos) o será transferido a otro lugar.

✓ **Base de datos de aplicaciones web:** Base de datos de las aplicaciones web existentes en la universidad.

✓ **Base de datos de páginas web:** Base de datos de las diferentes páginas web utilizadas en la universidad.

✓ **Bases de datos administrativa:** Base de datos de los sistemas administrativos utilizado para realizar los procesos diarios de la universidad entre los que encontramos al SIAF, SIGA, Planilla y Módulo administrativo.

✓ **Código fuente de aplicaciones:** código fuente de aplicaciones informáticas que permite hacer cambios a nivel funcional o corregir errores que se presentan en los mismos.

✓ **Copias de respaldo de sistemas de TI:** denominado a las copias de respaldo de los sistemas de tecnologías de la información, entre ello se tiene copias de base de datos, máquinas virtuales y archivos de configuración de proxy/firewall, y sistemas web.

✓ **Correo electrónico corporativo:** mensajes de correo electrónico institucional que se intercambia con personal docente, administrativo, y alumnos.

✓ **Credenciales de acceso a los sistemas informáticos:** son los usuarios y contraseñas asignadas al personal que utiliza algún sistema o aplicación que solicite autenticación mediante un usuario y una contraseña.

✓ **Datos de configuración de sistemas de TI:** son aquellos datos establecidos para configurar por defecto los diferentes sistemas de TI que se utilizan en la universidad, entre los cuales se tiene a cuentas de usuario y contraseña, número de puerto, plataforma de operatividad y licencia.

✓ **Directorio institucional:** contiene los nombres y datos de los funcionarios de las diferentes unidades orgánicas, así como también dirección y anexos telefónicos de la universidad.

✓ **Documentos estratégicos:** constituyen herramientas de gestión, acciones estratégicas que definen políticas institucionales, objetivos estratégicos, programas y proyectos que contribuyen al logro de resultados, efectos e impactos previstos en los planes de desarrollo de la universidad, entre este tipo de documentos se tiene al Plan Estratégico Institucional (PEI) y al Plan Estratégico de Tecnologías de la Información (PETI).

✓ **Documentos normativos administrativos:** abarca documentos como normas, reglamentos y estatutos, tales como el Reglamento de Organización y Funciones (ROF), Manual de Organización y Funciones (MOF), Reglamento General y el Estatuto de la UNAS.

✓ **Documentos normativos académicos:** documentos que norman o regulan la formación académica de los estudiantes universitarios, tales

como Reglamento de Estudios, Reglamento de Grados y Títulos, Reglamento de Traslado y Seguimiento Curricular, Reglamento de Prácticas Pre profesionales.

✓ **Documentos normativos de investigación:** tienen por objeto normar, fomentar y promover la investigación. Aquí se puede encontrar al Reglamento de Investigación y el Reglamento del Docente Investigador.

✓ **Documentos operativos:** contienen instrucciones de manera detallada para la ejecución de tareas, en este grupo está el Plan Operativo Institucional (POI), Cuadro para Asignación de Personal (CAP), Manual de Procedimientos Administrativos (MAPRO), Texto Único de Procedimientos Administrativos (TUPA) y Planillas.

✓ **Información académica:** sílabos, horarios, registros de notas, aulas, laboratorios.

✓ **Información de Página Web institucional:** cuenta con un espacio y dominio propio creado y diseñado exclusivamente para servir a fines de difusión de información institucional, resoluciones, comunicados, noticias y links de páginas web de las facultades, sistemas web utilizados en la universidad y correo corporativo.

✓ **Información de Transparencia Institucional:** Datos generales, planeamiento y organización, información presupuestal, proyectos de inversión, información de personal, información de contrataciones, actividades oficiales e información adicional.

✓ **Información financiera:** información que produce la contabilidad indispensable para la administración y el desarrollo de las empresas y por lo

tanto es procesada y concentrada para uso de la gerencia y personas que trabajan en la empresa, tales como estados de cuenta, flujo de fondos y gastos.

✓ **Informes, planes y proyectos:** Proyectos de inversión, Planes de mejora continua, Informes de investigación de pregrado y posgrado, Informes de actividades de Proyección Social y Extensión Universitaria, Informes de Bienestar Universitario, Infraestructura (Planes, Documentación, Proyectos), Informática (Planes, Documentación, proyectos).

✓ **Legajos de personal:** es un documento o carpeta que contiene información detallada acerca del personal contratado o nombrado y alumnos de pre y posgrado. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

✓ **Otros documentos administrativos:** son las cartas, oficios, memorándum, solicitudes almacenados en forma física o electrónica.

✓ **Producción intelectual y patentes:** son investigaciones realizadas por alumnos y docenes de la universidad, tales como: libros, tesis, PPP, artículos, revistas, manuales y textos universitarios.

✓ **Registro académico de estudiante:** documentos que contienen registros académicos de los estudiantes tales como Registro de notas y Récord académico.

✓ **Registro de actividad:** son las grabaciones en archivos o en una base de datos de la secuencia de ejecución (eventos, acciones) de los sistemas web, base de datos y sistemas operativos de servidores.

✓ **Resoluciones institucionales:** Resolución Asamblea Universitaria, Resolución Consejo Universitario, Resolución Rectorado, Resolución Consejo de Facultad, Resolución Decanato.

✓ **Transacciones bancarias:** cualquier tipo de operación de dinero en la cual interviene el banco, como por ejemplo el pago con una Tarjeta de Crédito o Débito, retiro de fondos desde la Cuenta Corriente, cambio de cheques, transferencias de dinero, giros desde un cajero automático, entre otras.

4.2.3 Sistemas y software

Tienen como objetivo fundamental satisfacer las necesidades que tiene la comunidad universitaria a través del almacenamiento, procesamiento y control de la información mediante el uso de tecnologías.

✓ **Active Directory:** permite gestionar objetos de la red, tales como usuarios, grupos y recursos de red (pc e impresoras) y además administrar los inicios de sesión en los equipos de red y los permisos asignados.

✓ **Antivirus Corporativo:** encargado de proveer actualizaciones diarias a los equipos clientes que tengan instalado y configurado la aplicación cliente, actualmente se utiliza como servidor a ESET Endpoint Antivirus que cuenta con licencia corporativa.

✓ **Internet Corporativo:** servicio de internet contratado a través de la empresa Telefónica, este servicio es administrado por el CTIC consta de una línea dedicada de 20 Mb, adicional a ello se tiene líneas Speedy contratadas por algunas oficinas y laboratorios de diferentes facultades.

✓ **Internet Speedy:** servicio de internet comercial contratado por algunas oficinas de la universidad para tener acceso al internet de independiente.

✓ **Intranet Biblioteca – BOOK:** este servicio permite realizar la consulta y solicitud de préstamo de la bibliografía que se dispone en la universidad.

✓ **Modulo Administrativo:** necesario para poder realizar los procesos de administrativos de la universidad como son, caja, tesorería, entre otros. Software obsoleto, basado en lenguaje de programación Visual Fox Pro; maneja base datos totalmente plana, sin jerarquía ni requisitos de diseño vigentes.

✓ **Páginas Web**: encuentra generalmente en formato HTML o XHTML, y puede proporcionar navegación a otras páginas web mediante enlaces de hipertexto. Frecuentemente incluyen otros recursos como hojas de estilo en cascada, guiones (scripts) e imágenes digitales, entre otros. En la universidad se tiene las siguiente páginas web: UNAS (Página web principal), Biblioteca, Dirección de Calidad y Acreditación, OIUNAS, Transparencia, OCDA, Facultad de Ciencias Económicas y Administrativas, Facultad de Agronomía, Facultad de Ingeniería en Industrias Alimentarias, Facultad de Ingeniería en Informática y Sistemas, Facultad de Recursos Naturales Renovables, Facultad de Zootecnia, Facultad de Recursos Naturales Renovables, Vice Investigación, Facultad de Administración, Escuela de Conservación de Suelos y Agua, Facultad de Ciencias Contables, Económicas y Administrativas, Escuela de Posgrado, Sistema de Notas de Exámenes de Admisión.

✓ **Revista de Investigación (REVIA):** página web en la que se realiza publicaciones semestrales de información científica que generan los académicos de la UNAS.

✓ **Seguridad Perimetral (Proxy/Firewall):** utilizado para poder realizar el filtro de acceso a internet mediante el uso de reglas de configuración en el *Proxy/Firewall* a cargo del administrador de la red corporativa de la universidad.

✓ **Servicio de Aplicaciones:** es un servidor de aplicaciones de software libre desarrollado por Sun Microsystems, compañía adquirida por Oracle Corporation, que implementa las tecnologías definidas en la plataforma Java EE y permite ejecutar aplicaciones que siguen esta especificación, como servidor de aplicaciones se tiene al GlassFish Server.

✓ **Servicio de Base de Datos:** permite administrar a través de gestores de base de datos utilizados en la universidad tales como SQLServer, MySql y PostgreSQL, diferentes bases de datos de los sistemas que se utilizan en la universidad.

✓ **Servicio de Transferencia de Archivos**: este tipo de servicio se encarga de almacenar archivos de manera lógica y permite que usuarios puedan acceder, almacenar y compartir archivos mediante acceso remoto.

✓ **Servicio Web:** es el encargado de dar respuestas a solicitudes de clientes al realizar consultas a través de una interfaz web a un sistema en particular, para el caso de la universidad se tiene al servidor HTTP Apache y servidor PHP.

✓ **Sistema de Aula Virtual:** sistema web que permite acceder a los docentes y estudiantes a un repositorio de documentos, foros, etc. con el objetivo de facilitar actividades que conduzcan al aprendizaje.

✓ **Sistema de Centro de Idiomas:** sistema web que permite hacer un seguimiento académico de alumnos, gestionar horarios, aulas de clase, reportes de pagos, etc.

✓ **Sistema de Convalidación Académica – FIIA:** sistema que permite realizar reportes del seguimiento curricular de los estudiantes de la FIIA

✓ **Sistema de Convalidación Académico – Economía:** permite realizar reportes del seguimiento curricular de los estudiantes de Economía

✓ **Sistema de Convalidación Académico – FIIS:** sistema que permite realizar reportes del seguimiento curricular de los estudiantes de la FIIS.

✓ **Sistema de Escuela de PostGrado – EPG:** permite realizar matricula, seguimiento curricular de alumnos, seguimiento de tesis, generar constancias, hacer reportes económicos.

✓ **Sistema de Gestión Académica:** sistema de gestión académica en el que se realiza el proceso de matrícula, registro de notas a cargo de los docentes, horarios y consulta de registros académicos por parte de los alumnos, es considerado uno de los sistemas más importantes en la universidad.

✓ **Sistema de Prácticas Pre Profesionales FIIS:** cuya finalidad es realizar el seguimiento del estado de las PPP de los alumnos, desde la solicitud hasta la sustentación de las prácticas.

✓ **Sistema de Repositorio Digital:** permite facilitar y mejorar la visibilidad de la producción científica y académica de la Universidad permitiendo

el acceso abierto a sus contenidos y garantizando la preservación y conservación de dicha producción, además de aumentar el impacto del legado Institucional.

✓ **Sistema de Seguimiento a Egresados:** permite realizar el seguimiento a los egresados de las diferentes facultades de la UNAS.

✓ **Sistema Integrado de Administración Financiera (SIAF):** permite administrar, mejorar y supervisar las operaciones de ingresos y gastos de las Entidades del Estado además de permitir la integración de los procesos presupuestarios, contables y de tesorería de cada entidad

✓ **Sistema Integrado de Gestión Administrativa (SIGA):** que contribuye al ordenamiento y simplificación de los procesos administrativos en el marco de las normas establecidas por los Órganos Rectores de los Sistemas Administrativos del Estado

✓ **Sistema Operativo de usuario final:** se utiliza en las Pc existentes en la universidad, para el caso de administrativos, todos trabajan con Windows (XP, 7, 8 y 10), por otro lado, en laboratorios de la FIIS se utiliza otros sistemas operativos como Linux.

✓ **Sistema Operativo para servidores:** se utiliza en los servidores de la universidad, actualmente se utiliza Windows Server 2008 R2, Windows Server 2012, CentOS y Red Hat Enterprise.

✓ **Sistema Presupuestal (UNASPOI):** en la que se realiza el Plan Operativo Institucional, Cuadro de necesidades.

✓ **Sistema Virtual de Autoevaluación (SVA):** software web que cuenta con cuatro módulos que permite cubrir el proceso de autoevaluación

✓ **Software Especializado Académico y de Investigación:** SPSS, Autocad, MatLab, Mnitab, E-views, Stella, Arc-view)

✓ **Software Inventario Mobiliario Institucional (SIMI):** software que permite llevar el control de la propiedad mobiliaria estatal en la universidad. Software desarrollado en lenguaje Fox Pro, actualmente obsoleto.

✓ **Software Utilitario:** Estos programas son básicos e imprescindibles para el desarrollo de las actividades en la universidad. Entre ellos se tiene al paquete de ofimática Word, Excel, PowerPoint, Access (en sus versiones 2007, 2010, 2013 y 2016), navegador web (Chrome, Mozilla Firefox e Internet Explorer), reproductor multimedia (VLC, Adobe Flash Player, Reproductor Windows Media Player), compresor de archivos (Winrar, Winzip), lector PDF (Foxit Reader).

✓ **Suite Office 365 Online:** Office 365 es una solución completa que ofrece a los usuarios la capacidad de trabajar en cualquier momento y desde cualquier lugar, comunicarse por videoconferencia, compartir su trabajo en tiempo real, etc. Se tiene entre ellos a Office Professional Plus, correo corporativo, Office Online, Project Online, SharePoint Online, OneDrive, Exchange online, Yammer y Skype).

4.2.4 Infraestructura de TI y Hardware

Consiste en un conjunto de dispositivos requeridos que permiten almacenar, procesar y transmitir datos e información de aplicaciones y servicios en toda la institución universitaria.

✓ **Cableado estructurado:** se refiere al cableado en las instalaciones del campus universitario para la transmisión de datos en la red corporativa, en la universidad se tiene cableado de fibra óptica para el enlace troncal y cableado de red con cable de par trenzado para los usuarios finales.

✓ **Dispositivos periféricos:** los equipos periféricos son aquellos que sirven para poder realizar la impresión y escaneo de documentos, entre ellos la universidad dispone de impresoras y escáneres.

✓ **Equipamiento de respaldo:** Las copias de respaldo se almacena en disco duro externos y DVD que son administrados por parte del CTIC.

✓ **Equipo biométrico:** equipos biométricos que sirven para poder realizar el control de asistencia de los trabajadores de la universidad, del mismo modo se tiene un equipo biométrico implementado en el comedor de la universidad que controla el acceso de los usuarios (alumnos).

✓ **Equipos de red:** estos activos se caracterizan porque sirven para poder transmitir los datos dentro de la red corporativa, entre los equipos de red que se utilizan en la universidad se tiene a los *Router, Switch y Wireless Access Point.*

✓ **Pc de escritorio:** Son los computadores existentes en la universidad y que están asignados al personal administrativo y docentes, así como también a los diferentes laboratorios de la universidad para poder realizar actividades académicas.

✓ **Pc portátil:** también denominados laptop son activos de la universidad que están asignados a algunos administrativos y docentes para

realizar actividades académicas, ya que estos equipos son portátiles están más expuestos a riesgos de pérdida.

✓ **Red eléctrica:** es un sistema interconectado que tiene el propósito de suministrar electricidad desde los proveedores hasta los consumidores, para el caso de la universidad el proveedor de este servicio es Electrocentro S.A.

✓ **Servidor:** es un equipo informático de altas prestaciones en la que se hospedan los diferentes sistemas de la universidad.

✓ **Soportes de información electrónicos:** equipos físicos en la que se almacena información en cantidades limitadas, entre los más utilizados en la universidad se tiene a memorias USB, DVD y CD.

✓ **Soportes de información no electrónicos:** es toda información que se encuentra impresa en cualquier tipo de material (papel, cartulina, láminas)

4.2.5 Equipamiento auxiliar

Aquellos equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionado con datos. Se tiene como ejemplo a (fuentes de alimentación, UPS, equipos de climatización, cableado, mobiliario)

✓ **Fuentes de alimentación:** dispositivo que convierte la corriente alterna a corriente continua, que permite alimentar los distintos circuitos del aparato electrónico que se conecta.

✓ **Gabinetes:** también llamada RACK es donde se encuentran ubicados dispositivos de red tales como switch, modem, router entre otros, de allí se envía el cableado al resto de la estructura para crear los puntos de trabajo.

✓ **Mobiliario:** son los muebles en el que se almacenan documentos que contienen información de la institución, en la universidad se tiene armarios, escritorios, archivadores, etc. en la mayoría de casos estos mobiliarios tienen llaves de seguridad.

✓ **Generador eléctrico:** dispositivo capaz de transformar cualquier otro tipo de energía como punto de partida a energía eléctrica.

✓ **Transformador eléctrico:** se denomina transformador a un dispositivo electromagnético (eléctrico y magnético) que permite aumentar o disminuir el voltaje y la intensidad de una corriente alterna de forma tal que su producto permanezca constante.

✓ **UPS:** es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía por un periodo terminado de tiempo a un dispositivo en el caso de interrupción eléctrica.

4.2.6 Personal

Aquellos que interactúan directamente con los sistemas de información y otros grupos anteriormente citados

✓ **Administrador de aplicaciones:** está a cargo del mantenimiento y actualización de contenidos de la página web, administración del Office 365 y otras aplicaciones de la universidad.

✓ **Administrador de red:** encargado de administrar y mantener la operatividad de la red corporativa y los servicios que se brinda.

✓ **Alta dirección:** conformado por las autoridades de alto nivel de la universidad, tales como el rector, vicerrectores y directores de oficinas.

✓ **Asamblea Universitaria:** es el máximo órgano de gobierno de la universidad compuesto por: el rector. vicerrector académico, vicerrector de investigación, los decanos, el director de la escuela de postgrado, representantes de docentes, representantes de estudiantes de pregrado y postgrado y finalmente con un representante de los graduados.

