Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

Tesis

Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca

Para optar el Titulo Profesional de:

Ingeniero de Sistemas

Presentado por:

Fuentes Serrate, Roberto Carlos
Autor

Dr. Ing. Ernesto Karlo Celi Arévalo
Asesor

Lambayeque – Perú
2020

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

Tesis

Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca

Para optar el Titulo Profesional de:

Ingeniero de Sistemas

Aprobado por los Miembros del Jurado:

Ing. Sandoval Jiménez, José Ramón
Presidente

Ing. Guzmán Valle, María de los Ángeles
Secretaria

Ing. Roberto Carlos Arteaga Lora
Vocal

Lambayeque – Perú
2020

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

Tesis

Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca

Para optar el Titulo Profesional de:

Ingeniero de Sistemas

Fuentes Serrate, Roberto Carlos
Autor

Dr. Ing. Ernesto Karlo Celi Arévalo
Asesor

Lambayeque – Perú
2020

DEDICATORIA

Esta tesis está dedicada a:
A Dios quien ha sido mi guía, fortaleza y su mano de fidelidad y Amor han estado conmigo hasta el día de hoy.

A mi Madre Elizabeth Serrate Ordoñez quien con su amor, Sacrificio y esfuerzo me han permitido llegar a cumplir cada meta que me he propuesto, esta tesis es gran parte gracias a ti, no sé dónde me encontraría de no ser por tus consejos y el gran amor que me brindas cada día de mi vida. Cada logro en mi vida está dedicado a ti, así como tú dedicaste tu vida a la mía.

A la memoria de mi segunda Madre mi abuela, Flor De Dalia Ordoñez Silva, quien me animó a perseguir esta meta y, durante lo largo de mi vida fue mi inspiración para cumplir cada meta que me he propuesto. Y aunque desapareció físicamente, su corazón sigue aquí conmigo. Este logro es para ella, sé que desde el Cielo este muy feliz al ver como cumplo uno de tus grandes Anhelos.

Ser padre y universitario es difícil, porque implica un mayor esfuerzo y porque sabes que alguien más se está sacrificando para que tú puedas lograr tus sueños, y esas personas son ustedes, mis hijos Roberto Anjhelo y Elizabeth Luana, la razón de que me levante cada día y esforzarme por construir un futuro para nuestra familia. Son mi principal motivación y este logro es para ustedes.

A mi abuelo Hugo Serrate Huamán, por ser un gran ejemplo para mí, y por exigirme a ser mejor cada día, tú me enseñaste que el esfuerzo es el único camino para triunfar en la vida.

Lambayeque 2020

AGRADECIMIENTOS

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia.

Agradecer al gran amor de mi vida Angela, la ayuda que me has brindado ha sido sumamente importante, estuviste a mi lado inclusive en los momentos y situaciones más tormentosas, siempre ayudándome. No fue sencillo culminar con éxito este proyecto, sin embargo, siempre fuiste muy motivadora y esperanzadora, me decías que lo lograría perfectamente. Me ayudaste hasta donde te era posible, incluso más que eso.
Muchas gracias, amor.

A mi padre Roberto, quien me enseñó a valorar los resultados de un gran esfuerzo, a conocer el precio de tener una gota de sudor en la frente, por ser un amigo y darme palabras de aliento cada momento que los necesite, padre, ocupas un lugar muy especial en mi corazón.

A mis tíos Hugo, José y Alicia por su cariño y apoyo incondicional, durante todo este proceso, agradezco los concejos sabios que en el momento indicado me han sabido dar para no dejarme caer y enfrentar con exito momentos difíciles.

A mis Primo Franco, Hugo y Mateo, agradecerles por ver un ejemplo en mí, y así motivarme a ser cada día un mejor profesional y sobre todo una mejor persona.

Agradezco a toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Lambayeque 2020

RESUMEN

Asegurar la confidencialidad, la integridad y la disponibilidad de la información, se ha convertido en una de las tareas fundamentales del gobierno de las tecnologías de la información (TI) en las organizaciones, sobre todo, si los procesos críticos son soportados por tecnologías de la información. Para gestionar los riesgos operativos que resultan de la dependencia de las TI, se hace necesario la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). La presente tesis, propone un SGSI para dar seguridad a la información que se gestiona en los procesos críticos de la Universidad Nacional de Cajamarca (UNC), específicamente, en aquellos procesos que son la razón de ser de la entidad, como son; la gestión académica y la investigación.

El marco de referencia teórico que se tomó como guía para el desarrollo de la propuesta fue la ISO/IEC 27003, norma que propone una metodología de implementación de un SGSI, y que, a su vez, se sustenta en las buenas prácticas y recomendaciones de las normas hermanas, ISO/IEC 27001 e ISO/IEC 27002. Para el análisis de riesgos de TI, que es una etapa crítica de la implementación del SGSI, se tomó como referencia la metodología española MagerIT.

La validación de SGSI propuesto se realizó a través de un procedimiento no experimental, como una encuesta de satisfacción, aplicada a los usuarios de TI de la universidad. El análisis estadístico de los datos recopilados en la encuesta, que la propuesta de SGSI tiene un nivel aceptable para que pueda ser implementado.

***Palabras clave**: sistema de gestión de seguridad de la información, gestión del riesgo de*
TI, ISO/IEC 27003.

ABSTRACT

Ensuring the confidentiality, integrity and availability of information has become one of the fundamental tasks of information technology (IT) governance in organizations, especially if critical processes are supported by information technology. information. To manage the operational risks resulting from IT dependency, the implementation of an Information Security Management System (ISMS) is necessary. This thesis proposes an ISMS to provide security to the information that is managed in the critical processes of the National University of Cajamarca (UNC), specifically, in those processes that are the reason for the entity, such as; academic management and research.

The theoretical frame of reference that was taken as a guide for the development of the proposal was ISO / IEC 27003, a standard that proposes a methodology for implementing an ISMS, and which, in turn, is based on good practices and recommendations of the sister standards, ISO / IEC 27001 and ISO / IEC 27002. For the IT risk analysis, which is a critical stage in the implementation of the ISMS, the Spanish MagerIT methodology was used as a reference.

The proposed ISMS validation was performed through a non-experimental procedure, such as a satisfaction survey, applied to university IT users. Statistical analysis of the data collected in the survey, that the ISMS proposal has an acceptable level for it to be implemented.

Key words: *information security management system, IT risk management, ISO / IEC 27003.*

INDICE DE CONTENIDOS

INDICE DE TABLAS

DATOS INFORMATIVOS

Título del proyecto

Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca

Personal investigador

- **Autor**

  Apellidos y Nombres: Roberto Carlos Fuentes Serrate

  Correo: roberto.fuentes.serrate@hotmail.com

  Teléfono: 998072784

- **Asesor**

  Dr. Ing. Ernesto Karlo Celi Arévalo

Tipo de investigación

Descriptiva propositiva, no experimental

Línea de la investigación

Gobierno y Gestión de TI

Localidad o Institución donde se realizará el proyecto

Universidad Nacional de Cajamarca

INTRODUCCION

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma.

Metodológicamente, implementar un SGSI en una organización no es una tarea fácil, implica tareas de planificación, evaluación, documentación de escenarios de riesgos y despliegue de controles para su mitigación. Esto se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos. No tener las medidas necesarias para mitigar estos riesgos puede llevar a la organización a pérdidas no solo de información, sino también a impactos negativos desde diferentes perspectivas: operativo, legal, económico, social, reputacional, etc.
La Universidad Nacional de Cajamarca necesidad implementar un conjunto de procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; y con ello, garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los usuarios que estén autorizados y permanezca tal y como fue creada por sus propietarios.

En la presente tesis se desarrolla una propuesta de sistema de gestión de seguridad de información para la Universidad Nacional de Cajamarca, cuyo desarrollo tomó como referencia a la norma ISO/IEC 27003.
El presente trabajo consta de cinco capítulos. Ellos son:

- En el capítulo I se presenta la descripción de la realidad problemática, el planteamiento del problema científico, la descripción del proyecto y los objetivos.

- El capítulo II muestra el marco teórico, en el que están planteadas las bases teóricas relacionadas con un sistema de gestión de seguridad de la información (SGSI), definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación

- En el capítulo III se especifican la metodología de la investigación utilizada para el desarrollo del trabajo de investigación. La metodología aplicada tiene dos partes, la primera se refiere al procedimiento utilizado para evaluar la situación actual de la seguridad de la información en la UNC, tomando como referencia los formatos establecidos por la ISO/IEC 27003 para este fin y la segunda parte se refiere a la metodología de la gestión de riesgos que se aplicó para la identificación y análisis de los riesgos de TI y posteriormente para el tratamiento de los niveles de riesgos no tolerables en base a la propuesta de salvaguardas.

- El capítulo IV está destinado a la presentación de los resultados del trabajo de investigación. Se desarrolla cada una de las tareas y actividades propuestos en el capítulo III y se discuten los resultados obtenidos.

- A partir de los resultados obtenidos se han planteado las conclusiones y recomendaciones pertinentes, y finalmente se consigna la bibliografía utilizada y los anexos respectivo

CAPÍTULO I. EL PROBLEMA

1.1. Descripción de la problemática

Hoy en día la mayoría de organizaciones, sin importar el tipo o la actividad a la se dediquen, están definitivamente relacionadas con las tecnologías actuales; las cuales a su vez avanzan día a día a pasos agigantados y por ello es muy importante que toda empresa siga el camino al desarrollo y crecimiento tecnológico.

Estas organizaciones manejan una gran cantidad de información en todos sus procesos, y de ocurrir algún incidente relacionado con la confidencialidad, integridad o disponibilidad de ésta, puede afectar de manera muy significativa las diferentes áreas existentes, ocasionando riesgos inmediatos que afectan el desarrollo óptimo de cada una de ellas.

Riesgos como pérdida, alteración o lectura no permitida de información, accesos no autorizados, sobrecalentamiento de servidores, presencia de software malicioso, etc. son solo algunos de los riesgos existentes, ocasionados muchas veces por la falta del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) que luego sea implementado en la organización.

“Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados” (NTP-ISO/IEC 17799, 2007).

En un Sistema de Información (SI) existen también las amenazas de carácter técnico e influyendo a la vez las de carácter humano; casos como equipos conectados a la red que son usados para uso personal y no institucional, empleados que no protegen la confiabilidad de sus credenciales de acceso a su área, uso de correos electrónicos personales para la comunicación institucional, uso de múltiples contraseñas para acceder a diferentes servicios ocasionando varias veces el olvido de sus datos de acceso, el no contar con un sistema automático de recuperación de contraseñas son solo algunos ejemplos de las diferentes amenazas existentes.

Por todo lo mencionado anteriormente es necesaria la implantación de políticas, procedimientos, herramientas, controles, pruebas que salvaguarden los tres principios básicos de la SI: confiabilidad, integridad y disponibilidad.

“El SGSI, tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados” (Solarte, Enriquez, & Benavides Ruano, 2015).

En el caso específico del sector educativo no existen leyes o normas establecidas por el Ministerio de Educación que regulen la SI en todas las instituciones de este rubro, teniendo conocimiento que en otros sectores si existen normas reguladoras que permiten a las organizaciones manejar de la manera más óptima este tema.

Sin embargo si existe desde hace más de diez años políticas del gobierno que han recomendado una adecuada gestión de la SI con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la SI. Adicionalmente en mayo de 2012 la Resolución Ministerial Nº 129-2012-PCM aprueba el uso obligatorio de la NTP ISO/IE 27001:2008 en las entidades del estado y la última publicación en enero del 2016 con la Resolución Ministerial 004-2016-PCM, aprueban el uso obligatorio de la NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática (entidades públicas del estado) demostrando la intención del gobierno peruano en establecer un modelo integral para el desarrollo de los planes de SI en la Administración Pública.

La Universidad Nacional de Cajamarca (UNC), no es ajena como muchas otras universidades nacionales a este gran problema, la falta de un SGSI. Hablando específicamente de UNC, la cual cuenta con tres sub-áreas existentes: Redes, Desarrollo y Soporte Técnico, y siendo una de las más importantes oficinas a nivel organizacional de dicha universidad, ésta no cuenta con controles, políticas o procedimientos oficiales que ayuden a proteger de manera correcta toda la información de dicha casa de estudios. Empezando por la falta de presupuesto e inversión en la SI, existe también la falta de políticas, procedimientos, normas

establecidas relacionadas con la seguridad, la gestión y tratamiento de riesgos, falta de diagramas acerca de los procesos que se desarrollan, falta de un inventario de los activos tecnológicos existentes y la relación que existe con cada uno de sus procesos, falta de controles para la seguridad de equipos y así evitar pérdida, daño o robo de los mismos, falta de documentación oficial de todas las incidencias y la atención de problemas, falta de una definición formal de los deberes y funciones dentro del cada sub-área existente, falta de políticas sobre el uso de la red, falta de documentación de los sistemas utilizados en la oficina, entre otros.

Considerando la problemática anteriormente identificada, surge la necesidad de diseñar un Sistema de Gestión de la Seguridad de la Información en la UNC que se ajuste a sus necesidades actuales, utilizando la norma ISO/IEC 27003, con el objetivo de cumplir los requerimientos en materia de seguridad de la información de dicha oficina, tales como la identificación y valoración de activos, identificación, análisis y evaluación de riesgos y amenazas, elaboración de un documento de Políticas de Seguridad, etc.

1.2. Formulación del problema científico

¿De qué manera mejora la Gestión de la Seguridad de la Información en la Universidad Nacional de Cajamarca a través de un Sistema de Gestión de la Seguridad de la Información basándose en la norma ISO/IEC 27003?

1.3. Descripción del trabajo de investigación

Debido a los riesgos a los que están expuestos los activos de información, el impacto que la interrupción de estos puede causar, es preponderante la definición de una metodología y el uso de herramientas que nos ayuden reducir y mitigar estos riesgos en la Universidad Nacional de Cajamarca.

Es por ello que se propone la implementación de un Sistema de gestión de seguridad de información (SGSI), basada en las normas ISO/IEC 27003, el cual nos brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información, implantar los controles necesarios que ayudarán a salvaguardar los activos de información de los procesos de tecnología, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de Información (SGSI), alineándolo de esta manera a los objetivos estratégicos de la organización.

Seguridad de Información (SGSI), alineándolo de esta manera a los objetivos estratégicos de la organización.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Desarrollar una propuesta de Sistema de Gestión de la Seguridad de la Información, basándose en la norma ISO/IEC 27003, que permite mejorar la gestión de la seguridad de la información en la Universidad Nacional de Cajamarca

1.4.2. Objetivos específicos

a. Determinar el nivel de cumplimiento de los controles de seguridad de la información en cada uno de sus dominios establecidos en la ISO/IEC 27002
b. Diseñar y modelar un procedimiento para identificar y analizar los riesgos de seguridad de información en los procesos académicos de la Universidad Nacional de Cajamarca.
c. Diseñar y modelar un procedimiento para identificar e implementar las salvaguardas como parte del desarrollo del Sistema de Seguridad de la Información basándose en la norma ISO/IEC 27003.
d. Definir la estructura organizativa de la seguridad de la información como parte del desarrollo del Sistema de Seguridad de la Información basándose en la norma ISO/IEC 27003.
e. Definir las políticas de seguridad de la información en cada uno de los dominios de seguridad de la ISO/IEC 27002.
f. Validar el sistema de gestión de seguridad de la información propuesto desde las perspectivas de su Contextualización en la organización, Liderazgo y Planificación de la seguridad de la información, a través de una evaluación no experimental.

CAPÍTULO II. MARCO TEÓRICO

De la revisión literaria realizada se elaboró los siguientes fundamentos teóricos, que sirvieron de base para el desarrollo de la propuesta de SGSI en la Universidad Nacional de Cajamarca:

2.1. La información como activo estratégico de las organizaciones

Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Estos son necesarios para que la organización funcione y alcance los objetivos que propone su dirección (Espinoza, 2013).

Según la ISO/IEC 17799 (2007), Código de Práctica para la Gestión de Seguridad de Información, un activo de información es: “algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger”.

Por su parte, los autores Andreu, Ricart y Valor (1998) explican como la información se convierte en un recurso estratégico para las empresas y se integra dentro de su proceso de planificación estratégica.

Así entonces la información se ha convertido en un recurso clave para las empresas a todos los niveles jerárquicos y para todos los departamentos ya que las organizaciones deben conseguir, procesar, usar y comunicar información, tanto interna como externa, en sus procesos de planificación, dirección y toma de decisiones (Carrasco, 2010).

La NTP-ISO/IEC 27005 (2009) clasifica el activo en dos tipos:

Los activos primarios: Son usualmente los procesos e información centrales de la actividad en cuestión. Otros activos primarios como los procesos de la organización también pueden considerarse, lo cual será más apropiado para diseñar una política de seguridad de la información o un plan de continuidad del negocio.

- Procesos y actividades de negocio
- Información

Los activos de apoyo: Estos activos tienen vulnerabilidades que son explotables por amenazas que tienen como objetivo desactivar los activos primarios del alcance (proceso e información). Son de varios tipos:

- Hardware
- Software
- Red
- Personal
- Sitio
- Estructura de la Organización

2.2. Propietario del activo de información

Según la NTP-ISO/IEC 27005 (2009), el propietario del activo es aquel que puede no tener derechos de propiedad sobre el activo, pero tiene responsabilidad sobre su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo a menudo es la persona más apropiada para determinar el valor que el activo tiene para la organización. Se debe identificar al propietario de un activo para cada activo, para determinar las disposiciones sobre responsabilidad y rendición de cuentas por el activo.

2.3. Seguridad de información

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (Aguirre Freire & Palacios Cruz, 2014).

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como (Talavera Álvarez, 2015):

a. Crítica: Es indispensable para la operación de la empresa.
b. Valiosa: Es un activo de la empresa y muy valioso.

c. Sensible: Debe ser conocida por las personas autorizadas

Los términos de seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.

2.4. Sistema de Gestión de Seguridad de la información

Un Sistema de Gestión de Seguridad de Información (SGSI) es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa (ISO 17799:2005; Alexander, 2007). Un SGSI está soportado en cuatro grandes y continuas etapas para su mantención en el tiempo, las cuales se muestran en el **¡Error! No se encuentra el origen de la referencia.**.

Gráfico N° 1. Etapas de un SGSI

Fuente: http://www.iso27000.es/

2.5. Principios de la seguridad de la Información

Los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables (Montesino Perurena, Baluja Garcia, & Porven Rubier, 2013).

Estos últimos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación.

a. Confidencialidad

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos. La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, como durante su procesamiento y tránsito, hasta llegar a su destino final (Condori Alejo, 2012).

b. Integridad

Este principio permite garantizar que la información no sea modificada o alterada en su contenido por personas no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos.

c. Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Adicionalmente, la disponibilidad hace referencia a la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo

desarrollo de la productividad de la organización sin mayores inconvenientes. (Condori Alejo, 2012).

2.6. Políticas de Seguridad de la Información

Una política de seguridad de la información es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen (Hernández Pinto, 2006).

Tiene como objetivo de dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones. La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización (NTP ISO/IEC 17799, 2007).

Peltier, considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo (Peltier, Peltier, & Blackley, 2005).

Rol Interno: Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.

Rol Externo: Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

Según Hernández Pinto (2006) una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

Seguridad Física
Seguridad Lógica
Seguridad en redes
Seguridad en los recursos humanos
Seguridad en el Outsourcing
Planes de Contingencia

2.7. Elementos de un SGSI

La ISO/IEC 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio) (ISO 27000.es, 2005):

a. Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

b. Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

c. Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

d. Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

e. Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

f. Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

g. Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

h. Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

i. Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

2.8. Proceso de implementación de un SGSI, según ISO/IEC 27003

Los siguientes pasos son expuestos por Robles & Rodríguez de Roa (2006), de modo sucinto y muy práctico:

PASO 1: Inicio del proyecto

En esta primera etapa se pretende asegurar para el éxito de todo el proyecto, el compromiso de la dirección general y seleccionar y formar a los miembros del equipo inicial del proyecto.

Para reducir la duración del proceso, el apoyo de la dirección debe estar presente a todos los niveles: operativo, técnico y presupuestario, así como en el de la planificación temporal. La dirección general debe comprender que su apoyo necesariamente conlleva un esfuerzo continuo. La infraestructura establecida requerirá con toda seguridad ajustes, así como una mejora continua.

Respecto al equipo inicial del proyecto (coordinadores, grupos de trabajo, etc.), se debe formar un comité de dirección del proyecto que puede estar compuesto por un director ejecutivo, el director del proyecto y representantes de las diferentes unidades operativas implicadas. Es habitual que en algunas organizaciones grandes, el responsable de seguridad pueda llevar a cabo gran parte de las tareas del director del proyecto. En la mayoría de los casos, la implementación de la norma ISO/IEC 27001 en una organización requiere la implicación de todas las unidades operativas.

PASO 2: Alcance del SGSI

Es una etapa clave para el éxito posterior del proyecto. Debe tenerse en cuenta lo siguiente:

Alcance del SGSI: determina qué unidades operativas y actividades estarán dentro del entorno de seguridad de la información

Limitaciones del SGSI: características específicas de la organización (tamaño, campo de acción, etc.), ubicación de la organización, activos (inventario de todos los datos críticos), tecnología.

Conexiones o Interfaces: se deberán tener en cuenta por parte de la organización las relaciones con otros sistemas, otras organizaciones y proveedores externos.

Requerimientos de Seguridad del SGSI: de naturaleza legal o del negocio.

Exclusiones y justificación de las exclusiones (Declaración de aplicabilidad).

Contexto estratégico: las medidas de seguridad planificadas deben tener en cuenta la posición actual y futura de la organización para alcanzar las metas fijadas por la dirección.

Recopilación de la documentación existente: para simplificar y mejorar la eficacia del proceso desde el inicio, es necesaria una revisión de la documentación existente para evaluar el alcance de las medidas existentes, como el manual de gestión de calidad de la norma ISO 9001, el de la 14001 en su caso, o el manual de políticas de seguridad.

Redacción de un inventario documental por los responsables de departamento (ejemplos):

- Documentos de la política de seguridad.

- Normas y procedimiento de las políticas (administrativos o técnicos).
- Informes de evaluación de riesgos
- Planes de tratamiento de riesgos.
- Documentos que indiquen la existencia de controles de seguridad y su gestión; por ejemplo, informes y planes de auditoría, informes de incidencias, etc.

PASO 3: Evaluación de riesgos

Con independencia del tipo o tamaño de la empresa, todas las organizaciones son vulnerables a las amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información importante.

Cuanto antes se adopten las medidas correctivas, la seguridad representará un menor coste y será más efectiva. Para poder realizar una identificación y selección de controles más sencillos que permitan una mejor gestión de los recursos humanos y financieros se debe conocer la fuente y naturaleza de las amenazas.

Esta etapa incluye:

Aplicabilidad de los controles de la ISO/IEC 27002: diagnóstico preliminar.
Identificación y evaluación de activos, datos a proteger.
Identificación y evaluación de amenazas y vulnerabilidades.

PASO 4: Tratamiento y administración del riesgo

En este paso es básico conocer cómo la selección y la implantación de los controles permiten reducir los riesgos a un nivel aceptable por la organización. Esta gestión generalmente es una función de la:

Política de seguridad inicial.
Nivel de seguridad requerido.
Resultados de la evaluación de riesgos.
Reglamentación y legislación aplicable.
Regulaciones y restricciones del negocio existentes.

En general existen cuatro opciones para el tratamiento del riesgo: reducir el riesgo, aceptar el riesgo, evitar el riesgo y transferencia del riesgo.

PASO 5: Programa de formación y Sensibilización para el personal

La organización debe asegurarse de que todos los miembros del personal con responsabilidades específicas en el SGSI están debidamente formados, cualificados y capacitados para realizar sus funciones. La organización debe también asegurarse de que el personal necesario está concienciado de la importancia de sus actividades en la seguridad de la información y de cómo contribuyen ellos a alcanzar los objetivos del SGSI.

Es importante desarrollar un programa de formación y sensibilización con el fin de "educar" a todos los empleados. Los empleados tienen que entender y respetar las buenas prácticas de seguridad de la información.

PASO 6: Documentación e implantación del SGSI

La documentación de un SGSI es una exigencia necesaria y previa a la implantación del sistema y se articula en torno a dos puntos estratégicamente claves:

La descripción de la estrategia de la organización, sus objetivos, la evaluación de riesgos y las medidas adoptadas para evitar o atenuar los mismos.
El control y el seguimiento del funcionamiento del SGSI. Es usual plantear por lo menos cuatro niveles de documentación como muestra el cuadro siguiente:

Tabla N° 1. Niveles de documentación en seguridad de la información

Nivel	Documento requerido	Contenido
Nivel 1	Manual de seguridad	Política, evaluación de riesgos, declaración de aplicabilidad
Nivel 2	Procedimientos	Procesos: ¿Qué?, ¿Quién?, ¿Cuándo?, ¿Dónde?
Nivel 3	Fichas de trabajo, formularios, etc.	Descripción de cómo se realiza el trabajo y actividades
Nivel 4	Registros	Este nivel proporciona pruebas objetivas de conformidad con las exigencias del SGSI

Fuente: (Robles & Rodriguez de Roa, 2006)

Una vez realizado lo anterior, o en paralelo, se lleva a cabo la implantación de los documentos creados y se complementa con la formación del personal en las etapas en que sea necesario.

PASO 7: Ajustes y preparación para la Auditoría de Certificación

El Diagnóstico es uno de los pasos "previos e imprescindibles" de toda organización que desee y tenga como objetivo la certificación de acuerdo a la norma ISO/IEC 27001, con el fin de validar si el sistema sigue las especificaciones necesarias para la implantación de su marco de gestión.

Este documento (que se convertirá en un registro imprescindible del SGSI de cara a la auditoría de certificación) proporciona la justificación para la aplicabilidad o no aplicabilidad de cada control ISO/IEC 27001 del SGSI en cuestión, incluyendo también dónde es aplicable el estado de implantación de cada control.

PASO 8: Control y mejora continua

Control y mejora continua del SGSI de acuerdo al Ciclo de DEMING (P-D-C-A) establecido en la norma debiéndose realizar antes de la Auditoría de Certificación en función de los resultados del diagnóstico.

2.9. Gestión de Riesgo

Alcántara Torres (2015) nos dice que la gestión de riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo, es así que tenemos a los siguientes parámetros como son los que detallaremos a continuación:

a. Análisis del Riesgo: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.
b. Clasificación: Determina si los riesgos encontrados y los riesgos restantes son aceptables.
c. Reducción: Define e implementa las medidas de protección. Además sensibiliza y capacita los usuarios conforme a las medidas.

d. Control: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sancionar el incumplimiento.

Para lograr el éxito de la gestión de riesgo, es vital tener en cuenta tanto la cultura como la estructura de la organización, la misión y los objetivos de negocio que se hayan trazado, la definición de los procesos organizacionales y el conocimiento de marcos de buenas prácticas generalmente aceptados (Huamán Monzón, 2014)

Huamán Monzón nos indica que en el escenario que una amenaza se materialice, la gestión de riesgos garantizara que el impacto que se tendrá internamente (en la organización) será manejable, es decir, que estará dentro de los límites de costos aceptables sin perturbar la continuidad del negocio.

Sabemos que en toda actividad empresarial hay riesgo (cuando hacemos algo o cuando dejamos de hacer algo), la gestión de Riesgos debe brindar garantía de seguridad en cualquier actividad que emprenda la institución apoyándose en la estrategia de seguridad que ésta esté llevando a cabo.

Gráfico N° 2. Fases de Gestión de Riesgos
Fuente: (Huamán Monzón, 2014)

2.10. Elementos evaluados en la Gestión de Riesgo

a. Amenaza

Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la perdida de información, o de su privacidad, o bien un fallo en los equipos físicos (Espinoza, 2013).

Una amenaza tiene el potencial de dañar activos como la información, los procesos y los sistemas y, por tanto, las organizaciones. Las amenazas pueden ser de origen natural o humano y pueden ser accidentales o deliberadas. Así mismo una amenaza puede surgir desde adentro o desde fuera de la organización (NTP-ISO/IEC 27005, 2009).

b. Vulnerabilidad

Estado, debilidad o incapacidad de resistencia cuando se presenta un fenómeno amenazante y que al ser explotado afecta el estado de los activos de un proyecto, de una área u organización. Una vulnerabilidad es un estado de debilidad que si ocurriese se materializa una o varias amenazas que afecta diversos activos, por lo que es indispensable identificarlas, valorarlas y priorizarlas (Reina García & Morales Ramírez , 2014).

c. Riesgo

Según Medina (2007) riesgo se define como la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: La confidencialidad, la integridad y la disponibilidad de la información.

Se considera riesgo la estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él causando daños a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente (Inteco, s/a).

Halvorson (2008) explica tres (3) naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales.

Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la información; sin embargo, se encuentran más orientados a los riesgos de las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.

Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.

Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para poder identificar el potencial daño o pérdida debido a un riesgo los dueños de los activos pueden responder estas cuatro preguntas (Ozier, 2004):

¿Qué puede suceder? (¿Cuál es la amenaza?)

¿Qué tan malo puede ser? (¿Cuál es el impacto?)

¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)

¿Qué tan ciertas son las respuestas de las tres primeras preguntas? (¿Cuál es el grado de confianza?)

2.11. Proceso de gestión de riesgos de TI

Costas Santos (2011) Establece que la gestión de los riesgos permite tener control sobre el desarrollo, la implementación y funcionamiento de los procesos, lo cual llevara a lograr de manera eficiente el cumplimiento de sus objetivos estratégicos y estar preparados para enfrentar cualquier incidente que pueda presentarse.

Sobre los procesos, se construyen controles con el objetivo de reducir la frecuencia de las amenazas o limitar el daño causado y llevar el nivel de riesgo a un nivel aceptable por la organización.

Dependiendo del tipo de riesgo, se puede optar por:

a. Evitar el riesgo: por ejemplo eliminando el activo.

b. Mitigar el riesgo: implementando controles para reducir la probabilidad y el impacto.
c. Transferir el riesgo: por ejemplo contratando un seguro con cobertura para ese riesgo. Aceptar el riesgo: reconociendo que el riesgo existe y monitorizarlo.

Según la NTP-ISO/IEC 27005 (2009), el proceso de gestión del riesgo en seguridad de la información consiste en establecer el contexto, evaluar el riesgo, tratar el riesgo, aceptar el riesgo, comunicar el riesgo y monitorear y revisar el riesgo.