✓ **Consejo Universitario:** es el máximo órgano de gestión, dirección, ejecución académica y administrativa de la universidad, integrada por: el rector, los vicerrectores, un cuarto del total de los decanos, el director de la escuela de postgrado.

✓ **Decanos y directores:** formado por los Decanos y Directores de Escuela y Posgrado, Directores de Departamento Académico y Administración y Directores de Oficina.

✓ **Director del CTIC:** encargado de gestionar eficiente y eficazmente los recursos, la infraestructura y servicios tecnológicos institucionales.

✓ **Personal de limpieza de planta:** centran sus actividades en la limpieza diaria y programada de los ambientes o zonas asignadas a cada trabajador.

✓ **Personal de vigilancia:** encargado de velar por la seguridad de acceso de la universidad y a los ambientes internos como son aulas de clase, laboratorios y áreas administrativas.

✓ **Proveedor de servicio de Internet y telefonía:** empresa encargada de prestar servicios de telefonía e internet.

✓ **Soporte técnico informático:** personal a cargo del mantenimiento y reparación de equipos informáticos (pc, impresoras, escáner, laptops) así como la instalación de software que se requiere.

✓ **Usuarios finales externos:** personas ajenas a la institución que realizan acceso a servicios como visualización de páginas web y uso de otros servicios que brinda la universidad.

✓ **Usuarios finales internos:** personas que hacen uso de los sistemas de información entre ellos se clasifican en (alumnos, docentes, administrativos)

4.2.7 Infraestructura

Estructura física de la universidad que acogen equipos informáticos y de comunicaciones

✓ **Campus universitario:** es el conjunto de terreno y módulos en que se ubican las instalaciones de diversas facultades, aulas completamente equipadas, laboratorios de cómputo, laboratorios de investigación, una biblioteca, salas de proyección(paraninfo), comedor universitario, zonas de esparcimiento, vivero forestal, museo, zoo criadero, zona de parqueo, entre otros servicios.

✓ **Laboratorios de cómputo:** es un ambiente para el aprendizaje a través del uso de programas de informática en computadores personales para cada alumno. Es un ambiente para estudiar, experimentar y aprender mediante el uso de programas de informática.

✓ **Laboratorios especializados:** ambientes que cuentan con equipamiento especializado de acuerdo a cada facultad, en la que se realizan experimentos y aprendizaje de las actividades académico científicas.

✓ **Modulo universitario:** son aquellos módulos que cuentan con un número específico de aulas en la que se desarrollan actividades académicas y/o actividades administrativas

✓ **Sala de servidores:** es un ambiente designado exclusivamente para alojar los servidores, equipos de red y otros medios informáticos en la que se almacena, procesa y transmite datos e información de la universidad.

✓ **Sedes o locales:** son aquellos locales ubicados fuera del campus universitario de tingo maría.

4.3 Identificación de amenazas

En esta actividad se identificará las causas potenciales de que un incidente pueda causar daños a un activo o grupo de activos, en el peor de los casos a toda la institución. Esta actividad se puede resumir a la expresión “conoce a tu enemigo”.

Cuadro 12. Catálogo de amenazas – Desastres naturales

[AN] Desastres naturales	
[AN01]	Daños por agua
[AN02]	Daños por fuego
[AN03]	Rayo, tormenta eléctrica
[AN04]	Sismos, terremotos

Fuente: Elaboración propia

Cuadro 13. Catálogo de amenazas – Origen Industrial

[AI] De origen industrial	
[AI01]	Avería de origen físico o lógico
[AI02]	Condiciones inadecuadas de temperatura o humedad
[AI03]	Contaminación electromagnética
[AI04]	Contaminación medioambiental
[AI05]	Corte del suministro eléctrico
[AI06]	Daños por agua
[AI07]	Degradación de los soportes de almacenamiento de información
[AI08]	Emanaciones electromagnéticas
[AI09]	Explosiones, derrumbes y contaminación
[AI10]	Fallo de servicios de comunicaciones
[AI11]	Fuego
[AI12]	Interrupción de otros servicios y suministros esenciales

Fuente: Elaboración propia

Cuadro 14. Catálogo de amenazas – Errores y Fallos

[AE] Errores y fallos	
[AE01]	Alteración de la información
[AE02]	Caída del sistema por agotamiento de recursos
[AE03]	Deficiencias en la organización
[AE04]	Destrucción de información
[AE05]	Difusión de software dañino
[AE06]	Errores de configuración
[AE07]	Errores de los usuarios
[AE08]	Errores de mantenimiento / actualización de hardware
[AE09]	Errores de mantenimiento / actualización de software
[AE10]	Errores de monitorización (log)
[AE11]	Errores del administrador del sistema / de la seguridad
[AE12]	Falta de capacitación al personal
[AE13]	Falta de mecanismos de verificación de normas y reglas
[AE14]	Fugas de información

[AE15]	Indisponibilidad del personal
[AE16]	Inexistencia de políticas de seguridad de la información
[AE17]	Pérdida de equipos
[AE18]	Sobrecarga eléctrica
[AE19]	Uso de Software falsificado (software pirata)
[AE20]	Vulnerabilidades de los programas (software)

Fuente: Elaboración propia

Cuadro 15. Catálogo de amenazas – Ataques Deliberados

[AD] Ataques deliberados	
[AD01]	Abuso de privilegios de acceso
[AD02]	Acceso no autorizado
[AD03]	Análisis de tráfico
[AD04]	Ataque destructivo
[AD05]	Denegación de servicio
[AD06]	Destrucción de la información
[AD07]	Difusión de software dañino
[AD08]	Distracción
[AD09]	Extorsión
[AD10]	Indisponibilidad del personal
[AD11]	Ingeniería social (picaresca)
[AD12]	Interceptación de información (escucha)
[AD13]	Manipulación de los archivos de configuración
[AD14]	Manipulación de los registros de actividad (log)
[AD15]	Manipulación de programas
[AD16]	Manipulación del hardware
[AD17]	Modificación de la información
[AD18]	Repudio (negación de actuaciones)
[AD19]	Robo de equipos
[AD20]	Suplantación de la identidad del usuario
[AD21]	Uso no previsto

Fuente: Elaboración propia

4.4 Descripción de las amenazas

4.4.1 [AN] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. Origen: Natural (accidental).

✓ ***[AN01] Fuego:*** son los incendios o posibilidad de que el fuego acabe con los activos de la institución.

✓ ***[AN02] Daños por agua:*** denominado a las inundaciones naturales y la posibilidad de que el agua acabe con los activos de la institución.

✓ ***[AN03] Rayo, tormenta eléctrica:*** incidentes que se producen en la atmósfera, que son descargas naturales de electricidad estática y que pueden impactar en cualquier lugar y que causan grandes daños materiales.

✓ ***[AN04] Sismos, terremotos:*** movimientos vibratorios, pueden ser lentos o rápidos y violentos de la superficie terrestre, provocados por perturbaciones en el interior de la tierra, pueden causar grandes destrozos de cualquier infraestructura física.

4.4.2 [AI] De origen industrial

Sucesos que pueden ocurrir por parte del entorno o derivados de la actividad humana de tipo industrial. Origen: Entorno (accidental) o Humano (accidental o deliberado)

✓ ***[AI01] Avería de origen físico o lógico:*** fallos en los equipos y/o fallos en los programas, puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

✓ ***[AI02] Condiciones inadecuadas de temperatura o humedad:*** deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío o exceso de humedad.

✓ ***[AI03] Contaminación electromagnética:*** Interferencias de radio, campos magnéticos, luz ultravioleta que dificultan el buen funcionamiento de equipos electrónicos.

✓ ***[AI04] Contaminación medioambiental:*** entre los más comunes se tiene a vibraciones, polvo, suciedad.

✓ ***[AI05] Corte del suministro eléctrico:*** es la pérdida de suministro eléctrico de manera parcial o total.

✓ ***[AI06] Daños por agua:*** debido a escapes, fugas o inundaciones y la posibilidad de que el agua acabe con los activos de la institución u ocasione algún perjuicio.

✓ ***[AI07] Degradación de los soportes de almacenamiento de la información:*** como consecuencia del paso del tiempo los soportes de información como papel, medios magnéticos y digitales tienden a deteriorarse hasta quedar inutilizables.

✓ ***[AI08] Emanaciones electromagnéticas:*** Es una amenaza donde el emisor es víctima pasiva del ataque, ya que prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

✓ ***[AI09] Explosiones, derrumbes y contaminación:*** aquellos desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, accidentes de tráfico, etc.

✓ ***[AI10] Fallo de servicios de comunicaciones:*** cese de la capacidad de transmitir datos de un sitio a otro, típicamente se debe a la

destrucción de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

✓ ***[AI11] Fuego:*** incendio o posibilidad de que el fuego acabe con los activos, cuyo origen puede ser accidental o deliberado derivados de la actividad humana.

✓ ***[AI12] Interrupción de otros servicios y suministros esenciales:*** otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante.

4.4.3 [AE] Errores y fallos

Fallos no intencionales causados por las personas, la numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto, derivados de la impericia, negligencia de usuarios y decisiones institucionales. Origen: Humano (accidental)

✓ ***[AE01] Alteración accidental de la información:*** alteración accidental de la información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

✓ ***[AE02] Caída del sistema por agotamiento de recursos:*** a carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

✓ ***[AE03] Deficiencias en la organización:*** cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión.

✓ ***[AE04] Destrucción de información:*** pérdida accidental de información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

✓ ***[AE05] Difusión de software dañino:*** propagación inocente de 4virus, espías (spyware), gusanos, troyanos, bombas lógicas.

✓ ***[AE06] Errores de configuración:*** introducción de datos de configuración erróneos, prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento.

✓ ***[AE07] Errores de los usuarios:*** equivocaciones de las personas cuando usan los servicios, datos o cualquier otro activo de información.

✓ ***[AE08] Errores de mantenimiento / actualización de equipos (hardware):*** defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

✓ ***[AE09] Errores de mantenimiento / actualización de programas (software):*** defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

✓ ***[AE10] Errores de monitorización (log):*** inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.

✓ ***[AE11] Errores del administrador:*** equivocaciones de personas con responsabilidades de instalación y operación

✓ ***[AE12] Falta de capacitación al personal:*** la falta de formación del personal es el eslabón más débil lo cual significa problemas serios para cualquier institución porque impacta de manera desfavorable interna y externamente.

✓ ***[AE13] Falta de mecanismos de verificación de normas y reglas:*** la inexistencia de mecanismos de verificación de normas y reglamentos implica que la institución no tiene claro el grado de cumplimiento de la normatividad vigente exigida por el estado peruano.

✓ ***[AE14] Fugas de información:*** revelación por indiscreción; incontinencia verbal, medios electrónicos, soporte papel.

✓ ***[AE15] Indisponibilidad del personal:*** ausencia accidental del puesto de trabajo: enfermedad o alteraciones del orden público.

✓ ***[AE16] Inexistencia de políticas de seguridad de la información:*** implica que no existe reglas con respecto a lo que se pueden realizar o lo que se tiene prohibido hacer, asimismo se carece de un documento formal que regule la gestión de la seguridad de la información al interior de la institución.

✓ ***[AE17] Pérdida de equipos:*** la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una

indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales en el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

✓ ***[AE18] Sobrecarga eléctrica:*** en un circuito o instalación hay sobrecarga o está sobrecargada, cuando la suma de la potencia de los aparatos que están a él conectados, es superior a la potencia para la cual está diseñado el circuito de la instalación.

✓ ***[AE19] Uso de software falsificado (software pirata):*** al utilizar programas *crackeados* se tiene abierto la posibilidad de verse infectado por virus o *malware*, entre otros. Por otra parte, la institución puede verse afectado en serios problemas legales por realizar uso indebido de este tipo de software.

✓ ***[AE20] Vulnerabilidades de los programas (software*)**: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

4.4.4 [AD] Ataques deliberados

✓ ***[AD01] Abuso de privilegios de acceso:*** cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

✓ ***[AD02] Acceso no autorizado:*** el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización

✓ ***[AD03] Análisis de tráfico:*** el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.

✓ ***[AD04] Ataque destructivo:*** vandalismo, terrorismo, acción militar, etc., ésta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personas contratadas de forma temporal.

✓ ***[AD05] Denegación de servicio:*** es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos.

✓ ***[AD06] Destrucción de información:*** eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.

✓ ***[AD07]*** **Difusión de software dañino:** propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas.

✓ ***[AD08] Distracción:*** ataques que causan interrupción en la organización para centrar su atención en un problema específico, mientras el verdadero ataque se centra en otro punto.

✓ ***[AD09] Extorsión:*** presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.

✓ ***[AD10] Indisponibilidad del personal:*** ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas.

✓ ***[AD11] Ingeniería social:*** abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

✓ ***[AD12] Interceptación de información (escucha):*** el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.

✓ ***[AD13] Manipulación de la configuración:*** prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento.

✓ ***[AD14] Manipulación de los registros de actividad (log):*** el log almacena toda la información correspondiente a los errores y/o eventos inesperados dentro de una aplicación para tener un registro de estas incidencias, al ser manipulados se pueden revelar información confidencial que no debe ser revelada por privacidad o incluso porque su revelación hace vulnerable la seguridad del sistema.

✓ ***[AD15] Manipulación de programas:*** alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

✓ ***[AD16] Manipulación del hardware:*** alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

✓ ***[AD17] Modificación de la información:*** alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.

✓ ***[AD18] Repudio:*** negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro

✓ ***[AD19] Robo:*** la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

✓ ***[AD20] Suplantación de la identidad del usuario:*** cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.

✓ ***[AD21] Uso no previsto:*** utilización de los recursos del sistema para fines no previstos, típicamente de interés personal tales como juegos, consultas personales en Internet, bases de datos personales, software no autorizado, almacenamiento de archivos personales, etc.

4.5 Criterios de valoración

Según la metodología MAGERIT, existe una escala detallada de diez valores tal como se aprecia en el Cuadro 16, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de menos niveles, como detalla el Cuadro 17.

Cuadro 16. Criterios de valoración MAGERIT

Valor Magerit		Criterio Magerit
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante para efectos prácticos

Fuente: MAGERIT – Libro II

Tomando como referencia los criterios que se establece en el Cuadro 16, para el caso de esta investigación se ha definido una escala de valores del 1 al 4, ya que las buenas prácticas y expertos como MAÑAS (2012) señalan que el uso de criterios simples es muy didáctico y fácil de realizar al realizar un análisis de riesgos.

Cuadro 17. Criterios definidos valor de activo / amenaza

Valor definido	Valor del activo	Magnitud del daño de la amenaza
4	Alto	Alto
3	Medio	Medio
2	Bajo	Bajo
1	Muy bajo	Insignificante

Fuente: Elaboración propia

De igual modo para el caso de la probabilidad de ocurrencia de las amenazas también se definieron valores entre 1 y 4 tal como se puede apreciar en el Cuadro 18.

Cuadro 18. Criterios de valor – probabilidad de la amenaza

Valor definido	Probabilidad de ocurrencia	Detalle
4	Probable	Muy frecuente (a diario)
3	Posible	Frecuente (semanal)
2	Poco probable	Normal (cada varios meses)
1	Muy raro	Poco frecuente (cada varios años)

Fuente: Elaboración propia

4.6 Valoración de amenazas frente al grupo de activos

Las dimensiones que se valoran son Disponibilidad (D), Integridad (I) y Confidencialidad (C), que son las que se ven afectadas directamente por las amenazas.

En el Cuadro 19 se puede apreciar la relación entre las amenazas de origen natural y el grupo de activos a los que afecta, para el caso de amenazas de origen industrial se detalla en el Cuadro 20; para las amenazas de errores y fallos en el Cuadro 21 y finalmente para las amenazas deliberadas en el Cuadro 22.

Cuadro 19. Valoración de amenazas naturales frente al grupo de activos

Amenaza	Dimensiones			Grupo de activos						
	D	I	C	PI	DI	SI	IH	EA	PE	IF
AN01	x	x		x	x		x	x		x
AN02	x	x		x	x		x	x		x
AN03	x	x		x		x	x	x		x
AN04	x	x		x			x	x	x	x
Total	4	4	0	4	2	1	4	4	1	4

Fuente: Elaboración propia

Cuadro 20. Valoración de amenazas de origen industrial frente al grupo de activos

Amenaza	Dimensiones			Grupo de activos						
	D	I	C	PI	DI	SI	IH	EA	PE	IF
AI01	x					x	x	x		
AI02	x	x		x	x		x	x		
AI03	x	x					x			
AI04	x						x	x		
AI05	x			x	x	x	x	x		
AI06	x	x		x	x		x	x	x	x
AI07	x	x			x					
AI08	x		x				x			
AI09	x									x
AI10	x			x		x				
AI11	x	x			x		x	x	x	x
AI12	x			x			x			
Total	**12**	**5**	**1**	**4**	**5**	**3**	**9**	**6**	**2**	**3**

Fuente: Elaboración propia

Cuadro 21. Valoración de amenazas fallos y errores frente al grupo de activos

Amenaza	Dimensiones			Grupo de activos						
	D	I	C	PI	DI	SI	IH	EA	PE	IF
AE01		x		x	x					
AE02	x					x				
AE03	x			x					x	
AE04	x			x	x					
AE05	x	x	x			x				
AE06		x				x				
AE07	x	x	x		x	x				
AE08	x						x	x		
AE09	x	x				x				
AE10		x				x				
AE11	x	x	x			x	x			
AE12		x	x	x		x				
AE13		x	x	x						
AE14			x	x	x				x	
AE15	x			x		x			x	
AE16	x	x	x	x	x	x	x	x	x	x
AE17	x		x	x	x		x			
AE18	x						x	x		
AE19	x	x	x	x		x				
AE20	x	x	x			x				
Total	**14**	**13**	**10**	**10**	**6**	**12**	**5**	**3**	**4**	**1**

Fuente: Elaboración propia

Cuadro 22. Valoración de amenazas ataques deliberados frente al grupo de activos

Amenaza	Dimensiones			Grupo de activos						
	D	I	C	PI	DI	SI	IH	EA	PE	IF
AD01	x	x	x			x				
AD02		x	x			x	x			x
AD03			x			x	x			
AD04	x				x		x	x		x
AD05	x					x	x			
AD06	x			x	x					
AD07	x	x	x		x	x				
AD08	x	x	x				x		x	
AD09	x	x	x	x					x	
AD10	x								x	
AD11	x	x	x			x			x	
AD12			x		x					
AD13	x	x	x			x				
AD14		x	x			x				
AD15	x	x	x			x				
AD16	x		x				x	x		
AD17		x		x	x					
AD18		x							x	
AD19	x		x		x		x	x		
AD20		x	x	x					x	
AD21	x	x	x			x	x	x		x
Total	**14**	**13**	**16**	**4**	**6**	**10**	**8**	**4**	**6**	**3**

Fuente: Elaboración propia

4.7 Estimación del riesgo, probabilidad e impacto

En función de los valores establecidos hasta el momento, se procederá a aplicar las fórmulas o funciones establecidas por la metodología MAGERIT para calcular los valores de riesgo. Generalmente, el cálculo del riesgo tendrá en cuenta el valor del activo, la degradación que provocan las amenazas cuando estas tienen lugar y la probabilidad de ocurrencia de las mismas.

La fórmula de calcular el riesgo, según cada metodología, puede ir desde complejas fórmulas matemáticas, hasta el uso de sencillas tablas de doble

entrada por lo cual cada investigador deberá seleccionar una metodología en función del nivel de detalle que haya decidido para la evaluación de los riesgos. A continuación, se modelan impacto, probabilidad y riesgo por medio de escalas cuantitativas y cualitativas:

Cuadro 23. Criterios de estimación del riesgo, probabilidad e impacto

Valor	Impacto	Probabilidad	Riesgo
4	**A:** alto	**A:** probable	**A:** importante
3	**M:** medio	**M:** posible	**M:** apreciable
2	**B:** bajo	**B:** poco probable	**B:** bajo
1	**MB:** muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: MAGERIT – Libro III: Técnicas

Del Cuadro 23 al realizar las operaciones aritméticas entre impacto y probabilidad dará como resultado una tabla con los resultados para calcular el riesgo, tal como se aprecia en la Figura 8.

RIESGO		Probabilidad			
		1	2	3	4
Impacto	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Figura 8. Valoración del riesgo
Fuente: Elaboración propia

La tabla de valoración del riesgo de la Figura 8 permite apreciar el riesgo resultante para todas las combinaciones posibles, por lo que los valores cuantitativos permiten obtener una escala cualitativa como la que se observa en la Figura 9.

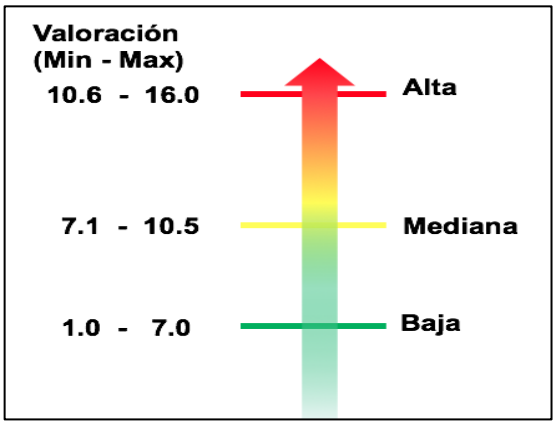


Figura 9. Escala del nivel del riesgo
Fuente: Elaboración propia

Teniendo en cuenta todos los criterios de valoración detallados anteriormente, se realiza el cálculo de riesgos en una matriz detallada (Ver Anexo 2) que como resultado nos da la consolidación de datos que se observa en la Figura 10, estos resultados representan los riesgos asociados a los activos de la universidad, siendo los riesgos más críticos los valores que se encuentran sombreado con el color rojo.

NIVEL DE RIESGO		Probabilidad			
		[AN]	[AI]	[AE]	[AD]
Magnitud de Daño	Procesos institucionales	6,00	9,33	10,18	7,20
	Datos e información	6,53	8,95	9,95	9,33
	Sistemas y Software	3,52	8,20	10,84	10,90
	Infraestructura de TI y Hardware	6,95	7,34	8,65	7,42
	Equipamiento auxiliar	5,25	7,50	11,00	6,75
	Personal	6,19	2,56	9,73	7,67
	Infraestructura física	4,25	5,67	8,50	7,56

Figura 10. Nivel de riesgos
Fuente: Elaboración propia

Las siguientes figuras muestran el umbral de riesgo en la que se encuentran los activos de información, este tipo de figuras nos sirven de referencia para estimar el tratamiento a dar a cada riesgo (mitigar, transferir, aceptar o eliminar).

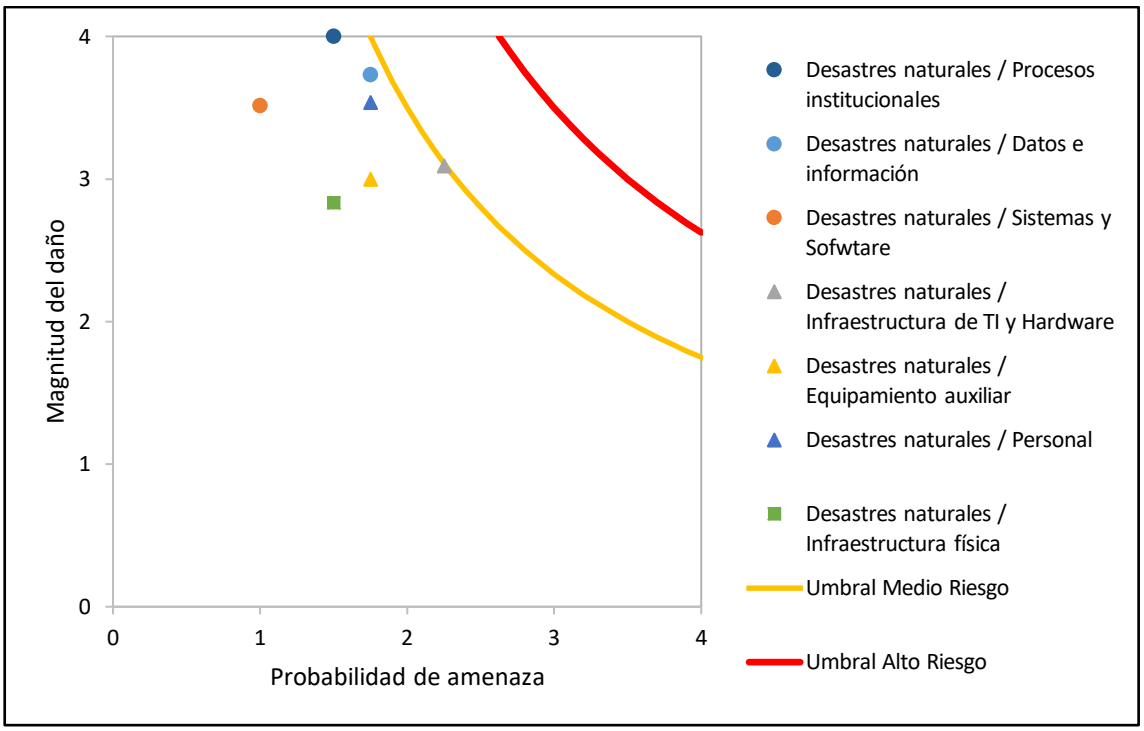


Figura 11. Análisis de factores de riesgo - Desastres Naturales
Fuente: Elaboración propia

Por ejemplo, en la Figura 11 se aprecia que los activos que se encuentren por debajo del umbral del riesgo medio, esto representa que el riesgo de los activos que se encuentren asociados a las amenazas de origen natural, puede ser asumido por la institución, aunque para el caso de los activos del grupo de Infraestructura de TI y Hardware se deben considerar controles a mediano y largo plazo para poder mitigar o mantener el riesgo por debajo del umbral de riesgo medio, ya que a futuro el riesgo puede aumentar considerablemente.

Para los demás casos se puede observar que existen más de cinco grupos de activos que se encuentran por encima del umbral del riesgo medio, como ejemplo se puede apreciar la Figura 12, esto representa una alerta ya que las probabilidades de que puedan materializarse las amenazas son grandes, esto implica que se deben tener en cuenta la implementación de controles a mediano plazo a fin de mitigar el riesgo.

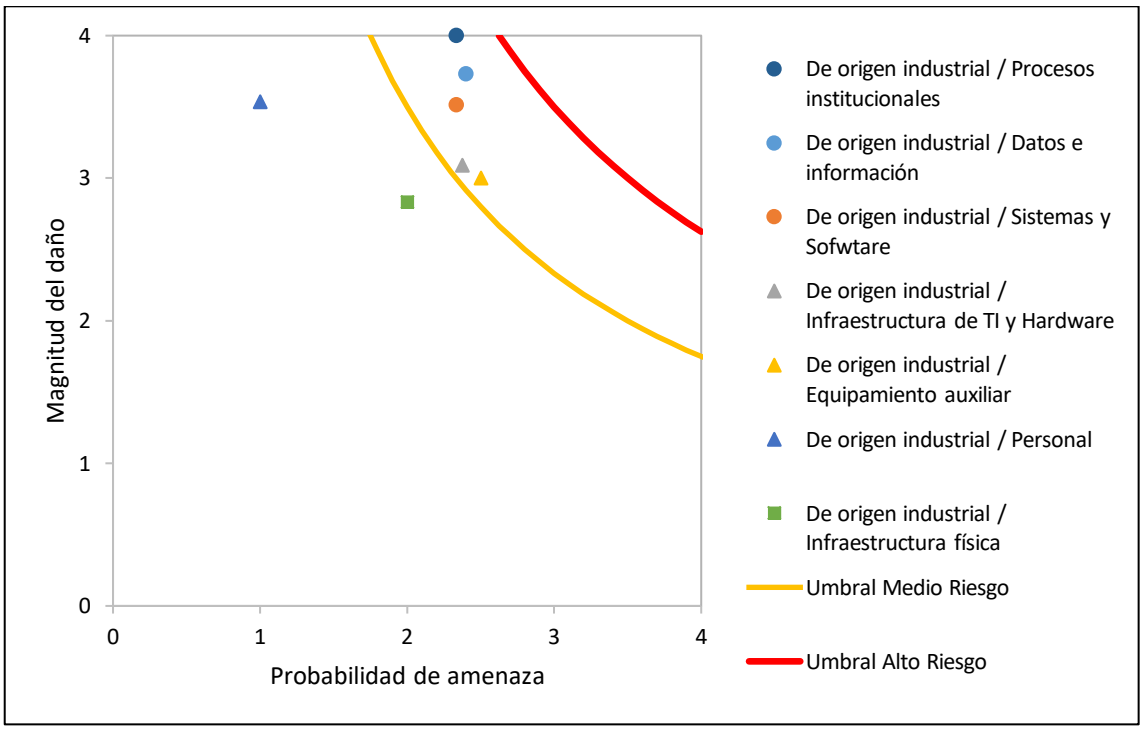


Figura 12. Análisis de factores de riesgo - De origen industrial
Fuente: Elaboración propia

Por otro lado, en la Figura 13 se observa que los activos Sistemas y Software y Equipamiento Auxiliar están por encima del umbral de riesgo alto, esto indica que se debe actuar a corto plazo a fin de tratar el riesgo. De forma similar se tiene en la Figura 14 los activos que están por encima del umbral del riesgo alto es Sistemas y Software, por lo tanto, requiere inmediata implementación de controles para poder mitigar el riesgo.

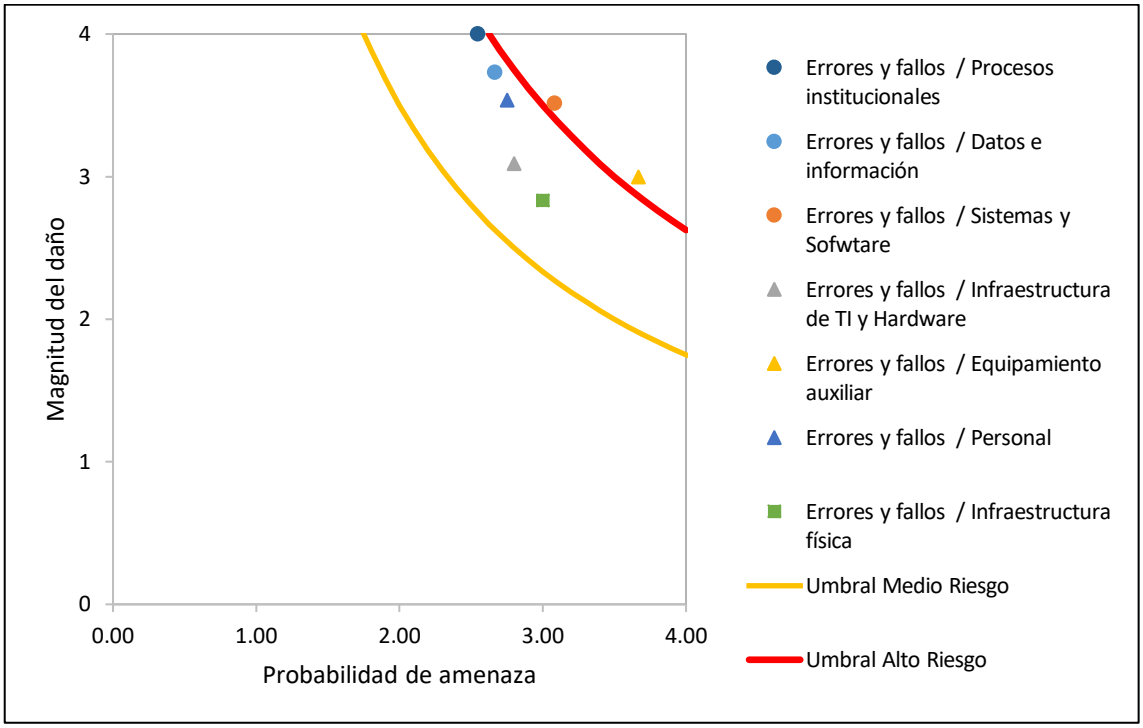


Figura 13. Análisis de factores de riesgo - Errores y fallos
Fuente: Elaboración propia

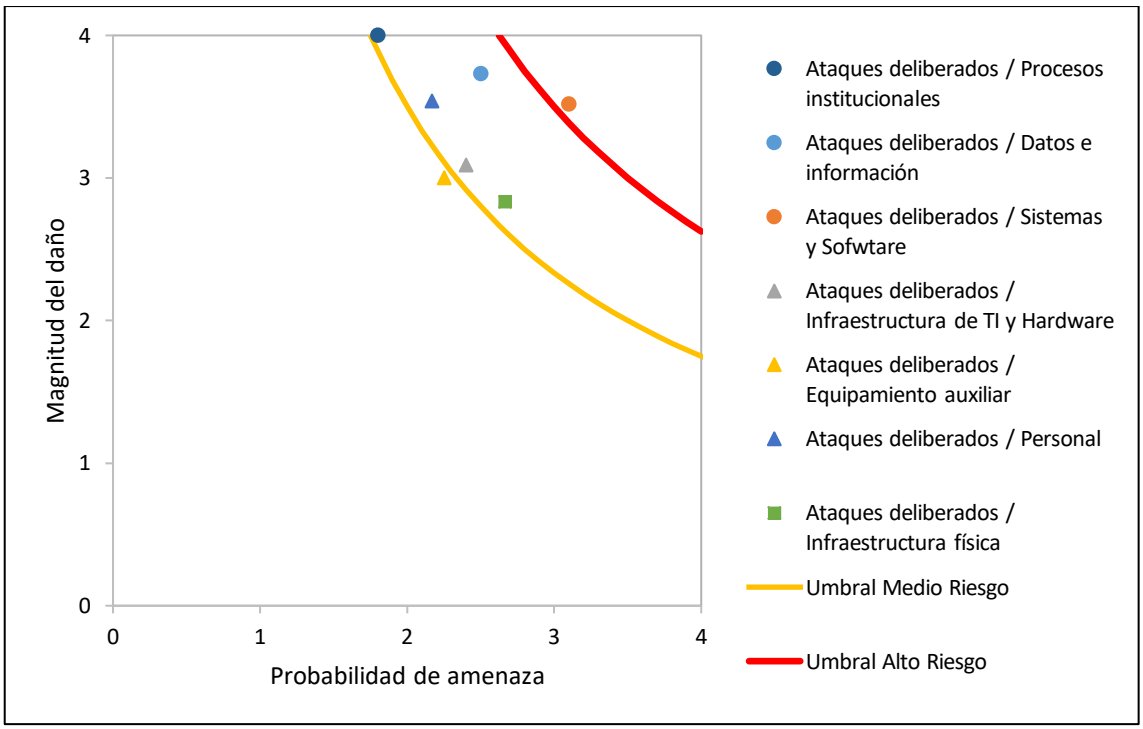


Figura 14. Análisis de factores de riesgo - Ataques deliberados
Fuente: Elaboración propia

4.8 Gestión de riesgos

Luego de haber realizado el análisis de riesgos queda en evidencia los riesgos a la que está expuesto cada grupo de activos de la universidad, lo que ha llevado a una calificación de cada riesgo significativo, determinándose si:

- ✓ Es Alto, en el sentido que se requiere atención urgente, por lo que se debe establecer controles a corto plazo.
- ✓ Es Medio, en el sentido de que pueda ser objeto de estudio para su tratamiento a corto o mediano plazo.
- ✓ Es Bajo, en el sentido de que no se van a tomar acciones a corto plazo por lo que los controles pueden ser planificados a largo plazo.