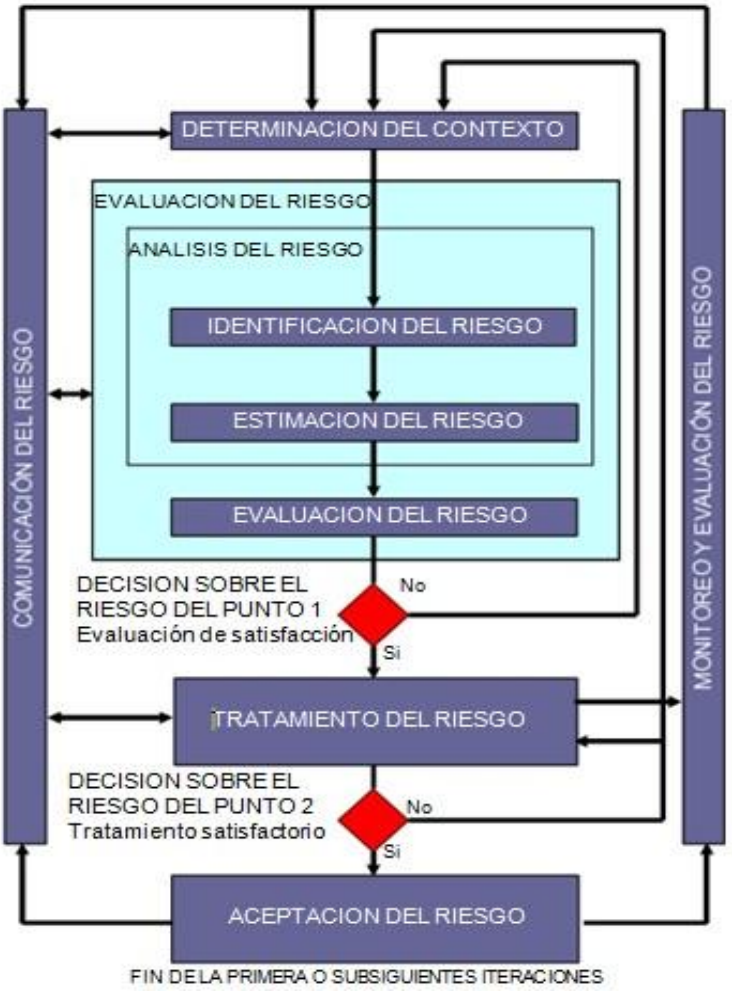

Gráfico N° 3. Proceso de gestión del riesgo de seguridad de la información
Fuente: (NTP-ISO/IEC 27005, 2009)

Tal como lo ilustra la figura anterior, el proceso de gestión de seguridad de la información puede ser iterativo para la evaluación del riesgo y/o para las actividades

de tratamiento del riesgo. Un enfoque iterativo para la conducción de la evaluación del riesgo puede incrementar la profundidad y detalle de la evaluación en cada iteración. El enfoque iterativo provee un buen balance entre minimizar el tiempo y el esfuerzo que se emplea en identificar los controles y a la vez asegurar que se evalúe apropiadamente los altos riesgos.

Primero se determina el contexto. Luego se realiza una evaluación del riesgo. Si esto provee suficiente información para determinar efectivamente las acciones requeridas para modificar los riesgos a un nivel aceptable, entonces la tarea está completa y sigue el tratamiento del riesgo. Si la información es suficiente, se conducirá otra iteración de la evaluación del riesgo con el contexto revisado (por ejemplo criterios de evaluación del riesgo, criterios de aceptación del riesgo o criterios de impacto) posiblemente en partes limitadas del alcance total (en la Figura véase Decisión sobre el Riesgo Punto 1).

La eficacia en el tratamiento del riesgo depende de los resultados de la evaluación del riesgo. Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel aceptable de riesgo residual. En esta situación, podría requerirse otra iteración de la evaluación del riesgo con parámetros de contexto cambiados (por ejemplo evaluación del riesgo, aceptación del riesgo o criterios de impacto), si fuera necesario, seguido de otro tratamiento del riesgo (en la figura véase, Decisión sobre el Riesgo Punto 2).

La actividad de aceptación del riesgo tiene que asegurar que los gerentes de la organización acepten explícitamente los riesgos residuales. Esto es especialmente importante en una situación donde la implementación de controles se omite o pospone, por ejemplo debido al costo.

Durante todo el proceso de gestión del riesgo en seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los gerentes apropiados y al personal operativo. Incluso antes del tratamiento de los riesgos puede ser muy valioso contar con información sobre los riesgos identificados para administrar los incidentes y puede ayudar a reducir el daño potencial. La conciencia de los gerentes y el personal respecto de los riesgos, la naturaleza de los controles empleados para mitigar los riesgos y las áreas de preocupación para la

organización ayudan a tratar los incidentes y los eventos inesperados de la manera más eficaz.

El Sistema de Gestión de Seguridad de la Información específica que los controles implementados dentro del alcance, límites y contexto deben basarse en el riesgo. La aplicación de un proceso de gestión del riesgo en seguridad de la información puede satisfacer este requisito.

En un SGSI, determinar el contexto, evaluar el riesgo, desarrollar un plan de tratamiento del riesgo y aceptar el riesgo son parte de la fase del "plan". En la fase de "hacer" del Sistema de Gestión de Seguridad de la Información, se implementan las acciones y controles requeridos para reducir el riesgo a un nivel aceptable de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar" del Sistema de Gestión de Seguridad de la Información, los gerentes municipales determinarán la necesidad de revisiones de la evaluación del riesgo y el tratamiento del riesgo a la luz de los incidentes y cambios en las circunstancias. En la fase de "actuar", se realizan todas las acciones requeridas, incluyendo la aplicación adicional del proceso de gestión del riesgo en seguridad de la información.

La tabla siguiente resume las actividades de gestión del riesgo en seguridad de la información relevantes a las cuatro fases del proceso del Sistema de Gestión de Seguridad de la Información:

Tabla N° 2. Alineamiento del SGSI y del Proceso de Gestión del Riesgo en Seguridad de la Información

Proceso del SGSI	Proceso de Gestión del Riesgo de TI
Plan	Determinar el contexto. Evaluar el riesgo. Desarrollar el plan de tratamiento del riesgo. Aceptar el riesgo.
Hacer	Implementar el plan de tratamiento del riesgo.
Verificar	Monitoreo y revisión continuos de los riesgos.
Actuar	Mantener y mejorar el Proceso de Gestión del Riesgo en Seguridad de la Información.

Fuente: (NTP-ISO/IEC 27005, 2009)

2.12. Ciclo de Deming

Es evidente que la seguridad de la información no se termina en la implementación de un “firewall” o con la contratación de una empresa de seguridad. Es necesario integrar las múltiples iniciativas puestas en ejecución dentro de una estrategia global con el fin de que cada elemento ofrezca un nivel óptimo de protección. Es a este nivel que intervienen los sistemas de gestión de la seguridad de la información permitiendo coordinar los esfuerzos para alcanzar una seguridad óptima (Robles & Rodriguez de Roa, 2006).

Un sistema de gestión debe incluir un método de evaluación, medidas de protección y un proceso de documentación y de revisión. Esto último es el principio del Modelo del PDCA (Establecer-Implantar-Monitorizar y Verificar Actuar, manteniendo y mejorando el SGSI). Este modelo popularizado por W.Edwards Deming (y conocido como el “Ciclo Deming”) recuerda fuertemente al modelo de gestión de la calidad ISO 9001 (Robles & Rodriguez de Roa, 2006).

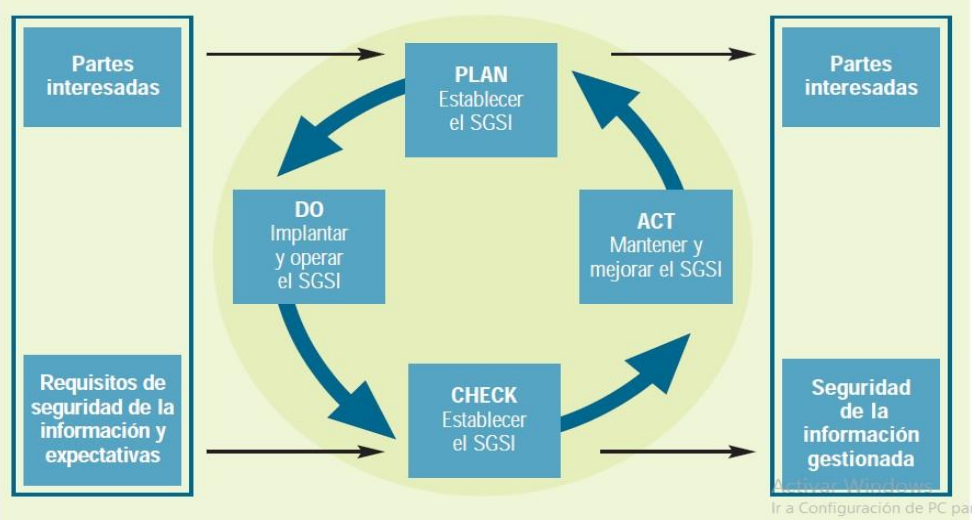

Gráfico N° 4. Ciclo Deming
Fuente: (Robles & Rodriguez de Roa, 2006)

a. PLAN. En esta fase necesaria para la planificación, definición y el establecimiento del SGSI, es importante considerar el entorno de la actividad de la organización que implementará el Sistema. Se deberían identificar, por ejemplo, directrices corporativas aplicables y requisitos legales. Además de esto, el contexto de la actividad de la organización debería quedar reflejado

en las políticas y objetivos de seguridad y se debería considerar al definir el alcance del SGSI. Durante esta fase la organización también diseña un procedimiento formal para la continua identificación y evaluación de riesgos y la selección de los objetivos de control y controles que le permitirán gestionar estos riesgos. Al final de este proceso, la organización prepara la declaración de aplicabilidad.

b. DO. Hacer, implementar. Es importante centrarse inicialmente en el desarrollo e implementación de un plan efectivo y a medio y largo plazo para la atenuación de los riesgos. Durante esta fase, los controles seleccionados en la fase de planificación se implementarán para alcanzar los objetivos de control. En esta fase se inicia el Plan de Formación para incrementar la concienciación y conocimiento del personal que garantice la correcta implementación de los controles.

c. CHECK. Seguimiento, monitorización y revisión del SGSI. Realización periódica de auditorías internas del SGSI y seguimiento regular de la eficiencia del sistema.

d. ACT. Actuar, mantener y mejorar el SGSI. Cuando se han identificado las vulnerabilidades y debilidades, se deben llevar a cabo las medidas correctivas y preventivas apropiadas para mejorar el SGSI, así como las planificaciones temporales de estas mejoras.

2.13. ISO/IEC 27000

La serie de normas ISO/IEC 27000 se denomina “Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)”, proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias:

a. Sistema de gestión de la seguridad de la información.
b. Valoración de riesgos.
c. Controles.

La norma técnica ISO/IEC 27000 está enfocada en procesos, toda la organización se ve involucrada en su implementación en lo que a cada una le corresponde de tal manera que la suma de cada uno de los esfuerzos individuales, apoyados por la gestión y dirección de las personas que lideran el proceso, termine formando un SGSI que logre ejecutar todas las actividades de administración de riesgos incluyendo la creación de medidas ante tales riesgos y los controles para evaluar la efectividad de tales medidas. (Reina García & Morales Ramírez , 2014)

Reina García & Morales Ramírez, nos indican que la familia de normas ISO/IEC 27000 son de aplicación voluntaria pero su uso a nivel mundial facilita las relaciones comerciales entre compañías internacionales y aumenta la competitividad en el mercado, también ayuda a mejorar la calidad y productos ofrecidos ya que este estándar internacional provee un modelo para establecer, implementar, operar y mantener un SGSI basado en los objetivos de la compañía, requisitos, requerimientos y expectativas de seguridad independiente del tamaño, estructura y razón de ser del negocio.

ISO/IEC 27000 contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

En nuestra investigación las normas de la familia ISO 27000, que utilizaremos serán las siguientes:

2.13.1. ISO/IEC 27001 – Sistema de Gestión de la Seguridad de la Información

Es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO/IEC 27002.

Este estándar brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación (Aguirre Mollehuanca, 2014).

Este estándar internacional “proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información dentro de cualquier organización“ (ISO/IEC 27001, 2005).

Indica las acciones que tiene que realizar una organización para poder alinearse a los requerimientos que tiene un SGSI. Para todos los procesos dentro del SGSI, la norma se basa en el modelo Plan-Do-Check-Act, el cual toma como input las expectativas que las partes interesadas de la organización tienen con respecto a la seguridad de información y, siguiendo este plan PDCA, produce un output de seguridad de información que satisfacen aquellas expectativas.

Gráfico N° 5. Modelo PDCA aplicado a los procesos de un SGSI
Fuente: (ISO/IEC 27001, 2005)

La ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un SGSI. Estos requerimientos describen el comportamiento previsto de un SGSI una vez que es completamente operacional. El estándar no es una guía paso a paso sobre cómo construir o crear un SGSI. (BSI Group México , s/a)

Estructura de la ISO/IEC 27001:2013

La estructura de la ISO/IEC 27001:2013 se muestra en la

Tabla N° 3

Tabla N° 3. Mapeo de las cláusulas de ISO/IEC 27001:2013

0	Introducción
1	Alcance
2	Referencias normativas
3	Términos o definiciones
4.1	Comprender la organización y su contexto
4.2	Comprender las necesidades y expectativas de las partes interesadas
4.3	Determinar el alcance del sistema de gestión de seguridad de la información
4.4	Sistema de gestión de seguridad de la información
5.1	Liderazgo y compromiso
5.2	Políticas
5.3	Roles organizacionales, responsabilidades y autoridades
6.1.1	Acciones para hacer frente a riesgos y oportunidades – general
6.1.2	Evaluación de riesgos de seguridad de la información
6.1.3	Tratamiento de riesgos de seguridad de la información
6.2	Objetivos de seguridad de la información y planeación de los mismos
7.1	Recursos
7.2	Competencia
7.3	Conocimiento
7.4	Comunicación
7.5	Información documentada
8.1	Planeación operacional y control
8.2	Evaluación de riesgos de seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información
9.1	Monitoreo, medición, análisis y evaluación
9.2	Auditoría interna
9.3	Revisión de la gestión
10.1	No conformidades y acciones correctivas
10.2	Mejora continua de la información

Fuente: (BSI Group México , s/a)

2.13.2. ISO/IEC 27002 - Código de prácticas para los controles de seguridad de la información

Esta norma internacional proporciona directrices para normas organizacionales de seguridad de la información y para las prácticas de gestión de seguridad de la información. Incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta los riesgos del entorno de seguridad de la información de la organización (ISO/IEC 27002, 2013).

La ISO/IEC 27002 (2013) está diseñada para ser utilizada por las organizaciones que pretenden:

a. Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de seguridad de la Información basado en la Norma ISO/IEC 27001.
b. Implementar los controles de seguridad de la información comúnmente aceptados;
c. Desarrollar sus propias directrices de gestión de seguridad de la información.

Esta norma nos muestra una serie de controles que buscan mitigar el impacto de ocurrencia de los diferentes riesgos que se expone una organización (ISO/IEC 27002, 2013).

La ISO/IEC 27002 (2013) presenta 14 dominios, 35 objetivos de control y 114 controles. Los 14 dominios mencionados previamente son:

Dominio 1: Políticas de seguridad Dominio
2: Organización de la seguridad Dominio 3:
Seguridad de recursos humanos Dominio 4:
Gestión de activos
Dominio 5: Control de acceso lógico
Dominio 6: Cifrado
Dominio 7: Seguridad física y ambiental Dominio
8: Seguridad en las operaciones Dominio 9:
Seguridad en las telecomunicaciones
Dominio 10: Adquisición, desarrollo y mantenimiento de los sistemas de información
Dominio 11: Relaciones con los suministradores
Dominio 12: Gestión de incidentes
Dominio 13: Aspectos de la SI en la continuidad del negocio
Dominio 14: Cumplimiento

2.13.3. ISO/IEC 27003 - Tecnología de la información - Técnicas de seguridad - Orientación para la implementación de un sistema de gestión de la seguridad de la información.

ISO/IEC 27003 es un estándar internacional que constituye una guía para la implantación de un SGSI. Se trata de una norma adaptada tanto para los que quieren lanzarse a implantar un SGSI como para los consultores en su trabajo diario, debido a que resuelve ciertas cuestiones que venían careciendo de un criterio normalizado (ISOTools Excellence, 2014).

ISO/IEC 27003 focaliza su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información – SGSI – según el estándar ISO/IEC 27001. Contiene una descripción del proceso de delimitación del SGSI, y además el diseño y ejecución de distintos planes de implementación (ISOTools Excellence, 2014).

La norma tiene el siguiente contenido:

1. Alcance.
2. Referencias Normativas.
3. Términos y Definiciones.
4. Estructura de esta Norma.
5. Obtención de la aprobación de la alta dirección para iniciar un SGSI.
6. Definición del alcance del SGSI, límites y políticas.
7. Evaluación de requerimientos de seguridad de la información.
8. Evaluación de Riesgos y Plan de tratamiento de riesgos.
9. Diseño del SGSI.

   Anexo A: lista de chequeo para la implementación de un SGSI.
   Anexo B: Roles y responsabilidades en seguridad de la información
   Anexo C: Información sobre auditorías internas.
   Anexo D: Estructura de las políticas de seguridad.
   Anexo E: Monitoreo y seguimiento del SGSI.

2.14. Metodología MagerIT para Análisis de Riesgos

Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos

de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (Magerit, 2012).

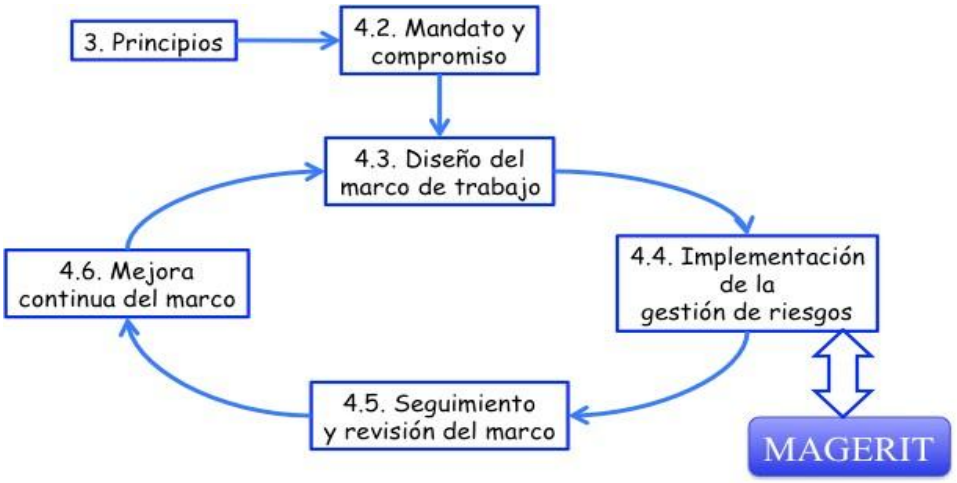

Gráfico N° 6. ISO 3100 - Marco de trabajo para la gestión de riesgos
Fuente: (Magerit, 2012)

Magerit, tiene como uno de sus principales objetivos, el ofrecer un método para analizar los riesgos y ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control (Espinoza Aguinaga, 2013).

El análisis de riesgos propuesto por MAGERIT es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos:

1. Determinar los activos relevantes para la empresa.
2. Determinar las amenazas a la que están expuestos aquellos activos.
3. Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza.
4. Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información.
5. Valorar las amenazas potenciales.
6. Estimar el riesgo.

Esta metodología propone para el análisis de riesgos las 4 etapas siguientes:

1. La etapa 1, Planificación del análisis y gestión de riesgos, establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos.
2. La etapa 2, Análisis de riesgos, permite identificar y valorar las entidades que intervienen en el riesgo.
3. La etapa 3, Gestión de riesgos, permite identificar las funciones o servicios de salvaguarda reductores del riesgo detectado.
4. La etapa 4, Selección de salvaguardas, permite seleccionar los mecanismos de salvaguarda que hay que implementar.

2.15. Definición de la terminología técnica básica

Activo: Cualquier elemento o información, que tenga valor para la UNC.

Control: Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Evento de seguridad de información: Es una ocurrencia identificada del estado de sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de información: Es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Amenaza: Una causa potencial de un incidente no-deseado, el cual puede resultar dañando a un sistema.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas

Riesgo: Es la combinación de la probabilidad de un evento y su ocurrencia

Análisis de riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo. Identifica los activos a proteger o evaluar.

Evaluación del riesgo: Proceso de comparar el nivel de riesgo estimado durante el proceso de análisis de riesgo con un criterio dado para determinar la importancia del riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. Normalmente incluye la evaluación, tratamiento, aceptación y comunicación del riesgo. Estas actividades se enfocan a manejar la incertidumbre relativa de las amenazas detectadas.

Aceptación del riesgo: Decisión de aceptar el riesgo

Tratamiento del riesgo: Proceso de tratamiento de la selección e implementación de controles para modificar el riesgo.

Riesgo residual: El riesgo remanente después del tratamiento del riesgo

Declaración de aplicabilidad (SOA): Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del SGSI.

Política: Intención y dirección general expresada formalmente por la gerencia.

Políticas de Seguridad: Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños informáticos.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

En este capítulo se describe la metodología aplicada para realizar la investigación. Para que esta metodología se aceptada epistemológicamente, se tomo como referencia los marcos normativos de las ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27003; así como la metodología de gestión de riesgos de TI MagerIT.

3.1. Para el análisis de brechas de seguridad de la información

El análisis de brechas se realizó comparando el estado actual de la organización con los requisitos establecidos en la ISO/IEC 27002.

Para dicho análisis se debe realizó un estudio a los procesos de la organización, determinado el porcentaje de cumplimiento para cada dominio de la ISO/IEC 27002.

Para cumplir con esta actividad se elaboró la siguiente tabla a modo de papel de trabajo:

Tabla N° 4. Formato para la evaluación de brechas de seguridad

Ítem	Dominio	Cumple (S/N)	Nivel de cumplimiento
1	Generalidades		
2	Seguridad lógica		
3	Seguridad de personal		
4	Seguridad física ambiental		
5	Inventario de activos y clasificación de la información		
6	Administración de las operaciones y comunicaciones		
7	Adquisición, desarrollo y mantenimiento de sistemas informáticos		
8	Procedimientos de respaldo		
9	Gestión de incidentes de seguridad de información		

Fuente: elaboración propia en base a los formatos guía de la norma ISO/IEC 27002

3.2. Para el análisis y evaluación de riesgos de TI

El objetivo del análisis de riesgos fue determinar y evaluar el riesgo de los activos de TI que forman parte de los procesos y servicios de la gestión académica pregrado que brinda la Oficina General de TI de la Universidad Nacional de Cajamarca, siguiendo los pasos establecidos por la metodología MagerIT. Los datos de esta etapa fueron obtenidos mediante entrevistas, llenado de formularios realizados en colaboración con del jefe de la Oficina General de TI.

3.2.1. Caracterización de los activos

El objetivo de las actividades englobadas en esta actividad fue identificar los activos que componen los servicios y procesos que se desarrollan en la gestión académica pre – grado en la Oficina General de TI de la Universidad Nacional de Cajamarca; así como también se definió las dependencias entre ellos. Paso siguiente se realizó la valoración según la importancia que tenga cada activo en el caso de estudio.

a. Identificación de los activos

El objetivo de la actividad fue identificar los activos que forman parte de los servicios y procesos de la gestión académica que brinda la Oficina General de TI de la Universidad Nacional de Cajamarca, determinando sus características y atributos del activo a tratar. Los cuales fueron código, nombre y una descripción.

Consideraciones previas

Para el desarrollo de esta tarea se tomó en cuenta lo siguiente.

- En el caso del código usado para cada activo se utilizó el código del grupo de activo al que pertenece (del catálogo que MAGERIT ofrece) seguido de dos letras más agregados por el autor, que en su mayor parte son primeras letras de las palabras que forman el nombre de cada activo.
- Para los nombres de cada activo se utilizó el que tiene asignado en la Oficina General de TI.
- Se agregó una columna titulada Descripción del activo cuya información fue obtenida de la entrevista con el jefe encargado de la Oficina General de TI.

Desarrollo de la actividad

La metodología MAGERIT nos plantea agrupar a los activos en 8 capas según su tipo, como son:

[S] Servicios

[SW] Aplicaciones

[HW] Equipos Informáticos

[COM] Redes de comunicaciones

[MEDIA] Soportes de información

[AUX] Equipamiento auxiliar

[L] Instalaciones

[P] Personal

En esta tarea se identificaron los activos que intervienen con la gestión académica de la Universidad Nacional de Cajamarca. Se decidió delimitar el análisis y gestión de riesgos en los activos de TI, y aplicarlo solo en la gestión académica pregrado de la Universidad Nacional de Cajamarca porque consideramos que dicha gestión es un elemento primordial en la institución, que si este servicio llegará a faltar o pueda verse afectado puede perjudicar tanto a la institución como a los usuarios ya sea internos o externos.

Los datos fueron obtenidos en una entrevista realizada con el Administrador de la Oficina General de TI, cuyos resultados pueden ser vistos en el anexo Metodología MAGERIT.

A continuación, describimos los 8 grupos en los cuales se dividen los activos de TI en la Oficina General de TI.

[S] Servicios. Son servicios auxiliares que forman parte de la Oficina General de TI.

[SW] Software. (Aplicaciones informáticas). Los aplicativos que forman parte de la Oficina General de TI.

[HW] Hardware (equipos informáticos). Los medios materiales, físicos, destinados a soportar directamente o indirectamente los servicios. Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratadas.

[COM] Redes de Comunicaciones. Los dispositivos físicos que permiten almacenar la información de forma permanente de la Oficina General de TI.

[MEDIA] Soportes de Información. Se consideran dispositivos físicos que permitan almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[AUX] Equipamiento auxiliar. Se consideran otros equipos que sirven de soporte, sin estar directamente relacionados con datos.

[L] Instalaciones. Es el local de la UNC, Unida de Red Telemática, donde se encuentran los equipos que brindan los servicios y el personal encargado de tener en funcionamiento óptimo para los equipos.

[P] Personal. Personas que trabajan en la Oficina General de TI.

b. Dependencias entre los activos

Identificar el grado de dependencia donde la seguridad de los activos que son superiores, depende de los activos inferiores de la Oficina General de TI de la Universidad Nacional de Cajamarca.

Consideraciones previas

Para el desarrollo de la tarea se realizaron las siguientes actividades.

- Identificación de los activos superiores e inferiores con la colaboración del jefe de la Unidad de Administración de la Red.
- Se utilizó la estructura que plantea MAGERIT para definir las dependencias agrupándolos en capas.

En la siguiente tabla, teniendo en cuenta las dependencias para operar, funcionalidad y almacenamiento de datos, se determina la siguiente matriz de dependencias entre activos (según el tipo de activo que corresponda).

Tabla N° 5. Matriz dependencia de activos según su la capa a la que pertenecen

	[S]	[SW]	[HW]	[COM]	[MEDIA]	[AUX]	[L]	[P]
[SERV]	-	x	x	x		X	X	x
[SW]		-	x	x	x	x	X	X
[HW]			-			x	X	X
[COM]				-		x	X	X
[MEDIA]					-		X	X
[AUX]						-	x	X
[L]							-	X
[P]								-

Fuente: Elaborado por los autores.

Desarrollo de la actividad

Como resultado de la matriz de dependencia podemos observar que:

- Los activos que pertenecen al grupo de servicios [S] dependen de los activos que forman parte de [SW], [HW], [COM], [AUX], [L] y [P].
- Los activos que forman parte del grupo de Software [SW] dependen de los activos del grupo de [HW], [COM], [MEDIA], [AUX], [L] Y [P].
- Los activos que forman parte del grupo de Hardware [HW], dependen de los activos del grupo de [AUX], [L] y [P].
- Los activos de Redes de Comunicaciones [COM] dependen de los activos de [AUX], [L] y [P].
- Los activos de Soportes de Comunicación [MEDIA] dependen de los activos que forman parte de los activos del grupo [L] y [P].
- Los activos que forman parte del grupo de Equipamiento Auxiliar [AUX], dependen de los activos que forman parte de los activos de los grupos [L] y [P].
- Los activos del grupo de Instalaciones [L] dependen de los activos del grupo [P].
- A continuación, observamos el árbol de dependencias con los activos de TI de la Oficina General de TI.

c. Valoración de los activos

El objetivo de la tarea fue identificar en qué dimensión es valioso el activo de TI perteneciente al sistema académico de la Oficina General de TI de la Universidad Nacional de Cajamarca.

Consideraciones previas

Para el desarrollo de la actividad se hizo lo siguiente:

- Se entrevistó al jefe de la Oficina General de TI, para obtener los datos a valorar.
- Valorar los activos en las 5 dimensiones que MAGERIT plantea para valorar el activo.
- Se utilizaron los criterios de valoración que brinda MAGERIT. Pero algunos de ellos fueron excluidos, más adelante se detalla las razones de porque fueron excluidos.

Se consideraron datos importantes como dimensiones y criterios de valuación.

a. Dimensiones

   [D] Disponibilidad

   [I] Integridad de los datos

   [C] Confidencialidad de los datos

   [A] Autenticidad de los usuarios y de la información

   [T] Trazabilidad del servicio y de los datos

b. Criterios de valoración

   MAGERIT nos plantea diferentes criterios de valoración. Para el presente proyecto solo se han elegido las que se acomodan a los procesos y servicios que ofrece la Oficina General de TI de la Universidad Nacional de Cajamarca.

Se excluyeron los siguientes criterios:

- *Obligaciones legales*. Se excluyó porque no se evalúa el complimiento de contrato con terceros o con entidades supervisoras por que las tecnologías de la Universidad no brindan servicios de ese tipo solo ofrece de carácter interno.
- *Interese comerciales o económicos.* Este criterio se excluyó ya que los servicios y proceso de la Oficina General de TI son de uso interno.
- *Orden Público.* Se excluyó porque los servicios que ofrece la Oficina General de TI son de uso interno.
- *Pérdida de confianza.* Este criterio se refiere a la publicidad negativa de la organización en caso se vea afectada por alguna amenaza. Se excluyó porque el Área de Red Telemática es una unidad que se encarga de

administrar el uso correcto de los servicios dentro de la organización no fuera de ella.