El resultado del análisis de riesgos consiste en partir de la información que se dispone para tomar decisiones conociendo lo que se quiere proteger, todo ello sintetizado en los valores de impacto y riesgo. Los criterios de aceptación del riesgo se establecen considerando: criterios institucionales, aspectos legales y regulatorios, operaciones, tecnología, finanzas y factores sociales

Los criterios de aceptación del riesgo corresponden a “criterios para aceptar riesgos e identificar el nivel aceptable del riesgo”, según se especifica en la norma ISO/IEC 27001 Capítulo 6.1.2 a).

V. IMPLEMENTACIÓN DE CONTROLES ISO/IEC 27002:2013

5.1 Mapeo de controles de seguridad Nivel 1

Identificando las amenazas y los riesgos que representan, se procede a realizar el mapeo de controles utilizando la ISO/IEC 27002:2013 esta norma establece las directrices para la seguridad de la información en las organizaciones incluyendo la selección, implantación y la gestión de controles teniendo en consideración el entorno de riesgos de seguridad de la información.

Para esta sección se tuvo en consideración la socialización con el equipo del Centro de Tecnologías de la Información y Comunicación de la universidad, por consiguiente los controles se seleccionan en función a los riesgos de los activos que previamente se identificaron, entonces se verifica el dominio y control al que aplica según revisión bibliográfica y la opinión de expertos y también la viabilidad de su implementación de cada control que la norma sugiere, para lo cual se realizaron reuniones con el equipo del CTIC para poder validar los controles seleccionados .

A continuación, se detallan el mapeo de controles de seguridad en función a las amenazas y los riesgos que representan.

Cuadro 24. Controles para errores y fallos en sistemas y software con riesgo alto.

	AMENAZA	RIESGO	CONTROL	RESUMEN DE CONTROLES SELECCIONADOS
AE07	Errores de los usuarios	Alto	**A.5.1.1** A.6.1.1 A.6.1.2 **A.7.2.2** **A.12.1.1**	✓ **A.5.1.1** Políticas para la seguridad de la información. ✓ **A.7.2.2** Concienciación, educación y capacitación de la seguridad de la información. ✓ **A.12.1.1** Documentación de procedimientos de operación. ✓ **A.12.5.1** Instalación de software en sistemas en producción. ✓ **A.12.6.1** Gestión de las vulnerabilidades técnicas. ✓ **A.12.6.2** Restricciones en la instalación de software. ✓ **A.14.2.1** Política de desarrollo seguro. ✓ **A.16.1.3** Notificación de puntos débiles de la seguridad de la información. ✓ **A.18.1.1** Identificación de la legislación aplicable. ✓ **A.18.1.2** Derechos de propiedad intelectual (DPI).
AE16	Inexistencia de políticas de seguridad de la información	Alto	**A.5.1.1** A.5.1.2 **A.18.1.1** A.18.2.2 A.18.2.3	
AE19	Uso de Software falsificado (software pirata)	Alto	**A.5.1.1** A.5.1.2 **A.12.5.1** **A.12.6.2** **A.18.1.1** **A.18.1.2** A.18.2.2 A.18.2.3	
AE20	Vulnerabilidades de los programas (software)	Alto	**A.12.6.1** **A.12.6.2** **A.14.2.1** **A.16.1.3**	

Fuente: Elaboración propia

Cuadro 25. Controles para errores y fallos en sistemas y software con riesgo medio.

	AMENAZA	RIESGO	CONTROL	RESUMEN DE CONTROLES SELECCIONADOS
AE02	Caída del sistema por agotamiento de recursos	Medio	**A.5.1.1** **A.11.2.4** **A.12.3.1** A.12.6.1 A.14.1.1 A.16.1.5 A.16.1.6 A.17.1.1 **A.17.2.1**	✓ **A.5.1.1** Políticas para la seguridad de la información. ✓ **A.7.2.2** Concienciación, educación y capacitación de la seguridad de la información. ✓ **A.11.2.4** Mantenimiento de equipos. ✓ **A.12.1.4** Separación de entornos de desarrollo, prueba y producción. ✓ **A.12.3.1** Copias de seguridad de la información. ✓ **A.12.6.2** Restricciones en la instalación de software. ✓ **A.13.2.1** Políticas y procedimientos de intercambio de información.
AE05	Difusión de software dañino	Medio	A.5.1.1 A.5.1.2 **A.7.2.2** A.12.2.1 **A.12.3.1** **A.12.6.2** **A.13.2.1** A.16.1.7	

AE06	Errores de configuración	Medio	A.5.1.1 A.12.1.1 A.12.1.2 **A.12.1.4** A.12.4.3 A.16.1.3	
AE09	Errores de mantenimiento / actualización de software	Medio	A.5.1.1 A.5.1.2 **A.11.2.4**	
AE12	Falta de capacitación al personal	Medio	A.5.1.1 A.6.1.1 A.6.1.2 **A.7.2.2** A.12.1.1	

Fuente: Elaboración propia

Cuadro 26. Controles para ataques deliberados en sistemas y software con riesgo alto.

	AMENAZA	RIESGO	CONTROL	RESUMEN DE CONTROLES SELECCIONADOS
AD05	Denegación de servicio	Alto	**A.9.1.2** **A.12.6.1** **A.13.1.1** **A.13.1.2** **A.13.1.3** **A.15.1.1** A.15.2.1 A.17.2.1	✓ **A.5.1.1** Políticas para la seguridad de la información. ✓ **A.9.1.1** Política de control de acceso. ✓ **A.9.1.2** Control de acceso a redes y servicios asociados. ✓ **A.9.2.5** Revisión de los derechos de acceso de usuarios. ✓ **A.10.1.1** Política sobre el uso de controles criptográficos. ✓ **A.12.2.1** Controles contra códigos maliciosos. ✓ **A.12.3.1** Copias de seguridad de la información. ✓ **A.12.6.1** Gestión de las vulnerabilidades técnicas. ✓ **A.13.1.1** Controles de red. ✓ **A.13.1.2** Mecanismos de seguridad en los servicios de red. ✓ **A.13.1.3** Segregación en las redes. ✓ **A.13.2.1** Políticas y procedimientos de intercambio de información. ✓ **A.15.1.1** Política de seguridad de la información para proveedores. ✓ **A.16.1.7** Recolección de evidencias.
AD07	Difusión de software dañino	Alto	**A.5.1.1** A.5.1.2 **A.12.2.1** **A.12.3.1** A.12.6.2 **A.13.2.1** **A.16.1.7**	
AD12	Interceptación de información (escucha)	Alto	**A.9.1.1** **A.9.1.2** **A.9.2.5** **A.10.1.1** A.12.6.1 A.13.1.1 A.13.1.2 **A.13.1.3** **A.13.2.1** A.13.2.3 A.16.1.2	

Fuente: Elaboración propia

Cuadro 27. Controles para ataques deliberados en sistemas y software con riesgo medio.

	AMENAZA	RIESGO	CONTROL	RESUMEN DE CONTROLES SELECCIONADOS
AD01	Abuso de privilegios de acceso	Medio	A.6.1.2 **A.7.2.2** A.7.2.3 **A.9.1.1** **A.9.1.2** **A.9.2.1** A.9.2.2 **A.9.2.3** A.9.2.5 A.9.2.6 A.9.3.1 A.9.4.1	✓ **A.7.2.2** Concienciación, educación y capacitación de la seguridad de la información. ✓ **A.7.2.3** Proceso disciplinario. ✓ **A.9.1.1** Política de control de acceso. ✓ **A.9.1.2** Control de acceso a redes y servicios asociados. ✓ **A.9.2.1** Gestión de altas/bajas en el registro de usuarios. ✓ **A.9.2.3** Gestión de derechos de acceso con privilegios especiales. ✓ **A.9.3.1** Uso de información confidencial para la autenticación. ✓ **A.9.4.2** Procedimientos seguros de inicio de sesión. ✓ **A.10.1.1** Política sobre el uso de controles criptográficos. ✓ **A.11.1.3** Seguridad de oficinas, despachos y recursos. ✓ **A.11.2.1** Ubicación y protección de los equipos. ✓ **A.13.1.3** Segregación en las redes.
AD02	Acceso no autorizado	Medio	**A.7.2.3** A.9.1.1 **A.9.1.2** **A.9.3.1** A.9.4.1 **A.9.4.2** A.11.1.2 **A.11.1.3**	
AD03	Análisis de tráfico	Medio	A.9.1.2 **A.10.1.1** A.12.6.1 A.13.1.1 A.13.1.2 **A.13.1.3** A.13.2.1 A.13.2.3 A.16.1.2	
AD15	Manipulación de programas	Medio	A.9.1.1 A.11.1.2 **A.11.2.1** A.11.2.9 A.16.1.5	
AD21	Uso no previsto	Medio	A.7.2.1 **A.7.2.2** A.7.2.3 A.8.1.3 A.8.2.3 A.11.2.5 A.11.2.6 A.12.4.1	

Fuente: Elaboración propia

Cuadro 28. Controles para errores y fallos en equipos auxiliares con riesgo alto.

	AMENAZA	RIESGO	CONTROL	RESUMEN DE CONTROLES SELECCIONADOS
AE16	Inexistencia de políticas de seguridad de la información	Alto	**A.5.1.1** **A.5.1.2** **A.18.1.1** **A.18.2.2** A.18.2.3	✓ **A.5.1.1** Políticas para la seguridad de la información. ✓ **A.5.1.2** Revisión de las Políticas para seguridad de la información. ✓ **A.11.2.4** Mantenimiento de equipos. ✓ **A.18.1.1** Identificación de la legislación aplicable. ✓ **A.18.2.2** Cumplimiento de las políticas y normas de seguridad.
AE18	Sobrecarga eléctrica	Alto	**A.5.1.1** A.11.2.1 A.11.2.3 **A.11.2.4** A.12.1.1	

Fuente: Elaboración propia

Cuadro 29. Controles para errores y fallos en equipos auxiliares con riesgo medio.

	AMENAZA	RIESGO	CONTROL	RESUMEN DE CONTROLES SELECCIONADOS
AE08	Errores de mantenimiento / actualización hardware	Medio	**A.5.1.1** **A.5.1.2** **A.11.2.4**	✓ **A.5.1.1** Políticas para la seguridad de la información. ✓ **A.5.1.2** Revisión de las Políticas para seguridad de la información. ✓ **A.11.2.4** Mantenimiento de equipos.

Fuente: Elaboración propia

En los cuadros anteriores se realizó el mapeo de controles en función a las amenazas, para los Riesgos Altos y Medios ya que son aquellos en los que la universidad debe enfocar la implementación de controles de seguridad necesarios para poder mitigar dichos riesgos.

5.2 Mapeo de controles de seguridad Nivel 2

En el Cuadro 30 se puede apreciar los controles finalmente seleccionados luego de socializar entre investigadores y directivos del CTIC para su implementación, cabe recalcar que para la selección de los controles se ha tomado en cuenta las amenazas que representan el nivel de riesgo alto, que en total son 7 amenazas, 5 amenazas de Errores y Fallos y 2 amenazas cuyo origen son los Ataques Deliberados, a fin de poder mitigar el riesgo y fortalecer la seguridad de la información en la universidad. Tal como se observa en el cuadro, para cada amenaza se tiene controles específicos que permitirán gestionar los riesgos identificados.

Cuadro 30. Plan de implementación de controles en Sistemas y Software.

AMENAZAS		VULNERABILIDADES	P[1]	I[2]	NR[3]	T[4]	TIPO DE CONTROL	CONTROLES
AE07	Errores de los usuarios.	Falta de capacitación, no se cuenta con procedimientos de operación, no eligen contraseñas seguras, uso inadecuado de sistemas y software.	4	4	Alto	Evitar	Preventivo	**A.7.2.2** Concienciación, educación y capacitación de la seguridad de la información. **A.12.1.1** Documentación de procedimientos de operación.
AE16	Inexistencia de políticas de seguridad de la información.	Ausencia de auditorías en seguridad de la información, falta de compromiso de la alta dirección, desconocimiento de la normatividad vigente.	4	4	Alto	Mitigar	Correctivo	**A.5.1.1** Políticas para la seguridad de la información. **A.18.1.1** Identificación de la legislación aplicable.

AE19	Uso de Software falsificado (software pirata).	Ausencia de mecanismos de identificación de software falsificado, inexistencia de control de cambios, falta de presupuesto, desconocimiento de la normatividad.	4	4	Alto	Mitigar	Detectivo	**A.12.5.1** Instalación de software en sistemas en producción. **A.12.6.2** Restricciones en la instalación de software. **A.18.1.1** Identificación de la legislación aplicable. **A.18.1.2** Derechos de propiedad intelectual (DPI).
AE20	Vulnerabilidades de los programas (software).	Uso de software desactualizado, configuración de fechas incorrectas, habilitación de servicios innecesarios, uso de contraseñas por defecto, falta de actualización y parches de seguridad.	4	4	Alto	Mitigar	Preventivo	**A.12.6.1** Gestión de las vulnerabilidades técnicas. **A.14.2.1** Política de desarrollo seguro. **A.16.1.3** Notificación de puntos débiles de la seguridad de la información.
AD05	Denegación de servicio.	Inexistencia de servicios de detección y prevención de intrusos, ausencia de VLAN, habilitación de servicios y puertos innecesarios, equipos de red obsoletos.	4	4	Alto	Evitar	Preventivo	**A.13.1.1** Controles de red. **A.13.1.2** Mecanismos de seguridad en los servicios de red.
AD07	Difusión de software dañino.	Uso de antivirus desactualizado y programas sin licencia, ejecución de aplicaciones sospechosas, acceso a sitios web dañinas.	4	4	Alto	Mitigar	Preventivo	**A.5.1.1** Políticas para la seguridad de la información. **A.12.2.1** Controles contra códigos maliciosos.
AD12	Interceptación de información (escucha).	Archivos compartidos sin restricción de acceso, servicios de sesión sin uso de cifrado, envío de información sin mecanismos de cifrado, ausencia de VLAN.	4	4	Alto	Evitar	Preventivo	**A.9.1.1** Política de control de acceso**.** **A.9.1.2** Control de acceso a redes y servicios asociados. **A.9.2.5** Revisión de los derechos de acceso de usuarios. **A.10.1.1** Política sobre el uso de controles criptográficos. **A.13.1.3** Segregación en las redes. **A.13.2.1** Políticas y procedimientos de intercambio de información.

[1] probabilidad. [2] impacto.[3] nivel de riesgo.[4] tratamiento.

Del mismo modo en el Cuadro 31 se observa los controles finalmente seleccionados para su implementación, para este caso se detallan los controles asociados a 2 amenazas de Errores y Fallos con Riesgo Alto y 1 con riesgo Medio que afectan a los activos Equipos Auxiliares, en total se seleccionaron 6 controles las mismas que se detallan en el siguiente cuadro.

Cuadro 31. Plan de implementación de controles en Equipos Auxiliares.

AMENAZAS		VULNERABILIDADES	P[1]	I[2]	NR[3]	T[4]	TIPO DE CONTROL	CONTROLES
AE08	Errores de mantenimiento / actualización hardware.	Falta de capacitación, inexistencia de un plan de mantenimiento, falta de registro de mantenimiento de equipos.	3	3	Medio	Evitar	Preventivo	**A.11.2.4** Mantenimiento de equipos.
AE16	Inexistencia de políticas de seguridad de la información.	Ausencia de auditorías en seguridad de la información, falta de compromiso de la alta dirección, desconocimiento de la normatividad vigente.	4	3	Alto	Mitigar	Correctivo	**A.5.1.1** Políticas para la seguridad de la información. **A.5.1.2** Revisión de las Políticas para seguridad de la información. **A.18.1.1** Identificación de la legislación aplicable. **A.18.2.2** Cumplimiento de las políticas y normas de seguridad.
AE18	Sobrecarga eléctrica.	Exceso de dispositivos conectados a una sola fuente de alimentación, uso inadecuado de estabilizadores, falta de equipos UPS.	4	3	Alto	Mitigar	Correctivo	**A.11.2.4** Mantenimiento de equipos.

[1] probabilidad. [2] impacto. [3] nivel de riesgo. [4] tratamiento.

5.3 Declaración de aplicabilidad de los controles de Nivel 2

La declaración de aplicabilidad (SOA, por sus siglas en inglés) es un documento en que se especifican todos los controles de seguridad basados en la norma ISO/IEC 27002:2013 que se establecieron para la organización y con el detalle de su aplicabilidad. Es potestad de la oficina del CTIC determinar si se aplica o no, esto en función de la recomendación del investigador. En consecuencia, la declaración de aplicabilidad se muestra en el Cuadro 32.

Cuadro 32. Declaración de aplicabilidad de controles seleccionados.

CONTROLES	APLICA	EVIDENCIA
A.5.1.1 Políticas para la seguridad de la información.	SI	Documento de política firmado por la alta dirección.
A.5.1.2 Revisión de las Políticas para seguridad de la información.	SI	Actas de revisión periódica.
A.7.2.2 Concienciación, educación y capacitación de la seguridad de la información.	SI	Plan de capacitación revisado y aprobado.
A.9.1.1 Política de control de acceso	SI	Política de control de acceso
A.9.1.2 Control de acceso a redes y servicios asociados.	SI	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento).
A.9.2.5 Revisión de los derechos de acceso de usuarios.	SI	Formato de revisión de derechos de acceso de usuarios
A.10.1.1 Política sobre el uso de controles criptográficos.	SI	Política sobre el uso de controles criptográficos
A.11.2.4 Mantenimiento de equipos.	SI	Plan de mantenimiento, manual de procedimientos y proponer un registro de control de mantenimiento.
A.12.1.1 Documentación de procedimientos de operación.	SI	Procedimientos de instalación de software, copias de respaldo, reinicio de sistemas y recuperación de incidentes.
A.12.2.1 Controles contra códigos maliciosos.	SI	Checklist de software anti malware, registro de software no autorizado.
A.12.5.1 Instalación de software en sistemas en producción.	SI	Procedimientos para controlar la instalación de software pirata.
A.12.6.1 Gestión de las vulnerabilidades técnicas.	SI	Realizar un registro de vulnerabilidades de los sistemas más críticos.
A.12.6.2 Restricciones en la instalación de software.	SI	Procedimientos para controlar la instalación de software pirata.
A.13.1.1 Controles de red.	SI	Propuesta de implementación de IDS/IPS.
A.13.1.2 Mecanismos de seguridad en los servicios de red.	SI	Procedimientos de control de acceso.

A.13.1.3 Segregación en las redes.	SI	Documentación de implementación de VLAN.
A.13.2.1 Políticas y procedimientos de intercambio de información.	SI	Propuesta de políticas y procedimientos de intercambio de información.
A.14.2.1 Política de desarrollo seguro.	SI	Política de desarrollo seguro
A.16.1.3 Notificación de puntos débiles de la seguridad de la información.	SI	Registro de notificación de vulnerabilidades.
A.18.1.1 Identificación de la legislación aplicable.	SI	Registro de legislación aplicable
A.18.1.2 Derechos de propiedad intelectual (DPI).	SI	Política para el cumplimiento de los DPI. Registro de activos que requieran protección de DPI
A.18.2.2 Cumplimiento de las políticas y normas de seguridad.	SI	Matriz de cumplimiento

Fuente: Elaboración propia

5.4 Implementación de controles ISO/IEC 27002:2013

El aumento en el nivel de implementación de los controles implica una mejora general de cada uno de los dominios de la ISO/IEC 27002:2013. Dicha mejora puede ser comparada contra el nivel de implementación realizado en el análisis diferencial inicial de la Figura 6 y el Cuadro 3. A modo de resumen se presenta en el Cuadro 33 y Cuadro 34 los controles definidos en función al grupo de activos y detallados por tipo de amenaza, cada uno de los ítems de implementación pueden apreciarse en los anexos.

Cuadro 33. Implementación de controles de seguridad en Sistemas y Software.

AMENAZA	CONTROLES	DETALLE
AE07	A.7.2.2 Concienciación, educación y capacitación de la seguridad de la información. A.12.1.1 Documentación de procedimientos de operación.	✓ Plan de capacitación alineado a las políticas más relevantes. ✓ Documentar y mantener políticas y/o procedimientos (instalación de software, copias de respaldo, reinicio de sistemas y procedimientos de recuperación).
AE16	A.5.1.1 Políticas para la seguridad de la información. A.18.1.1 Identificación de la legislación aplicable.	✓ Política general, definido y aprobado. ✓ Definir y documentar todos los requisitos legales, regulatorios o contractuales.

AE19	A.12.5.1 Instalación de software en sistemas en producción. A.12.6.2 Restricciones en la instalación de software. A.18.1.1 Identificación de la legislación aplicable. A.18.1.2 Derechos de propiedad intelectual (DPI).	✓ Desarrollar e implementar políticas y/o procedimientos para controlar la instalación de software pirata. ✓ Establecer e implementar reglas que rijan la instalación de software por parte de los usuarios. ✓ Definir y documentar todos los requisitos legales, regulatorios o contractuales. ✓ Definir, documentar y aplicar una política para el cumplimiento de los DPI. ✓ Realizar un registro de activos que requieran protección de DPI.
AE20	A.12.6.1 Gestión de las vulnerabilidades técnicas. A.14.2.1 Política de desarrollo seguro. A.16.1.3 Notificación de puntos débiles de la seguridad de la información.	✓ Realizar un inventario de Sistemas y Software. ✓ Realizar un registro de vulnerabilidades de los sistemas más críticos. ✓ Realizar la sincronización de fechas de los sistemas más críticos. ✓ Propuesta de política de desarrollo seguro. ✓ Implementar parches de seguridad. ✓ Realizar un registro de notificación de vulnerabilidades de los sistemas.
AD05	A.13.1.1 Controles de red. A.13.1.2 Mecanismos de seguridad en los servicios de red.	✓ Propuesta de implementación de IDS/IPS. ✓ Participación de la implementación de VLAN. ✓ Identificación de servicios y puertos sospechosos. ✓ Realizar un registro de incidencias de caídas del servicio de internet corporativo.
AD07	A.5.1.1 Políticas para la seguridad de la información. A.12.2.1 Controles contra códigos maliciosos.	✓ Política integral, definido, aprobado y publicado. ✓ Registro de software autorizado. ✓ Registro de software no autorizado y listas negra de páginas web. ✓ Actualización del servidor antivirus.
AD12	A.9.1.1 Política de control de acceso. A.9.1.2 Control de acceso a redes y servicios asociados. A.9.2.5 Revisión de los derechos de acceso de usuarios. A.10.1.1 Política sobre el uso de controles criptográficos. A.13.1.3 Segregación en las redes. A.13.2.1 Políticas y procedimientos de intercambio de información.	✓ Desarrollo de política de control de acceso. ✓ Desarrollo de políticas para el uso de redes y servicios de red. ✓ Formato de revisión de los derechos de acceso de usuarios. ✓ Desarrollo de política sobre el uso de controles criptográficos ✓ Implementación de VLAN. ✓ Implementación de cifrado en redes inalámbricas. ✓ Desarrollo de políticas y procedimientos de intercambio de información.

Fuente: Elaboración propia

Cuadro 34. Implementación de controles de seguridad en Equipos Auxiliares.

AMENAZA	CONTROLES	DETALLE
AE08	A.11.2.4 Mantenimiento de equipos.	-Desarrollar un plan de mantenimiento. -Desarrollar un manual de procedimientos. -Realizar un registro de control de mantenimiento de hardware.
AE16	A.5.1.1 Políticas para la seguridad de la información. A.5.1.2 Revisión de las Políticas para seguridad de la información. A.18.1.1 Identificación de la legislación aplicable. A.18.2.2 Cumplimiento de las políticas y normas de seguridad.	-Política integral, definido, aprobado y publicado. -Definir y documentar todos los requisitos legales, regulatorios o contractuales. -Identificar legislación aplicable. -Realizar matriz de cumplimiento.
AE18	A.11.2.4 Mantenimiento de equipos.	-Realizar un plan de mantenimiento de equipos. -Realizar charlas informativas. -Realizar ordenamiento de fuentes de alimentación.

Fuente: Elaboración propia

VI. MATERIALES Y MÉTODOS

6.1 Tipo y diseño

Para la presente tesis se desarrolla una investigación del tipo Aplicada. De acuerdo con Baena (2014), la investigación aplicada, concentra su atención en las posibilidades concretas de llevar a la práctica las teorías generales y destinan sus esfuerzos a resolver las necesidades que se plantean la sociedad y los hombres. Esto se resume en investigar para actuar, modificar o producir cambios en una determinada realidad a través del tiempo (estudio longitudinal).

Con respecto a Hernández (2014), el diseño de la investigación indica al investigador lo que debe hacer para alcanzar sus objetivos de estudio, contestar las interrogantes que se ha planteado y analizar la certeza de la hipótesis formulada en un contexto particular. Los diseños cuasi-experimentales son semejantes a los experimentos “puros” y se encuentran en la sub división del método experimental, con la diferencia que los grupos no son equivalentes porque no hubo aleatorización ni emparejamiento puesto que los grupos ya están conformados antes del experimento.

Por lo tanto, el diseño de esta investigación es cuasi-experimental ya que se realizará mediciones al mismo grupo de estudio y como los datos recolectados serán realizados por el propio investigador la investigación tiene carácter prospectivo longitudinal.

6.2 Población y muestra

La población está representada por los Activos de información de la universidad, los mismos que se encuentran clasificados en 7 grupos: procesos institucionales, datos e información, sistemas y software, infraestructura de TI y hardware, equipamiento auxiliar, personal e infraestructura física. Por lo tanto, la población queda representada según los 07 grupos de activos los mismos que fueron agrupados en estratos: 03 procesos institucionales, 26 datos e información, 32 sistemas y software, 11 infraestructura de TI y hardware, 06 equipamiento auxiliar, 13 personal y 06 infraestructura física. Por lo tanto, se trabajará con la totalidad de la población y en ese sentido para esta tesis no existe muestra.

6.3 Métodos y técnicas de investigación

Métodos de investigación: Cuasi-experimental, porque se realiza la manipulación intencional de la variable independiente en un escenario controlado para ver el efecto en la variable dependiente bajo el control del investigador en la que no existe aleatoriedad.

Instrumentos de investigación: Los instrumentos de investigación cumplen un rol importante en la recolección de datos y se aplican según la naturaleza y características del problema y la intencionalidad del objetivo de la investigación, manifiesta Carrasco (2006). Para esta investigación se utiliza las entrevistas, fichas de observación, escalas, checklist.

Análisis estadístico: Para la validación de hipótesis se utilizará el análisis de la estadística no paramétrica.

VII. RESULTADOS

7.1 Implementación de controles

Se realizó la implementación de 24 controles de un total de 144 que sugiere la norma ISO/IEC 27002:2013 las mismas que se detallan en el Cuadro 35. En las siguientes secciones del capítulo se van detallando cada uno de los resultados alcanzados en función a la implementación de cada control.

Cuadro 35. Resultado de controles implementados.

Nº	CONTROLES IMPLEMENTADOS	TIPO DE CONTROL
1	A.5.1.1 Políticas para la seguridad de la información.	Estratégico
2	A.5.1.2 Revisión de las Políticas para seguridad de la información.	Estratégico
3	A.6.2.1 Política para dispositivos móviles. *	Estratégico
4	A.7.2.2 Concienciación, educación y capacitación de la seguridad de la información.	Operativo
5	A.9.1.1 Política de control de acceso	Estratégico
6	A.9.1.2 Control de acceso a redes y servicios asociados.	Estratégico
7	A.9.2.5 Revisión de los derechos de acceso de usuarios.	Estratégico
8	A.10.1.1 Política sobre el uso de controles criptográficos.	Operativo
9	A.11.2.4 Mantenimiento de equipos.	Operativo
10	A.11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. *	Operativo
11	A.12.1.1 Documentación de procedimientos de operación.	Operativo
12	A.12.2.1 Controles contra códigos maliciosos.	Operativo
13	A.12.5.1 Instalación de software en sistemas en producción.	Operativo
14	A.12.6.1 Gestión de las vulnerabilidades técnicas.	Operativo
15	A.12.6.2 Restricciones en la instalación de software.	Operativo
16	A.13.1.1 Controles de red.	Operativo
17	A.13.1.2 Mecanismos de seguridad en los servicios de red.	Operativo
18	A.13.1.3 Segregación en las redes.	Operativo
19	A.13.2.1 Políticas y procedimientos de intercambio de información.	Operativo
20	A.14.2.1 Política de desarrollo seguro.	Operativo
21	A.16.1.3 Notificación de puntos débiles de la seguridad de la información.	Operativo
22	A.18.1.1 Identificación de la legislación aplicable.	Estratégico
23	A.18.1.2 Derechos de propiedad intelectual (DPI).	Estratégico
24	A.18.2.2 Cumplimiento de las políticas y normas de seguridad.	Estratégico

Fuente: Elaboración propia

*Controles no definidos de acuerdo con el análisis de riesgos sino por criterio del investigador

Los controles de tipo estratégico son 9 y los controles de tipo operativo son 15 tal como se aprecia como resumen en la Figura 15.

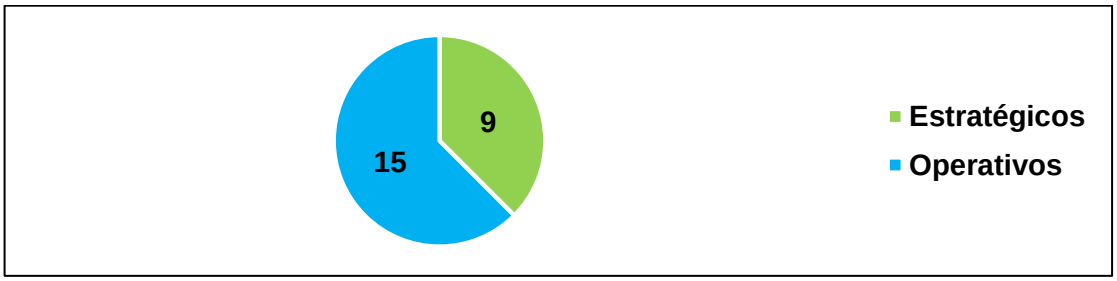


Figura 15. Resultado de controles implementados
Fuente: Elaboración propia

7.2 Nivel de implementación de controles

Inicialmente, en la etapa de diagnóstico se pudo evidenciar que, el nivel de implementación de controles estaba representado por el 12% de controles estratégicos y el 16% de controles operativos. Posterior a la implementación de controles de la ISO/IEC 27002:2013 se tiene como resultado un incremento respecto a los resultados iniciales. El nivel de implementación actual es de 14% que representa a controles estratégicos y un 20% a controles operativos.

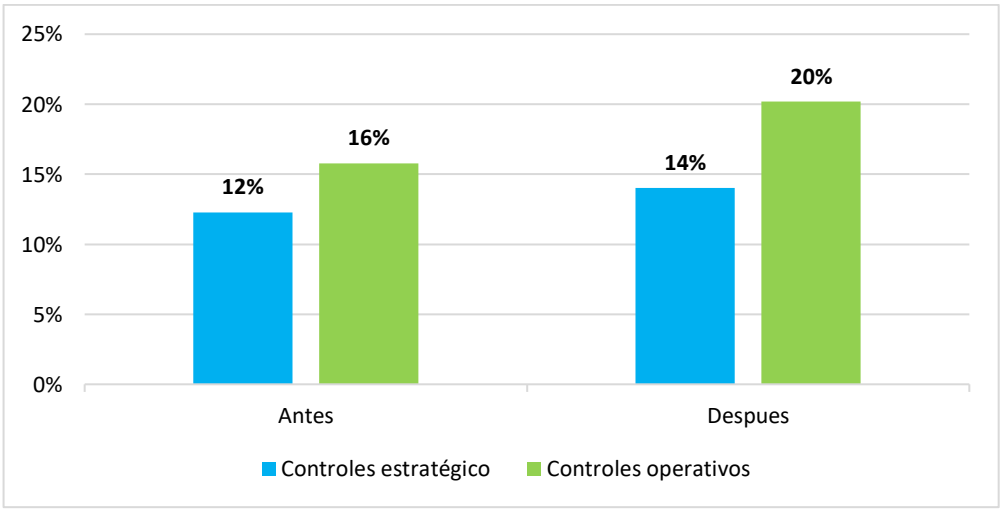


Figura 16. Resultado de controles ISO/IEC27002:2013 implementados
Fuente: Elaboración propia

7.3 Resultado del modelo de madurez de controles ISO/IEC 27002:2013

Como resultado del modelo de madurez de capacidades CMM de los controles de la ISO/IEC 27002, se puede observar que el 15% representa a los controles que se encuentran en un nivel de madurez Inicial, 51% de los controles tienen un nivel de madurez Repetible, el 26% un nivel de madurez Definido, solo 8% representan controles con un nivel de madurez Gestionado y por último en el nivel de madurez Optimizado se tiene 0%.

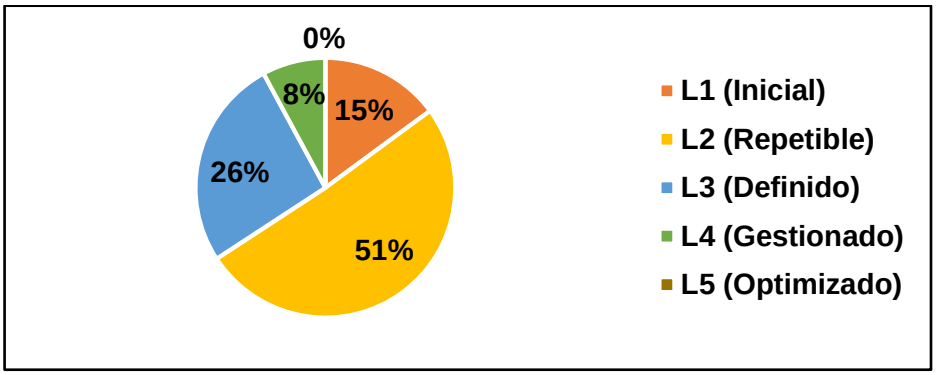


Figura 17. Nivel de madurez de controles post implementación de controles
Fuente: Elaboración propia

7.4 Resultado del modelo de madurez según tipo de seguridad

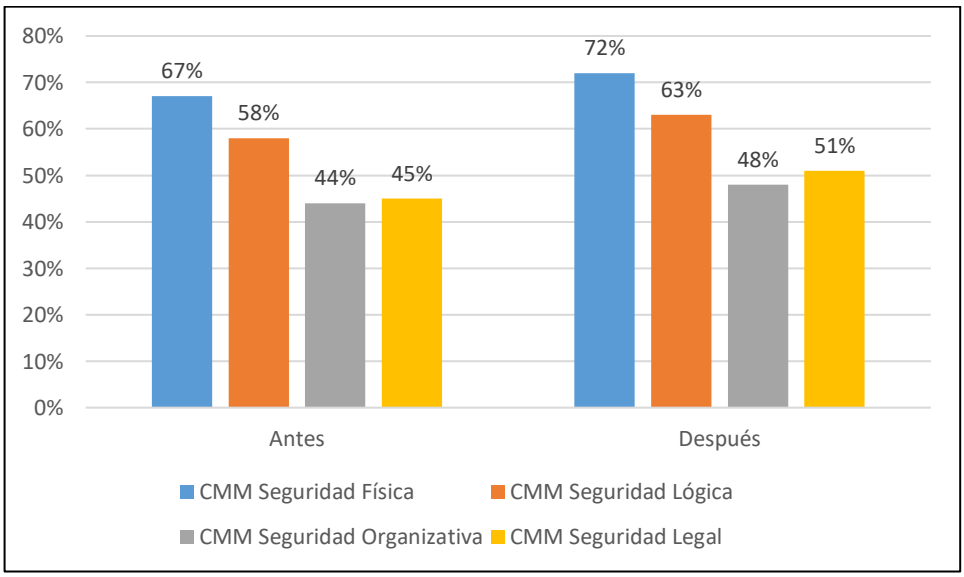


Figura 18. Nivel de madurez según el tipo de seguridad
Fuente: Elaboración propia

7.5 Nivel de riesgo de desastres naturales

La siguiente figura muestra el umbral de riesgo en la que se encuentran los activos de información respecto a las amenazas que tienen como origen los desastres naturales.