- *Persecución de delitos.*
- Tiempo de recuperación del servicio. Se excluyó este servicio ya que el proyecto de investigación se está evaluando lo que sucedería si algún activo se ve afectado, sino solo plantea si la metodología utilizada ayuda a mejorar la gestión de riesgos en la Oficina General de TI.
- Información clasificada (nacional). La información que se maneja en la Oficina General de TI es solo de carácter interno y si se necesita información debe solicitarla con un oficio autorizado. Por eso se excluyó
- Información clasificada (europea)

Los criterios que se utilizaron son los que veremos a continuación:

Tabla N° 6. Criterios de evaluación de Activos

Niveles	[pi] Información de carácter personal	[si] Seguridad	[da] Interrupción del servicio	[olm] Operaciones	[adm] Administración y gestión
1 0		probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios		Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística	
8 Y 9		probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios	9.da Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones 9.da2 Probablemente tenga un serio impacto en otras organizaciones	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística	9.adm probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre.
7		probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves	7.da Probablemente cause una interrupción seria de las actividades propias de la Or-ganización con un impacto significativo en otras organizaciones 7.da2 Probablemente tenga un gran	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística	7.adm probablemente impediría la operación efectiva de la Organización

			impacto en otras organizaciones		
6	6.pi1 probablemente afecte gravemente a un grupo de individuos 6.pi2 probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.				
5	5.pi1 probablemente afecte gravemente a un individuo 5.pi2 probablemente quebrante seriamente leyes o regulaciones		5.da Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones 5.da2 Probablemente cause un cierto impacto en otras organizaciones	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local	5.adm probablemente impediría la operación efectiva de más de una parte de la organización
4	4.pi1 probablemente afecte a un grupo de individuos 4.pi2 probablemente quebrante leyes o regulaciones				
3	3.pi1 probablemente afecte a un individuo 3.pi2 probablemente suponga el incumplimiento de una ley o regulación	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente	3.da Probablemente cause la interrupción de actividades propias de la Organización	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)	3.adm probablemente impediría la operación efectiva de una parte de la Organización
2	2.pi1 pudiera causar molestias a un individuo 2.pi2 pudiera quebrantar de forma leve leyes o regulaciones				
1	1.pi1 pudiera causar molestias a un individuo	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente		Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)	1.adm pudiera impedir la operación efectiva de una parte de la Organización

Fuente: Elaborada propia en base a los criterios de valoración que plantea la metodología Magerit.

Los criterios que se utilizaron para valorar los activos tienen una escala del 0 a 10. En la siguiente tabla mostramos los niveles.

Tabla N° 7. Escala de evaluación

ESCALA DE VALOR		
VALOR		CRITERIO
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
8-6	alto	daño grave
5-3	medio	daño importante
2-1	bajo	daño menor

Fuente: MAGERIT - V 3.0. Libro 1: Método

Desarrollo de la actividad

Para el desarrollo de la actividad se elaboró una tabla con los activos identificados y en colaboración del jefe encargado de la Oficina General de TI se fue valorando el activo de acuerdo a las 5 dimensiones que MAGERIT plantea teniendo en cuenta los criterios mencionados anteriormente para poder dar el valor de dicho activo en cada dimensión como resultado obtuvimos el valor del activo, el cual se obtuvo promediando cada valor de la dimensión en la que este se vio afectado.

3.2.2. Caracterización de las amenazas

El objetivo de las actividades englobadas en esta tarea fue identificar las posibles amenazas que se pueden materializar sobre los activos, así como estimar la frecuencia de ocurrencia y degradación que causan en los activos.

a. Identificación de las amenazas

El objetivo de la actividad fue identificar las amenazas relevantes sobre cada activo de la Oficina General de TI de la Universidad Nacional de Cajamarca.

Consideraciones previas

Para realizar esta tarea se tuvo en consideración lo siguiente:

- Se utilizaron las amenazas que nos brinda MAGERIT en el libro II catálogo de Amenazas.

Las amenazas según nos plantea la metodología MAGERIT los clasifica en 4 grupos:

[N] Desastres Naturales

[I] De origen Industrial

[E] Errores y fallos no intencionados

[A] Ataque intencionados

Estas a su vez pueden atacar en más de una dimensión, para esto MAGERIT la dimensión atacada de la más a menos relevante.

- Se utilizó la lista de activos identificados en la Oficina General de TI.

Desarrollo de la actividad

Para el desarrollo de la actividad se realizó una entrevista con el jefe encargado de la Oficina General de TI de la Universidad Nacional de Cajamarca. Se utilizó la lista completa de amenazas por cada activo y se fue marcando con una X la amenaza que podría afectar a al activo.

b. Valoración de las amenazas

El objetivo de la actividad fue determinar cuan afectado se vería el activo en caso la amenaza se materializará.

Consideraciones previas

Se utilizó la tabla de degradación de activos que brinda MAGERIT, la cual vemos a continuación.

Tabla N° 8. Degradación de activos

PORCENTAJE	NIVEL
100%	MA
90%	MA
80%	A
70%	A
60%	A
50%	M
40%	M
30%	M
20%	B
10%	B
5%	MB

1%	MB

Fuente: MAGERIT - V 3.0. Libro 1: Método

Desarrollo de la actividad

Para calcular la degradación se tomó en cuenta los valores que se proporcionan en la tabla valoración de activos. Se valoró la degradación de cada activo teniendo en cuenta que para algunas amenazas afectan a hasta en
3 dimensiones como vemos en la siguiente tabla.

Tabla N° 9. Escala cualitativa de degradación de activos

Escalas cualitativas de degradación de activos	
Rojo	Mayor desgaste
Amarillo	Medio desgaste
Verde	Bajo desgaste

Fuente: Elaborada MAGERIT - V 3.0. Libro 1: Método

Para determinar el nivel de la amenaza se utilizó la tabla de escala cuantitativa de degradación definida por la entidad en un rango de 0.01 a 1 como vemos a continuación:

Tabla N° 10. Rangos de valoración de degradación de activos

Escalas cuantitativas de degradación definida por la entidad	
Nivel	Rango
Muy alto	0.81 a 1.00
Alto	0.51 a 0.80
Medio	0.21 a 0.5
Bajo	0.06 a 0.2
Muy bajo	0.01 a 0.05

Fuente: Elaborada en base a MAGERIT - V 3.0. Libro 1: Método

3.2.3. Determinación del impacto

El objetivo fue determinar el impacto que las amenazas identificadas causan en el activo en caso estas se llegaran a materializar.

Consideraciones Previas

- Se obtuvo el valor de cada activo de la Oficina General de TI de la Universidad Nacional de Cajamarca.
- Se obtuvo el nivel de desgaste de cada activo de acuerdo a las posibles amenazas a las cuales este se vea expuesto.

Desarrollo de la actividad

Para obtener el impacto se multiplicó el valor del activo y el desgaste del mismo obtenidos en las actividades anteriores.

Para determinar el nivel de impacto se elaboró una tabla de escalas cualitativas de impacto definidas por la entidad.

Tabla N° 11. Escala cualitativa de impacto

Escalas cualitativas de impacto definida por la entidad		
Nivel	Escala cualitativa	**Rango**
5	Muy alto	7.01 a 10
4	Alto	3.01 a 7
3	Medio	2.01 a 3
2	Bajo	0.06 a 2
1	Muy bajo	0.01 a 0.05

Fuente: Elaborada en base a MAGERIT - V 3.0. Libro 1: Método

3.2.4. Determinación de la probabilidad de ocurrencia

El objetivo de la tarea fue determinar cuan probable o improbable es que se materialice la amenaza.

Consideraciones previas

Se utilizó la tabla de probabilidad de ataque que platea la metodología MAGERIT para determinar la probabilidad en que una amenaza se materialice. La Probabilidad se trabajó para cada 2 años.

Tabla N° 12. Probabilidad de Ocurrencia de una amenaza

Nivel	Escala cualitativa	Significado
5	Muy Frecuente	Se espera que la amenaza ocurra más de tres veces al año.
4	Frecuente	Se espera que la amenaza ocurra al menos dos veces en el último año
3	Normal	Se espera que la amenaza se presente al menos una vez en el último año.
2	Poco Frecuente	Se espera que la amenaza se presente al menos una vez en los últimos 2 años.
1	Muy Poco Frecuente	No se ha presentado en los últimos 2 años.

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método

Desarrollo de la actividad

Se determinó la probabilidad de impacto en colaboración del jefe encargado de la Oficina General de TI de la Universidad Nacional de Cajamarca, utilizando la escala cualitativa mencionada anteriormente.

3.2.5. Mapa de Riesgo

El objetivo de la tarea fue obtener el mapa de riesgo o de calor para determinar el estado de riesgo.

Consideraciones previas

Se utilizó la tabla de escala de riesgos planteada por MAGERIT

Tabla N° 13. Escalas del riesgo

NIVEL	ESCALA CUALITATIVA	NMÓNICO
5	Critico	MA
4	Importante	A
3	Apreciable	M
2	Bajo	B
1	Despreciable	MB

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método

Desarrollo de la actividad

Con ayuda del jefe de la Oficina General de TI se determinó cuáles fueron los niveles de riesgo para la Unidad.

Tabla N° 14. Mapa del calor del riesgo

		Impacto				
		5	4	3	2	1
Probabilidad	5	MA	MA	A	M	B
	4	MA	MA	A	M	B
	3	A	A	M	B	MB
	2	M	M	B	MB	MB
	1	B	B	MB	MB	MB

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método

3.2.6. Determinación del riesgo

El objetivo de la tarea fue determinar el riesgo de cada activo con sus respectivas amenazas.

Consideraciones previas

Se estableció los niveles de riesgo con la colaboración del jefe de la Oficina General de TI de la Universidad Nacional de Cajamarca.

Tabla N° 15. Nivel de tolerancia

Nivel	Escala	Rango
5	Critico	16 a 25
4	Importante	13 a 15
3	Apreciable	7 a 12
2	Bajo	5 a 6
1	Despreciable	1 a 4

Fuente: Elaborada por los autores en base a MAGERIT - V 3.0. Libro 1: Método

Desarrollo de la actividad

Para determinar el nivel de riesgo se multiplicó el impacto por la probabilidad de ocurrencia, de acuerdo a ese resultado se calificó en la escala de tolerancia cual era nivel que pertenecía.

3.2.7. Evaluación del riesgo

Determinar cuáles de los riesgos obtenidos son los más críticos.

Consideraciones previas

Se utilizó el mapa de calor para saber cuál de los riesgos obtenidos eran los más críticos.

Desarrollo de la actividad

Se evaluó cada riesgo con la probabilidad de impacto en escalas cualitativas y se fue completando hasta determinar cuál de ellos eran los más críticos.

3.3. Tratamiento del riesgo

Para mitigar el actuar de las amenazas representadas por el riesgo, planteamos una seria de salvaguardas que podrán controlar el imparto que estas tengan en los activos.

3.3.1. Caracterización de las salvaguardas

a. Identificación de las salvaguardas

Identificar las salvaguardas que nos permitan prevenir, acotan o consolidad el efecto de la amenaza en caso esta se llegara a materializar.

Consideraciones previas

Para el desarrollo de la tarea se utilizó el catálogo de Salvaguardas que brinda MAGERIT.

Tabla N° 16. Catálogo de salvaguardas

Código	Nombre
PROTECCION A SERVICIOS	
S	Protección de los Servicios
S.A	Aseguramiento de la disponibilidad
S.start	Aceptación y puesta en operación
S.SC	Se aplican perfiles de seguridad
S.op	Explotación
S.CM	Gestión de cambios (mejoras y sustituciones)
S.end	Terminación
S.www	Protección de servicios y aplicaciones web
S.email	Protección del correo electrónico
S.dir	Protección del directorio
S.dns	Protección del servidor de nombres de dominio (DNS)
S.TW	Teletrabajo
PROTECCIÓN DE LAS APLICACIONES	
SW	Protección de las Aplicaciones Informáticas
SW.A	Copias de seguridad (backup)
SW.start	Puesta en producción
SW.SC	Se aplican perfiles de seguridad
SW.op	Explotación / Producción
PROTECCIÓN DE LOS EQUIPOS	
HW	Protección de los Equipos Informáticos

HW.start	Puesta en producción
HW.SC	Se aplican perfiles de seguridad
HW.A	Aseguramiento de la disponibilidad
HW.op	Operación
HW.CM	Cambios (actualizaciones y mantenimiento)
HW.end	Terminación
HW.PCD	Informática móvil
HW.print	Reproducción de documentos
HW.pabx	Protección de la centralita telefónica (PABX)
PROTECCION DE LAS COMUNICACIONES	
COM	Protección de las Comunicaciones
COM.start	Entrada en servicio
COM.SC	Se aplican perfiles de seguridad
COM.A	Aseguramiento de la disponibilidad
COM.aut	Autenticación del canal
COM.I	Protección de la integridad de los datos intercambiados
COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op	Operación
COM.CM	Cambios (actualizaciones y mantenimiento)
COM.end	Terminación
COM.internet	Internet: uso de acceso a
COM.wifi	Seguridad Wireless (WiFi)
COM.mobile	Telefonía móvil
COM.DS	Segregación de las redes en dominios
| **PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN**	
MP	Protección de los Soportes de Información
MP.A	Aseguramiento de la disponibilidad
MP.IC	Protección criptográfica del contenido
MP.clean	Limpieza de contenidos
MP.end	Destrucción de soportes
PROTECCIÓN DE ELEMENTOS AUXILIARES	
AUX	Elementos Auxiliares
AUX.A	Aseguramiento de la disponibilidad
AUX.start	Instalación
AUX.power	Suministro eléctrico
AUX.AC	Climatización
AUX.wires	Protección del cableado
SEGURIDAD FISICA-PROTECCIÓN DE LAS INSTALACIONES	
L	Protección de las Instalaciones
L.design	Diseño

L.depth	Defensa en profundidad
L.AC	Control de los accesos físicos
L.A	Aseguramiento de la disponibilidad
L.end	Terminación
SALVAGUARDAS RELATIVAS AL PERSONAL	
PS	Gestión del Personal
PS.AT	Formación y concienciación
PS.A	Aseguramiento de la disponibilidad

También se utilizó la tabla de tipos de salvaguardas, la cual vemos a continuación.

Tabla N° 17. Tipos de Salvaguardas

Efecto	**Tipo**	
	Código	**Nombre**
Preventivas	[PR]	Preventivas
	[DR]	Disuasorias
	[EL]	Eliminatorias
acotan la degradación	[IM]	Minimizadoras
	[CR]	Correctivas
	[RC]	recuperativas
consolidan el efecto de las demás	[MN]	De monotorización
	[DC]	de detección
	[AW]	de concienciación
	[AD]	administrativas

Desarrollo de la actividad

Para el desarrollo de la actividad se utilizaron los activos que tenían el nivel de riesgo MUY CRITICO e IMPORTANTE. Para cada riesgo se eligió la correspondiente salvaguarda, considerando el tipo y el efecto que estas tenían en el riesgo.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

En este capítulo se describe la aplicación de la metodología en el capítulo anterior y los resultados que se obtuvieron en cada una de las actividades y tareas.

4.1. Evaluación de la seguridad de la información

4.1.1. Política general del SGSI

Se decidió implantar un Sistema de Gestión de Seguridad de Información (SGSI), que se suscribe bajo la siguiente política general.

1. El Comité del SGSI define y revisa los objetivos del SGSI, enfocados a la conservación de la confidencialidad, disponibilidad e integridad de los activos de información, considerados como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios. Cumpliendo todos los requisitos legales, reglamentarios y contractuales que le sean de aplicación, que incrementa de esta manera, la confianza de nuestros clientes, accionistas y otras partes interesadas.

2. El diseño, implantación y mantenimiento del SGSI se apoya en los resultados de un proceso continuo de análisis y gestión de riesgos, del que se derivan las acciones a desarrollar en materia de seguridad dentro del Alcance del SGSI.

3. El comité del SGSI establece los criterios de evaluación del riesgo de manera que todos aquellos escenarios que impliquen un nivel de riesgo inaceptable sean tratados adecuadamente.

4. Se debe implantar las medidas requeridas para la formación y concientización del personal en seguridad de la información. Asimismo, en caso de que los trabajadores incumplan las políticas de seguridad, la dirección podrá ejecutar las medidas disciplinarias que se encuentren dentro del marco legal aplicable.

5. La Oficina General de TI se compromete con la implantación, mantenimiento y mejora del SGSI facilitando los medios y recursos que sean necesarios.

6. Es responsabilidad del oficial de seguridad de Información asegurar el buen funcionamiento del SGSI.

7. La presente política es de aplicación a todo el personal y recursos que se encuentran dentro del Alcance del SGSI. Se pone en su conocimiento y es comunicada a todas las partes interesadas.

4.1.2. Análisis de brechas en la seguridad de la información

Para el análisis de brechas, se realizó una evaluación de cumplimiento de cada uno de los controles determinados por la ISO/IEC 27002, con la finalidad de determinar el Nivel de aplicabilidad de la norma (SOA) en la Universidad Nacional de Cajamarca. Los controles que no están considerados, se debe a que la universidad no los aplica.

La tabla siguiente muestra los resultados de ese análisis:

Tabla N° 18. Análisis de brechas de cumplimiento de los controles de la ISO/IEC 27002

Control ISO	Requerimiento Objetivo de control	Control	¿Se cumple?	Nivel de cumplimiento
5. Política de seguridad				
5.1	**Política de Seguridad de la Información**			
5.1.1	Se tiene documento de la política de seguridad de la Información	Un documento de política de seguridad de la información debería ser aprobado por la Dirección y debería ser publicado y comunicado a todos los empleados y terceras partes.	SI	70%
5.1.2	Se hace revisión y evaluación de este documento y se promulga su lectura y aplicación.	La política de seguridad de la información se debería revisar a intervalos planificados o en el caso de que se produzcan cambios significativos para asegurar la idoneidad, adecuación y la eficiencia de la continuidad.	NO	
6. Organización de la Seguridad de la Información				
6.1	**Organización Interna**			
6.1.1	Compromiso de las Dirección con la seguridad de la información	La Dirección deberá dar un activo soporte a la seguridad dentro de la organización a través de directivas claras, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de seguridad de la información.	SI	60%

6.1.2	Coordinación de la Seguridad de la Información	Las actividades relativas a la seguridad de la información deberían ser coordinadas por representantes de las diferentes partes de la organización con los correspondientes roles y funciones de trabajo.	NO	
6.1.3	Asignación de responsabilidades sobre la seguridad de la información	Debería definirse claramente todas las responsabilidades de seguridad de la información.	NO	
6.1.4	Proceso de Autorización de recursos para el procesamiento/tratamiento de información	Debería definirse e implantarse un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información.	NO	
6.1.5	Acuerdos de confidencialidad	Debería identificarse y revisarse de una manera regular los requisitos de los acuerdos de confidencialidad o no revelación que refleje las necesidades de la organización para la protección de la información.	NO	
6.1.6	Contacto/Cooperación con las autoridades	Se debería mantener contactos adecuados con las autoridades que corresponda.	NO	
6.1.7	Contacto con grupos de especial interés	Se deberían mantener contactos apropiados con grupos de interés especial u otros foros especialistas en seguridad y asociaciones profesionales.	NO	
6.1.8	Se realiza Auditoría interna - Revisiones independientes de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implantación debería revisarse de una manera independiente a intervalos planificados o cuando se producen cambios significativos en la implantación de la seguridad.	NO	
6.2	**Seguridad de acceso de terceras partes**			
6.2.1	Identificación de riesgos de acceso de terceras partes	Cuando el negocio requiera de partes externas, deberían identificarse los riesgos de la información de la organización y de los dispositivos de tratamiento de la información, así como la implantación de los controles adecuados antes de garantizar el acceso.	NO	
6.2.2	Consideraciones de seguridad en contratos con clientes	Todos los requisitos de seguridad que se hayan identificado deberían ser dirigidos antes de dar acceso a los clientes a los activos o a la información de la seguridad.	NO	
6.2.3	Consideraciones de seguridad en contratos con terceros	Los acuerdos que comparten el acceso de terceros a recurso de tratamiento de información de la organización deben basarse en un contrato formal que tenga o se refiera a todos los requisitos de la seguridad que cumpla con las políticas y normas de seguridad de la organización. El contrato debe asegurar que no hay malentendidos entre la organización y los terceros. Las organizaciones deben verse compensadas hasta la indemnización de sus suministradores.	NO	
7. Gestión de activos				

7.1	**Responsabilidad sobre los activos**			
7.1.1	Inventario de activos tecnológicos y de la información.	Todos los activos deberían ser claramente identificados y deberían prepararse y mantenerse un inventario de todos los activos importantes.	SI	70%
7.1.2	Responsables/Propietarios de los activos tecnológicos	Toda la información y los activos asociados con los recursos para el tratamiento de la información deberían ser propiedad de una parte designada de la organización.	NO	
7.1.3	Uso aceptable de los activos tecnológicos	Las reglas de uso aceptable de la información y los activos asociados con el tratamiento de la información deberían ser identificadas, documentadas e implantadas.	SI	55%
7.2	**Clasificación de la información**			
7.2.1	Normas y directrices para clasificación de la información	La información debería estar clasificada, según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.	NO	
7.2.2	Identificación, etiquetado y manejo de la información	Debería desarrollarse un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización.	NO	
8. Seguridad ligada a los Recursos Humanos				
8.1	**Seguridad en actividades previas en la contratación**			
8.1.1	Inclusión de la seguridad en las funciones y responsabilidades del trabajo	Las funciones y responsabilidades de seguridad para los empleados, contratistas y usuarios de tercera parte deberían ser definidas y documentadas de acuerdo con la política de seguridad de la información de la organización.	NO	
8.1.2	Investigación del personal que va a ser contratado	La comprobación de los antecedentes de todos los candidatos al puesto de trabajo, los contratistas o los usuarios de tercera parte deberían ser llevadas a cabo de acuerdo con la legislación aplicable, las reglamentaciones y éticas de manera proporcional a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos considerados.	SI	80%
8.1.3	Términos y condiciones laborales	Como parte de las obligaciones contractuales, los empleados, contratistas y usuarios de tercera parte deberían aceptar y firmar los términos y condiciones de su contrato de trabajo, que deberían establecer sus responsabilidades, así como las de la organización en lo relativo a la seguridad de la información.	SI	80%
8.2	**Seguridad en actividades durante el desempeño de las funciones**			

8.2.1	Responsabilidades de la Dirección	La Dirección debería requerir a los empleados, contratistas y de tercera parte, el aplicar la seguridad de acuerdo a lo establecido en las políticas y procedimientos de la organización.	NO	
8.2.2	Conciencia y formación sobe la seguridad de la información: educación y entrenamiento	Todos los empleados de la organización y, cuando corresponda, los contratistas y los usuarios de tercera parte, deberían recibir una formación y concientización adecuadas y actualizadas de las políticas y procedimientos, según corresponda a su puesto de trabajo.	NO	
8.2.3	Procesos disciplinarios	Debería existir un proceso disciplinario formal para los empleados que hayan provocado alguna brecha de seguridad.	NO	
8.3	**Fin de contrato o cambio de funciones**			
8.3.1	Responsabilidades en la terminación del contrato	Las responsabilidades para llevar a cabo la finalización o cambio de puesto de trabajo deberían estar claramente definidas y asignadas.	NO	
8.3.2	Devolución/restitución de activos tecnológicos	Todos los empleados, contratistas y usuarios de tercera parte deberían devolver los activos de la organización que tengan en posesión a la finalización de su empleo, contrato o acuerdo.	NO	
8.3.3	Eliminación de permisos sobre los activos	Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados, contratistas y usuarios de tercera parte, debería ser retirada a la finalización de la contratación o del acuerdo, o adaptados según los cambios.	NO	
9. Seguridad física y del entorno				
9.1	**Áreas seguras/restringidas**			
9.1.1	Perímetro de Seguridad Física	Debería usarse perímetros de seguridad (barreras tales como muros, puertas de entrada con control a través de tarjeta o mesas de recepción tripuladas) para proteger las áreas que contienen la información y los recursos de tratamiento de la información.	SI	40%
9.1.2	Controles físicos de entrada	Las áreas seguras deberías estar protegidas por controles de entrada adecuados para asegurar que únicamente se permita el acceso al personal autorizado.	SI	50%
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	Se debería diseñar y aplicar la seguridad física para las oficinas, despachos y recursos.	SI	50%
9.1.4	Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar una protección física contra el daño por fuego, inundación, terremoto, explosión, malestar social y otras formas de desastres naturales o provocadas por el hombre.	SI	55%

9.1.5	Trabajo en áreas restringidas	Se debería diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.	SI	70%
9.1.6	Acceso público, envíos y áreas de carga	Deberían controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos donde pueda acceder personal no autorizado, y si es posible, dichos puntos deberías estar aislados de los recursos de tratamiento de la información para evitar accesos no autorizados.	NO	
9.2	**Seguridad de los equipos**			
9.2.1	Ubicación, instalación y protección de equipos tecnológicos	Los equipos deberías estar situados o protegidos para reducir los riesgos de las amenazas y los riesgos del entorno, así como de las oportunidades de acceso no autorizado.	SI	80%
9.2.2	Seguridad en el suministro de electricidad y servicios (utilities)	Los equipos deberías estar protegidos de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	NO	
9.2.3	Seguridad en el cableado	El cableado eléctrico y de telecomunicaciones que transmiten datos a los servicios de soporte de la información debería estar protegido de interceptación o de daños.	SI	60%
9.2.4	Mantenimiento de equipos	Los equipos deberías ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	SI	70%
9.2.5	Seguridad de equipos fuera de las áreas seguras	Se debería aplicar medidas de seguridad a los equipos fuera de los locales de la organización, teniéndose en cuenta los diferentes riesgos de trabajar fuera de los locales de la organización.	SI	45%
9.2.6	Destrucción y reutilización de equipos	Todos los elementos del equipo que contengan medios de almacenamiento deberían ser comprobados para asegurar que todo dato sensible y software bajo licencia se ha borrado o sobrescrito, previamente a su utilización.	NO	
9.2.7	Traslado de activos fuera de la organización	Los equipos, la información o el software no deberían sacarse fuera de las instalaciones sin previa autorización.	NO	
10. Gestión de las comunicaciones y las operaciones				
10.1	**Procedimientos y responsabilidades operativas**			
10.1.1	Documentación de procesos operativos	Se debería implantar, mantener procedimientos operacionales y estar disponibles para todos los usuarios que lo necesiten.	SI	35%
10.1.2	Control de Cambios	Se deberían controlar los cambios en los recursos y sistemas de tratamiento de la información.	NO	

10.1.3	Segregación de funciones y tareas	Las tareas y áreas de responsabilidad deberían segregarse para reducir la posibilidad de modificaciones no autorizadas y no intencionadas o el mal uso de los activos de la organización.	NO	
10.1.4	Separación de los ambientes de Desarrollo, prueba y producción	Deberían separarse los recursos para el desarrollo, las pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema operativo.	SI	70%
10.2	**Gestión de la provisión de servicios contratados con terceros**			
10.2.1	Entrega de servicios	Deberían asegurarse de que los controles de seguridad, los niveles de entrega y definiciones del servicio incluido en el acuerdo de entrega del servicio por tercera parte se implantan, se ponen en funcionamiento y son mantenidos por la tercera parte.	NO	
10.2.2	Monitoreo y revisión de servicios de terceros	Los servicios, informes y registros proporcionados por las terceras partes deberían ser controlados y revisados regularmente, y también se deberían llevar a cabo auditorías regularmente.	NO	
10.2.3	Administración de cambios a servicios de terceros	Se deberían gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio implicados y la revalorización de los riesgos.	NO	
10.3	**Planificación y aceptación de sistemas**			
10.3.1	Gestión de capacidades	La utilización de los recursos debería controlarse y ajustarse y se deberían hacer proyecciones de los requisitos de capacidad futura para asegurar el comportamiento requerido del sistema.	NO	
10.3.2	Aceptación de sistemas	Debería establecerse un criterio e aceptación para los nuevos sistemas, las actualizaciones y las nuevas versiones; así como llevarse a cabo las pruebas adecuadas del (de los) sistema(s) durante el desarrollo y previamente a la aceptación.	NO	
10.4	**Protección contra software malicioso y código móvil**			
10.4.1	Controles contra código malicioso	Se debería implantar procedimientos de concienciación del usuario adecuados; así como controles de detección, prevención y recuperación para proteger contra código malicioso.	SI	95%
10.4.2	Controles contra código móvil	Cuando se autoriza el uso de código ambulante, la configuración debería asegurar que está operando un código ambulante autorizado de acuerdo a una política de seguridad claramente definida, y debería prevenirse la ejecución de código ambulante no autorizado.	NO	

10.5	**Copias de seguridad**			
10.5.1	Copias de respaldo de la información.	Se debería hacer copias de seguridad de la información y del software y ser comprobadas regularmente de acuerdo con la política de copias de seguridad acordadas.	SI	80%
10.6	**Gestión de la seguridad de red**			
10.6.1	Controles de la Red	Las redes deberían estar adecuadamente gestionadas y controladas, para estar protegidas de amenazas y para mantener la seguridad de los sistemas y aplicaciones que usan estas redes, incluyendo la información en tránsito.	NO	
10.6.2	Seguridad de los Servicios de Red	Las características de seguridad, los niveles de servicio, los requisitos de gestión para todos los servicios de red deberían estar identificadas e incluidas en todo acuerdo de servicio de red, aunque estos servicios se proporcionen desde dentro de la organización o sean subcontratados.	NO	
10.7	**Utilización de los soportes de información**			
10.7.1	Administración de medios removibles	Debería haber procedimientos para la gestión de los soportes desmontables.	NO	
10.7.2	Destrucción de medios	Debería deshacerse de los soportes de una manera segura y fuera de peligro cuando no se vaya a requerir su uso durante más tiempo, mediante procedimientos formales.	NO	
10.7.3	Procedimientos de manejo de la información	Se debería establecer procedimientos para el tratamiento y el almacenamiento de la información para proteger esta información de revelación no autorizada o mal uso.	NO	
10.7.4	Seguridad de la documentación de los sistemas	El sistema de documentación debería estar protegido contra accesos no autorizados.	NO	
10.8	**Intercambio de información**			
10.8.1	Políticas y procedimientos del intercambio de información	Se debería establecer políticas de intercambio formal, procedimientos y controles para proteger el intercambio de la información mediante el uso de todos los tipos de servicios de comunicación.	NO	
10.8.2	Acuerdos para el intercambio de información.	Se debería establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.	NO	
10.8.3	Medios físicos en movimiento	Los recursos que contienen información deberían estar protegidos contra el acceso no autorizado, el mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	NO	

10.8.4	Mensajería electrónica	La información implicada en el envío de mensajes electrónicos debería estar adecuadamente protegida.	NO	
10.8.5	Sistemas de información de negocios	Se debería desarrollar e implantar políticas y procedimientos para proteger la información asociada a la interconexión de sistemas de información entre organizaciones.	NO	
10.9	**Servicios de comercio electrónico**			
10.9.1	Comercio electrónico	La información implicada en el comercio electrónico realizado a través de rede públicas debería protegerse de las actividades fraudulentas, los litigios contra contratos, y la revelación o modificación no autorizada de la información.	NO	
10.9.2	Transacciones en línea	La información implicada en las transacciones online debería estar protegida para evitar la transmisión incompleta, las rutas erróneas, la alteración no autorizada del mensaje, la revelación no autorizada, la duplicación no autorizadas del mensaje.	NO	
10.9.3	Información de difusión pública	La integridad de la información que se hace disponible en el sistema públicamente disponible debería estar protegida para prevenir la modificación no autorizada.	NO	
10.10	**Seguimiento/Monitoreo**			
10.10.1	Registros de auditoría	Se debería efectuar registros de auditoría de las actividades del usuario, excepciones e incidencias de información, y mantenerse durante un periodo acordado para ayudar en investigaciones futuras y en el seguimiento y monitorización del control de accesos.	NO	
10.10.2	Seguimiento del uso de los sistemas	Se debería establecer procedimientos para el seguimiento del uso de los recursos de tratamiento de la información y revisarse regularmente los resultados del seguimiento de estas actividades.	NO	
10.10.3	Protección de registros de monitoreo	Los dispositivos de registro y el diario de información deberán estar protegidos contra la manipulación y los accesos no autorizados.	NO	
10.10.4	Registros de monitoreo de administradores y operadores	Las actividades de administrador del sistema y del operador del sistema deberán ser registradas.	NO	
10.10.5	Registro de fallas y errores	Los fallos deberían ser registrados, analizados y tomar las acciones adecuadas	NO	
10.10.6	Sincronía de relojes	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o dominio de seguridad deberían estar sincronizados con una precisión de tiempo acordada.	NO	

11. Control de accesos				
11.1	**Requerimientos de negocio para control de acceso**			
11.1.1	Política de Control de Acceso	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad para el acceso.	SI	90%
11.2	**Gestión de acceso de los usuarios**			
11.2.1	Registro de usuarios	Debería haber un procedimiento de registro formal de usuarios y de retirada del registro para conceder y revocar el acceso a todos los sistemas y servicios de información.	SI	100%
11.2.2	Administración de privilegios	La asignación y el uso de privilegios debería estar restringidos y controlados.	SI	90%
11.2.3	Administración de contraseñas de usuario (passwords)	La asignación de contraseñas debería ser controlada a través de un proceso formal de gestión.	SI	100%
11.2.4	Revisión de los permisos asignados a los usuarios	La Dirección debería revisar los derechos de acceso de los usuarios a intervalos regulares y utilizando un procedimiento formal.	SI	75%
11.3	**Responsabilidad de los usuarios**			
11.3.1	Uso de las contraseñas	Se debería requerir a los usuarios el seguir las buenas prácticas de seguridad en la selección y el uso de contraseñas.	SI	100%
11.3.2	Equipos desatendidos	Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada.	SI	60%
11.3.3	Política de escritorios y pantallas limpias	Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	SI	40%
11.4	**Control de acceso a la red**			
11.4.1	Políticas para el uso de los servicios de la red de datos	Únicamente se debería proporcionar a los usuarios el acceso a los servicios para los que específicamente se les haya autorizado el uso.	SI	100%
11.4.2	Autenticación de usuarios para conexiones externas	Se debería utilizar los métodos apropiados de autenticación para el control de acceso a los usuarios en remoto.	NO	
11.4.3	Identificación de equipos en la red	Debería considerarse la identificación automática del equipo como un medio de autenticación de las conexiones para las posiciones y equipos específicos.	SI	100%

11.4.4	Diagnóstico remoto y protección de la configuración de puertos	Se debería controlar acceso físico y lógico al diagnóstico y configuración de los puertos.	NO	
11.4.5	Segregación en la red	Los grupos de servicio de información, de usuarios y de sistema de información deberían estar segregados en redes.	SI	80%
11.4.6	Control de conexión a la red	Se debería restringir la capacidad de los usuarios a conectarse a la red en el caso de redes compartidas, especialmente para aquellas que traspasan las fronteras de la organización, en línea con la política de control de acceso y los requisitos de las aplicaciones de negocio.	NO	
11.4.7	Control de enrutamiento de la red	Los controles de direccionamiento deberían estar implantados para las redes, para asegurar que las conexiones de las computadoras y los flujos de información no violen la política de control de acceso a las aplicaciones del negocio.	NO	
11.5	**Control de acceso a los sistemas operativos**			
11.5.1	Procedimientos para inicio de sesión de las estaciones de trabajo	Se debería controlar el acceso al sistema operativo mediante un procedimiento de entrada seguro.	SI	80%
11.5.2	Identificación y autenticación de los usuarios.	Todos los usuarios deberían tener un identificador de usuario (ID) para su uso personal y único. Se debería elegir una técnica adecuada de autenticación para la conformación de la identidad de un usuario.	SI	100%
11.5.3	Sistema de administración de contraseñas.	Los sistemas para la administración de contraseñas deberían ser interactivos y asegurar la calidad de la contraseña.	SI	100%
11.5.4	Uso de las utilidades del sistema	El uso de los programas que pueden ser capaces de invalidar los controles del sistema y de la aplicación, deberían estar restringidos y estrictamente controlados.	NO	
11.5.5	Desconexión automática de sesión.	Las sesiones interactivas deberían cerrase después de un periodo de inactividad definido.	NO	
11.5.6	Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	Se debería usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.	NO	
11.6	**Control de acceso a la información y aplicaciones**			
11.6.1	Restricción de acceso a los sistemas de información	Debería restringirse el acceso de los usuarios y del personal de apoyo a la información y a las funciones del sistema de aplicación, de acuerdo con la política de control de acceso definida.	NO	

11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles deberían tener un entorno de computadores dedicados y aislados.	NO	
11.7	**Computación móvil y teletrabajo**			
11.7.1	Computación y comunicaciones móviles	Debería implantarse una política formal y debería adoptarse las apropiadas medidas de seguridad para proteger contra los riesgos de la utilización de computadores y comunicaciones móviles.	NO	
11.7.2	Teletrabajo	Se deberían desarrollar e implantar procedimientos, planes operacionales y una política para las actividades de teletrabajo.	NO	
12. Adquisición, desarrollo y mantenimiento de sistemas de información				
12.1	**Requisitos de seguridad de los sistemas de información**			
12.1.1	Análisis y especificaciones de los requerimientos de seguridad		NO	
12.2	**Procesamiento correcto en aplicaciones**			
12.2.1	Validación de los datos de entrada	La introducción de datos en las aplicaciones debería validarse para garantizar que dichos datos son correctos y adecuados.	NO	
12.2.2	Control del procesamiento interno	Debería incorporarse comprobaciones de validación a las aplicaciones para detectar cualquier corrupción de la información debida a errores de procesamiento o actos intencionados.	NO	
12.2.3	Integridad de los mensajes	Debería identificarse los requisitos para garantizar la autenticidad y proteger la integridad de los mensajes en las aplicaciones y deberían identificarse e implantarse controles adecuados.	NO	
12.2.4	Validación de los datos de salida	Los datos resultantes de una aplicación deberían ser validados para garantizar que el procesamiento de la información almacenada es correcto y resulta adecuado a las circunstancias.	NO	
12.3	**Controles criptográficos**			
12.3.1	Política para el uso de controles criptográficos	Debería desarrollarse e implementarse una política acerca del uso de controles criptográficos para proteger la información.	NO	
12.3.2	Administración de claves/llaves	Debería existir una gestión de las claves que apoye el uso de técnicas criptográficas por parte de la organización.	NO	
12.4	**Seguridad de los ficheros del sistema**			

12.4.1	Control del software operacional (en producción)	Deberían existir procedimientos para controlar la instalación de software en los sistemas operativos.	NO	
12.4.2	Protección de los datos en sistemas de prueba	Los datos de prueba deberían seleccionarse atentamente, protegerse y controlarse.	SI	70%
12.4.3	Control de acceso a las librerías de código fuente	Debería restringirse el acceso al código fuente de los programas.	SI	80%
12.5	**Seguridad en los procesos de desarrollo y soporte**			
12.5.1	Procedimientos para el control de cambios	La implementación de cambios debería estar controlada mediante el uso de procedimientos formales de control de cambios.	SI	90%
12.5.2	Revisión técnica de aplicaciones después de cambios al sistema operativo	Cuando se realizan cambios en los sistemas debería revisarse y probarse las aplicaciones, sobre todas las críticas, para garantizar que no existen efectos adversos en las operaciones organizativas o la seguridad.	SI	90%
12.5.3	Restricciones a cambios en paquetes de software	No debería estimularse las modificaciones a los paquetes de software, debería limitarse a los cambios necesarios y todos los cambios deberían estar estrictamente controlados.	SI	90%
12.5.4	Fuga de información	Debería evitarse la oportunidad de fuga de información.	NO	
12.5.5	Desarrollo de software por parte de Outsourcing	La externalización del desarrollo del software debería ser supervisada y monitorizada por la organización.	NO	
12.6	**Gestión de vulnerabilidades técnicas**			
12.6.1	Control de vulnerabilidades técnicas	Debería obtenerse información oportuna a cerca de las vulnerabilidades técnicas de los sistemas de información que se estén utilizando. Asimismo, deberían evaluarse la exposición de la organización a dichas vulnerabilidades y deberían adoptarse medidas adecuadas para afrontar el riesgo asociado.	NO	
13. Gestión de incidentes de seguridad de la información				
13.1	**Comunicación de eventos y debilidades de seguridad de la información**			
13.1.1	Reporte de eventos de Seguridad de la información.	Los eventos de seguridad de la información deberían comunicarse mediante canales adecuados de gestión lo antes posible.	NO	
13.1.2	Reporte de debilidades de seguridad	Todos los trabajadores, contratistas y usuarios terceros de los sistemas y servicios de comunicación deberían estar obligados a anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios.	NO	

13.2	**Gestión de incidentes de seguridad de la información y de su mejoramiento**			
13.2.1	Responsabilidades y procedimientos	Debería establecerse responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	SI	60%
13.2.2	Aprendizaje a partir de los incidentes de seguridad	Deberían existir mecanismos para permitir que los tipos, volúmenes y costes de los incidentes de seguridad de la información se cuantifiquen y se supervisen.	NO	
13.2.3	Recolección de evidencia	Cuando una acción contra una persona u organización después de un incidente de seguridad de la información implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas establecidas en la jurisdicción pertinente con respecto a las pruebas.	NO	
14. Gestión de la continuidad del negocio				
14.1	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**			
14.1.1	Inclusión de seguridad de la información en el proceso de administración de la continuidad del negocio	Debería desarrollarse y mantenerse un proceso controlado para la continuidad del negocio en toda la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	NO	
14.1.2	Continuidad del negocio y análisis de impacto (BIA)	Deberían identificarse los eventos que provocan interrupciones en los procesos del negocio; así como la probabilidad y los efectos de dichas interrupciones y sus consecuencias con respecto a la seguridad de la información.	NO	
14.1.3	Desarrollo e implementación de planes de continuidad	Debería desarrollarse e implantarse planes para mantener o restaurar las actividades y garantizar la disponibilidad de la información en el nivel y la escala temporal requeridos después de una interrupción o un fallo de los procesos críticos de un negocio.	NO	
14.1.4	Marco de planeación para la continuidad del negocio	Se debería mantener un único marco de referencia para los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, para dirigir de una manera coherente los requisitos de seguridad de la información, y para identificar prioridades para las pruebas y el mantenimiento.	NO	
14.1.5	Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	Los planes de continuidad del negocio deberían probarse y actualizarse periódicamente para garantizar que están al día y que son efectivos.	NO	
15. Conformidad				
15.1	**Cumplimiento con requerimientos legales**			

15.1.1	Identificación de la legislación aplicable	Todos los requisitos pertinentes, tanto legales como reglamentarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse explícitamente, documentarse y mantenerse actualizados para cada sistema de información y la organización.	NO	
15.1.2	Derechos de autor y propiedad intelectual	Deberían implantarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales acerca del uso de materiales con respecto a los cuales puedan existir derechos de propiedad intelectual y acerca del uso de productos de software exclusivo.	NO	
15.1.3	Salvaguardar los registros de la organización	Los registros importantes deberían estar protegidos contra la pérdida, destrucción y falsificación de acuerdo con los requisitos legales, reglamentarios contractuales y empresariales.	NO	
15.1.4	Protección de los datos y privacidad de la información personal	Debería garantizarse la protección de datos y la privacidad según se requiera en la legislación, las normativas y, si fuera aplicable, las cláusulas contractuales pertinentes.	NO	
15.1.5	Prevención del mal uso de los componentes tecnológicos	Debería impedirse que los usuarios utilizaran las instalaciones de procesamiento de la información para fines no autorizados.	NO	
15.1.6	Regulación de controles criptográficos	Los controles criptográficos deberían utilizarse de acuerdo con todos los contratos, leyes y normativas pertinentes.	NO	
15.2	**Conformidad con políticas y normas de seguridad y conformidad técnica**			
15.2.1	Cumplimiento de los diferentes requerimientos y controles establecidos por la política de seguridad	Los gestores deberían asegurarse de que todos los procedimientos de seguridad, dentro de su área de responsabilidad, se realicen con el fin de cumplir las políticas y normas de seguridad.	NO	
15.2.2	Chequeo del cumplimiento técnico	Debería comprobarse periódicamente que los sistemas de información cumplan las normas de implementación de seguridad.	NO	
15.3	**Consideraciones sobre la auditoría de sistemas de información**			
15.3.1	Controles para auditoría del sistema	Los requisitos y actividades de la auditoría que impliquen comprobaciones en los sistemas operativos, deberían planificarse cuidadosamente y acordarse, para minimizar los riesgos de interrupciones de los procesos.	NO	
15.3.2	Protección de las herramientas para auditoría del sistema	El acceso a las herramientas de auditoría de los sistemas de información debería estar protegidos para evitar cualquier posible peligro o uso indebido.	NO	

4.2. Análisis de riesgos de TI

4.2.1. Identificación de los activos

Del análisis de los procesos académicos de la UNC, se identificó los activos de TI que dan soporte a los mismos, describiendo los servicios que se brindan y los encargados o responsables de su gestión. La técnica utilizada para recopilar esta información, fue el análisis documental de los inventarios, manuales de funcionamiento; así como entrevistas a los responsables de la Oficina General de TI.

El catálogo de activos se dividió en 8 capas. En la primera capa se identificaron los servicios de Gestión de Actas virtuales y matricula online y Gestión de Actas virtuales, en la capa de aplicaciones se identificaron las aplicaciones Sistema académico actas virtuales UNC y Sistema académico. La tercera capa está compuesta por los servidores como Servidor de dominio, proxy, base de datos, base de datos - backup, web, de archivos, de datos - OCCA, base de datos - backup-OCCA y soportes de red como Switch, Router y Firewall. Redes de comunicaciones cuarta capa está compuesta por Internet y Red Inalámbrica; Cintas Magnética, Disco externo USB, Storage de respaldo de BD, No electrónico, Material impreso conforman la capa número cinco. La capa de Equipamiento auxiliar la conforman Acumulador de energía UPS, Sistema de aire acondicionado, Grupo electrógeno y el cableado. El data center en la capa de instalaciones y por último el personal conformado por usuario externo, personal de TI y administrador del data center.

La siguiente tabla muestra los resultados de la identificación de los activos de TI a los cuales se les realizó el análisis de riesgos.

Tabla N° 19. Activos de la Oficina General de TI de la Universidad Nacional de Cajamarca

ACTIVO		DESCRIPCIÓN	ENCARGADO
CÓDIGO	NOMBRE		
[S] SERVICIOS			
[sges]	Gestión de Actas virtuales y matricula online	Este servicio tiene cuatro plataformas, uno para alumnos (matricula, historial, horario, plan de estudios, notas), registros académicos (registrar actas de docentes e ingresarlos al sistema), para el docente (carga horaria, horarios e ingreso de notas) y el administrador de aplicaciones y base de datos (generar actas, cambio de notas, bloqueos de actas, conteo de actas , proceso de matrícula, activar actas, cronograma de matrículas, programación de semestres, programación de cursos, grupos).	[adm1] Administrador del data center
[sgeo]	Gestión de Actas virtuales	Sistema para ver notas antiguas, podemos ver las guías de matrícula, mensajes adicionales de la parte académica, Se ingresa como el administrador o por el estudiante. El estudiante puede ver datos como estudiante, constancia de matrícula de cualquier semestre académico y su historial académico con respecto a su carrera profesional.	[adm1] Administrador del data center
[SW] APLICACIONES			
[swsc]	Sistema académico actas virtuales UNC	El sistema de actas virtuales, es el sistema de gestión académica para pregrado. Esta desarrollado bajo la plataforma JAVA y utiliza una base de datos elaborada en ORACLE.	[adm1] Administrador del data center
[swoc]	Sistema académico	Es la aplicación del sistema de gestión académica. Esta desarrollado bajo la plataforma visual Basic y utiliza una base de datos elaborada en SQL SERVER.	[adm1] Administrador del data center
[HW] EQUIPOS INFORMÁTICOS			
[serv]	Servidores		
[ser1]	Servidor de dominio	Servidor en donde se encuentran las aplicaciones de sistemas operativos Windows Server, servicios de active directory, a la cual se conectan todas las computadoras de la Universidad Nacional de Cajamarca.	[adm1] Administrador del data center
[ser2]	Servidor de proxy	Es el servidor encargado de la validad de los acceso y permisos a la red de computadoras.	[adm1] Administrador del data center
[ser3]	Servidor de base de datos	Es el servidor que almacena la base de datos del sistema académico para pregrado.	[adm1] Administrador del data center
[ser4]	Servidor de base de datos - backup	Es el servidor donde se almacenan los Backup de las bases de datos del sistema de pre grado de la Universidad Nacional de Cajamarca	[adm1] Administrador del data center
[ser5]	Servidor web	Es el servidor encargado de almacenar las aplicaciones entre ellas al sistema de gestión académica para pregrado.	[adm1] Administrador del data center
[ser6]	Servidor de archivos	Es el servidor que almacena la base de datos del sistema de gestión académica para pregrado.	[adm1] Administrador del data center
[ser7]	Servidor de datos - OCCA	Es el servidor que almacena la base de datos del sistema de gestión académica.	[adm1] Administrador del data center
[ser8]	Servidor de base de datos - backup-OCCA	Es el servidor que brinda soporte al servidor base de datos - OCCA, almacena la base de datos del sistema de gestión académica.	[adm1] Administrador del data center
[netw]	Soporte de red		
[swit]	Switch	Switch principal de la red- UNC, el cual se configura y se administra el acceso y restricciones a la red. Mediante el cual permite tener un control de los equipos que se conectan y los permisos que se les debe otorgar.	[adm1] Administrador del data center
[rout]	Router	Servidor que se configura y se administra el acceso y restricciones a las aplicaciones que se encuentran alojadas en los servidores de la UNC y a internet.	[adm1] Administrador del data center
[fire]	Firewall	Router principal de la red - UNC, realiza el enrutamiento de la red y permite acceso al servicio de internet.	[adm1] Administrador del data center
[COM] REDES DE COMUNICACIONES			
[cint]	Internet	Servicio brindado por terceros, a través de líneas dedicadas que son distribuidas para los diferentes servicios que se tiene en la universidad.	

[cwfi]	Red Inalámbrica	Servicio de wifi que sirve para conectar a los dispositivos como laptop para los diferentes servicios que brinda la Oficina General de TI.	
[MEDIA] SOPORTE DE INFORMACIÓN			
[elect]	Electrónicos		
[ele1]	Cintas Magnéticas	Se utilizan para el soporte de almacenamiento de datos.	[adm1] Administrador del data center
[ele2]	Disco externo USB	Se utilizan para el soporte de almacenamiento de datos.	[adm1] Administrador del data center
[store]	Storage de respaldo de BD	Se almacenan las bases de datos de las diferentes aplicaciones y servicios que ofrece la Oficina General de TI.	[adm1] Administrador del data center
[noel]	No electrónico		
[mimp]	Material impreso	Material impreso como inventario de la Oficina General de TI, resoluciones, ingresos y salidas de dispositivos, notas de servicio.	[adm1] Administrador del data center
[AUX] EQUIPAMIENTO AUXILIAR			
[powr]	Acumulador de energía UPS	Sistema de alimentación ininterrumpida (UPS), encargados de brindar energía por un tiempo determinado a los servidores en caso que la energía eléctrica se pierda.	[adm1] Administrador del data center
[psis]	Sistema de aire acondicionado	Es un equipo de aire acondicionado encargado de mantener a una temperatura adecuada el data center.	[adm1] Administrador del data center
[gelc]	Grupo electrógeno	1 Motor generador de energía que funciona cuando hay una pérdida de energía eléctrica o algún problema eléctrico, se aproximó u uso por promedio de 2 días de autonomía sin ser recargado.	[adm1] Administrador del data center
[cable]	Cableado		
[cab1]	Cableado de red	Cable por el cual se conectan los dispositivos de la Oficina General de TI.	[adm1] Administrador del data center [uex1]Personal de TI
[cab2]	Fibra óptica	Filamento por donde se transmite los servicios que ofrece la Oficina General de TI a los diferentes departamentos académicos de la Universidad Nacional de Cajamarca.	[adm1] Administrador del data center
[L] INSTALACIONES			
[site]	Data Center	Es el local de la UNC, Unida de Red Telemática, donde se encuentran los equipos que brindan los servicios y el personal encargado de tener en funcionamiento óptimo para los equipos.	[adm1] Administrador del data center
[P] PERSONAL			
[ueex]	Usuario externo	Estudiantes, docentes y Trabajadores Administrativos. Los estudiantes que ingresan al portal web para matricularse, ver sus notas, etc.; el personal administrativo principalmente de las oficinas de OFICINA DE PROCESOS ACADÉMICOS y dirección de escuelas.	
[uex1]	Personal de TI	Practicantes que ayudan con el correcto funcionamiento de la Oficina General de TI. También se encargan de brindar soporte técnico a las diferentes áreas de la Universidad Nacional de Cajamarca.	
[adm1]	Administrador del data center	El encargado de dirigir y autorizar todas las actividades y procesos de la Oficina General de TI	

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II

4.2.2. Identificación de Amenazas

Se elaboró una tabla Identificación de amenazas de activos de TI de la Oficina General de TI – UNC. En total fueron identificadas 312 amenazas, la mayoría pertenecientes a las del grupo de Origen físico como y Errores no intencionados.

Tabla N° 20. Identificación de Amenazas de activos de TI de la Oficina General de TI – UNC

ACTIVO		AMENAZA		
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	DIMENSIÓN AFECTADA
[S] SERVICIOS				
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[sgeo]	Gestión de Actas virtuales	[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[A.5]	Suplantación de la identidad del usuario	Confidencialidad
				Autenticidad
				Integridad
		[A.24]	Denegación del servicio	Disponibilidad
[SW] APLICACIONES				
[swsc]	Sistema académico actas virtuales UNC	[N.1]	Fuego	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[swoc]	Sistema académico	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad

				Autenticidad
				Integridad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[HW] EQUIPOS INFORMÁTICOS				
[serv]	Servidores			
[ser1]	Servidor de dominio	[N.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.4]	Manipulación de la configuración	Integridad
				Confidencialidad
				Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser2]	Servidor de proxy	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.4]	Errores de configuración	Integridad
				Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser3]	Servidor de base de datos	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad

		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.14]	Escapes de información	Confidencialidad
		[E.15]	Alteración accidental de la información	Integridad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Autenticidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.15]	Modificación deliberada de la información	Integridad
		[A.24]	Denegación del servicio	Disponibilidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.14]	Escapes de información	Confidencialidad
		[E.15]	Alteración accidental de la información	Integridad
		[E.18]	Destrucción de la información	Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.15]	Modificación deliberada de la información	Integridad
		[A.18]	Destrucción de información	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[ser5]	Servidor web	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.14]	Escapes de información	Confidencialidad
		[E.15]	Alteración accidental de la información	Integridad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad

		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser6]	Servidor de archivos	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.14]	Escapes de información	Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.5]	Suplantación de la identidad del usuario	Confidencialidad
				Integridad
				Autenticidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad

				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.6]	Abuso de privilegios de acceso	Confidencialidad
				Integridad
				Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[netw]	Soporte de red			
[swit]	Switch	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.2]	Errores del administrador	Integridad
				Disponibilidad
				Confidencialidad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[rout]	Router	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.2]	Errores del administrador	Disponibilidad
				Integridad
				Confidencialidad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[fire]	Firewall	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.21]	Errores de mantenimiento / actualización de programas (software)	Integridad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.4]	Manipulación de la configuración	Integridad

				Confidencialidad
				Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[COM] REDES DE COMUNICACIONES				
[cint]	Internet	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.4]	Errores de configuración	Integridad
		[E.9]	Errores de re-encaminamiento	Confidencialidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
				Confidencialidad
		[A.24]	Denegación del servicio	Disponibilidad
[MEDIA] SOPORTE DE INFORMACIÓN				
[elect]	Electrónicos			
[ele1]	Cintas Magnéticas	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
[ele2]	Disco externo USB	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
				Confidencialidad
[store]	Storage de respaldo de BD	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[I.10]	Degradación de los soportes de almacenamiento de la información	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[A.24]	Denegación del servicio	Disponibilidad
[noel]	No electrónico			
[mimp]	Material impreso	[I.1]	Fuego	Disponibilidad
		[E.7]	Deficiencias en la organización	Disponibilidad
		[E.14]	Escapes de información	Confidencialidad
		[E.19]	Fugas de información	Confidencialidad
		[A.19]	Divulgación de información	Confidencialidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
[AUX] EQUIPAMIENTO AUXILIAR				
[powr]	Acumulador de energía UPS	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad

		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.*]	Desastres industriales	Disponibilidad
		[I.3]	Contaminación mecánica	Disponibilidad
		[I.4]	Contaminación electromagnética	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.11]	Acceso no autorizado	Confidencialidad
				Integridad
		[A.23]	Manipulación de los equipos	Confidencialidad
				Disponibilidad
		[A.25]	Robo	Disponibilidad
[gelc]	Grupo electrógeno	[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.4]	Contaminación electromagnética	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[I.6]	Corte de suministro	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[cable]	Cableado			
[cab1]	Cableado de red	[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.4]	Contaminación electromagnética	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[A.7]	Uso no previsto	Disponibilidad
				Confidencialidad
				Integridad
		[A.23]	Manipulación de los equipos	Integridad
				Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad

		[A.28]	Indisponibilidad del personal	Disponibilidad
[cab2]	Fibra óptica	[I.1]	Fuego	Disponibilidad
		[I.5]	Avería de origen físico o lógico	Disponibilidad
		[E.7]	Deficiencias en la organización	Disponibilidad
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Disponibilidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.23]	Manipulación de los equipos	Confidencialidad
				Disponibilidad
[L] INSTALACIONES				
[site]	Data Center	[N.*]	Desastres naturales	Disponibilidad
		[I.1]	Fuego	Disponibilidad
		[I.2]	Daños por agua	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.9]	Interrupción de otros servicios y suministros esenciales	Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
				Confidencialidad
		[A.11]	Acceso no autorizado	Confidencialidad
				Integridad
		[A.26]	Ataque destructivo	Disponibilidad
		[A.27]	Ocupación enemiga	Disponibilidad
				Confidencialidad
		[A.28]	Indisponibilidad del personal	Disponibilidad
[P] PERSONAL				
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.18]	Destrucción de la información	Disponibilidad
		[E.19]	Fugas de información	Confidencialidad
		[E.20]	Vulnerabilidades de los programas (software)	Integridad
				Disponibilidad
				Confidencialidad
		[E.24]	Caída del sistema por agotamiento de recursos	Disponibilidad
		[E.25]	Pérdida de equipos	Disponibilidad
		[A.6]	Abuso de privilegios de acceso	Confidencialidad
				Integridad
		[A.7]	Uso no previsto	Disponibilidad
				Confidencialidad
				Integridad
		[A.15]	Modificación deliberada de la información	Integridad
		[A.18]	Destrucción de información	Disponibilidad
		[A.25]	Robo	Disponibilidad
				Confidencialidad
		[A.29]	Extorsión	Confidencialidad
				Integridad
				Disponibilidad
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[E.1]	Errores de los usuarios	Integridad
				Confidencialidad
				Disponibilidad
		[E.7]	Deficiencias en la organización	Disponibilidad
		[A.19]	Divulgación de información	Confidencialidad
		[A.29]	Extorsión	Confidencialidad
				Integridad
				Disponibilidad

		[A.30]	Ingeniería social	Confidencialidad
				Integridad
				Disponibilidad
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	Disponibilidad
		[I.7]	Condiciones inadecuadas de temperatura o humedad	Disponibilidad
		[I.11]	Emanaciones electromagnética	Confidencialidad
		[E.28]	Indisponibilidad del personal	Disponibilidad
		[A.28]	Indisponibilidad del personal	Disponibilidad

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas

4.2.3. Dependencia entre activos

Se elaboró una tabla de dependencia de activos, en la que se identificaron los servicios que se verían afectados, si el activo de TI que les da soporte, se ve afectado por una amenaza, parcial o totalmente.