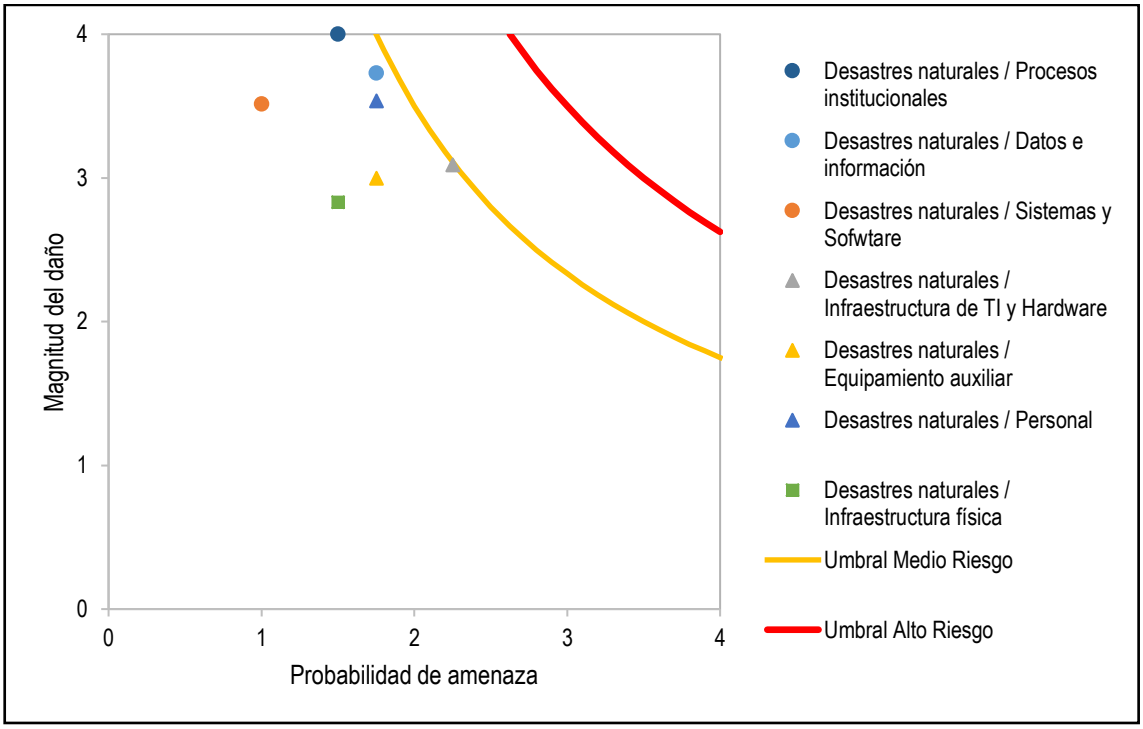


Figura 19. Resultado del nivel de riesgo - Desastres Naturales
Fuente: Elaboración propia

En efecto, en la Figura 19 se observa el resultado del nivel de riesgos en el que se encuentran los activos. Se tiene a los activos de información ubicados debajo del umbral que representa el riesgo medio, sobre el umbral de riesgo medio no se aprecia a ningún activo, de igual modo no hay activos de información situados sobre el umbral de riesgo alto.

7.6 Nivel de riesgo de origen industrial

En la Figura 20 se puede apreciar que existen cinco grupos de activos los cuales se encuentran sobre el umbral de riesgo medio, entre ellos se tiene a Procesos Institucionales, Datos e Información, Sistemas y Software, Infraestructura de TI y Hardware y por último se tiene a Equipamiento Auxiliar.

En otro escenario se tiene a dos grupos de activos que están bajo el umbral del riesgo medio, esto representa que activos como Persona e Infraestructura Física tienen un riesgo bajo.

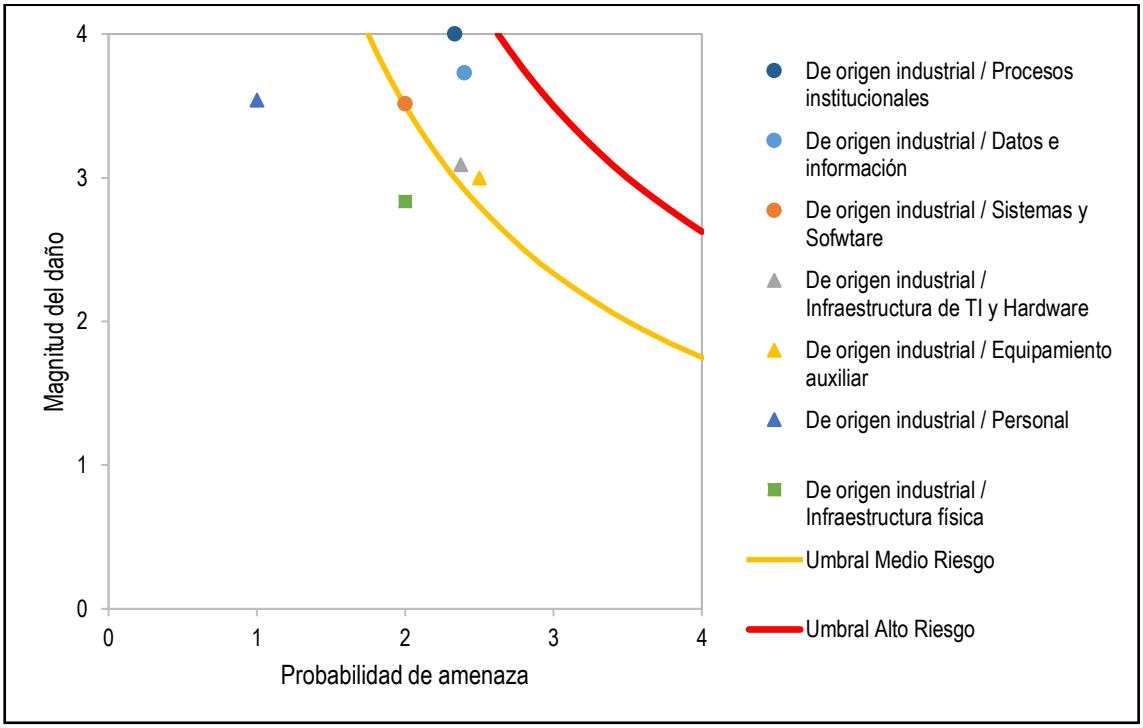


Figura 20. Resultado del nivel de riesgo - Origen Industrial
Fuente: Elaboración propia

7.7 Nivel de riesgo de errores y fallos

En la Figura 21 se puede apreciar que existen también cinco grupos de activos los cuales se encuentran sobre el umbral de riesgo medio, entre ellos se encuentran los Procesos Institucionales, Datos e Información, Sistemas y Software, Infraestructura de TI y Hardware y por último se tiene a Equipamiento Auxiliar. Aunque en este escenario, se puede apreciar que la tendencia es acercarse más hacia el umbral de riesgo alto, por lo que se debe poner énfasis en las amenazas cuyo origen son Errores y Fallos.

En el caso de activos como Infraestructura de TI y Hardware aun encontrándose por debajo del umbral de riesgo medio, se aprecia que está muy próximo a alcanzar dicho umbral, por otro lado, activos como Infraestructura Física se encuentra distante y por debajo del umbral de riesgo medio.

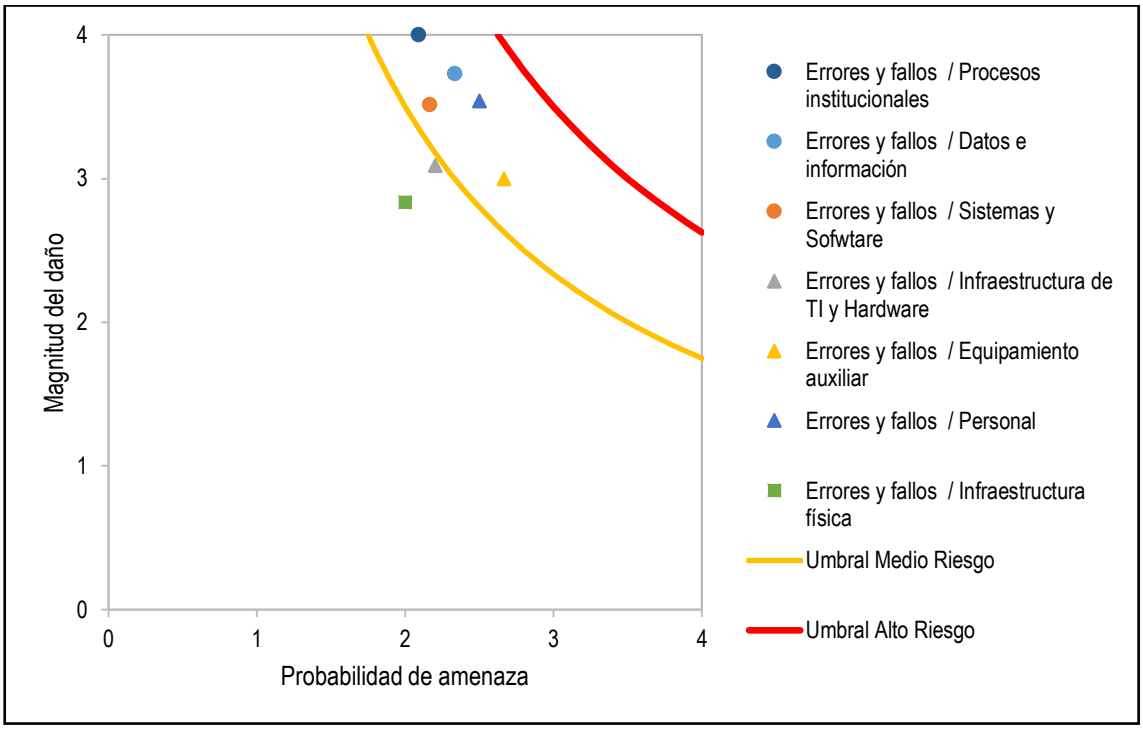


Figura 21. Resultado del nivel de riesgo - Errores y Fallos
Fuente: Elaboración propia

7.8 Nivel de riesgo de ataques deliberados

En este último escenario se puede observar en la Figura 22 que activos como Infraestructura de TI y Hardware, Equipamiento Auxiliar e Infraestructura Física aun estando debajo del umbral de riesgo medio, están muy próximos a alcanzar dicho umbral, por lo que se tiene que poner énfasis en estos activos. Por otro lado, activos como Procesos Institucionales y Personal están sobre el umbral medio y muy próximo a ello, lo que indica que el riesgo que representan puede ser asumido o tratado a mediano plazo.

Por último, en el caso de activos como Datos e Información y Sistemas y Software están sobre el umbral medio y un poco distante, esto indica que los riesgos tienen que ser tratados antes que pueda alcanzar un riesgo alto y pueda ser crítico para la institución.

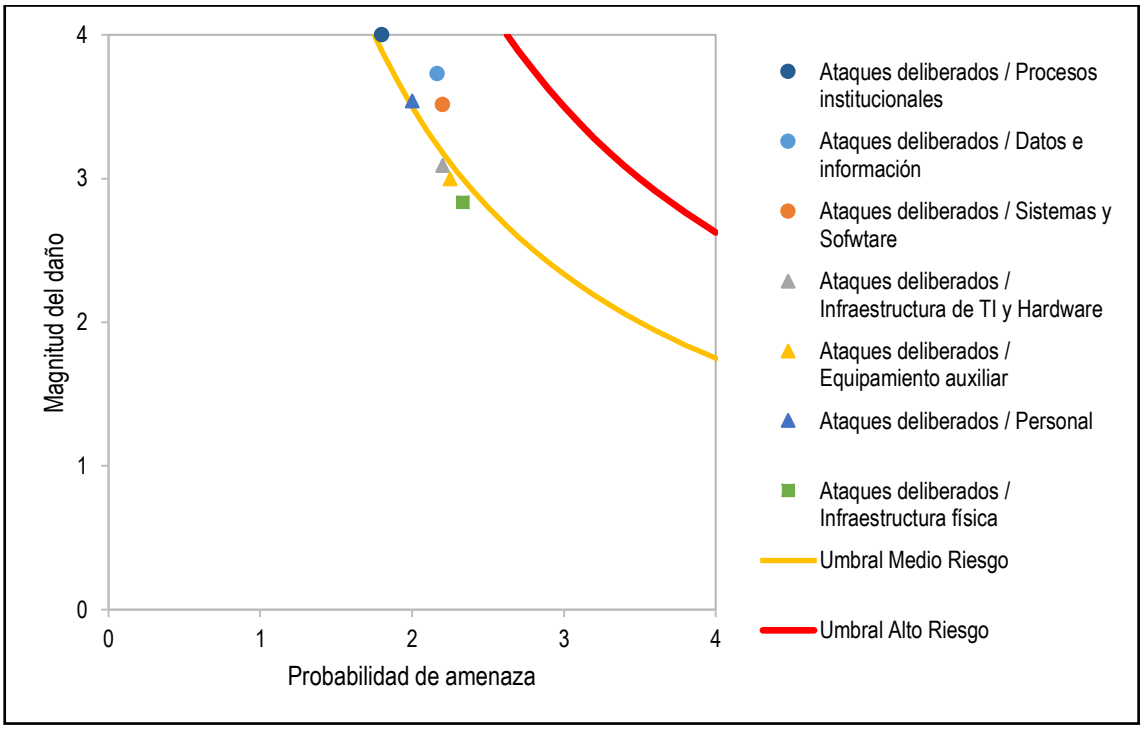


Figura 22. Resultado del nivel de riesgo - Ataques Deliberados
Fuente: Elaboración propia

7.9 Resultado global del nivel de riesgo

Finalmente se puede apreciar el nivel de riesgo en términos cuantitativos, para los siete grupos de activos y cuatro grupos de amenazas que se han definido en capítulos anteriores. En la Figura 23 se puede observar la valoración de riesgo promedio existe y el color que representa el tipo de riesgo en el caso de riesgo bajo se traduce al color verde, para el caso de riesgo medio el color que lo representa es el amarillo y para el riesgo alto el color utilizado es el rojo. Aunque para el resultado final se observa que solo existe riesgo bajo y medio.

NIVEL DE RIESGO		Probabilidad			
		[AN]	[AI]	[AE]	[AD]
Magnitud de Daño	Procesos institucionales	6,00	9,33	8,36	7,20
	Datos e información	6,53	8,95	8,71	8,08
	Sistemas y Software	3,52	7,03	7,62	7,73
	Infraestructura de TI y Hardware	6,95	7,34	6,80	6,80
	Equipamiento auxiliar	5,25	7,50	8,00	6,75
	Personal	6,19	2,56	8,85	7,08
	Infraestructura física	4,25	5,67	5,67	6,61

Figura 23. Resultado global del nivel de riesgo.
Fuente: Elaboración propia

7.10 Resultado del nivel de madurez de la norma ISO/IEC 27002:2013

El nivel de madurez se realizó sobre los 14 dominios de la norma ISO/IEC 27002:2013, evaluando a los 114 controles bajo el modelo de madurez de capacidad CMM que permite dar cuenta del progreso de implementación de controles en el contexto de la seguridad de la información.

Los resultados presentados en la Figura 24 son una visión general del estado actual de la gestión de la información respecto a la aplicación de la norma ISO /IEC 27002:2013, como se observa el estado actual aun difiere del estado deseado, pero del mismo modo se puede observar una mejora positiva en comparación con el diagnóstico situacional realizado en un primer instante.

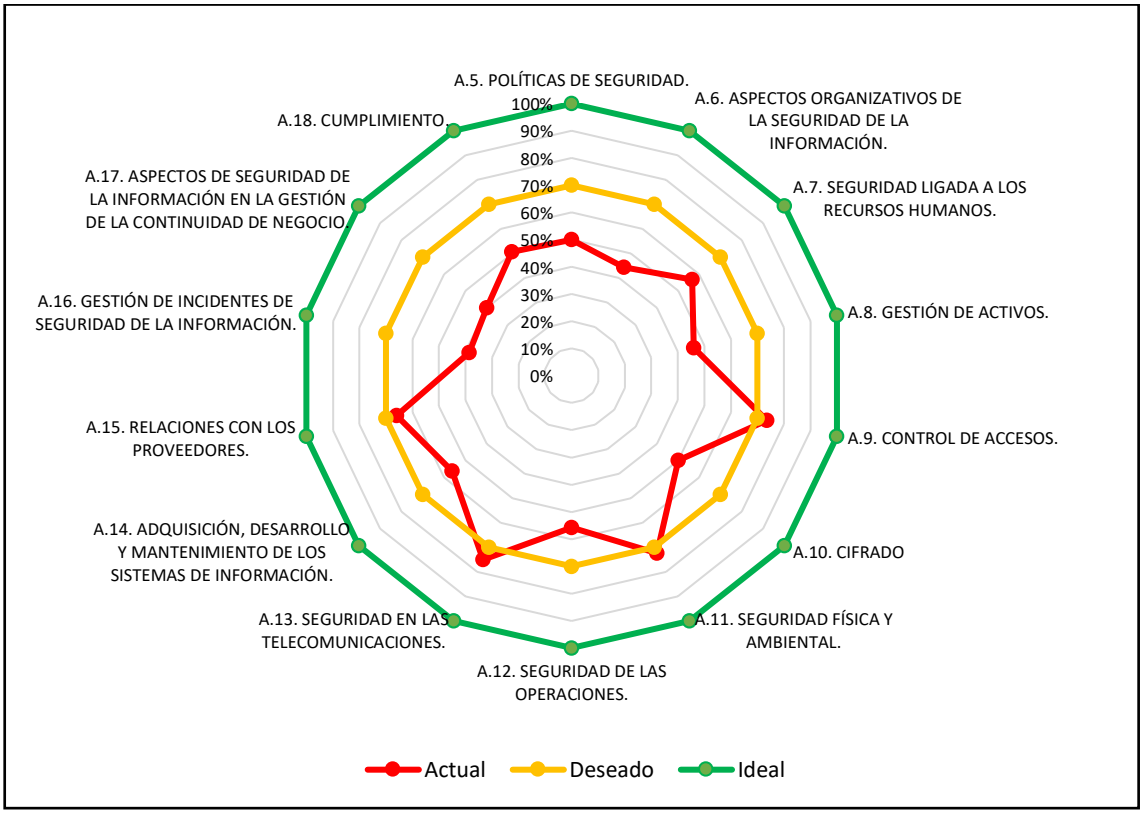


Figura 24. Resultado del nivel de madurez de la norma ISO/IEC 27002:2013
Fuente: Elaboración propia

7.11 Resultados de indicadores

A continuación, se presenta en el Cuadro 36 el resumen del cálculo de los 10 indicadores de la variable dependiente (VD) que sirven como datos para realizar la prueba de hipótesis, cabe mencionar que los datos que se muestran son los resultados de las secciones anteriores.