Tabla N° 21. Tabla dependencia entre activos

ACTIVO		DEPENDENCIA
CÓDIGO	NOMBRE	
[S] SERVICIOS		
[sges]	Gestión de Actas virtuales y matricula online	[ser1] Servidor de dominio [ser2] Servidor de proxy [ser3] Servidor de base de datos [ser4] Servidor de base de datos - backup [ser5] Servidor web [ser6] Servidor de archivos [ser7] Servidor de datos - OCCA [ser8] Servidor de base de datos - backup-OCCA [swit]Switch [rout] Router [fire] Firewall [cint] Internet [cwfi] Red Inalámbrica [store] Storage de respaldo de BD [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [ueex] Usuario externo [uex1] Personal de TI
[sgeo]	Gestión de Actas virtuales	[ser1] Servidor de dominio [ser2] Servidor de proxy [ser3] Servidor de base de datos [ser4] Servidor de base de datos - backup [ser5] Servidor web [ser6] Servidor de archivos [ser7] Servidor de datos - OCCA [ser8] Servidor de base de datos - backup-OCCA [swit]Switch [rout] Router [fire] Firewall [cint] Internet [cwfi] Red Inalámbrica [store] Storage de respaldo de BD [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [ueex] Usuario externo [uex1] Personal de TI
[SW] APLICACIONES		
[swsc]	Sistema académico actas virtuales UNC	[sges] Gestión de Actas virtuales y matricula online [ser3] Servidor de base de datos

		[ser4] Servidor de base de datos - backup [swit]Switch [rout] Router [fire] Firewall [cint] Internet [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[swoc]	Gestión de Actas virtuales	[sgeo] Gestión de Actas virtuales [ser3] Servidor de base de datos [swit]Switch [rout] Router [cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [site] Data Center
[HW] EQUIPOS INFORMÁTICOS		
[serv]	Servidores	
[ser1]	Servidor de dominio	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser2]	Servidor de proxy	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser3]	Servidor de base de datos	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser4]	Servidor de base de datos - backup	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser5]	Servidor web	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser6]	Servidor de archivos	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ser7]	Servidor de datos - OCCA	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center

[ser8]	Servidor de base de datos - backup-OCCA	[cint] Internet [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[netw]	Soporte de red	
[swit]	Switch	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[rout]	Router	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[fire]	Firewall	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[COM] REDES DE COMUNICACIONES		
[cint]	Internet	[swit]Switch [rout] Router [fire] Firewall [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[cwfi]	Red Inalámbrica	[swit]Switch [rout] Router [fire] Firewall [powr] Acumulador de energía UPS [psis] Sistema de aire acondicionado [gelc] Grupo electróngeno [cab1] Cableado de red [cab2] Fibra óptica [site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[MEDIA] SOPORTE DE INFORMACIÓN		
[elect]	Electrónicos	
[ele1]	Cintas Magnéticas	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[ele2]	Disco externo USB	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[store]	Storage de respaldo de BD	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[noel]	No electrónico	
[mimp]	Material impreso	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[AUX] EQUIPAMIENTO AUXILIAR		
[powr]	Acumulador de energía UPS	[site] Data Center [uex1] Personal de TI
[psis]	Sistema de aire acondicionado	[site] Data Center [uex1] Personal de TI
[gelc]	Grupo electrógeno	[site] Data Center [uex1] Personal de TI
[cable]	Cableado	
[cab1]	Cableado de red	[uex1] Personal de TI
[cab2]	Fibra óptica	[site] Data Center [uex1] Personal de TI [adm1] Administrador del data center
[L] INSTALACIONES		
[site]	Data Center	[uex1] Personal de TI [adm1] Administrador del data center
[P] PERSONAL		
[ueex]	Usuario externo	
[uex1]	Personal de TI	
[adm1]	Administrador del data center	

4.2.4. Valorización de activos

Para la valoración de los activos se elaboró la tabla Valoración de Activos. En ella valoramos a los activos identificados en las 5 dimensiones de los cuales el Sistema académico actas virtuales UNC, Servidor de base de datos - backup, Cintas Magnéticas, Material impreso, Cableado de red, Fibra óptica, Data Center y Administrador del data center, fueron los activos que obtuvieron mayor valor de importancia.

Tabla N° 22. Valoración de Activos

ACTIVO	DIMENSIÓN	TOTAL					
CÓDIGO	NOMBRE	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	TOTAL
[S] SERVICIOS							
[sges]	Gestión de Actas virtuales y matricula online	3					3
[sgeo]	Gestión de Actas virtuales	3	3	1	3	2	2.4
[SW] APLICACIONES							
[swsc]	Sistema académico actas virtuales UNC	4	7		7	2	5
[swoc]	Sistema académico	3	5		4	1	3.3
[HW] EQUIPOS INFORMÁTICOS							
[serv]	Servidores						
[ser1]	Servidor de dominio	3	4		4	4	3.8
[ser2]	Servidor de proxy	2					2
[ser3]	Servidor de base de datos	6	7	1	6	5	5
[ser4]	Servidor de base de datos - backup	2	7		6	3	4.5
[ser5]	Servidor web	3	3	1	3	1	2.2
[ser6]	Servidor de archivos	2	2		2		2
[ser7]	Servidor de datos - OCCA	3	3	1	3	1	2.2
[ser8]	Servidor de base de datos - backup-OCCA	3	4		3	1	2.8
[netw]	Soporte de red						
[swit]	Switch	3				1	2
[rout]	Router	3				1	2
[fire]	Firewall		5		4	2	3.7
[COM] REDES DE COMUNICACIONES							
[cint]	Internet	4				2	3
[cwfi]	Red Inalámbrica	4				2	3
[MEDIA] SOPORTE DE INFORMACIÓN							
[elect]	Electrónicos						
[ele1]	Cintas Magnéticas	3	6		5	4	4.5
[ele2]	Disco externo USB	3	5		4	3	3.8
[store]	Storage de respaldo de BD	3	6		5	4	4.5
[noel]	No electrónico						
[mimp]	Material impreso	4	6	6			5.3
[AUX] EQUIPAMIENTO AUXILIAR							
[powr]	Acumulador de energía UPS	4				6	5
[psis]	Sistema de aire acondicionado	4				6	5

[gelc]	Grupo electrógeno	4				6	5
[cable]	Cableado						
[cab1]	Cableado de red	4				7	5.5
[cab2]	Fibra óptica	4				7	5.5
[L] INSTALACIONES							
[site]	Data Center	4			7		5.5
[P] PERSONAL							
[ueex]	Usuario externo	3				2	2.5
[uex1]	Personal de TI	3				2	2.5
[adm1]	Administrador del data center	8				3	5.5

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

4.2.5. Valorización de amenazas

Se elaboró la tabla de Valoración de las amenazas en los activos de TI de la Oficina General de TI – UNC, identificándose 5 dimensiones. De acuerdo a la valoración dada por el responsable de la Administración de la red, algunas de las amenazas identificadas en los activos, arrojaron niveles de criticidad de muy alto y alto. Como por ejemplo el Sistema académico actas virtuales UNC tuvo un nivel de criticidad de muy alto y alto en las amenazas como fuego, fallo de servicios de comunicaciones e Interrupción de otros servicios y suministros esenciales, caída del sistema por agotamiento de recursos y Denegación del servicio.

Tabla N° 23. Valoración de las amenazas en los activos de TI

ACTIVO		AMENAZA		DIMENSIÓN						NIVEL
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	TOTAL	
[S] SERVICIOS										
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	0.9					0.9	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					0.8	ALTO
		[E.1]	Errores de los usuarios	0.1	0.1	0.1			0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.1	0.1			0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					0.5	MEDIO
		[A.24]	Denegación del servicio	0.6					0.6	ALTO
[sgeo]	Gestión de Actas virtuales	[I.8]	Fallo de servicios de comunicaciones	0.5					0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.6					0.6	ALTO
		[E.1]	Errores de los usuarios	0.01	0.1	0.1			0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.1	0.1			0.1	BAJO
		[A.5]	Suplantación de la identidad del usuario		0.7	0.8	0.8		0.8	ALTO
		[A.24]	Denegación del servicio	0.6					0.6	ALTO
[SW] APLICACIONES										
[swsc]	Sistema académico actas virtuales UNC	[N.1]	Fuego	1					1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.6					0.6	ALTO
		[E.2]	Errores del administrador	0.7	0.1	0.1			0.3	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.5	0.1				0.3	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5					0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	1					1	MUY ALTO
		[A.24]	Denegación del servicio	1					1	MUY ALTO
[swoc]	Sistema académico	[I.1]	Fuego	1					1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					0.5	MEDIO
		[I.6]	Corte de suministro	0.8					0.8	ALTO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.7					0.7	ALTO

		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5				0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.7				0.7	ALTO
		[E.2]	Errores del administrador	0.1	0.1	0.1		0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.3	0.6	0.5		0.5	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.9	0.5			0.7	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1				1	MUY ALTO
		[A.24]	Denegación del servicio	1				1	MUY ALTO
			[HW] EQUIPOS INFORMÁTICOS						
[serv]	Servidores								
		[N.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.6]	Corte de suministro	0.5				0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5				0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5				0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.2				0.2	BAJO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1				0.1	BAJO
[ser1]	Servidor de dominio	[E.9]	Errores de re-encaminamiento			0.2		0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.9	0.9	0.7		0.8	MUY ALTO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.3	0.1			0.2	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.2				0.2	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.6				0.6	ALTO
		[A.4]	Manipulación de la configuración	0.1	0.1	0.1		0.1	BAJO
		[A.24]	Denegación del servicio	0.9				0.9	MUY ALTO
		[I.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.6]	Corte de suministro	0.5				0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5				0.5	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5				0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.2				0.2	BAJO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1				0.1	BAJO
[ser2]	Servidor de proxy	[E.2]	Errores del administrador	0.1	0.05	0.05		0.1	BAJO
		[E.4]	Errores de configuración		0.2	0.2		0.2	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.2	0.3	0.5		0.3	MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.1			0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.7				0.7	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5				0.5	MEDIO
		[E.28]	Indisponibilidad del personal	0.2				0.2	BAJO
		[A.24]	Denegación del servicio	0.9				0.9	MUY ALTO

		[I.1]	Fuego	1					MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5					MEDIO
		[I.6]	Corte de suministro	0.5					MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.3					MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1					BAJO
		[E.2]	Errores del administrador	0.1	0.2	0.2			BAJO
[ser3]	Servidor de base de datos	[E.14]	Escapes de información			0.7			ALTO
		[E.15]	Alteración accidental de la información		0.5				MEDIO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.2	0.4			MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.1				BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5					MEDIO
		[A.15]	Modificación deliberada de la información		0.4				MEDIO
		[A.24]	Denegación del servicio	0.5					MEDIO
		[A.28]	Indisponibilidad del personal	0.8					ALTO
		[I.1]	Fuego	0.1					BAJO
		[I.6]	Corte de suministro	0.5					MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5					MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					MEDIO
		[E.2]	Errores del administrador	0.5	0.1	0.1			MEDIO
		[E.14]	Escapes de información			0.9			MUY ALTO
		[E.15]	Alteración accidental de la información		0.5				MEDIO
[ser4]	Servidor de base de datos - backup	[E.18]	Destrucción de la información	0.5				0.5	MEDIO
		Vulnerabili	0.5	0.2	0.1	0.3		M	
		Errores de	0.5	0.2		0.4		M	
		Errores de	0.5			0.5		M	
		Caída del	0.5			0.5		M	
		Indisponibi	0.2			0.2			
		Modificaci		0.5		0.5		M	
		Destrucció	0.6			0.6			
		Denegació	0.5			0.5		M	
		Indisponibi	0.1			0.1			
[ser5]	Servidor web	[I.5]	Avería de origen físico o lógico	0.9				0.9	MUY ALTO

		[I.6]	Corte de suministro	0.05					MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5					MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5					MEDIO
		[E.14]	Escapes de información			0.05			MUY BAJO
		[E.15]	Alteración accidental de la información		0.2				BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.2	0.3			BAJO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.05				BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	1					MUY ALTO
		[A.24]	Denegación del servicio	1					MUY ALTO
		[I.1]	Fuego	0.9					MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9					MUY ALTO
		[I.6]	Corte de suministro	0.05					MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.1					BAJO
[ser6]	Servidor de archivos	[E.1]	Errores de los usuarios	0.05	0.1	0.1			BAJO
		[E.14]	Escapes de información			0.2			BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.05	0.1	0.1			BAJO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.2				BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1					BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	1					MUY ALTO
		[A.5]	Suplantación de la identidad del usuario		0.1	0.2	0.4		MEDIO
		[A.24]	Denegación del servicio	1					MUY ALTO
		[I.1]	Fuego	0.9					MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9					MUY ALTO
		[I.6]	Corte de suministro	0.05					MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1					MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1					MUY ALTO
[ser7]	Servidor de datos - OCCA	[I.9]	Interrupción de otros servicios y suministros esenciales	0.8					ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.8					ALTO
		[E.20]	Vulnerabilidades de los programas (software)	0.1	0.3	0.4			MEDIO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.2	0.05				BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.6					ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1					MUY ALTO

[ser8]	Servidor de base de datos - backup-OCCA	[A.24]	Denegación del servicio	1				1	MUY ALTO
		[I.1]	Fuego	0.9				0.9	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.9				0.9	MUY ALTO
		[I.6]	Corte de suministro	0.05				0.05	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1				1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1				1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.9				0.9	MUY ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.8				0.8	ALTO
		[E.2]	Errores del administrador	0.1	0.05	0.05		0.1	BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.05	0.1	0.2		0.1	BAJO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.05	0.1			0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.1				0.1	BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	1				1	MUY ALTO
		[A.6]	Abuso de privilegios de acceso	0.05	0.1	0.2		0.1	BAJO
		[A.24]	Denegación del servicio	1				1	MUY ALTO
[netw]	Soporte de red								
[swit]	Switch	[I.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	1				1	MUY ALTO
		[I.6]	Corte de suministro	1				1	MUY ALTO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1				1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1				1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	1				1	MUY ALTO
		[E.1]	Errores de los usuarios	0.05	0.1	0.05		0.1	BAJO MUY
		[E.2]	Errores del administrador	0.1	0.05	0		0.1	BAJO MUY
		[E.9]	Errores de re-encaminamiento			0.05		0.1	BAJO MUY
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.9				0.9	ALTO MUY
		[E.24]	Caída del sistema por agotamiento de recursos	0.9				0.9	ALTO MUY
		[A.24]	Denegación del servicio	1				1	ALTO MUY
[rout]	Router	[I.1]	Fuego	1				1	ALTO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.6]	Corte de suministro	0.05				0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	1				1	MUY ALTO
		[I.8]	Fallo de servicios de comunicaciones	1				1	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	1				1	MUY ALTO
		[E.2]	Errores del administrador	0.1	0.05	0.01		0.1	
		[E.9]	Errores de re-encaminamiento			0.9		0.9	MUY ALTO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5				0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5				0.5	MEDIO

		[A.24]	Denegación del servicio	0.5				0.5	MEDIO
		[I.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.6]	Corte de suministro	0.05				0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.4				0.4	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.5				0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5				0.5	MEDIO
[fire]	Firewall	[I.10]	Degradación de los soportes de almacenamiento de la información	0.5				0.5	MEDIO
		[E.20]	Vulnerabilidades de los programas (software)	0.8	0.9	0.6		0.8	ALTO
		[E.21]	Errores de mantenimiento / actualización de programas (software)	0.1	0.1			0.1	BAJO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5				0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5				0.5	MEDIO
		[A.4]	Manipulación de la configuración	0.05	0.2	0.1		0.1	BAJO
		[A.24]	Denegación del servicio	0.5				0.5	MEDIO
[COM] REDES DE COMUNICACIONES									
		[I.1]	Fuego	0.6				0.6	ALTO
		[I.5]	Avería de origen físico o lógico	0.8				0.8	ALTO
		[I.6]	Corte de suministro	0.5				0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.8				0.8	ALTO
		[I.8]	Fallo de servicios de comunicaciones	1				1	MUY ALTO
[cint]	Internet	[I.9]	Interrupción de otros servicios y suministros esenciales	0.2				0.2	BAJO
		[E.4]	Errores de configuración		0.01			0.0	MUY BAJO
		[E.9]	Errores de re-encaminamiento			0.05		0.1	MUY BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.5				0.5	MEDIO
		[A.24]	Denegación del servicio	0.5				0.5	MEDIO
		[I.6]	Corte de suministro	0.5				0.5	MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.3				0.3	MEDIO
		[I.8]	Fallo de servicios de comunicaciones	0.9				0.9	MUY ALTO
[cwfi]	Red Inalámbrica	[I.9]	Interrupción de otros servicios y suministros esenciales	0.6				0.6	ALTO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5				0.5	MEDIO
		[E.25]	Pérdida de equipos	0.9		0.1		0.5	MEDIO
		[A.24]	Denegación del servicio	0.8				0.8	ALTO
[elect]	Electrónicos		[MEDIA] SOPORTE DE INFORMACIÓN						
		[I.1]	Fuego	1				1	MUY ALTO
[ele1]	Cintas Magnéticas	[I.5]	Avería de origen físico o lógico	1				1	MUY ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	1				1	MUY ALTO
		[A.25]	Robo	1		0.9		0.95	MUY ALTO

[ele2]	Disco externo USB	[I.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5				0.5	MEDIO
		[E.1]	Errores de los usuarios	0.05	0.8	0.1		0.3	MEDIO
		[E.25]	Pérdida de equipos	0.9		0.5		0.7	ALTO
[store]	Storage de respaldo de BD	[I.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.8				0.8	ALTO
		[I.10]	Degradación de los soportes de almacenamiento de la información	0.5				0.5	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5				0.5	MEDIO
		[A.24]	Denegación del servicio	0.05				0.1	MUY BAJO
[noel]	No electrónico								
[mimp]	Material impreso	[I.1]	Fuego	1				1	MUY ALTO
		[E.7]	Deficiencias en la organización	0.4				0.4	MEDIO
		[E.14]	Escapes de información			0.1		0.1	BAJO
		[E.19]	Fugas de información			0.2		0.2	BAJO
		[A.19]	Divulgación de información			0.1		0.1	BAJO
		[A.25]	Robo	0.5		0.2		0.4	MEDIO
[AUX] EQUIPAMIENTO AUXILIAR									
[powr]	Acumulador de energía UPS	[I.1]	Fuego	1				1	MUY ALTO
		[I.5]	Avería de origen físico o lógico	1				1	MUY ALTO
		[I.6]	Corte de suministro	0.05				0.1	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.1				0.1	BAJO MUY
		[I.8]	Fallo de servicios de comunicaciones	0.01				0.0	BAJO MUY
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.05				0.1	BAJO
		[E.1]	Errores de los usuarios	0.3	0.5	0		0.3	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.7				0.7	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1				1	MUY ALTO
[pcic]	Sistema de aire acondicionado	[I.1]	Fuego	1				1	MUY ALTO
		[I.2]	Daños por agua	0.5				0.5	MEDIO
		[I.*]	Desastres industriales	0.5				0.5	MEDIO
		[I.3]	Contaminación mecánica	0.05				0.1	MUY BAJO
		[I.4]	Contaminación electromagnética	0.05				0.1	MUY BAJO
		[I.5]	Avería de origen físico o lógico	0.5				0.5	MEDIO
		[I.6]	Corte de suministro	0.1				0.1	BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5				0.5	MEDIO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.9				0.9	MUY ALTO
		[E.1]	Errores de los usuarios	0.7	0.5	0		0.4	MEDIO

		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.5				0.5	MEDIO
		[E.24]	Caída del sistema por agotamiento de recursos	1				1	MUY ALTO
		[A.11]	Acceso no autorizado		0.05	0		0.03	MUY BAJO
		[A.23]	Manipulación de los equipos		0.5	0		0.3	MEDIO
		[A.25]	Robo	1		0		0.5	MEDIO
		[I.1]	Fuego	1				1	MUY ALTO
		[I.2]	Daños por agua	1				1	MUY ALTO
		[I.4]	Contaminación electromagnética	0.05				0.1	MUY BAJO
		[I.5]	Avería de origen físico o lógico	1				1	MUY ALTO
		[I.6]	Corte de suministro	0.05				0.1	MUY BAJO
[gelc]	Grupo electrógeno	[I.9]	Interrupción de otros servicios y suministros esenciales	0.2				0.2	BAJO
		[E.1]	Errores de los usuarios	0.3	0.4	0		0.2	MEDIO
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.6				0.6	ALTO
		[E.24]	Caída del sistema por agotamiento de recursos	1				1	MUY ALTO
		[A.25]	Robo	1		0		0.5	MEDIO
		[A.28]	Indisponibilidad del personal	0.3				0.3	MEDIO
[cable]	Cableado								
		[I.1]	Fuego	0.7				0.7	ALTO
		[I.2]	Daños por agua	0.7				0.7	ALTO
		[I.4]	Contaminación electromagnética	0.1				0.1	BAJO
		[I.5]	Avería de origen físico o lógico	0.7				0.7	ALTO
[cab1]	Cableado de red	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.2				0.2	BAJO
		[A.7]	Uso no previsto	0.2	0.01	0.5		0.2	MEDIO
		[A.23]	Manipulación de los equipos	0.2	0.05			0.1	BAJO
		[A.25]	Robo	0.1		0		0.05	MUY BAJO
		[A.28]	Indisponibilidad del personal	0.05				0.05	MUY BAJO
		[I.1]	Fuego	0.7				0.7	ALTO
		[I.5]	Avería de origen físico o lógico	0.3				0.3	MEDIO
		[E.7]	Deficiencias en la organización	0.1				0.1	BAJO
[cab2]	Fibra óptica	[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	0.2				0.2	BAJO
		[E.28]	Indisponibilidad del personal	0.05				0.05	MUY BAJO
		[A.23]	Manipulación de los equipos	0.1		0		0.05	MUY BAJO
			[L] INSTALACIONES						
		[N.*]	Desastres naturales	1				1	MUY ALTO
		[I.1]	Fuego	1				1	MUY ALTO
[site]	Data Center	[I.2]	Daños por agua	0.05				0.05	MUY BAJO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.9				0.9	MUY ALTO
		[I.9]	Interrupción de otros servicios y suministros esenciales	0.5				0.5	MEDIO

		[E.25]	Pérdida de equipos	0.2		0.05		0.1	BAJO
		[A.11]	Acceso no autorizado		0.3	0.4			MEDIO
		[A.26]	Ataque destructivo	0.9					MUY ALTO
		[A.27]	Ocupación enemiga	1		0.5			ALTO
		[A.28]	Indisponibilidad del personal	0.8					ALTO
			[P] PERSONAL						
		[I.8]	Fallo de servicios de comunicaciones	0.6					ALTO
		[E.1]	Errores de los usuarios	0.1	0.5	0.2			MEDIO
		[E.18]	Destrucción de la información	0.2					BAJO
		[E.19]	Fugas de información			0.2			BAJO
		[E.20]	Vulnerabilidades de los programas (software)	0.2	0.3	0.1			BAJO
		[E.24]	Caída del sistema por agotamiento de recursos	0.4					MEDIO
[ueex]	Usuario externo	[E.25]	Pérdida de equipos	0.1	0.05				BAJO
		[A.6]	Abuso de privilegios de acceso		0.1	0.2			BAJO
		[A.7]	Uso no previsto	0.2	0.05	0.1			BAJO
		[A.15]	Modificación deliberada de la información		0.2				BAJO
		[A.18]	Destrucción de información	0.5					MEDIO
		[A.25]	Robo	0.5		0.5			MEDIO
		[A.29]	Extorsión	0.6	0.5	0.7			ALTO
		[I.4]	Contaminación electromagnética	0.5					MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					MEDIO
		[E.1]	Errores de los usuarios	0.3	0	0			BAJO
[uex1]	Personal de TI	[E.7]	Deficiencias en la organización	0.5					MEDIO
		[A.19]	Divulgación de información			0.2			BAJO
		[A.29]	Extorsión	0.05					MUY BAJO
		[A.30]	Ingeniería social	0.1	0.2	0.3			BAJO
		[I.4]	Contaminación electromagnética	0.5					MEDIO
		[I.7]	Condiciones inadecuadas de temperatura o humedad	0.5					MEDIO
[adm1]	Administrador del data center	[I.11]	Emanaciones electromagnética			0.3			MEDIO
		[E.28]	Indisponibilidad del personal	0.9					MUY ALTO
		[A.28]	Indisponibilidad del personal	0.2					BAJO

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

4.2.6. Estimación del Impacto

Se elaboró la tabla Valoración del Impacto de las amenazas en los activos de TI de la Oficina General de TI - UNC. El impacto se obtuvo de la multiplicación del valor del activo por el desgaste que puede ser causado por las amenazas. De eso se obtuvo el nivel de impacto de las amenazas en los activos. Amenazas como fuego, fallo en el servicio de comunicaciones, caída del sistema por agotamiento de recursos y denegación del servicio son amenazas que tendrían un nivel de impacto de alto y muy alto en los activos de TI de la Oficina General de TI de la Universidad Nacional de Cajamarca.

Tabla N° 24. Valoración del Impacto de las Amenazas en los activos de TI

VALORACIÓN DEL IMPACTO								
ACTIVO		AMENAZA		VALOR DE	DESGASTE	IMPACTO	ESCALA	NIVEL
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE					
[S] SERVICIOS								
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	3	0.9	2.7	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		0.5	1.5	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	2.4	MEDIO	3
		[E.1]	Errores de los usuarios		0.1	0.3	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.3	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1.5	BAJO	2
		[A.24]	Denegación del servicio		0.6	1.8	BAJO	2
[sgeo]	Gestión de Actas virtuales	[I.8]	Fallo de servicios de comunicaciones	2.4	0.5	1.2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.6	1.44	BAJO	2
		[E.1]	Errores de los usuarios		0.07	0.168	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.24	BAJO	2
		[A.5]	Suplantación de la identidad del usuario		0.8	1.84	BAJO	2
		[A.24]	Denegación del servicio		0.6	1.44	BAJO	2
[SW] APLICACIONES								
[swsc]	Sistema académico actas virtuales UNC	[N.1]	Fuego	5	1	5	ALTO	4
		[I.8]	Fallo de servicios de comunicaciones		1	5	ALTO	4
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.6	3	MEDIO	3
		[E.2]	Errores del administrador		0.3	1.5	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.3	1.5	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.5	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
		[A.24]	Denegación del servicio		1	5	ALTO	4
[swoc]	Sistema académico	[I.1]	Fuego	3.25	1	3.25	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.625	BAJO	2
		[I.6]	Corte de suministro		0.8	2.6	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1.625	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.7	2.275	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	1.625	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.7	2.275	MEDIO	3

		[E.2]	Errores del administrador		0.1	0.325	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.5	1.51667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.7	2.275	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	3.25	ALTO	4
		[A.24]	Denegación del servicio		1	3.25	ALTO	4
[HW] EQUIPOS INFORMÁTICOS								
[serv]	Servidores							
[ser1]	Servidor de dominio	[N.1]	Fuego	3.75	1	3.75	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.875	BAJO	2
		[I.6]	Corte de suministro		0.5	1.875	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1.875	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.5	1.875	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	0.75	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.375	BAJO	2
		[E.9]	Errores de re-encaminamiento		0.2	0.75	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.8	3.125	ALTO	4
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.2	0.75	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.2	0.75	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.6	2.25	MEDIO	3
		[A.4]	Manipulación de la configuración		0.1	0.375	BAJO	2
		[A.24]	Denegación del servicio		0.9	3.375	ALTO	4
[ser2]	Servidor de proxy	[I.1]	Fuego	2	1	2	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.5	1	BAJO	2
		[I.6]	Corte de suministro		0.5	1	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.5	1	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	0.4	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.2	BAJO	2
		[E.2]	Errores del administrador		0.07	0.13333	BAJO	2
		[E.4]	Errores de configuración		0.2	0.4	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.3	0.66667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.2	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.7	1.4	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1	BAJO	2
		[E.28]	Indisponibilidad del personal		0.2	0.4	BAJO	2
		[A.24]	Denegación del servicio		0.9	1.8	BAJO	2
[ser3]	Servidor de base de datos	[I.1]	Fuego	5	1	5	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	2.5	MEDIO	3
		[I.6]	Corte de suministro		0.5	2.5	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.5	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		0.5	2.5	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.3	1.5	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.5	BAJO	2
		[E.2]	Errores del administrador		0.2	0.83333	BAJO	2
		[E.14]	Escapes de información		0.7	3.5	ALTO	4
		[E.15]	Alteración accidental de la información		0.5	2.5	MEDIO	3
		[E.20]	Vulnerabilidades de los programas (software)		0.2	1.16667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.5	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.5	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	2.5	MEDIO	3
		[A.15]	Modificación deliberada de la información		0.4	2	BAJO	2
		[A.24]	Denegación del servicio		0.5	2.5	MEDIO	3

		[A.28]	Indisponibilidad del personal		0.8	4	ALTO	4
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	4.5	0.1	0.45	BAJO	2
		[I.6]	Corte de suministro		0.5	2.25	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.25	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		0.5	2.25	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	2.25	MEDIO	3
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	2.25	MEDIO	3
		[E.2]	Errores del administrador		0.2	1.05	BAJO	2
		[E.14]	Escapes de información		0.9	4.05	ALTO	4
		[E.15]	Alteración accidental de la información		0.5	2.25	MEDIO	3
		[E.18]	Destrucción de la información		0.5	2.25	MEDIO	3
		[E.20]	Vulnerabilidades de los programas (software)		0.3	1.2	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.35	1.575	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.25	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	2.25	MEDIO	3
		[E.28]	Indisponibilidad del personal		0.2	0.9	BAJO	2
		[A.15]	Modificación deliberada de la información		0.5	2.25	MEDIO	3
		[A.18]	Destrucción de información		0.6	2.7	MEDIO	3
		[A.24]	Denegación del servicio		0.5	2.25	MEDIO	3
		[A.28]	Indisponibilidad del personal		0.1	0.45	BAJO	2
[ser5]	Servidor web	[I.1]	Fuego	2.2	0.9	1.98	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.9	1.98	BAJO	2
		[I.6]	Corte de suministro		0.05	0.11	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2.2	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		1	2.2	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	1.1	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	1.1	BAJO	2
		[E.14]	Escapes de información		0.05	0.11	BAJO	2
		[E.15]	Alteración accidental de la información		0.2	0.44	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.2	0.44	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.165	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.22	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2.2	MEDIO	3
		[A.24]	Denegación del servicio		1	2.2	MEDIO	3
[ser6]	Servidor de archivos	[I.1]	Fuego	2	0.9	1.8	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.9	1.8	BAJO	2
		[I.6]	Corte de suministro		0.1	0.1	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		1	2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	1.6	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.1	0.2	BAJO	2
		[E.1]	Errores de los usuarios		0.1	0.16667	BAJO	2
		[E.14]	Escapes de información		0.2	0.4	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.16667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.15	0.3	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.2	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2	BAJO	2
		[A.5]	Suplantación de la identidad del usuario		0.2	0.46667	BAJO	2
		[A.24]	Denegación del servicio		1	2	BAJO	2
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	2.2	0.9	1.98	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.9	1.98	BAJO	2
		[I.6]	Corte de suministro		0.05	0.11	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2.2	MEDIO	3

		[I.8]	Fallo de servicios de comunicaciones		1	2.2	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	1.76	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.8	1.76	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.3	0.58667	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.125	0.275	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.6	1.32	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2.2	MEDIO	3
		[A.24]	Denegación del servicio		1	2.2	MEDIO	3
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	2.75	0.9	2.475	MEDIO	3
		[I.5]	Avería de origen físico o lógico		0.9	2.475	MEDIO	3
		[I.6]	Corte de suministro		0.05	0.1375	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2.75	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		1	2.75	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.9	2.475	MEDIO	3
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.8	2.2	MEDIO	3
		[E.2]	Errores del administrador		0.1	0.18333	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.1	0.32083	BAJO	2
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.075	0.20625	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.1	0.275	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		1	2.75	MEDIO	3
		[A.6]	Abuso de privilegios de acceso		0.1	0.32083	BAJO	2
		[A.24]	Denegación del servicio		1	2.75	MEDIO	3
[netw]	Soporte de red							
[swit]	Switch	[I.1]	Fuego	2	1	2	BAJO	2
		[I.5]	Avería de origen físico o lógico		1	2	BAJO	2
		[I.6]	Corte de suministro		1	2	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		1	2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		1	2	BAJO	2
		[E.1]	Errores de los usuarios		0.1	0.13333	BAJO	2
		[E.2]	Errores del administrador		0.05	0.1	BAJO	2
		[E.9]	Errores de re-encaminamiento		0.05	0.1	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.9	1.8	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.9	1.8	BAJO	2
		[A.24]	Denegación del servicio		1	2	BAJO	2
[rout]	Router	[I.1]	Fuego	2	1	2	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.5	1	BAJO	2
		[I.6]	Corte de suministro		0.05	0.1	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		1	2	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		1	2	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		1	2	BAJO	2
		[E.2]	Errores del administrador		0.1	0.10667	BAJO	2
		[E.9]	Errores de re-encaminamiento		0.9	1.8	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	1	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1	BAJO	2
		[A.24]	Denegación del servicio		0.5	1	BAJO	2
[fire]	Firewall	[I.1]	Fuego	3.7	1	3.66667	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.83333	BAJO	2
		[I.6]	Corte de suministro		0.05	0.18333	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.4	1.46667	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.5	1.83333	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	1.83333	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	1.83333	BAJO	2

		[E.20]	Vulnerabilidades de los programas (software)		0.8	2.81111	MEDIO	3
		[E.21]	Errores de mantenimiento / actualización de programas (software)		0.1	0.36667	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	1.83333	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1.83333	BAJO	2
		[A.4]	Manipulación de la configuración		0.1	0.42778	BAJO	2
		[A.24]	Denegación del servicio		0.5	1.83333	BAJO	2
[COM] REDES DE COMUNICACIONES								
[cint]	Internet	[I.1]	Fuego	3	0.6	1.8	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.8	2.4	MEDIO	3
		[I.6]	Corte de suministro		0.5	1.5	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.8	2.4	MEDIO	3
		[I.8]	Fallo de servicios de comunicaciones		1	3	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	0.6	BAJO	2
		[E.4]	Errores de configuración		0.01	0.03	MUY BAJO	1
		[E.9]	Errores de re-encaminamiento		0.05	0.15	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.5	1.5	BAJO	2
		[A.24]	Denegación del servicio		0.5	1.5	BAJO	2
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	3	0.5	1.5	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.3	0.9	BAJO	2
		[I.8]	Fallo de servicios de comunicaciones		0.9	2.7	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.6	1.8	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	1.5	BAJO	2
		[E.25]	Pérdida de equipos		0.5	1.5	BAJO	2
		[A.24]	Denegación del servicio		0.8	2.4	MEDIO	3
[MEDIA] SOPORTE DE INFORMACIÓN								
[elect]	Electrónicos							
[ele1]	Cintas Magnéticas	[I.1]	Fuego	4.5	1	4.5	ALTO	4
		[I.5]	Avería de origen físico o lógico		1	4.5	ALTO	4
		[I.10]	Degradación de los soportes de almacenamiento de la información		1	4.5	ALTO	4
		[A.25]	Robo		0.95	4.275	ALTO	4
[ele2]	Disco externo USB	[I.1]	Fuego	3.75	1	3.75	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	1.875	BAJO	2
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	1.875	BAJO	2
		[E.1]	Errores de los usuarios		0.3	1.1875	BAJO	2
		[E.25]	Pérdida de equipos		0.7	2.625	MEDIO	3
[store]	Storage de respaldo de BD	[I.1]	Fuego	4.5	1	4.5	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.5	2.25	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.8	3.6	ALTO	4
		[I.10]	Degradación de los soportes de almacenamiento de la información		0.5	2.25	MEDIO	3
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.25	MEDIO	3
		[A.24]	Denegación del servicio		0.05	0.225	BAJO	2
[noel]	No electrónico							
[mimp]	Material impreso	[I.1]	Fuego	5.3	1	5.33333	ALTO	4
		[E.7]	Deficiencias en la organización		0.4	2.13333	MEDIO	3
		[E.14]	Escapes de información		0.1	0.53333	BAJO	2
		[E.19]	Fugas de información		0.2	1.06667	BAJO	2
		[A.19]	Divulgación de información		0.1	0.53333	BAJO	2
		[A.25]	Robo		0.35	1.86667	BAJO	2
[AUX] EQUIPAMIENTO AUXILIAR								
[powr]	Acumulador de energía UPS	[I.1]	Fuego	5	1	5	ALTO	4
		[I.5]	Avería de origen físico o lógico		1	5	ALTO	4
		[I.6]	Corte de suministro		0.05	0.25	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.1	0.5	BAJO	2

		[I.8]	Fallo de servicios de comunicaciones		0.01	0.05	MUY BAJO	1
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.05	0.25	BAJO	2
		[E.1]	Errores de los usuarios		0.3	1.33333	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.7	3.5	ALTO	4
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	5	1	5	ALTO	4
		[I.2]	Daños por agua		0.5	2.5	MEDIO	3
		[I.*]	Desastres industriales		0.5	2.5	MEDIO	3
		[I.3]	Contaminación mecánica		0.05	0.25	BAJO	2
		[I.4]	Contaminación electromagnética		0.05	0.25	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.5	2.5	MEDIO	3
		[I.6]	Corte de suministro		0.1	0.5	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.5	MEDIO	3
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.9	4.5	ALTO	4
		[E.1]	Errores de los usuarios		0.4	2	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.5	2.5	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
		[A.11]	Acceso no autorizado		0.025	0.125	BAJO	2
		[A.23]	Manipulación de los equipos		0.25	1.25	BAJO	2
		[A.25]	Robo		0.5	2.5	MEDIO	3
[gelc]	Grupo electrógeno	[I.1]	Fuego	5	1	5	ALTO	4
		[I.2]	Daños por agua		1	5	ALTO	4
		[I.4]	Contaminación electromagnética		0.05	0.25	BAJO	2
		[I.5]	Avería de origen físico o lógico		1	5	ALTO	4
		[I.6]	Corte de suministro		0.05	0.25	BAJO	2
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.2	1	BAJO	2
		[E.1]	Errores de los usuarios		0.2	1.16667	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.6	3	MEDIO	3
		[E.24]	Caída del sistema por agotamiento de recursos		1	5	ALTO	4
		[A.25]	Robo		0.5	2.5	MEDIO	3
		[A.28]	Indisponibilidad del personal		0.3	1.5	BAJO	2
[cable]	Cableado							
[cab1]	Cableado de red	[I.1]	Fuego	5.5	0.7	3.85	ALTO	4
		[I.2]	Daños por agua		0.7	3.85	ALTO	4
		[I.4]	Contaminación electromagnética		0.1	0.55	BAJO	2
		[I.5]	Avería de origen físico o lógico		0.7	3.85	ALTO	4
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.2	1.1	BAJO	2
		[A.7]	Uso no previsto		0.2	1.30167	BAJO	2
		[A.23]	Manipulación de los equipos		0.125	0.6875	BAJO	2
		[A.25]	Robo		0.05	0.275	BAJO	2
		[A.28]	Indisponibilidad del personal		0.05	0.275	BAJO	2
[cab2]	Fibra óptica	[I.1]	Fuego	5.5	0.7	3.85	ALTO	4
		[I.5]	Avería de origen físico o lógico		0.3	1.65	BAJO	2
		[E.7]	Deficiencias en la organización		0.1	0.55	BAJO	2
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)		0.2	1.1	BAJO	2
		[E.28]	Indisponibilidad del personal		0.05	0.275	BAJO	2
		[A.23]	Manipulación de los equipos		0.05	0.275	BAJO	2
[L] INSTALACIONES								
[site]	Data Center	[N.*]	Desastres naturales	5.5	1	5.5	ALTO	4
		[I.1]	Fuego		1	5.5	ALTO	4
		[I.2]	Daños por agua		0.05	0.275	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.9	4.95	ALTO	4
		[I.9]	Interrupción de otros servicios y suministros esenciales		0.5	2.75	MEDIO	3
		[E.25]	Pérdida de equipos		0.125	0.6875	BAJO	2

		[A.11]	Acceso no autorizado		0.35	1.925	BAJO	2
		[A.26]	Ataque destructivo		0.9	4.95	ALTO	4
		[A.27]	Ocupación enemiga		0.75	4.125	ALTO	4
		[A.28]	Indisponibilidad del personal		0.8	4.4	ALTO	4
[P] PERSONAL								
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	2.5	0.6	1.5	BAJO	2
		[E.1]	Errores de los usuarios		0.3	0.66667	BAJO	2
		[E.18]	Destrucción de la información		0.2	0.5	BAJO	2
		[E.19]	Fugas de información		0.2	0.5	BAJO	2
		[E.20]	Vulnerabilidades de los programas (software)		0.2	0.5	BAJO	2
		[E.24]	Caída del sistema por agotamiento de recursos		0.4	1	BAJO	2
		[E.25]	Pérdida de equipos		0.075	0.1875	BAJO	2
		[A.6]	Abuso de privilegios de acceso		0.15	0.375	BAJO	2
		[A.7]	Uso no previsto		0.12	0.29167	BAJO	2
		[A.15]	Modificación deliberada de la información		0.2	0.5	BAJO	2
		[A.18]	Destrucción de información		0.5	1.25	BAJO	2
		[A.25]	Robo		0.5	1.25	BAJO	2
		[A.29]	Extorsión		0.6	1.5	BAJO	2
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	2.5	0.5	1.25	BAJO	2
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	1.25	BAJO	2
		[E.1]	Errores de los usuarios		0.1	0.25	BAJO	2
		[E.7]	Deficiencias en la organización		0.5	1.25	BAJO	2
		[A.19]	Divulgación de información		0.2	0.5	BAJO	2
		[A.29]	Extorsión		0.05	0.125	BAJO	2
		[A.30]	Ingeniería social		0.2	0.5	BAJO	2
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	5.5	0.5	2.75	MEDIO	3
		[I.7]	Condiciones inadecuadas de temperatura o humedad		0.5	2.75	MEDIO	3
		[I.11]	Emanaciones electromagnética		0.3	1.65	BAJO	2
		[E.28]	Indisponibilidad del personal		0.9	4.95	ALTO	4
		[A.28]	Indisponibilidad del personal		0.2	1.1	BAJO	2

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

4.2.7. Determinación de Probabilidad de la amenaza

Se elaboró la tabla Probabilidad de amenaza en los activos de TI de la Oficina General de TI – UNC. Se obtuvo que el 33% de las amenazas serían muy poco frecuente de que ocurrieran, 27% de las amenazas identificadas serían poco frecuentes de que ocurran, 29 % recibieron la probabilidad de que ocurran de manera normal, 9% con probabilidad de ocurrencia frecuente y 2% con probabilidad de ocurrencia de muy frecuente.

Tabla N° 25. Probabilidad de Amenaza en los activos de TI

ACTIVO		AMENAZA		VALORACIÓN DE LA PROBABILIDAD	
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE	NIVEL	ESCALA CUALITATIVA
[S] SERVICIOS					
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	5	Muy Frecuente
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[sgeo]	Gestión de Actas virtuales	[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[E.1]	Errores de los usuarios	5	Muy Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[A.5]	Suplantación de la identidad del usuario	2	Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[SW] APLICACIONES					
[swsc]	Sistema académico actas virtuales UNC	[N.1]	Fuego	1	Muy Poco Frecuente
		[I.8]	Fallo de servicios de comunicaciones	2	Poco Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.24]	Denegación del servicio	3	Normal
[swoc]	Sistema académico	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	1	Muy Poco Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	Poco Frecuente

		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[HW] EQUIPOS INFORMATICOS					
[serv]	Servidores				
[ser1]	Servidor de dominio	[N.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	2	Poco Frecuente
		[A.4]	Manipulación de la configuración	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[ser2]	Servidor de proxy	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	4	Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	5	Muy Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.4]	Errores de configuración	1	Muy Poco Frecuente

		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	2	Poco Frecuente
		[E.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[ser3]	Servidor de base de datos	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.2]	Errores del administrador	2	Poco Frecuente
		[E.14]	Escapes de información	2	Poco Frecuente
		[E.15]	Alteración accidental de la información	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.15]	Modificación deliberada de la información	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	3	Normal
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.14]	Escapes de información	1	Muy Poco Frecuente

		[E.15]	Alteración accidental de la información	1	Muy Poco Frecuente
		[E.18]	Destrucción de la información	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	1	Muy Poco Frecuente
		[E.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
		[A.15]	Modificación deliberada de la información	1	Muy Poco Frecuente
		[A.18]	Destrucción de información	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	2	Poco Frecuente
[ser5]	Servidor web	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	1	Muy Poco Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.14]	Escapes de información	2	Poco Frecuente
		[E.15]	Alteración accidental de la información	1	Muy Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.24]	Denegación del servicio	2	Poco Frecuente
[ser6]	Servidor de archivos	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal

		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.1]	Errores de los usuarios	3	Normal
		[E.14]	Escapes de información	3	Normal
		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.5]	Suplantación de la identidad del usuario	2	Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	2	Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	1	Muy Poco Frecuente
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente

		[E.20]	Vulnerabilidades de los programas (software)	1	Muy Poco Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.6]	Abuso de privilegios de acceso	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[netw]	Soporte de red				
		[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	Frecuente
[swit]	Switch	[E.1]	Errores de los usuarios	1	Muy Poco Frecuente
		[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.24]	Denegación del servicio	2	Poco Frecuente
		[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
[rout]	Router	[E.2]	Errores del administrador	1	Muy Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[fire]	Firewall	[I.1]	Fuego	1	Muy Poco Frecuente

		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	Normal
		[E.20]	Vulnerabilidades de los programas (software)	5	Muy Frecuente
		[E.21]	Errores de mantenimiento / actualización de programas (software)	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	5	Muy Frecuente
		[A.4]	Manipulación de la configuración	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[COM] REDES DE COMUNICACIONES					
[cint]	Internet	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	4	Frecuente
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.4]	Errores de configuración	1	Muy Poco Frecuente
		[E.9]	Errores de re-encaminamiento	1	Muy Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	1	Muy Poco Frecuente
		[A.24]	Denegación del servicio	1	Muy Poco Frecuente
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	5	Muy Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[E.25]	Pérdida de equipos	2	Poco Frecuente
		[A.24]	Denegación del servicio	2	Poco Frecuente
[MEDIA] SOPORTE DE INFORMACION					
[elect]	Electrónicos				
[ele1]	Cintas Magnéticas	[I.1]	Fuego	1	Muy Poco Frecuente

		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[A.25]	Robo	2	Poco Frecuente
[ele2]	Disco externo USB	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	1	Muy Poco Frecuente
		[I.10]	Degradación de los soportes de almacenamiento de la información	1	Muy Poco Frecuente
		[E.1]	Errores de los usuarios	1	Muy Poco Frecuente
		[E.25]	Pérdida de equipos	1	Muy Poco Frecuente
[store]	Storage de respaldo de BD	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[A.24]	Denegación del servicio	3	Normal
[noel]	No electrónico				
[mimp]	Material impreso	[I.1]	Fuego	1	Muy Poco Frecuente
		[E.7]	Deficiencias en la organización	3	Normal
		[E.14]	Escapes de información	2	Poco Frecuente
		[E.19]	Fugas de información	2	Poco Frecuente
		[A.19]	Divulgación de información	2	Poco Frecuente
		[A.25]	Robo	1	Muy Poco Frecuente
[AUX] EQUIPAMIENTO AUXILIAR					
[powr]	Acumulador de energía UPS	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	3	Normal
		[I.6]	Corte de suministro	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.8]	Fallo de servicios de comunicaciones	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal

[psis]	Sistema de aire acondicionado	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	2	Poco Frecuente
		[I.*]	Desastres industriales	1	Muy Poco Frecuente
		[I.3]	Contaminación mecánica	2	Poco Frecuente
		[I.4]	Contaminación electromagnética	3	Normal
		[I.5]	Avería de origen físico o lógico	3	Normal
		[I.6]	Corte de suministro	3	Normal
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	4	Frecuente
		[A.11]	Acceso no autorizado	2	Poco Frecuente
		[A.23]	Manipulación de los equipos	1	Muy Poco Frecuente
		[A.25]	Robo	1	Muy Poco Frecuente
[gelc]	Grupo electrógeno	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	2	Poco Frecuente
		[I.4]	Contaminación electromagnética	3	Normal
		[I.5]	Avería de origen físico o lógico	2	Poco Frecuente
		[I.6]	Corte de suministro	5	Muy Frecuente
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	Normal
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[A.25]	Robo	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	2	Poco Frecuente
[cable]	Cableado				
[cab1]	Cableado de red	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	1	Muy Poco Frecuente
		[I.4]	Contaminación electromagnética	3	Normal
		[I.5]	Avería de origen físico o lógico	4	Frecuente
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	Normal
		[A.7]	Uso no previsto	2	Poco Frecuente
		[A.23]	Manipulación de los equipos	3	Normal

		[A.25]	Robo	4	Frecuente
		[A.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
[cab2]	Fibra óptica	[I.1]	Fuego	1	Muy Poco Frecuente
		[I.5]	Avería de origen físico o lógico	3	Normal
		[E.7]	Deficiencias en la organización	3	Normal
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	Poco Frecuente
		[E.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
		[A.23]	Manipulación de los equipos	3	Normal
[L] INSTALACIONES					
[site]	Data Center	[N.*]	Desastres naturales	1	Muy Poco Frecuente
		[I.1]	Fuego	1	Muy Poco Frecuente
		[I.2]	Daños por agua	1	Muy Poco Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	Normal
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	Poco Frecuente
		[E.25]	Pérdida de equipos	1	Muy Poco Frecuente
		[A.11]	Acceso no autorizado	1	Muy Poco Frecuente
		[A.26]	Ataque destructivo	1	Muy Poco Frecuente
		[A.27]	Ocupación enemiga	1	Muy Poco Frecuente
		[A.28]	Indisponibilidad del personal	1	Muy Poco Frecuente
[P] PERSONAL					
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	2	Poco Frecuente
		[E.1]	Errores de los usuarios	2	Poco Frecuente
		[E.18]	Destrucción de la información	3	Normal
		[E.19]	Fugas de información	2	Poco Frecuente
		[E.20]	Vulnerabilidades de los programas (software)	3	Normal
		[E.24]	Caída del sistema por agotamiento de recursos	3	Normal
		[E.25]	Pérdida de equipos	1	Muy Poco Frecuente
		[A.6]	Abuso de privilegios de acceso	2	Poco Frecuente
		[A.7]	Uso no previsto	2	Poco Frecuente
		[A.15]	Modificación deliberada de la información	1	Muy Poco Frecuente
		[A.18]	Destrucción de información	1	Muy Poco Frecuente

		[A.25]	Robo	2	Poco Frecuente
		[A.29]	Extorsión	2	Poco Frecuente
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	4	Frecuente
		[E.1]	Errores de los usuarios	3	Normal
		[E.7]	Deficiencias en la organización	3	Normal
		[A.19]	Divulgación de información	2	Poco Frecuente
		[A.29]	Extorsión	2	Poco Frecuente
		[A.30]	Ingeniería social	2	Poco Frecuente
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	4	Frecuente
		[I.7]	Condiciones inadecuadas de temperatura o humedad	4	Frecuente
		[I.11]	Emanaciones electromagnética	4	Frecuente
		[E.28]	Indisponibilidad del personal	2	Poco Frecuente
		[A.28]	Indisponibilidad del personal	2	Poco Frecuente

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

4.2.8. Estimación del riesgo

Los resultados obtenidos, se resume de la siguiente manera:

- La amenaza interrupción de otros servicios y suministros esenciales identificada en el activo [sges] recibe un nivel importante de riesgo.
- Interrupción de otros servicios y suministros esenciales, caída del sistema por agotamiento de recursos, denegación del servicio del activo [swsc] reciben un nivel de riesgo importante.
- Caída del sistema por agotamiento de recursos del activo [swoc] representa un nivel de riesgo crítico.
- Caída del sistema por agotamiento de recursos e indisponibilidad del personal del activo [ser3] representa un nivel de riesgo importante.
- Las amenazas de fuego e interrupción de otros servicios y suministros esenciales del activo [ser4] reciben un nivel de riesgo importante.
- Las amenazas: vulnerabilidades de los programas de activo [fire] representa un nivel de riesgo importante.
- Las amenazas avería de origen físico o lógico identificada del activo [cinf] representa un nivel importante de riesgo.

- El activo [store] cuyas amenazas identificada interrupción de otros servicios y suministros esenciales representa un nivel importante de nivel de riesgo.
- Las amenazas de avería de origen físico o lógico y caída del sistema por agotamiento de recursos del activo [powr] representan un nivel de riesgo importante en el activo.
- El activo [psis] cuyas amenazas identificas como interrupción de otros servicios y suministros esenciales representa un nivel de riesgo importante.
- Y la amenaza caída del sistema por agotamiento de recursos representa un nivel de riesgo muy crítico de riesgo.
- La amenaza identificada en el activo [gelc] caída del sistema por agotamiento de recursos representa un nivel de riesgo importante.
- La amenaza avería de origen físico o lógico identificada en el activo [cab1] representa un nivel crítico en el activo.
- El activo [site] una de las amenazad identificadas como Condiciones inadecuadas de temperatura o humedad representa un nivel importante en el nivel de riesgo.
- Las amenazas contaminación electromagnética y condiciones inadecuadas de temperatura o humedad representan un nivel de riesgo importante de riesgo en el activo [adm1].

Tabla N° 26. Estimación del nivel de riesgo

ACTIVO		AMENAZA		IMPACTO	PROBABILIDAD	CÓDIGO RIESGO	RIESGO	NIVEL	ESCALA
CÓDIGO	NOMBRE	CÓDIGO	NOMBRE						
[S] SERVICIOS									
[sges]	Gestión de Actas virtuales y matricula online	[I.6]	Corte de suministro	3	3	R1	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	2	3	R2	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	5	R3	15	4	Importante
		[E.1]	Errores de los usuarios	2	2	R4	4	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R5	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	4	R6	8	3	Apreciable
		[A.24]	Denegación del servicio	2	2	R7	4	1	Despreciable
[sgeo]	Gestión de Actas virtuales	[I.8]	Fallo de servicios de comunicaciones	2	3	R8	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R9	8	3	Apreciable
		[E.1]	Errores de los usuarios	2	5	R10	10	3	Apreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R11	4	1	Despreciable
		[A.5]	Suplantación de la identidad del usuario	2	2	R12	4	1	Despreciable
		[A.24]	Denegación del servicio	2	3	R13	6	2	Bajo
[SW] APLICACIONES									
[swsc]	Sistema académico actas virtuales UNC	[N.1]	Fuego	4	1	R14	4	1	Despreciable
		[I.8]	Fallo de servicios de comunicaciones	4	2	R15	8	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	4	R16	12	4	Importante
		[E.2]	Errores del administrador	2	1	R17	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3	R18	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	3	R19	9	3	Apreciable
		[E.24]	Caída del sistema por agotamiento de recursos	4	3	R20	12	4	Importante
		[A.24]	Denegación del servicio	4	3	R21	12	4	Importante
[swoc]	Sistema académico	[I.1]	Fuego	4	1	R22	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R23	2	1	Despreciable
		[I.6]	Corte de suministro	3	3	R24	9	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R25	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	3	1	R26	3	1	Despreciable

		[I.9]	Interrupción de otros servicios y suministros esenciales	2	2	R27	4	1	Despreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	1	R28	3	1	Despreciable
		[E.2]	Errores del administrador	2	1	R29	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R30	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	3	1	R31	3	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	4	4	R32	16	5	Crítico
		[A.24]	Denegación del servicio	4	2	R33	8	3	Apreciable
[HW] EQUIPOS INFORMÁTICOS									
[serv]	Servidores								
[ser1]	Servidor de dominio	[N.1]	Fuego	4	1	R34	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R35	4	1	Despreciable
		[I.6]	Corte de suministro	2	4	R36	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R37	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R38	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R39	8	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R40	4	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R41	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	4	2	R42	8	3	Apreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	2	R43	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R44	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	2	R45	6	2	Bajo
		[A.4]	Manipulación de la configuración	2	1	R46	2	1	Despreciable
		[A.24]	Denegación del servicio	4	2	R47	8	3	Apreciable
[ser2]	Servidor de proxy	[I.1]	Fuego	2	1	R48	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R49	4	1	Despreciable
		[I.6]	Corte de suministro	2	3	R50	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R51	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	4	R52	8	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	5	R53	10	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R54	4	1	Despreciable
		[E.2]	Errores del administrador	2	1	R55	2	1	Despreciable
		[E.4]	Errores de configuración	2	1	R56	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R57	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R58	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R59	4	1	Despreciable

		[E.24]	Caída del sistema por agotamiento de recursos	2	2	R60	4	1	Despreciable
		[E.28]	Indisponibilidad del personal	2	1	R61	2	1	Despreciable
		[A.24]	Denegación del servicio	2	3	R62	6	2	Bajo
[ser3]	Servidor de base de datos	[I.1]	Fuego	4	1	R63	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	1	R64	3	1	Despreciable
		[I.6]	Corte de suministro	3	3	R65	9	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R66	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R67	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R68	8	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R69	4	1	Despreciable
		[E.2]	Errores del administrador	2	2	R70	4	1	Despreciable
		[E.14]	Escapes de información	4	2	R71	8	3	Apreciable
		[E.15]	Alteración accidental de la información	3	1	R72	3	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R73	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R74	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R75	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	4	R76	12	4	Importante
		[A.15]	Modificación deliberada de la información	2	1	R77	2	1	Despreciable
		[A.24]	Denegación del servicio	3	2	R78	6	2	Bajo
		[A.28]	Indisponibilidad del personal	4	3	R79	12	4	Importante
[ser4]	Servidor de base de datos - backup	[I.1]	Fuego	2	1	R80	2	1	Despreciable
		[I.6]	Corte de suministro	3	4	R81	12	4	Importante
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R82	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R83	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	4	R84	12	4	Importante
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	1	R85	3	1	Despreciable
		[E.2]	Errores del administrador	2	1	R86	2	1	Despreciable
		[E.14]	Escapes de información	4	1	R87	4	1	Despreciable
		[E.15]	Alteración accidental de la información	3	1	R88	3	1	Despreciable
		[E.18]	Destrucción de la información	3	1	R89	3	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R90	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	2	R91	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R92	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	3	1	R93	3	1	Despreciable
		[E.28]	Indisponibilidad del personal	2	1	R94	2	1	Despreciable

		[A.15]	Modificación deliberada de la información	3	1	R95	3	1	Despreciable
		[A.18]	Destrucción de información	3	1	R96	3	1	Despreciable
		[A.24]	Denegación del servicio	3	2	R97	6	2	Bajo
		[A.28]	Indisponibilidad del personal	2	2	R98	4	1	Despreciable
[ser5]	Servidor web	[I.1]	Fuego	2	1	R99	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R100	2	1	Despreciable
		[I.6]	Corte de suministro	2	1	R101	2	1	Despreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R102	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R103	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R104	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	1	R105	2	1	Despreciable
		[E.14]	Escapes de información	2	2	R106	4	1	Despreciable
		[E.15]	Alteración accidental de la información	2	1	R107	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R108	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	2	R109	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R110	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	3	R111	9	3	Apreciable
		[A.24]	Denegación del servicio	3	2	R112	6	2	Bajo
[ser6]	Servidor de archivos	[I.1]	Fuego	2	1	R113	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R114	2	1	Despreciable
		[I.6]	Corte de suministro	2	4	R115	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R116	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R117	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R118	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	1	R119	2	1	Despreciable
		[E.1]	Errores de los usuarios	2	3	R120	6	2	Bajo
		[E.14]	Escapes de información	2	3	R121	6	2	Bajo
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R122	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R123	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R124	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	4	R125	8	3	Apreciable
		[A.5]	Suplantación de la identidad del usuario	2	2	R126	4	1	Despreciable
		[A.24]	Denegación del servicio	2	3	R127	6	2	Bajo
[ser7]	Servidor de datos - OCCA	[I.1]	Fuego	2	1	R128	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R129	2	1	Despreciable

		[I.6]	Corte de suministro	2	4	R130	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R131	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R132	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R133	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	2	R134	4	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	2	R135	4	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R136	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R137	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	1	R138	3	1	Despreciable
		[A.24]	Denegación del servicio	3	1	R139	3	1	Despreciable
[ser8]	Servidor de base de datos - backup-OCCA	[I.1]	Fuego	3	1	R140	3	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	2	R141	6	2	Bajo
		[I.6]	Corte de suministro	2	3	R142	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R143	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R144	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	3	R145	9	3	Apreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	2	R146	6	2	Bajo
		[E.2]	Errores del administrador	2	1	R147	2	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	1	R148	2	1	Despreciable
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	1	R149	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	1	R150	2	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	3	3	R151	9	3	Apreciable
		[A.6]	Abuso de privilegios de acceso	2	1	R152	2	1	Despreciable
		[A.24]	Denegación del servicio	3	3	R153	9	3	Apreciable
[netw]	Soporte de red								
[swit]	Switch	[I.1]	Fuego	2	1	R154	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R155	4	1	Despreciable
		[I.6]	Corte de suministro	2	3	R156	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R157	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R158	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	4	R159	8	3	Apreciable
		[E.1]	Errores de los usuarios	2	1	R160	2	1	Despreciable
		[E.2]	Errores del administrador	2	1	R161	2	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R162	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R163	6	2	Bajo

		[E.24]	Caída del sistema por agotamiento de recursos	2	3	R164	6	2	Bajo
		[A.24]	Denegación del servicio	2	2	R165	4	1	Despreciable
[rout]	Router	[I.1]	Fuego	2	1	R166	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R167	4	1	Despreciable
		[I.6]	Corte de suministro	2	4	R168	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R169	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R170	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R171	6	2	Bajo
		[E.2]	Errores del administrador	2	1	R172	2	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R173	2	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R174	4	1	Despreciable
		[E.24]	Caída del sistema por agotamiento de recursos	2	4	R175	8	3	Apreciable
		[A.24]	Denegación del servicio	2	2	R176	4	1	Despreciable
[fire]	Firewall	[I.1]	Fuego	4	1	R177	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	2	R178	4	1	Despreciable
		[I.6]	Corte de suministro	2	4	R179	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R180	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	2	3	R181	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R182	6	2	Bajo
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	3	R183	6	2	Bajo
		[E.20]	Vulnerabilidades de los programas (software)	3	5	R184	15	4	Importante
		[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3	R185	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R186	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	2	5	R187	10	3	Apreciable
		[A.4]	Manipulación de la configuración	2	1	R188	2	1	Despreciable
		[A.24]	Denegación del servicio	2	2	R189	4	1	Despreciable
[COM] REDES DE COMUNICACIONES									
[cint]	Internet	[I.1]	Fuego	2	1	R190	2	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	4	R191	12	4	Importante
		[I.6]	Corte de suministro	2	3	R192	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R193	9	3	Apreciable
		[I.8]	Fallo de servicios de comunicaciones	3	3	R194	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R195	6	2	Bajo
		[E.4]	Errores de configuración	1	1	R196	1	1	Despreciable
		[E.9]	Errores de re-encaminamiento	2	1	R197	2	1	Despreciable