Cuadro 36. Resumen de indicadores.

INDICADORES	ANTES	DESPUÉS
I1: Capacidad de respuesta a incidentes.	Alta	Alta
I2: Costos de recuperación de incidentes respecto al presupuesto	Alto	Alto
I3: Tiempo de recuperación de un incidente	Medio	Medio
I4: Nivel de riesgo en procesos institucionales	8.18	7.72
I5: Nivel de riesgo en datos e información	8.69	8.07
I6: Nivel de riesgo en sistemas y software	8.36	6.47
I7: Nivel de riesgo infraestructura de TI y hardware	7.59	6.97
I8: Nivel de riesgo en equipamiento auxiliar	7.63	6.88
I9: Nivel de riesgo en personal	6.54	6.17
I10: Nivel de riesgo en Infraestructura física	6.49	5.55

Fuente: Elaboración propia

Los indicadores detallados en el Cuadro 36, son los datos por ingresar al programa estadístico SPSS para determinar mediante la aplicación de una prueba estadística no paramétrica los resultados obtenidos antes y después de la implementación de los controles de seguridad.

7.12 Validación de hipótesis

Para la validación de la hipótesis se realizará cinco procedimientos que describe Supo (2014): plantear el sistema de hipótesis, establecer el nivel

de significancia, elegir el estadístico de prueba, dar lectura del p-valor calculado y por último tomar una decisión estadística.

De esta manera se empieza planteando el sistema de hipótesis, que consiste en trasladar la estructura gramatical, lógica y científica hacia la estructura matemática la cual tiene dos versiones: la primera, la hipótesis nula a la que se denota como H_0 y la segunda, la hipótesis alterna que se denota por H_1, por lo tanto, el sistema de hipótesis queda determinado de la siguiente manera:

H_0: Si se implementa controles de seguridad de la información de la Norma ISO/IEC 27002:2013 entonces no existe una mejora de al menos un 5% en la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva.

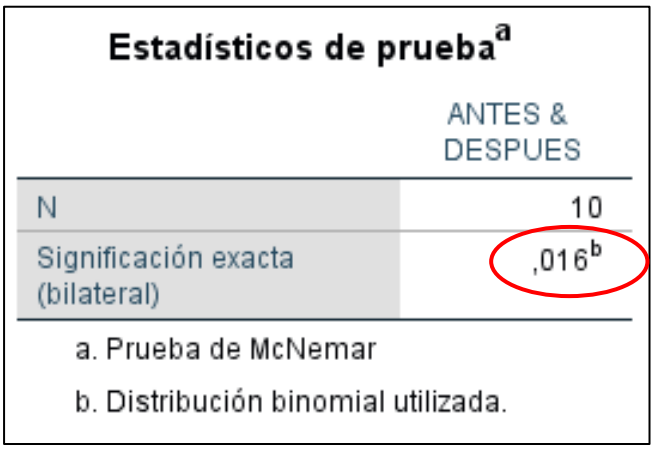
H_1: Si se implementa controles de seguridad de la información de la Norma ISO/IEC 27002:2013 entonces existe una mejora de al menos un 5% en la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva.

Ahora como segundo paso, se debe establecer el nivel de significancia, que viene a ser el valor máximo de error que el investigador está dispuesto a aceptar para dar por válida la hipótesis del investigador. Por lo tanto, se establece el valor convencional para el nivel de significancia que es 5%.

En el tercer paso, se realiza la elección del estadístico de prueba, para lo cual se tomará en cuenta seis criterios: tipo de estudio, nivel investigativo, diseño de la investigación, objetivo estadístico, escalas de medición de las

variables y comportamiento de los datos. Por consiguiente, los criterios mencionados anteriormente quedan determinados de la siguiente manera: el tipo de estudio es longitudinal, el nivel investigativo es aplicativo, el diseño de la investigación tiene carácter prospectivo longitudinal, el objetivo estadístico es comparar, la escala de medición de variables es nominal y el comportamiento de los datos son categóricos. En consecuencia, el estadístico de prueba a elegir es el estadístico no paramétrico de McNemar.

El paso cuatro es cuantificar el p-valor, para ello se utilizó el programa estadístico SPSS, de modo que si el p-valor es menor al nivel de significancia, rechazamos la hipótesis nula y concluimos que la hipótesis alterna es verdadera. Por el contrario, si el p-valor es mayor al nivel de significancia, no se puede rechazar la hipótesis nula.



Estadísticos de prueba[a]

	ANTES & DESPUES
N	10
Significación exacta (bilateral)	,016[b]

a. Prueba de McNemar

b. Distribución binomial utilizada.

Figura 25. Prueba estadística de McNemar
Fuente: SPSS Statistic trial version

En consecuencia, después del procesamiento de los datos, el cálculo que nos arroja el programa estadístico del p-valor es 0.016. Para apreciar a más detalle se recomienda revisar el Anexo 4.

Finalmente, el último paso corresponde a la toma de decisiones por lo que se tendrá que decidir con cuál de las hipótesis planteadas nos vamos a quedar, entonces como el p-valor tiene un valor de 0.016 y se encuentra por debajo del nivel de significancia 0.05 (p-valor < nivel de significancia) se rechaza la hipótesis nula H_0 y aceptamos la hipótesis alterna H_1.

Interpretación

Se puede afirmar con un 95% de confianza que, si se implementa controles de seguridad de la información de la Norma ISO/IEC 27002:2013 entonces existe una mejora positiva de al menos un 5% en la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva.

VIII. DISCUSIÓN

A partir de los resultados obtenidos, se acepta la hipótesis alterna general la cual establece que, si se implementa controles de seguridad de la información de la Norma ISO/IEC 27002:2013 entonces existe una mejora positiva de al menos un 5% en la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva. Estos resultados guardan relación con lo que sostiene Areitio (2008) quien señala que para mejorar la gestión de la seguridad de la información es necesario implementar controles de seguridad pudiendo ser de nivel organizativo, físico, lógico o legal que permiten proteger los activos, reducir riesgos y facilitar la recuperación de incidentes en una organización.

Gómez y Andrés (2012) afirman que la norma ISO/IEC 27002 establece las directrices y principios generales para el inicio, implementación, mantenimiento y mejora de la gestión de la seguridad de la información en una organización. Por ello la elección de los controles de seguridad está sujeto a los resultados del análisis de riesgos previo y el grado de implementación de cada uno de los controles de la norma.

En la universidad inicialmente el nivel de implementación de controles estratégicos era del 12% y para el caso de controles operativos el nivel de implementación inicial era del 16%. Posterior a la implementación de controles de seguridad según la Norma ISO/IEC 27002:2013 el nivel de

implementación existente para el caso de controles estratégicos es de 14% y para controles operativos se tiene un 20% de implementación tal como se detalla en la Figura 16.

En cuanto al indicador capacidad de respuesta a incidentes antes de la implementación de controles inicialmente era alta cuya representación en porcentajes es del 77% de atención en promedio, de todos los incidentes reportados y se mantuvo del mismo modo aun con la implementación de controles, esto se debe a que el personal con que se cuenta en la oficina a cargo de gestionar las tecnologías de la información y comunicación (CTIC) aunque no son suficientes para atender estos requerimientos en un plazo tan corto son eficaces al desarrollar sus actividades, ya que cada personal cumple con múltiples tareas técnicas y administrativas.

Con respecto al indicador costos de recuperación de incidentes respecto al presupuesto, el resultado es que los costos de recuperación son altos, debido a que en la actualidad la universidad no dispone de presupuesto destinado para la recuperación de incidentes de seguridad de la información, por lo que cualquier incidente que demande recursos financieros, es considerado como un costo alto de asumir, a modo de ejemplo se puede plantear que al no existir políticas internas para el uso de software legal, la universidad podría ser multada hasta con 180 UIT según el Decreto Legislativo N° 822 (Ley de Derechos de Autor).

Para el caso de del indicador de tiempo de recuperación de incidentes, el resultado también no presento variación, puesto que en la medición previa a la implementación de controles el resultado del tiempo de recuperación

de un incidente fue medio en su representación numérica era de 2 horas y media en promedio y se mantuvo de la misma manera después de la implementación.

En otro sentido, el nivel de cumplimiento de controles de la ISO/IEC 27002:2013 se ha incrementado positivamente pasando de un 28% a un 34% tal como se aprecia en la Figura 26, ello indica que aún se tiene pendiente trabajar en controles que ayuden a proteger a los activos de información y minimizar los riesgos, ya que un estado ideal sería tener un nivel de cumplimiento del 70% de la norma, esto dependerá también de los requisitos y los recursos disponibles de la organización.

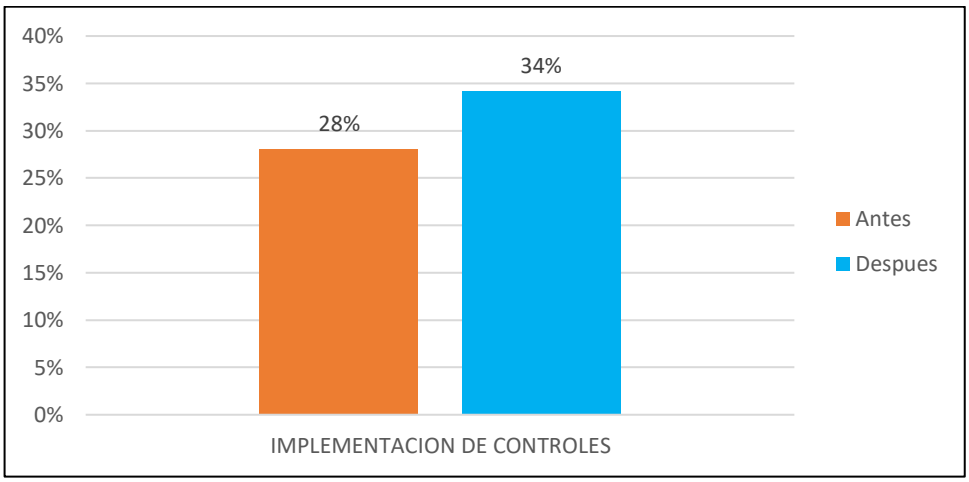


Figura 26. Nivel de cumplimiento de controles (Antes - Después)
Fuente: Elaboración propia

Entrando a más detalle se analizaron indicadores como el nivel de madurez de capacidades CMM en cuanto a seguridad física, lógica, organizativa y legal, los mismos que tuvieron un incremento de 5%, 5%, 4% y 6% respectivamente en el nivel de madurez, tal como se aprecia en la Figura 27.

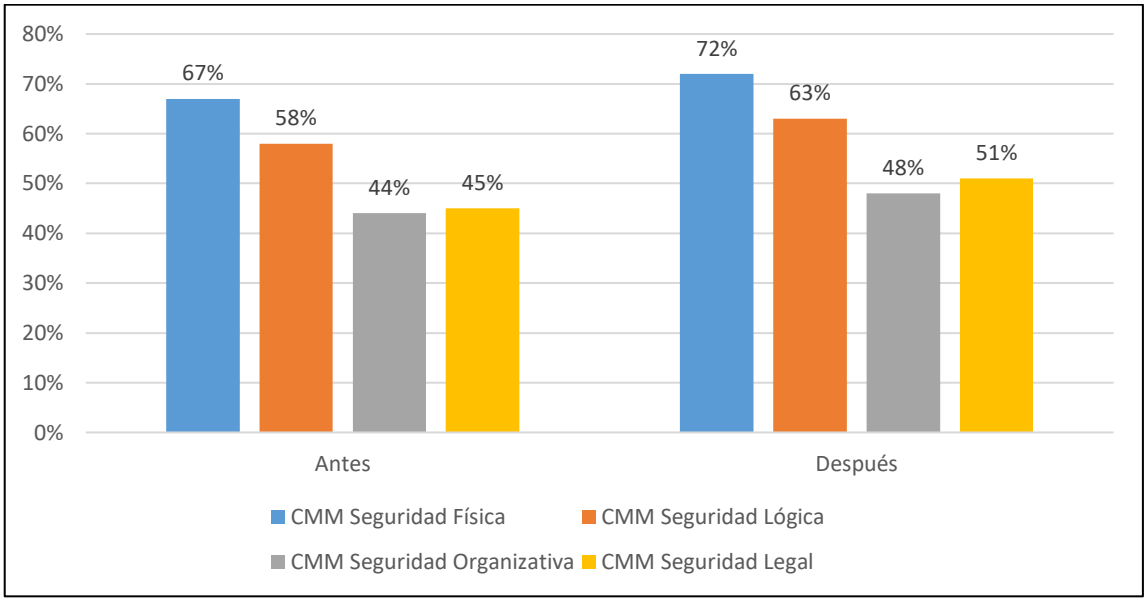


Figura 27. Nivel de madurez de capacidades CMM según tipo de seguridad (Antes - Después)
Fuente: Elaboración propia

Tal como manifiesta Corletti (2011), la implementación de controles de seguridad permite cubrir aquellos aspectos valorados en el análisis de riesgos es decir los riesgos identificados con un valor alto pueden ser minimizados con la aplicación de controles que implican medidas técnicas, procedimientos, documentos, etc.

Dentro de los resultados de la tesis el nivel de riesgo en los activos como procesos institucionales y datos e información no tuvieron variación ya que se conservó como resultado el nivel de riesgo medio. De modo similar para el caso de activos como personal e infraestructura física el nivel de riesgo inicialmente era bajo y se mantuvo del mismo modo en el análisis posterior a la implementación de controles de la norma ISO/IEC27002:2013.

Para activos como equipamiento auxiliar, sistemas y software y por último infraestructura de TI y software el nivel promedio de riesgo si presento variación, pasando de riesgo medio a riesgo bajo en todos los casos.

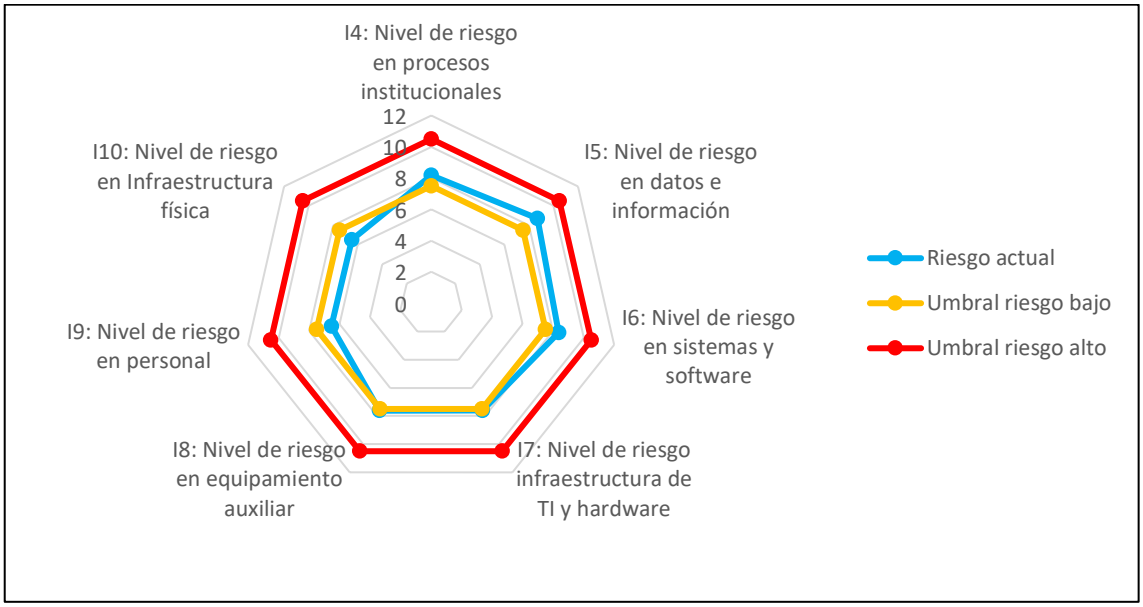


Figura 28. Nivel de riesgo de activos (Antes)
Fuente: Elaboración propia

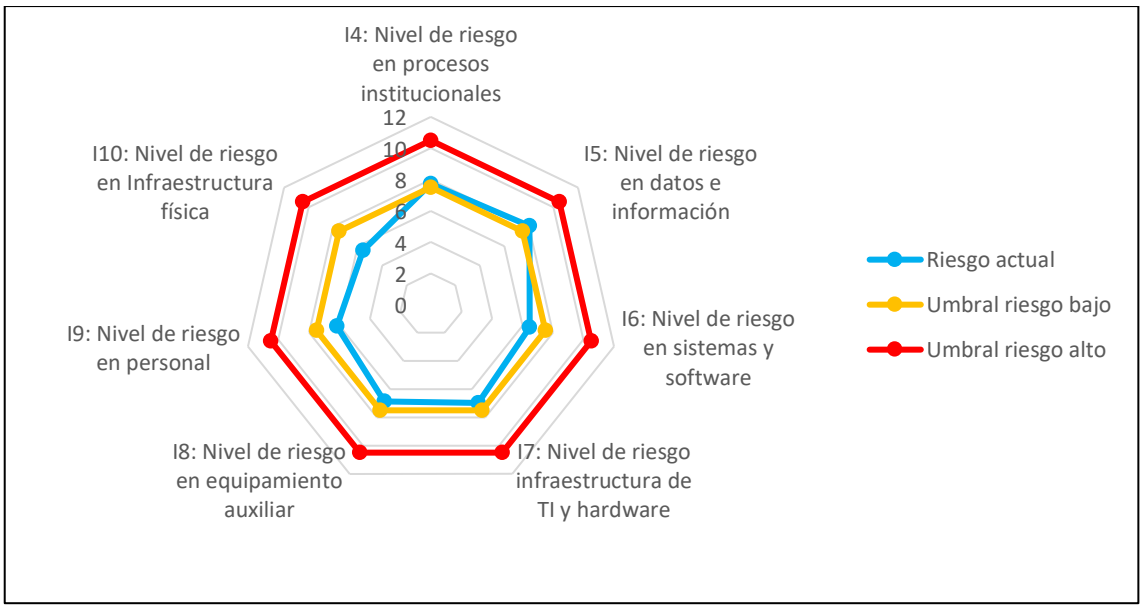


Figura 29. Nivel de riesgo de activos (Después)
Fuente: Elaboración propia

Finalmente se realizó la evaluación del modelo de madurez de capacidades CMM de los 14 dominios, 35 objetivos de control y 114 controles que presenta la norma ISO/IEC 27002:2013 en la que se pudo evidenciar un incremento positivo en la madurez del Dominio A.5, A.6, A.7, A.10 y A.12.