		[E.24]	Caída del sistema por agotamiento de recursos	2	1	R198	2	1	Despreciable
		[A.24]	Denegación del servicio	2	1	R199	2	1	Despreciable
[cwfi]	Red Inalámbrica	[I.6]	Corte de suministro	2	5	R200	10	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R201	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	3	3	R202	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R203	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R204	6	2	Bajo
		[E.25]	Pérdida de equipos	2	2	R205	4	1	Despreciable
		[A.24]	Denegación del servicio	3	2	R206	6	2	Bajo
[MEDIA] SOPORTE DE INFORMACIÓN									
[elect]	Electrónicos								
[ele1]	Cintas Magnéticas	[I.1]	Fuego	4	1	R207	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	4	1	R208	4	1	Despreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	4	1	R209	4	1	Despreciable
		[A.25]	Robo	4	2	R210	8	3	Apreciable
[ele2]	Disco externo USB	[I.1]	Fuego	4	1	R211	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	1	R212	2	1	Despreciable
		[I.10]	Degradación de los soportes de almacenamiento de la información	2	1	R213	2	1	Despreciable
		[E.1]	Errores de los usuarios	2	1	R214	2	1	Despreciable
		[E.25]	Pérdida de equipos	3	1	R215	3	1	Despreciable
[store]	Storage de respaldo de BD	[I.1]	Fuego	4	1	R216	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	3	2	R217	6	2	Bajo
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	3	R218	12	4	Importante
		[I.10]	Degradación de los soportes de almacenamiento de la información	3	2	R219	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R220	6	2	Bajo
		[A.24]	Denegación del servicio	2	3	R221	6	2	Bajo
[noel]	No electrónico								
[mimp]	Material impreso	[I.1]	Fuego	4	1	R222	4	1	Despreciable
		[E.7]	Deficiencias en la organización	3	3	R223	9	3	Apreciable
		[E.14]	Escapes de información	2	2	R224	4	1	Despreciable
		[E.19]	Fugas de información	2	2	R225	4	1	Despreciable
		[A.19]	Divulgación de información	2	2	R226	4	1	Despreciable
		[A.25]	Robo	2	1	R227	2	1	Despreciable
[AUX] EQUIPAMIENTO AUXILIAR									
[powr]		[I.1]	Fuego	4	1	R228	4	1	Despreciable

	Acumulador de energía UPS	[I.5]	Avería de origen físico o lógico	4	3	R229	12	4	Importante
		[I.6]	Corte de suministro	2	4	R230	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	R231	6	2	Bajo
		[I.8]	Fallo de servicios de comunicaciones	1	3	R232	3	1	Despreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R233	6	2	Bajo
		[E.1]	Errores de los usuarios	2	2	R234	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	4	2	R235	8	3	Apreciable
		[E.24]	Caída del sistema por agotamiento de recursos	4	3	R236	12	4	Importante
[psis]	Sistema de aire acondicionado	[I.1]	Fuego	4	1	R237	4	1	Despreciable
		[I.2]	Daños por agua	3	2	R238	6	2	Bajo
		[I.*]	Desastres industriales	3	1	R239	3	1	Despreciable
		[I.3]	Contaminación mecánica	2	2	R240	4	1	Despreciable
		[I.4]	Contaminación electromagnética	2	3	R241	6	2	Bajo
		[I.5]	Avería de origen físico o lógico	3	3	R242	9	3	Apreciable
		[I.6]	Corte de suministro	2	3	R243	6	2	Bajo
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	3	R244	9	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	4	3	R245	12	4	Importante
		[E.1]	Errores de los usuarios	2	2	R246	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R247	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	4	4	R248	16	5	Critico
		[A.11]	Acceso no autorizado	2	2	R249	4	1	Despreciable
		[A.23]	Manipulación de los equipos	2	1	R250	2	1	Despreciable
		[A.25]	Robo	3	1	R251	3	1	Despreciable
[gelc]	Grupo electrógeno	[I.1]	Fuego	4	1	R252	4	1	Despreciable
		[I.2]	Daños por agua	4	2	R253	8	3	Apreciable
		[I.4]	Contaminación electromagnética	2	3	R254	6	2	Bajo
		[I.5]	Avería de origen físico o lógico	4	2	R255	8	3	Apreciable
		[I.6]	Corte de suministro	2	5	R256	10	3	Apreciable
		[I.9]	Interrupción de otros servicios y suministros esenciales	2	3	R257	6	2	Bajo
		[E.1]	Errores de los usuarios	2	2	R258	4	1	Despreciable
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	3	2	R259	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	4	3	R260	12	4	Importante
		[A.25]	Robo	3	2	R261	6	2	Bajo
		[A.28]	Indisponibilidad del personal	2	2	R262	4	1	Despreciable
[cable]	Cableado								

[cab1]	Cableado de red	[I.1]	Fuego	4	1	R263	4	1	Despreciable
		[I.2]	Daños por agua	4	1	R264	4	1	Despreciable
		[I.4]	Contaminación electromagnética	2	3	R265	6	2	Bajo
		[I.5]	Avería de origen físico o lógico	4	4	R266	16	5	Critico
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	3	R267	6	2	Bajo
		[A.7]	Uso no previsto	2	2	R268	4	1	Despreciable
		[A.23]	Manipulación de los equipos	2	3	R269	6	2	Bajo
		[A.25]	Robo	2	4	R270	8	3	Apreciable
		[A.28]	Indisponibilidad del personal	2	1	R271	2	1	Despreciable
[cab2]	Fibra óptica	[I.1]	Fuego	4	1	R272	4	1	Despreciable
		[I.5]	Avería de origen físico o lógico	2	3	R273	6	2	Bajo
		[E.7]	Deficiencias en la organización	2	3	R274	6	2	Bajo
		[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	2	2	R275	4	1	Despreciable
		[E.28]	Indisponibilidad del personal	2	1	R276	2	1	Despreciable
		[A.23]	Manipulación de los equipos	2	3	R277	6	2	Bajo
[L] INSTALACIONES									
[site]	Data Center	[N.*]	Desastres naturales	4	1	R278	4	1	Despreciable
		[I.1]	Fuego	4	1	R279	4	1	Despreciable
		[I.2]	Daños por agua	2	1	R280	2	1	Despreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	4	3	R281	12	4	Importante
		[I.9]	Interrupción de otros servicios y suministros esenciales	3	2	R282	6	2	Bajo
		[E.25]	Pérdida de equipos	2	1	R283	2	1	Despreciable
		[A.11]	Acceso no autorizado	2	1	R284	2	1	Despreciable
		[A.26]	Ataque destructivo	4	1	R285	4	1	Despreciable
		[A.27]	Ocupación enemiga	4	1	R286	4	1	Despreciable
		[A.28]	Indisponibilidad del personal	4	1	R287	4	1	Despreciable
[P] PERSONAL									
[ueex]	Usuario externo	[I.8]	Fallo de servicios de comunicaciones	2	2	R288	4	1	Despreciable
		[E.1]	Errores de los usuarios	2	2	R289	4	1	Despreciable
		[E.18]	Destrucción de la información	2	3	R290	6	2	Bajo
		[E.19]	Fugas de información	2	2	R291	4	1	Despreciable
		[E.20]	Vulnerabilidades de los programas (software)	2	3	R292	6	2	Bajo
		[E.24]	Caída del sistema por agotamiento de recursos	2	3	R293	6	2	Bajo
		[E.25]	Pérdida de equipos	2	1	R294	2	1	Despreciable
		[A.6]	Abuso de privilegios de acceso	2	2	R295	4	1	Despreciable

		[A.7]	Uso no previsto	2	2	R296	4	1	Despreciable
		[A.15]	Modificación deliberada de la información	2	1	R297	2	1	Despreciable
		[A.18]	Destrucción de información	2	1	R298	2	1	Despreciable
		[A.25]	Robo	2	2	R299	4	1	Despreciable
		[A.29]	Extorsión	2	2	R300	4	1	Despreciable
[uex1]	Personal de TI	[I.4]	Contaminación electromagnética	2	4	R301	8	3	Apreciable
		[I.7]	Condiciones inadecuadas de temperatura o humedad	2	4	R302	8	3	Apreciable
		[E.1]	Errores de los usuarios	2	3	R303	6	2	Bajo
		[E.7]	Deficiencias en la organización	2	3	R304	6	2	Bajo
		[A.19]	Divulgación de información	2	2	R305	4	1	Despreciable
		[A.29]	Extorsión	2	2	R306	4	1	Despreciable
		[A.30]	Ingeniería social	2	2	R307	4	1	Despreciable
[adm1]	Administrador del data center	[I.4]	Contaminación electromagnética	3	4	R308	12	4	Importante
		[I.7]	Condiciones inadecuadas de temperatura o humedad	3	4	R309	12	4	Importante
		[I.11]	Emanaciones electromagnética	2	4	R310	8	3	Apreciable
		[E.28]	Indisponibilidad del personal	4	2	R311	8	3	Apreciable
		[A.28]	Indisponibilidad del personal	2	2	R312	4	1	Despreciable

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

4.2.9. Mapa de calor de los niveles de riesgo

Finalmente, se elaboró el mapa de calor general que resumen los resultados obtenidos en la estimación de los niveles de riesgos calculados para cada activo de TI

Tabla N° 27. Mapa de calor de los niveles de riesgo

		IMPACTO				
		5	4	3	2	1
PROBABILIDAD	5			R3,R184	R53,R187,R200,R256	
	4		R32,R248,R266	R16,R76,R81,R84,R191,R308,R309	R6,R9,R36,R39,R52,R68,R115,R125,R130,R159,R168,R175,R179,R230,R270,R301,R302,R310	
	3		R20,R21,R79,R218,R229,R236,R245,R260,R281	R1,R19,R24,R65,R66,R67,R82,R83,R102,R103,R111,R131,R132,R143,R144,R145,R151,R153,R193,R194,R202,R223,R242,R244	R2,R13,R18,R25,R37,R38,R50,R51,R62,R104,R116,R117,R118,R119,R120,R121,R127,R133,R142,R156,R157,R158,R163,R164,R169,R170,R171,R181,R182,R183,R185,R186,R192,R195,R201,R203,R204,R221,R231,R233,R241,R243,R254,R257,R265,R267,R269,R273,R274,R277,R290,R292,R293,R303,R304	R232
	2		R15,R33,R42,R47,R71,R210,R235,R253,R255,R311	R8,R45,R78,R92,R97,R112,R141,R146,R206,R217,R219,R220,R238,R247,R259,R261,R282	R4,R5,R7,R11,R12,R27,R30,R35,R40,R43,R44,R49,R54,R59,R60,R69,R70,R73,R90,R91,R98,R106,R109,R110,R126,R134,R135,R155,R165,R167,R174,R176,R178,R189,R205,R224,R225,R226,R234,R240,R246,R249,R258,R262,R268,R275,R288,R289,R291,R295,R296,R299,R300,R305,R306,R307,R312	
	1		R14,R22,R34,R63,R87,R177,R207,R208,R209,R211,R216,R222,R228,R237,R252,R263,R264,R272,R278,R279,R285,R286,R287	R26,R28,R31,R64,R72,R85,R88,R89,R93,R95,R96,R138,R139,R140,R215,R239,R251	R17,R23,R29,R41,R46,R48,R55,R56,R57,R58,R61,R74,R75,R77,R80,R86,R94,R99,R100,R101,R105,R107,R108,R113,R114,R122,R123,R124,R128,R129,R136,R137,R147,R148,R149,R150,R152,R154,R160,R161,R162,R166,R172,R173,R190,R197,R198,R199,R212,R213,R214,R227,R250,R271,R276,R280,R283,R284,R294,R297,R298	R196

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Ya conociendo el nivel de riesgo que representan las amenazas, las colocamos en el mapa de calor para determinar a cuál de ellas se le van plantear las salvaguardas necesarias para poder reducir o eliminar el nivel de riesgo en los activos. En este caso las amenazas R32, R248, R266, R3, R184, R16, R76, R81, R84, R191, R308, R309, R53, R187, R200, R256, R20, R21, R79,R218, R229, R236, R245, R260, R281 son las amenazas que fueron utilizadas para el tratamiento de riesgo

4.3. Tratamiento del riesgo

Luego que se ha estimado los niveles de riesgo que se tienen en los diferentes activos de TI en la UNC, en la fase de identificación y análisis de riesgo, corresponde plantear las correspondientes salvaguardas para mitigar los niveles de riesgo no aceptables o tolerables por la Oficina General de TI de la UNC.

Utilizando el catálogo de salvaguardas que propone la metodología MagerIT, se contextualizaron un conjunto de salvaguardas, que se muestran en la tabla siguiente:

Tabla N° 28. Salvaguardas para el tratamiento de los riesgos

ANÁLISIS DE RIESGO								TRATAMIENTO DE RIESGO					
ACTIVO	AMENAZA	IMPACTO	PROBABILIDAD	CÓDIGO RIESGO	RIESGO	NIVEL	ESCALA	SALVAGUARDA					
											TIPO		EFECTO
CÓDIGO	CÓDIGO							CÓDIGO	NOMBRE	DESCRIPCIÓN	CÓDIGO	NOMBRE	
[S] SERVICIOS													
[sges]	[I.9]	3	5	R3	15	4	Importante	S.A	Aseguramiento de la disponibilidad	Implementar procedimientos para controlar la interrupción del servicio en caso este se vea afectado por la carencia de otro recurso.	[PR]	Preventivas	Preventiva
[SW] APLICACIONES													
[swsc]	[I.9]	3	4	R16	12	4	Importante	SW.A	Copias de seguridad (backup)	Generar copias de seguridad de la información y del software, y ser comprobadas regularmente de acuerdo con la política de copias de seguridad de la organización.	[PR]	Preventivas	Preventiva
	[E.24]	4	3	R20	12	4	Importante	SW.SC	Se aplican perfiles de seguridad	Definir politicas de seguridad para mantener la continuidad del servico en caso este haya caido por carga de trabajo desmesurada.	[PR]	Preventivas	Preventiva
	[A.24]	4	3	R21	12	4	Importante	SW.SC	Se aplican perfiles de seguridad	Definir politicas de seguridad para mantener la continuidad del servico en caso este haya caido por carga de trabajo desmesurada.	[PR]	Preventivas	Preventiva

[swoc]	[E.24]	4	4	R32	16	5	Critico	SW.SC	Se aplican perfiles de seguridad	Definir politicas de seguridad para mantener la continuidad del servico en caso este haya caido por carga de trabajo desmesurada.	[PR]	Preventivas	Preventiva
								SW.A	Copias de seguridad (backup)	Generar copias de seguridad de la información y del software y ser comprobadas regularmente de acuerdo con la política de copias de seguridad de la organización.	[PR]	Preventivas	Preventiva
[HW] EQUIPOS INFORMÁTICOS													
[serv]													
[ser3]	[E.24]	3	4	R76	12	4	Importante	HW.A	Aseguramiento de la disponibilidad	Implementar procedimientos para controlar la interrupción del servicio en caso este se vea afectado por la carencia de otro recurso.	[PR]	Preventivas	Preventivas
	[A.28]	4	3	R79	12	4	Importante	HW.op	Operación	Se debe realizar un plan de acción en caso los trabajadores de la Oficina General de TI no puedan ingresar a su lugar de trabajo para que los servicios no se vean afectados.	[PR]	Preventivas	Preventivas
[ser4]	[I.6]	3	4	R81	12	4	Importante	HW.op	Operación	Se debería aplicar un perfil de seguridad en caso el generador de energía se apague. Cuando el combustible de este se termina los servidores se apagan. para realizar la compra de mas combustible se tiene que mandar a realizar una solictud retrazando así la disponibilidad.	[PR]	Preventivas	Preventivas
	[I.9]	3	4	R84	12	4	Importante	HW.A	Aseguramiento de la disponibilidad	Deberían existir procedimientos para controlar la interrupción del servicio en caso este se vea afectado por la carencia de otro recurso.	[PR]	Preventivas	Preventivas
[netw]													
[fire]	[E.20]	3	5	R184	15	4	Importante	HW.CM	Cambios (actualizaciones y mantenimiento)	Llevar un correcto registro de las actualizaciones y mantenimientos en los programas para que agentes externos no provoquen la caída del activo.	[PR]	Preventivas	Preventivas
[COM] REDES DE COMUNICACIONES													
[cint]	[I.5]	3	4	R191	12	4	Importante	COM.A	Aseguramiento de la disponibilidad	La provisión del servicio proporcionados por las terceras partes deberían ser controlados y revisados regularmente, y también se deberían llevar a cabo auditorías regularmente.	[PR]	Preventivas	Preventivas
								COM.internet	Internet: uso de acceso a red lan UNC	Gestionar la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de la organización.	[MN]	De monotorización	consolidan el efecto de las demás
[MEDIA] SOPORTE DE INFORMACIÓN													

[store]	[I.9]	4	3	R218	12	4	Importante	MP.clean	Limpieza de contenidos	El storage debe ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	[PR]	Preventivas	Preventivas
								MP	Protección de los Soportes de Información	El storage de resplado debe estar situado o protegido para reducir los riesgos de las amenazas y los riesgos del entorno.	[PR]	Preventivas	Preventivas
[AUX] EQUIPAMIENTO AUXILIAR													
[powr]	[I.5]	4	3	R229	12	4	Importante	AUX.A	Aseguramiento de la disponibilidad	El acumulador de energía UPS equipo debería ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	[IM]	Minimizadoras	acotan la degradación
	[E.24]	4	3	R236	12	4	Importante	AUX.power	Suministro eléctrico	El acumulador de energía UPD debería estar protegido de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	[PR]	Preventivas	Preventiva
[psis]	[I.9]	4	3	R245	12	4	Importante	AUX.A	Aseguramiento de la disponibilidad	El equipo de sistema de aire acondicionado debería ser mantenido de una manera correcta para asegurar su continuidad, disponibilidad e integridad.	[PR]	Preventivas	Preventiva
	[E.24]	4	4	R248	16	5	Critico	AUX.power	Suministro eléctrico	El sistema de aire acondicionado debería estar protegido de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	[PR]	Preventivas	Preventiva
[gelc]	[E.24]	4	3	R260	12	4	Importante	AUX.power	Suministro eléctrico	El grupo electrógeno debería estar protegido de los fallos de energía y de otras interrupciones causadas por fallos en las instalaciones de suministro.	[PR]	Preventivas	Preventiva
[cable]													
[cab1]	[I.5]	4	4	R266	16	5	Critico	AUX.wires	Protección del cableado	El cableado de red debería estar situado o protegido para reducir los riesgos de las amenazas y del entorno, así como de las oportunidades de robo.	[IM]	Minimizadoras	acotan la degradación
[L] INSTALACIONES													
[site]	[I.7]	4	3	R281	12	4	Importante	L.design	Diseño	Diseñar y aplicar una protección física contra el daño por fuego, inundación, humendad y otras formas de desastres industriales o provocadas por el hombre.	[MN]	De monotorización	consolidan el efecto de las demás
[P] PERSONAL													
[adm1]	[I.4]	3	4	R308	12	4	Importante	PS.AT	Formación y concienciación	Todos los empleados de la organización y, cuando corresponda, deberían recibir una formación y concientización adecuadas y actualizadas de las políticas y procedimientos de seguridad y salud en el trabajo, según corresponda a su puesto de trabajo.	[PR]	Preventivas	Preventiva

	[I.7]	3	4	R309	12	4	Importante	PS.A	Aseguramiento de la disponibilidad	Diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.	[PR] [AW]	Preventivas de concienciación	Preventiva consolidan el efecto de las demás

Fuente: Elaborada en base a MAGERIT- V 3.0 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Se elaboró la tabla Tratamiento del Riesgo para las amenazas que representaban un nivel de riesgo importante y crítico para los activos de TI de la Oficina General de TI. Se identificaron las salvaguardas que podrían mitigar los niveles de riesgo no aceptables, de la siguiente manera:

- Para el activo [sges] se planteó la salvaguarda aseguramiento de la disponibilidad que tendría un efecto preventivo en el activo.
- En el caso del activo [swsc] se plantearon salvaguardas de copias de seguridad y aplicar perfiles de seguridad que tendrían un efecto preventivo.
- Para el activo [swoc] se planteó las salvaguardas perfiles de seguridad y copias de seguridad con tendrían un efecto preventivo.
- Aseguramiento de la disponibilidad, operación fueron las salvaguardas planteadas para los activos [ser3] y [ser4] con un efecto preventivo.
- Para el activo [fire] se planteó la salvaguarda cambios (actualizaciones y mantenimiento) con un efecto preventivo para el tratamiento del riesgo.
- Aseguramiento de la disponibilidad e internet: uso de acceso a red LAN UNC fueron las salvaguardas planteadas para el activo [cinf] con tendrían un efecto preventivo y en el caso de internet un efecto de consolidar el efecto de las demás.
- Para el activo [store] se plantearon las salvaguardas limpieza de contenidos y protección de los soportes de seguridad con un efecto preventivo.

- Aseguramiento de la disponibilidad y suministro fueron las salvaguardas planteadas para el activo [powr] que tendrían un efecto que acotan la degradación y preventivo.
- Para el activo [psis] se plantearon las salvaguardas aseguramiento de la disponibilidad y suministro eléctrico con un efecto preventivo. Suministro eléctrico fue la salvaguarda planteada para el activo [gelc] que tendría un efecto preventivo.
- Se planteó la salvaguarda protección del cableado del activo [cab1] con un efecto de acotación de degradación para tratar el nivel de riesgo.
- Para tratar el nivel de riesgo en el activo [site] se planteó la salvaguarda de diseño con un efecto que consolide el efecto de las demás.
- Finalmente, las salvaguardas formación con un efecto preventivo y aseguramiento de la disponibilidad con un efecto preventivo y de concientización fueron planteadas para el activo [adm1].

4.4. Aspectos organizativos de la seguridad de la información

Como parte de la metodología propuesta por la ISO/IEC 27003, se debe definir los aspectos organizativos de la seguridad de la información en la UNC.

Se definen los roles y responsabilidades que se dan en la UNC, respecto a la protección de recursos de seguridad de información. Esta política se aplica a todos los empleados, ya sean estas autoridades, jefes de oficinas relacionadas a los procesos académicos, personal administrativo y otros que forman parte de la UNC, cada uno de los cuales cumple un rol en la administración de la seguridad de la información. Todos los trabajadores son responsables de mantener un ambiente seguro, en tanto que el Oficial de Seguridad de la Información debe monitorear el cumplimiento de la política de seguridad definida y realizar las actualizaciones que sean necesarias, producto de los cambios en el entorno informático y las necesidades del negocio que estos ameritan.

Es importante mencionar que las responsabilidades referentes a la Gestión de la Seguridad de la Información son distribuidas dentro de toda la UNC y no son de entera responsabilidad del Oficina General de TI, en ese sentido existen roles adicionales que recaen en los propietarios de la información y los usuarios de información.

A continuación, se propone los roles y responsabilidades relacionadas a la Gestión de la Seguridad de la Información para la UNC:

4.4.1. Comité de Seguridad de la Información (CSI)

La UNC, constituirá un Comité de Seguridad para atender las temáticas relacionadas a la Seguridad de la Información en los procesos académicos, ante el cual se propondrán los planes, se informará de las acciones llevadas a cabo y se evaluarán los avances de dichos planes; estará conformado por:

Vicerrector académico
Jefe de la Oficina General de Procesos Académicos
Jefe de la Oficina General de TI

Teniendo entre sus principales funciones:

a) Proponer la inclusión de roles y responsabilidades de seguridad en el manual de organización y funciones de la UNC, cuando corresponda.
b) Revisar los resultados de los "análisis de riesgos" y aprobar los "controles de

tratamiento de riesgo" que sean necesarios.

c) Verificar la efectividad en la implementación de la política de información.
d) Evaluar y recomendar las sanciones en caso de "incidentes de seguridad", de conformidad con las normas vigentes.

4.4.2. Comité Operativo de Seguridad de la Información (COSI)

Es el grupo designado por el Comité de Seguridad de la Información para supervisar, revisar, informar y coordinar de manera permanente los aspectos operativos del cumplimiento de las políticas y procedimientos de seguridad de la información y está conformado por:

Oficial de Seguridad de la Información.
Jefe de la Unidad de Administración de Red de la Oficina General de TI
Jefe de la Unidad de Desarrollo de Sistemas de la Oficina General de TI
Jefe de la Unidad de Soporte Técnico.

Sus funciones específicas son:

a) Supervisar la ejecución periódica de análisis de riesgos y proponer controles de tratamiento de riesgos al CSI.
b) Coordinar el inventario periódico de los activos de seguridad de la información de la UNC.
c) Proponer al Comité de Seguridad de la Información (CSI) los niveles de clasificación de la información que se deben manejar en la UNC.
d) Preparar y recomendar al Comité de Seguridad de la Información la aprobación de planes y programas para la concientización del personal en la seguridad de la información.
e) Revisar las directivas y procedimientos de seguridad de la información verificando su efectividad y correcta implementación, proponiendo oportunamente su modificación o actualización.
f) Revisar y hacer seguimiento de los incidentes de seguridad de la información e informar al Comité de Seguridad de Información.
g) Informar al Comité de Seguridad de Información el incumplimiento de las directivas y procedimientos de Seguridad de la Información.
h) Proponer al Comité de Gestión de Seguridad de la Información el establecimiento de Convenios con entidades especializadas en seguridad de la información con la finalidad de recibir asesoría continua e implementar las mejores prácticas de seguridad de la Información.

4.4.3. Oficial de Seguridad de la Información

Sus funciones específicas son:

a) Ser el nexo entre el CSI y COSI para los usuarios finales.
b) Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de la UNC.
c) Monitorear la asignación de perfiles de usuario, permisos u accesos concedidos y uso en el sistema.
d) Actualizar las políticas y estándares de seguridad de la información.
e) Monitorear el cumplimiento de políticas de seguridad.
f) Verificar que cada activo de información haya sido asignado a un “propietario” el cual debe definir los requerimientos de seguridad como políticas de protección, perfiles de acceso, respuesta ante incidentes y sea responsable final del mismo.
g) Monitorear la aplicación de controles de seguridad física de los principales activos de información.
h) Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información.
i) Evaluar los incidentes de seguridad de la información.
j) Registrar los incidentes de seguridad y recomendar acciones de respuesta apropiadas para mitigarlos.
k) Evaluar y desarrollar especificaciones técnicas de seguridad de la información en los proyectos de implementación de nuevas tecnologías informáticas.
l) Elaborar con las unidades orgánicas los proyectos de políticas específicas de seguridad de la información que resulten como consecuencia de la Política General de Seguridad de la Información y proponerlos al Comité Operativo de Seguridad de la Información.
m) Apoyar a los usuarios de los sistemas de información de la UNC en los temas relacionados con la seguridad de su información.
n) Elaboración de un programa de mantenimiento preventivo-correctivo de los equipos informáticos de la UNC, para el encargado de Soporte Técnico de la Oficina General de TI, en trabajo conjunto para su realización, a fin de mantener la seguridad informática del trabajador asignado al equipo.
o) Dar seguimiento a las políticas de seguridad, establecido en el presente documento.

4.4.4. Responsabilidad de la Oficina General de TI

El jefe de la Oficina General de TI es responsable de revisar las políticas específicas de seguridad de la información propuestas por el Oficial de Seguridad de la Información.

Las funciones específicas del jefe de la Oficina General de TI son:

a) Informar al Comité Operativo de Seguridad de la Información (COSI) sobre los resultados de la gestión de seguridad de la información.
b) Proteger los sistemas informáticos de la UNC ante posibles amenazas.
c) Coordinar con el responsable de la administración y supervisión de las bases de datos, la operatividad, seguridad y diseño de las mismas.
d) Solicitar la realización de mantenimiento preventivo y correctivo del equipo de cómputo a fin de prolongar la vida útil del equipo.
e) Coordinar, implementar y verificar los sistemas de seguridad, monitoreo de sistemas y mecanismos electrónicos necesarios para el acceso y resguardo de la información.
f) Supervisar la obtención de respaldo de Información de la UNC.
g) Garantizar la protección, privacidad, disponibilidad y correcto funcionamiento del correo electrónico ya sea en la red interna como en Internet.

4.4.5. Responsabilidades de las Áreas académicas

Los jefes de las áreas relacionadas a los procesos académicos son responsables de la aplicación y control de las políticas de seguridad de la información.

Sus funciones específicas son:

a) Difundir de una manera adecuada la política de seguridad de la información asegurando su correcto entendimiento en el personal a su cargo.
b) Supervisar, controlar y permitir solo el acceso necesario a los activos de seguridad de información en la relación y contratos con terceros.

4.4.6. El propietario de los activos de seguridad de información

El jefe de un área académica específica es el responsable de la seguridad de los activos de seguridad de la información que están bajo su control. Podrá delegar expresamente algunas tareas de la misma asegurándose de la competencia y capacitación de aquellos en que recaiga la delegación.

Sus funciones específicas son:

a) Tomar medidas para minimizar el riesgo por pérdida o exposición de los activos de seguridad de información que están bajo su responsabilidad.
b) Asegurar que el personal a su cargo cumpla con las responsabilidades ya sea como propietario, custodio y/o usuario de la información.
c) Clasificar la información de acuerdo con los niveles de clasificación que se establezcan.
d) Realizar el inventario de los activos de seguridad de información y mantenerlo actualizado.
e) Autorizar accesos sobre la información de la que son propietarios, ratificar periódicamente estos accesos e informar inmediatamente a las áreas competentes sobre el personal que no debería tener acceso a la misma.
f) Plantear requerimientos de control y protección de la información.
g) Establecer la criticidad de la información y los niveles mínimos de servicio cuando se requiere recuperar información en casos de desastres.
h) Es responsable por la calidad y consistencia de los datos bajo su control.

4.5. Políticas de seguridad de la información propuestas

En base a los resultados del análisis y tratamiento de riesgos de TI y la organización de la seguridad de la información que se plantea, a continuación de detallan el conjunto de políticas de seguridad de la información que se proponen para el SGSI de la UNC. Estas políticas han sido clasificadas de acuerdo a los dominios de seguridad de la información de la ISO/IEC 27002.

Estas políticas de seguridad deberán seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: cambio en la infraestructura computacional, desarrollo de nuevos servicios académicos en la UNC, entre otros.

Estas políticas deberán ser difundidas a todo el personal involucrado en los procesos académicos de la UNC.

4.5.1. Gestión de activos de información

La UNC tiene conocimiento sobre los activos de TI que posee como parte importante de la administración de riesgos.