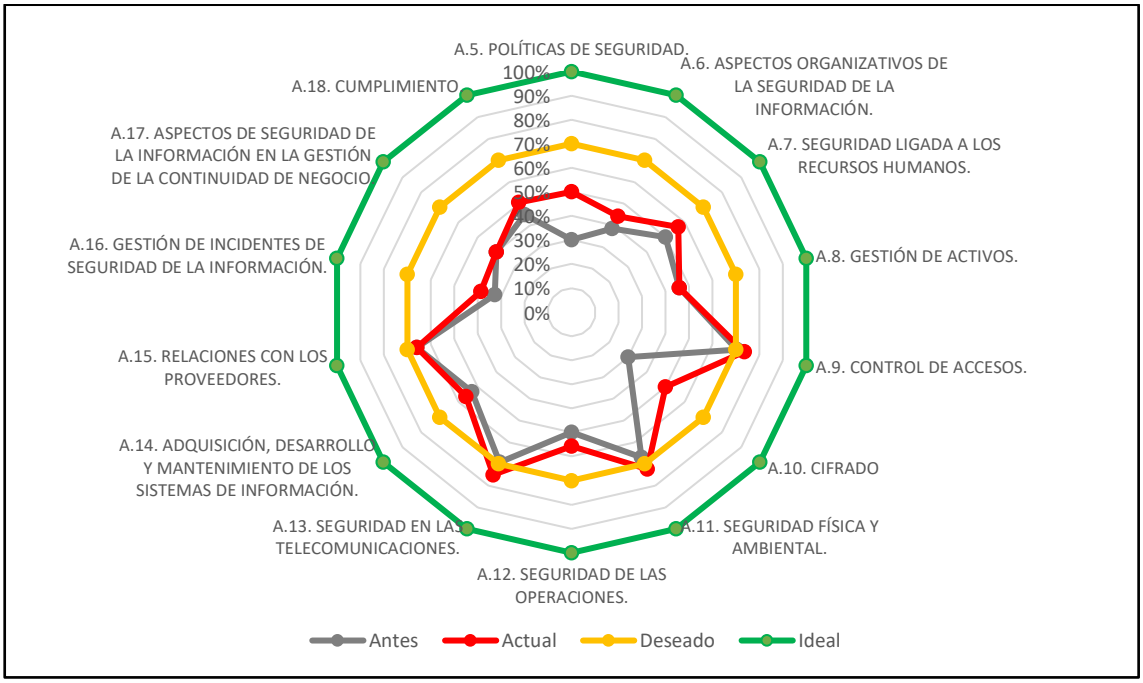


Figura 30. Modelo de madurez de ISO/IEC 27002:2013 (Antes - Después)
Fuente: Elaboración propia

Las indicaciones que la norma ISO/IEC 27002 proporciona son bastantes exhaustivas, por lo que resultan muy útiles, pero no son obligatorias. El grado de implementación de cada uno de los controles es algo que la organización debe decidir en función de sus necesidades y sus recursos disponibles y por supuesto el modo en que se implementen es de competencia exclusiva de la organización, manifiestan Gómez y Andrés (2012)

Cuadro 37. Resumen de discusión de resultados con los antecedentes.

Antecedentes	Resultados de los antecedentes	Resultados de la tesis
Aguirre Mollehuanca, DA. 2014	• Identificación de activos. • Identificación y evaluación de riesgos. • Definición del alcance y políticas del Sistema de Gestión de la Seguridad de la Información. • Identificación de procesos del negocio • Análisis y tratamiento de riesgos • Desarrollo del Sistema de Gestión de la Seguridad de la Información. • Declaración de aplicabilidad. • Políticas base para el SGSI	• Diagnostico situacional (Nivel de madurez de los dominios de control de la norma ISO 27002:2013). • Identificación y clasificación de activos primarios y secundarios. • Identificación y clasificación de amenazas. • Estimación del riesgo utilizando la metodología MAGERIT. • Informe de evaluación de riesgos • Declaración de aplicabilidad (SOA) • Resultado post implementación del del nivel de madurez de los dominios de control de la norma ISO 27002:2013Plan de gestión de riesgos. • Políticas generales. • Políticas de control de acceso. • Política para el uso de controles criptográficos. • Manual de procedimientos para el buen uso de TI • Formato de inventario de sistemas y software. • Plan de capacitación y sensibilización. • Revisión de políticas. • Prueba y validación de hipótesis.
Ampuero Chang, CE. 2011		
Lamilla Rubio, E. 2009	• Implementación de políticas de seguridad. • Valoración de activos. • Identificación, análisis y evaluación de vulnerabilidades. • Plan de tratamiento de riesgosos.	

Fuente: Elaboración propia

Como se aprecia en el Cuadro 37, los resultados poseen mucha relación con los antecedentes revisados, a modo de síntesis se concluye que para la implementación de controles es necesario realizar la identificación de activos, identificación y valoración de amenazas, gestión de riesgos, elaborar el documento de la declaración de aplicabilidad (SOA) y el plan de implementación de los controles seleccionados.

En efecto, el desarrollo de la tesis ha seguido en detalle todos los procedimientos recomendados por expertos en tema y la extensa bibliografía consultada, de modo que, se inició analizando el estado de la seguridad de la información en la universidad, utilizando los 14 dominios que sugiere la norma

ISO/IEC27002:2013, lo que dio un panorama inicial para luego utilizando la metodología de Análisis y Gestión de Riesgos (MAGERIT) obtener como producto final una matriz de riesgos que además genera gráficos que muestran el nivel de riesgo asociados a los activos, documento que debe ir actualizándose en el tiempo. Por otro lado, se generó un catálogo de amenazas más recurrentes en la universidad, que también es otro documento que tiene que ir actualizándose. Es preciso resaltar que también se tiene como producto documentos como la Declaración de Aplicabilidad (SOA), políticas, plan de tratamiento de riesgos, procedimientos de operación para la gestión de TI, requisitos estatutarios y otros documentos que se mencionan en el Cuadro 37 y que todos ellos se encuentran alineados a los requerimientos que plantea la ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información, que es el objetivo a futuro de la UNAS.

En efecto, la presente tesis ha tenido que contrastar mediante una prueba de hipótesis la mejora que representa la seguridad de la información en una organización al implementar controles de seguridad según la Norma ISO/IEC 27002:2013 ya que constituye un marco para diseñar y operar un Sistema de Gestión de Seguridad de la Información basado en experiencias.

CONCLUSIONES

1. Se puede afirmar con un 95% del nivel de confianza que la implementación de controles de seguridad según la norma ISO/IEC 27002:2013 permite mejorar la gestión de seguridad de la información en la Universidad Nacional Agraria de la Selva. En resumen, la implementación de controles estratégicos pasó de un 12% inicial a un 14%, los controles operativos de un 16% a un 20%, por lo tanto, se aprecia de modo global un incremento de 28% a un 34% que representa en síntesis un incremento en un 6% en la implementación de controles. Este incremento se ve reflejado en el nivel de riesgo promedio de los activos de información que se obtienen de los indicadores de eficacia (del I4 al I10) que pasaron de 7.64 a un 6.83, esto se interpreta que actualmente la eficacia de la gestión de la seguridad de la información en la universidad es medio. Los indicadores I1, I2 e I3 no presentan variación por lo que la eficiencia de la gestión de la seguridad de la información sigue siendo medio. Sin embargo, hay que tener en cuenta que la clasificación de los activos de información, el análisis de riesgos y elección de los controles puede ir variando en función a la complejidad la institución a través del tiempo, de modo que, según los datos expuestos se puede concluir que la eficiencia y la eficacia de la gestión de la seguridad de la información en la universidad es medio, aún después de la implementación de los controles de seguridad de la Norma ISO/IEC 27002:2013.

2. El análisis de riesgos es la base fundamental para tomar acciones que permitan mejorar la gestión de la seguridad de la información, en definitiva, la metodología MAGERIT permitió identificar y clasificar en 07 grupos los activos de información: Procesos institucionales, Datos e Información, Sistemas y Software, Infraestructura de TI y Hardware, Equipamiento Auxiliar, Personal e Infraestructura Física; de igual modo valorar las amenazas según el origen: 04 de origen Natural, 12 de Industrial, 20 de Errores y Fallos y por último 21 de Ataques deliberados, para finalmente calcular el riesgo promedio total, cuyo valor es 6.83 el cual representa un riesgo medio y a partir de ello definir los 24 controles que se implementaron para gestionar el riesgo.

3. Determinar las vulnerabilidades de los activos de información permite conocer las debilidades que pueden ser explotadas por las amenazas identificadas, entre las vulnerabilidades más comunes que se identificaron está la ausencia de políticas y procedimientos de seguridad, para el caso sistemas y software una de las vulnerabilidades que más resalta es que los sistemas web transmiten información sin cifrar lo que representa alto riesgo que esa información sea interceptada fácilmente, otra de las vulnerabilidades más representativas es la falta de concienciación y capacitación al personal en temas de seguridad de la información, inexistencia de registros de acceso a áreas restringidas, ausencia de un plan de mantenimiento de la infraestructura de TI y hardware, uso de sistemas operativos obsoletos en los servidores (Windows Server 2008 R2) y los equipos de usuario final (Windows XP y Windows 7) y sistemas de gestión administrativa como es el caso del Módulo Administrativo, uno de los motivos es la ausencia de presupuesto para la compra de licencias.

En ese contexto se identificaron las vulnerabilidades con la aplicación de la metodología PDCA y la NTP-ISO/IEC 27005, de igual modo se utilizaron herramientas de pruebas de intrusión entre los más resaltantes se tiene a Nessus, Nmap, WireShark, Metasploit, Foca y Airckack), ver Anexo 10.

4. Se realizó la definición e implementación de 24 controles de seguridad de un total de 114 que plantea norma ISO/IEC 27002:2013, entre los controles implementados se tiene 9 controles estratégicos (A.5.1.1, A.5.1.2, A.6.2.1, A.9.1.1, A.9.1.2, A.9.2.5, A.18.1.1, A.18.1.2, A.18.2.2) y 15 controles operativos (A.7.2.2, A.10.1.1, A.11.2.4, A.11.2.9, A.12.1.1, A.12.2.1, A.12.5.1, A.12.6.1, A.12.6.2, A.13.1.1, A.13.1.2, A.13.1.3, A.13.2.1, A.14.2.1, A.16.1.3), con esto se puede evidenciar un incremento en el nivel de implementación de la norma puesto que pasamos de un 28% a un 34%, en consecuencia, también se consiguió reducir el riesgo promedio de los activos de un 7.64 a 6.83. Asimismo, el nivel de madurez controles en seguridad física y en seguridad lógica aumento un 5%, en controles de seguridad organizativa se incrementó un 4% y en seguridad legal el incremento fue de un 6%. Además, se consiguió elaborar los documentos base que serán utilizados en la implementación de la NTP-ISO/IEC 27001:2014, entre los que se puede mencionar son a las Políticas de Seguridad de la Información, Matriz de Riesgos, Declaración de aplicabilidad, Procedimientos para la Operación y Gestión de TI. En efecto la seguridad de la información viene siendo un factor crítico dentro de las instituciones, por lo tanto, deben establecerse continuamente requisitos que garanticen la seguridad de los activos.

RECOMENDACIONES

Es necesario implementar un Sistema de Gestión de Seguridad de la Información siguiendo las especificaciones de la NTP-ISO/IEC 27001 que mediante la resolución ministerial Nº 129-2012-PCM, el estado peruano aprueba para el uso obligatorio de esta norma. De este modo se podrá cumplir con los requisitos legales relacionados con la seguridad de la información y aspirar a una certificación internacional a largo plazo.

La seguridad de la información que se logra a través de procedimientos técnicos es limitada en consecuencia siempre debe apoyarse en estándares como por ejemplo la familia ISO 27000, buenas prácticas de gestión por ejemplo ITIL y COBIT, que busquen equilibrar la seguridad entre procesos, tecnología y personas.

Los resultados de la evaluación y análisis de riesgos deben ser revisados y actualizados periódicamente porque esto permitirá conducir a la elaboración de políticas de seguridad integrales, que consiste un documento que indica el compromiso de la alta dirección, así como el papel que debe jugar en la consecución de los objetivos de la institución.

Los controles de seguridad implementados deben ser monitoreados constantemente e ir implementando nuevos controles de ser necesario para mitigar aún más los riesgos identificados, estos controles deben estar equilibrados entre personas, tecnología y procesos.

Se debe implementar en la universidad programas de capacitación en temas de seguridad de información, comenzando por la cima de la escala jerárquica hasta llegar a los usuarios internos y externos de los activos de información. Esta formación creará una cultura de seguridad que sirva como base para la protección de la información a nivel institucional.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, G., Pérez, P. 2004. Seguridad informática para empresas y particulares. Madrid, España, McGraw-Hill. 442 p.

Areitio, J. 2008. Seguridad de la información; Redes, informática y sistemas de información. Madrid, España, Paraninfo. 566 p.

Ampuero, C. 2011. Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Tesis Ing. Informático. Lima, Perú, Pontificia Universidad Católica del Perú. 106 p.

Arjonilla, S., Medina, A. 2013. La gestión de los sistemas de información en la empresa; Teoría y casos prácticos. 3 ed. Madrid, España, Pirámide. 424 p.

Baena, G. 2014. Metodología de la investigación: Serie integral por competencias. Mexico DF, Mexico, Patria. 157 p.

Cárdenas, F. 2008. Gestiones de seguridad de la información en las organizaciones. Bogotá, Colombia. 13 p.

Carrasco, S. 2006. Metodología de la investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación. Lima, Perú, San Marcos. 474 p.

Chicano, E. 2014. Auditoría de seguridad informática. Madrid, España, IC Editorial. 308 p.

Corletti A. 2011. Seguridad por niveles. Madrid, España, darFE Learning Consulting. 708 p.

Escrivá, G., Romero, R., Ramada, D., Onrubia, R. 2013. Seguridad informática. Madrid, España, Macmillan. 217 p.

Fernández, D. 2013. Introducción a los sistemas de gestión de la seguridad basados en ISO 27001 y desarrollo de herramienta de soporte a la implantación. Tesis Ing. Informática. Valencia, Madrid. Universidad Politécnica de Madrid. 128 p.

Gómez, L., Andrés, A. 2012. Guía de aplicaciones de la norma UNE-ISO/ IEC 27001 sobre seguridad en sistemas de información para PYMES. 2 ed. Madrid, España, AENOR. 216 p.

Gómez, L., Fernández P. 2015. Cómo implantar un SGSI según UNE-ISO/ 27001:2014 y su aplicación en el esquema nacional de seguridad. Madrid, España, AENOR. 164 p.

Hernández, S., Fernández, C., Baptista, P. 2014. Metodología de la investigación. 6 ed. Mexico DF, Mexico, McGraw-Hill. 600 p.

Lamilla, E. 2009. Desarrollo de políticas de seguridad informática e implementación de cuatro dominios en base a la Norma ISO/IEC 27002 para el Área de Hardware en la empresa UNIPLEX SYSTEMS S.A. en

Guayaquil. Tesis Ing. Electrónica. Guayaquil, Ecuador, Escuela Superior Politécnica del Litoral. 567 p.

Laudon, K., Laudon, J. 2012. Sistemas de información gerencial. 12 ed. Naucalpan de Juárez, México, Pearson Educación. 776 p.

MINHAFP (Ministerio de Hacienda y Función Pública, España). 2012. Metodología de análisis y gestión de riesgos de los sistemas de información: Libro I Método. Madrid, España. Versión 3.0. 127 p.

MINHAFP (Ministerio de Hacienda y Función Pública, España). 2012. Metodología de análisis y gestión de riesgos de los sistemas de información: Libro II Catalogo de elementos. Madrid, España. Versión 3.0. 75 p.

MINHAFP (Ministerio de Hacienda y Función Pública, España). 2012. Metodología de análisis y gestión de riesgos de los sistemas de información: Libro III Guía de técnicas. Madrid, España. Versión 3.0. 42 p.

Peso, E. 2004. El documento de seguridad: Análisis técnico y jurídico. Madrid, España. Díaz de Santos-IEE. 820 p.

Supo, J. 2014. Cómo probar una hipótesis; El ritual de la significancia estadística. 1 ed. Arequipa, Perú, Bioestadístico EIRL. 68 p.

Von-Solms, B. 2010. Las cinco olas de la seguridad de la información; De Kristian Beckman al presente. Johannesburgo, Sudáfrica. 6 p.