Se pueden distinguir dos tipos de activos:

- Los activos primarios, son:
  Procesos académicos

Información

- Los activos de apoyo: Estos activos tienen vulnerabilidades que son explotables por amenazas que tienen como objetivo desactivar los activos primarios del alcance (proceso académicos e información). Son de varios tipos:
  Hardware
  Software
  Red
  Personal
  Sitio
  Estructura de la organización

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad que tienen para la UNC ante una posible contingencia. Esta clasificación deberá realizarse de acuerdo a la funcionalidad que cumplen en la entidad y en función a ello establecer medidas de seguridad para su resguardo y protección, dicha clasificación se realizará en un documento de Sistema de Gestión de Seguridad de la Información de la UNC.

Responsabilidad sobre los activos

Para garantizar que los activos de información reciban un apropiado nivel de protección, para ello deberá tener en cuenta las siguientes políticas.

a) Los activos de información solamente pueden ser utilizados con el objetivo de ejecutar tareas vinculadas con los procesos de la UNC.
b) Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.
c) Utilizar los activos de información de manera tal que no ocupen innecesariamente capacidad, y como consecuencia disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad.
d) Está prohibido descargar archivos de imágenes o vídeos que no estén vinculados con las actividades de los procesos académicos, enviar cadenas de correos electrónicos, juegos, etc.
e) Está prohibido instalar software en un ordenador local sin el permiso explícito de la Oficina General de TI.
f) Está prohibido descargar códigos de programa de soportes externos desde

internet.

g) Está prohibido instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del Oficina General de TI.

h) Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo de la Oficina General de Administración de la UNC.

i) Mientras que los activos permanecen fuera de la UNC, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

j) Al finalizar un contrato/préstamo de empleo, o de otro tipo, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información a la dependencia respectiva.

k) El Oficina General de TI debe almacenar en medios ópticos (CD/DVD) las copias de respaldo de la(s) base(s) de datos de los sistemas informáticos, como mínimo, una vez por día. Para ello debe elaborarse un "*Reglamento Operativo de copias de respaldo*".

l) En cada estación de trabajo debe estar instalado el antivirus, el cual deberá estar configurado para actualizar la base de firmas de virus automáticamente.

m) Los usuarios solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados.

n) Los usuarios pueden utilizar los sistemas de información únicamente para las actividades/funciones para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.

o) Todos los usuarios que acceden a los recursos informáticos de la red requieren de una única e intransferible identidad, normalmente un "nombre de usuario" para una persona, y un nombre de máquina para una computadora personal. Esta regla se usa para representar un usuario o dispositivo en los ambientes informáticos de la red. La Oficina General de TI, proporcionara este identificador como parte del proceso de autorización.

p) La Oficina General de TI, administrará las cuentas de usuarios y mantendrá registros del uso de las mismas, que permitan realizar auditorías o revisiones, en caso de existir situaciones que así lo ameriten.

q) El usuario solo podrá utilizar la infraestructura de la red de datos institucional para aquellos servicios que se le haya concedido acceso y únicamente para el desarrollo de actividades relacionadas con su función. Esta cuenta es de uso exclusivo y no debe ser compartida.

r) Los usuarios tendrán derecho a la confidencialidad de su información, con la salvedad de aquellos casos en que se detecten acciones que se pongan en riesgo la seguridad de la red de datos y/o fuga de información.

s) La cuenta es individual e intransferible y su dueño será responsable de mantener la confidencialidad de la contraseña de la cuenta, de hacer uso adecuado de la misma y de responder sobre las actividades que ocurran bajo su cuenta o contraseña.

t) Para efectos de asegurar la confidencialidad de accesos y claves, la autorización de acceso a los recursos es exclusiva al usuario al que se le fue asignada.

u) Se utilizará como base, una lista actualizada del personal activo, proporcionada por la Oficina General de Administración, y servirá como control en caso de que no se haya procedido con la eliminación correcta de los usuarios.

v) Los nombres de usuarios no activos encontrados en el proceso, deberán ser eliminados del sistema junto con todos sus derechos concedidos.

Inventario de Activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de no mayor a 6 meses.

El encargado de elaborar el inventario de activos de TI y mantenerlo actualizado es la Oficina General de TI.

Clasificación de la Información

Para evaluar la clasificación de un activo de información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

a) Confidencialidad
   - (1) PÚBLICO: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la UNC o no.
   - (2) RESERVADA – USO INTERNO: Información que puede ser conocida y utilizada por todos los empleados de la UNC y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría

ocasionar riesgos o pérdidas leves para la UNC.

- (3) RESERVADA – CONFIDENCIAL: Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas y graves a la UNC.

b) Integridad
   - (1) Información cuya modificación no autorizada puede repararse fácilmente y no afecta las actividades de la UNC.
   - (2) Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la UNC.
   - (3) Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas y graves para la UNC.

c) Disponibilidad:
   - (1) Información cuya inaccesibilidad no afecta las actividades de la UNC.
   - (2) Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas a la UNC.
   - (3) Información cuya inaccesibilidad permanente durante un día o incluso horas podría ocasionar pérdidas significativas y graves a la UNC.

Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.
- CRITICIDAD MEDIA: alguno de los valores asignados es 2
- CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al custodio del recurso.
- Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

4.5.2. Seguridad en recursos humanos

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones.

Por tanto, a fin de asegurar que los trabajadores que forman parte de la UNC, sean seleccionados adecuadamente antes de ser contratados y puedan ser fácilmente identificados mientras formen parte de la UNC; además que el acceso sea oportunamente revocado cuando un empleado es despedido o transferido. Se deberá establecer un *“Reglamento Interno de trabajo”*, en el que define las normas que deben de observar los empleados de la UNC.

Las políticas que a continuación se detallarán serán aplicadas a todos los empleados y personal contratado:

a) La Oficina General de Administración, es responsable de la constante revisión y optimización de los procedimientos de selección del personal. La misma que considera como otros filtros necesarios de validación satisfactoria de las referencias laborales, la exactitud de lo señalado en la hoja de vida, sus referencias en las diferentes centrales de riesgo, entre otros.
b) La Oficina General de Administración, pondrá énfasis en la selección de

personal optimizando los controles de previsión de posibles actos dolosos internos, así como la aplicación de políticas de rotación de personal, vacaciones y capacitación.

c) La Oficina General de Administración, notifica a la Oficina General de TI, mediante un memorando, la renuncia o despido de los trabajadores; así como, el inicio y fin del periodo vacacional de los mismos. Después de que se notifique un despido o transferencia, el encargado en Soporte Técnico, se asegurará que el identificador de usuario sea revocado. Cuando se notifique dicha transferencia o despido, el personal de la Oficina General de Administración, se asegura que cualquier ítem entregado al personal, como llaves, fotocheck, documentación, manuales, etc. deban de ser entregados a su superior inmediato.

d) La seguridad es responsabilidad de todos los empleados y personas involucradas con la UNC. Por ende, todos los empleados y personas con acceso a las instalaciones e información, deben de acatar los estándares documentados en el presente plan e incluir la seguridad como una de sus responsabilidades.

e) Promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información, dar a conocer el programa de concientización referente a seguridad, que ayuden al personal recordar a cada momento el papel importante que cumple en el mantenimiento de la seguridad de la información.

f) Dentro del programa de inducción, se debe de considerar capacitación al personal ingresante sobre temas como el conocimiento de las amenazas y problemas de seguridad de información, en procedimientos de seguridad y el uso correcto de las instalaciones. La capacitación en seguridad debe de incluir, al menos los siguientes aspectos:

   Requerimientos de identificador de nombre de usuario y contraseña
   Seguridad de PC, incluyendo protección de virus
   Responsabilidades de la entidad de seguridad de información.

g) La UNC sigue un determinado proceso para la selección de su personal, cuenta con un Manual de Organización y funciones; así como aplica ciertos controles al personal que labora dentro de la entidad, de forma que le permita reducir sus riesgos por error humano, robo, fraude, entre otros.

h) A la incorporación de un nuevo empleado se le entregara un reglamento interno de trabajo, así como las normas y procedimientos para el uso de las aplicaciones y el acceso a los sistemas de información.

i) El personal debe de ser comunicado de las implicancias de seguridad en relación a las responsabilidades y funciones de su trabajo.

Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados firmarán un Acuerdo de Confidencialidad, en lo que respecta al tratamiento de la información de la UNC. La copia firmada del Compromiso deberá ser retenida en forma segura por el la Oficina General de Administración y será guardada en cada archivo de cada trabajador.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Respuesta a Incidentes

Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Para ello, se deberá establecer un *"Procedimiento formal de comunicación y de respuesta a incidentes",* indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento contempla que, ante la detección de un incidente o violación de la seguridad, el personal reportará el incidente tan pronto como se haya detectado el evento, la Oficina General de Administración. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Oficial de Seguridad de la Información al tanto de la ocurrencia de incidentes de seguridad.

4.5.3. Seguridad física y del entorno

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la UNC. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental, mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la UNC, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas de la UNC.

Control físico de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina General de Administración, en conjunto con la Oficina General de TI, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área.
b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.
c) Implementar el uso de una identificación única visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
d) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará el Oficial de Seguridad de la Información.
e) El espacio ocupado por el personal de la Oficina General de TI, está considerado como un Área de Acceso Limitado. La puerta de acceso debe permanecer cerrada las 24 horas del día durante los 7 días de la semana, con la finalidad de no permitir el ingreso de personal no autorizado.
f) Ante la posibilidad de que alguien pretenda ingresar sin autorización a las Áreas de acceso restringido, la Oficina General de TI o personal a cargo, dará aviso de inmediato al personal de vigilancia, quedando registrado dicho incidente en la

bitácora de Incidencias de Seguridad.

g) Solo personal autorizado contará con acceso a los equipos de cómputo instalados en la Oficina General de TI, la libertad de acceso en especial a los servidores principales, pueden crear un significativo problema de seguridad. El acceso solo está permitido a las personas que regularmente trabajan en esta Oficina.

h) Los usuarios deberán acatar estos lineamientos para cualquier computadora o red usada dentro o fuera de la UNC. Está terminantemente prohibido el ingreso y salida de equipos, software, sin la autorización correspondiente y/o la conformidad de la Oficina General de Administración y Oficina General de TI.

Protección de los equipos

a) Las instalaciones de la Oficina General de TI, están provistos de equipos para la extinción de incendios como son extintores de tipo gas Carbónico (CO2), ya que estos no dañan los equipos de cómputo y sensores de humo.

b) Los mecanismos de ventilación en la Oficina General de TI, se han colocado en razón al hardware en la Oficina. La temperatura se mantiene no menor de 18° C ni mayor 22° C (estándares internacionales).

c) La UNC realizara acciones necesarias para asegurar la buena condición y continuidad de los equipos de cómputo, tomando en cuenta aspectos de temperatura ambiental, seguridad física, control de incendios, entre otros.

d) Queda terminantemente prohibido fumar y el consumo de alimentos y bebidas en el interior de las Áreas de acceso restringido.

Instalaciones de suministro

a) El centro de cómputo o data center cuenta con un sistema de alimentación ininterrumpida (UPS), en situación normal el mismo debe ser probado por lo menos una vez cada seis (6) meses. El jefe de la Oficina General de TI y el encargado en Soporte Técnico, son responsables de esta actividad, así como de coordinar que el personal a su cargo reciba la capacitación del manejo del equipo.

b) El suministro de energía establecido donde se encuentra situado el hardware de red, enrutadores y otros dispositivos que son necesarios para el buen funcionamiento normal de la UNC, mantiene un suministro estable y continuo de energía eléctrica, utilizando sistemas UPS (Sistema de suministro interrumpido de energía), la cual se encarga de regular la tensión llegando a evitar los picos de voltaje, además de proporcionar un tiempo de autonomía por medio de

baterías en caso de corte de suministro eléctrico. La ubicación de los UPS se encuentra dentro de la misma sala de servidores, en el cual no puedan ser desactivados por un supuesto intruso o por una falla de usuario.

c) La Oficina General de TI, coordinara con la Oficina General de TI, la realización de una prueba para evaluar la operatividad del UPS, ante una contingencia.
d) Realizar pruebas de operatividad de los equipos UPS, a fin de evaluar su tiempo respaldo ante una contingencia.
e) Las instalaciones eléctricas de las Áreas de acceso restringido deberán contar con un sistema de conexión a tierra, en lo posible independiente, de alta calidad y dentro de los rangos permisibles.

Seguridad del cableado

a) El cableado de red, se encuentra físicamente separado de cualquier otro tipo de cables, siendo estos de corriente o energía eléctrica. Para evitar interferencias, los servidores se encuentran localmente separados, para lo cual estos equipos críticos de información y proceso se encuentran aislados y seguros, protegidos con un nivel de seguridad verificable y manejable por los administradores de seguridad y las personas responsables por estos activos.
b) Proteger el cableado de red contra intercepción no autorizada o daño (ejemplo: el uso de conductos o evitando trayectos que atraviesen áreas públicas).
c) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

Mantenimiento de equipos

a) El mantenimiento y supervisión permanente de las condiciones de seguridad física y ambiental del centro de cómputo o data center, así como de los denominados otros activos de informática de alto riesgo ubicados fuera del centro de cómputo, es responsabilidad de la Oficina General de TI.
b) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de la Oficina General de TI.
c) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
d) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

4.5.4. Gestión de comunicaciones y operaciones

La administración de las operaciones y comunicaciones de la UNC, son esenciales para mantener un adecuado nivel de servicio a comunidad universitaria. Los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las operaciones y comunicaciones.

Los procedimientos operacionales y las responsabilidades para mantener accesos adecuados a los sistemas, así como el control y la disponibilidad de los mismos, deben ser incluidos en las funciones operativas de la UNC. Todas las comunicaciones e intercambios de información, tanto dentro de las instalaciones y sistemas como externas a ella, deben ser aseguradas, de acuerdo al valor de la información protegida.

La UNC, establecerá las siguientes medidas de administración de las operaciones y comunicaciones:

Gestión de Cambios

a) Todos los cambios realizados en los sistemas de la UNC deben seguir los procedimientos de cambios establecidos.
b) Solo el personal encargado de la administración de la seguridad puede realizar o aprobar un cambio. Dicho cambio debe ser documentado y aprobado luego de haberse producido el cambio.
c) Los roles del personal involucrado en la ejecución de los cambios en los sistemas deben encontrarse debidamente especificados.
d) Los cambios deben ser aprobados por la jefatura del área usuaria, el personal encargado de la administración de la seguridad de la información y el encargado de la Oficina General de TI. Todos los requerimientos de cambios deben ser debidamente documentados, siguiendo los procedimientos para cambios existentes. Antes de la realización de cualquier cambio a los sistemas se debe generar copias de respaldo de dichos sistemas.
e) El ambiente de producción es aquel en el cual residen los programas ejecutables de producción y los datos necesarios para el funcionamiento de los mismos. Solo el personal autorizado a efectuar los cambios en los sistemas debe contar con privilegios de escritura en los mismos.
f) Las pruebas deben de realizarse utilizando datos de prueba. Sin embargo, copias de datos de producción pueden ser usadas para las pruebas,

siempre y cuando los datos sean autorizados por el propietario y manejados de manera confidencial.

g) El personal de desarrollo puede tener acceso de solo lectura a los datos de producción. La actualización de los permisos de acceso a los datos de producción debe de ser autorizada por el encargado de soporte y otorgada por un periodo limitado.
h) Los cambios deben ser autorizados por el jefe de la Oficina General de TI, quien deberá evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
i) El jefe de la Oficina General de TI, es el responsable de verificar que los cambios se han implementado de acuerdo al requerimiento.
j) El encargado de Soporte Técnico, es el responsable de probar y verificar la estabilidad del sistema; no se debe activar el sistema antes de haber realizado pruebas exhaustivas.

Separación de los recursos de desarrollo, prueba y Operación.

a) La Oficina General de TI, debe mantener recursos de hardware y software para evitar el acceso no autorizado a la red.
b) Cada estación de trabajo requerirá de un password de acceso para evitar que se copie, visualice, altere o destruya información contenida en el mismo.
c) La Oficina General de TI, inspeccionará todos los equipos informáticos conectados o no a la red, para los propósitos de resolución de problemas y/o para supervisar las políticas de seguridad, toda vez que se necesite y sin previo trámite. El libre acceso debe preverse especialmente en periodos de acceso parcial de la actividad laboral y cuando se crea conveniente por razones de mantenimiento correctivo y/o preventivo, incluyendo las actualizaciones de librerías.

Protección contra el código malicioso

a) El usuario no instalará ningún tipo de software (estandarizado o no, o de dominio público, etc.) en los equipos personales y/o servidores, sin la aprobación expresa del jefe de la Oficina General de TI. Toda instalación no autorizada, será considerado como falta, sujeto de sanción disciplinaria.
b) El uso del correo electrónico estará sujeto a las disposiciones internas vigentes.
c) Todas las PCs, y en especial aquellas en donde se instalaron cuentas de correo electrónico, deberán tener instalados antivirus activos para su aplicación.
d) La Oficina General de TI establecerá las medidas necesarias para minimizar el

riesgo ante posibles infecciones de virus informáticos.

e) Verificará que los equipos tengan instalada la última versión del software antivirus que la UNC tenga amparada con la licencia correspondiente.
f) Revisará que periódicamente (una vez a la semana), se active la rutina de verificación del software antivirus autorizado por la UNC. Procederá de igual manera cuando se pretenda ingresar información por los medios de almacenamiento externo (USB, CDs, etc.), o de los servicios de Internet.
g) Registrar los virus que aparezcan en la entidad y tratar de determinar quiénes lo introducen, identificando si se realizó de forma intencional o no.
h) Ante indicios de contaminación por un virus informático nuevo o desconocido, aislarlo o apagar el equipo y preservar la computadora infectada y comunicarse de inmediato con la Oficina General de TI o con el encargado de Soporte técnico.
i) Todos los equipos de cómputo cuentan con un software antivirus instalado, el cual se actualizado en forma automática vía Internet.

Copias de seguridad

Se cuenta con un procesamiento de sistemas de backups para la generación de copias de respaldo sobre las diferentes operaciones de la UNC. Actualmente se vienen manteniendo copias de respaldo distribuidos, replicando los backups en una de las oficinas que conforman la entidad, y en la misma Oficina General de TI, para prevenir la perdida de datos por problemas de seguridad física en alguno de los sistemas u oficinas. Existe un responsable de su custodia que es el encargado de Soporte Técnico.

La elección de alojamiento para los backups, es una decisión que el personal de la Oficina General de TI ha tenido en cuenta por una serie de razones como, la seguridad, necesidad, disponibilidad inmediata de los backups o el tiempo que estos deben de almacenarse, como regla general se debe de mantener al menos una copia de los backups fuera de la UNC.

La periodicidad de la generación de copias de seguridad se realiza de manera diaria, lo cual van de acorde con la criticidad de la información y frecuencia de cambios que se realizan.

Se deberá establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups, debiéndose incluir:

a) Periodicidad de cada tipo de Backup.

b) Uso obligatorio de un formulario estándar para el registro y control de los backups.
c) Nemónico de los rótulos y etiquetado de los backups
d) Almacenamiento de los backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
e) Almacenamiento de los backups en locales diferentes donde reside la información primaria.
f) Pruebas periódicas trimestrales de los backups, verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables
g) El encargado de Soporte Técnico es el responsable del proceso de creación de copias de seguridad.
h) Se lleva un registro del proceso de creación de copias de seguridad.
i) Las copias de seguridad y el proceso de restauración deben ser probados al menos una vez cada tres meses.
j) El encargado de Soporte Técnico es el responsable de probar las copias de seguridad.

Gestión de la seguridad de las redes

a) La Oficina General de TI, deberá evaluar, proponer e implementar soluciones tecnológicas necesarias para mejorar la seguridad y administración de la red.
b) Se cuenta con un servidor firewall (cortafuegos) en un sitio estratégico de la red, para ofrecer seguridad frente a accesos no autorizados de la misma.
c) Las conexiones que se requieran entre la red de datos institucional con redes de otras instituciones (bancos, RENIEC, etc.) se deben realizar verificando que se garanticen los niveles de seguridad exigidos por las entidades involucradas e igualmente que los niveles de riesgo y accesos indebidos se minimicen, estableciendo mecanismos de control de acceso que se consideren necesarios.
d) Los usuarios que accedan a servicios de otras redes a través de una conexión habilitada por la UNC, estarán sujetos a las normas estipuladas y las violaciones a las mismas, serán penalizados de acuerdo a los reglamentos correspondientes.
e) La Oficina General de TI, deberá reportar las fallas, controlar los accesos locales y remotos de la red, los eventos del sistema operativo, problemas del software base instalado y las alertas de fallas en programas o dispositivos de hardware.
f) Los equipos de red importantes como routers, switchs y servidores se encuentran en un lugar donde se lleva un control de acceso a los mismos. Se deben vigilar a través del mismo personal de la unidad o mediante el aislamiento

de la sala de servidores por medio de una cerradura, por el cual el ingreso es a través del personal responsable de la custodia.

g) Los usuarios del sistema de seguridad pueden acceder a los servicios de red sólo si cuentan con autorización, de acuerdo a lo establecido en la presente Política. Los usuarios no pueden acceder a servicios de red para los cuales no cuentan con autorización.

Manipulación de los soportes

Todos los datos y software con licencia almacenado en soportes móviles (por ej., CD, DVD, unidades USB, tarjetas de memoria, etc., y también en papel) y en todos los equipos que tienen soportes de almacenamiento (por ej. ordenadores, teléfonos móviles, etc.) deben ser borrados antes de que sean entregados a otro usuario), esta política deberá realizarse previa generación de una copia de respaldo de la información almacenada en dispositivos y equipos.

La persona responsable de realizar este proceso deberá informar al propietario del activo, acerca del borrado o eliminación de datos.

Intercambio de Información de los sistemas de Información

La información de la UNC puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, teléfonos y soportes móviles.

El jefe de la Oficina General de TI, en conjunto con la Jefatura del área usuaria, determinara que canales de comunicación se pueden utilizar para cada tipo de información y las posibles restricciones sobre los permisos para usar dichos canales; es decir, definirán qué actividades están prohibidas.

4.5.5. Control de acceso

Con el objetivo de impedir el acceso no autorizado a la información, se definen políticas para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Gestión de accesos usuarios

Registro de Usuarios

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
b) Verificar que el usuario tiene la autorización de la Oficina General de Administración, para el uso de los sistemas, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario.
d) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
e) Mantener un registro formal de todas las personas registradas para utilizar el sistema.
f) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la UNC.
g) Efectuar revisiones periódicas con el objeto de:
    Cancelar identificadores y cuentas de usuario redundantes
    Inhabilitar cuentas inactivas por más de 60 días.
    Bloquear cuentas inactivas por más de 120 días.
h) En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
i) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

Gestión de privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los accesos.
b) Asignar los privilegios al personal teniendo en cuenta las actividades que realizara como parte de sus funciones asignadas.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados.
d) Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
e) El mal uso de los privilegios concedidos (por ser necesarios realizar actividades de soporte, mantenimiento y operación), se considerará como abuso de autoridad y como tal será sancionada de acuerdo al Reglamento interno de trabajo.
f) El acceso a los subsistemas, módulos, sub módulos, transacciones, menús, opciones, y cualquier otro componente de un sistema deberá definirse mediante el uso de los perfiles de usuario, de acuerdo con el rol o función que los usuarios tienen asignados para el cumplimiento adecuado de sus funciones y que serán definidos por la Oficina General de TI en coordinación con las Jefaturas de las áreas involucradas.

Gestión de contraseñas de usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

a) Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a la Oficina General de TI.

b) No se deben revelar las claves a otras personas, incluyendo la gerencia y los administradores del sistema.

c) No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el Oficina General de TI.

d) Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.).

e) Las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).

f) Se deben escoger claves seguras de la siguiente forma:

Utilizando al menos ocho caracteres;

Utilizando al menos un carácter numérico;

Utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;

Una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;

Las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);

No se deben usar nuevamente las últimas tres claves.

g) Se deben cambiar las claves cada mes.

h) Se deben cambiar las claves en el primer ingreso al sistema.

i) Las cuentas tendrán una duración limitada y se regularán por un procedimiento específico.

j) Los intentos infructuosos de acceso a los sistemas se limitarán a tres (3) intentos, luego de los cuales la contraseña será revocada y/o el usuario bloqueado.

k) Al firmar la Declaración de aceptación de los documentos del SGSI, los usuarios aceptan la obligación de mantener sus claves en forma confidencial. Este documento deberá ser entregado por Recursos Humanos al personal antiguo y nuevo que ingresa a la UNC, a fin de dar a conocer las medidas de seguridad que se han establecido para la protección de los activos de información.

l) Cada usuario debe utilizar su propio nombre de usuario asignado de forma exclusiva.

m) Cada usuario tiene la posibilidad de escoger su propia clave.

n) Las claves de primer acceso deben ser comunicadas al usuario de forma

segura, y se debe verificar previamente la identidad del usuario.

o) El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez, además de requerir que el usuario escoja contraseñas seguras y que cambien sus claves cada mes.

Revisión de derechos de acceso de usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios del Sistema Integrado de Administración Financiera (SIAF), el encargado de Soporte Técnico revisara los accesos de los usuarios. Para ello se deberán contemplar los siguientes controles.

a) Revisar los derechos de acceso de los usuarios a intervalos de 2 a 6 meses.
b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 1 a 3 meses. Este seguimiento será realizado por el Oficial de Seguridad de la Información.
c) Revisar las asignaciones de privilegios a intervalos de 2 a 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados. Este seguimiento será realizado por el Jefe de Recursos Humanos.

Responsabilidades de los usuarios

Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el responsable del Activo de Información de que se trate, que:

Sean fáciles de recordar.

No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.

No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión.
f) Notificar mediante “El procedimiento para el registro de Incidentes”, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Equipos desatendidos en áreas de usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
b) Proteger las PC’s o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

Política de pantalla y escritorio limpio

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán las siguientes medidas:

a) Política de escritorio limpio

   Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

b) Política de pantalla limpia

   Si la persona autorizada no se encuentra en su puesto de trabajo, deberá quitar toda la información sensible de la pantalla, y deberá denegar el acceso a todos los sistemas para los cuales tiene autorización.

   En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el puesto de trabajo.

   Está permitido el acceso al personal a todas las instalaciones de la UNC, excepto a aquellas áreas que han sido consideradas como áreas de acceso restringido.

Control de acceso a la red

Las conexiones no seguras a los servicios de red pueden afectar a toda la UNC, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El responsable de Soporte Técnico tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del jefe de una Área o Unidad Organizativa que lo solicite para personal.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la UNC.

El responsable de Soporte Técnico junto con el jefe de la Oficina General de TI definirá las pautas para garantizar la seguridad de los servicios de red de la UNC, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.

Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.

Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el responsable de Soporte Técnico.

4.5.6. Adquisición, desarrollo y mantenimiento de sistemas

Esta política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Protección de los datos de prueba del sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba, a continuación, se establecen algunas políticas para su protección.

a) Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso.
b) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
c) Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a pruebas, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva. Para todo desarrollo de software se deberán utilizar herramientas, de las cuales se tengan certeza que su comportamiento es seguro y confiable.

Control de cambios

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El encargado en Desarrollo de Sistemas definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a) El encargado de Desarrollo de Sistemas, no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos por la UNC. A su vez, la UNC contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.
b) Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados. La suficiencia de este material deberá ser determinada por los usuarios responsables en la UNC.
c) La documentación de todos los cambios hechos al software en la UNC, se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software de la UNC, éste deberá firmar un acuerdo de no-divulgación y utilización no autorizada del mismo.
d) Todo acceso a los sistemas operativos o módulos de los sistemas informáticos y a sus respectivas aplicaciones, tanto para consulta como para actualización de la información contenida en estos, debe hacerse mediante el uso de un código de acceso y un password o contraseña.

Control de acceso al código fuente de los programas

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) Todo sistema debe ser capaz de definir códigos de acceso en forma individual y personal para todo funcionario o empleado a quien se le quiera dar acceso y se deberá llevar un registro de los correspondientes códigos de acceso otorgados a cada empleado, no así de la contraseña.

b) El encargado de Desarrollo, mantendrá custodia de los programas fuentes, manteniendo en todo momento la correlación programa fuente / ejecutable.

c) Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, Analista responsable, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación, en producción).

d) Administrar las distintas versiones de una aplicación.

e) Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

f) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

g) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la UNC en los procedimientos que surgen de la presente política.

h) Para el caso de los códigos fuentes, se tendrá en consideración los siguientes procedimientos:

Backups del Sistema de Información (en caso de tener varios Sistemas o versiones, se contará con una copia de cada uno de ellos).

Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se deben considerar las copias de los listados fuentes de los programas definitivos, para casos de problemas.

Backups de los Datos y de estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, usuarios, roles y todo archivo necesario para el funcionamiento de los Sistemas de Información de la UNC y la pronta recuperación de los mismos en caso de fallas).

La frecuencia de obtención de éstos backups es semestral en caso de que no se registren modificaciones; y cada vez que se elabore una nueva versión del sistema.

i) Los desarrollos de sistemas de información, adquisición de paquetes informáticos, adquisición de bienes informáticos, asesorías,

consultorías, mantenimiento, capacitación, se realizarán utilizando los estándares establecidos por la UNC, siempre y cuando este haya sido aprobado formalmente por las instancias correspondientes y su aplicación estará sujeta al nivel de inversión y tamaño del proyecto asociado.

j) Las actualizaciones de software requerido de la UNC deberán cumplir con los procedimientos de licenciamiento respectivo.
k) Evaluará periódicamente el comportamiento de los sistemas y el nivel de conformidad de los usuarios.

4.5.7. Cumplimiento

En el presente punto se definirán las funciones y responsabilidades para que la UNC, cumpla con las obligaciones estatutarias, legales y contractuales relacionadas con la seguridad de la información y con la continuidad del negocio.

El Oficial de Seguridad de la Información cumplirá las siguientes funciones:

a) Realizar revisiones periódicas de todas las áreas a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
b) Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
c) Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

La sección de Recursos Humanos cumplirá la siguiente función.

a) Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Derecho de propiedad intelectual

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

La Oficina General de TI, con la asistencia del Área Legal de la UNC, analizará los términos y condiciones de la licencia, y deberá tener en cuenta los siguientes controles:

a) Mantener un adecuado registro de activos.
b) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

c) Verificar que sólo se instalen productos con licencia y software autorizado.
d) Utilizar herramientas de auditoría adecuadas.
e) Cumplir con los términos y condiciones establecidos para obtener software.
f) En todos los bienes informáticos de la UNC, queda prohibido el uso de software o programas que no cuenten con la licencia correspondiente.

Protección de datos y privacidad de la información.

Todos trabajadores deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La UNC redactará un “Acuerdo de Confidencialidad”, el cual deberá ser suscrito por todos los trabajadores. La copia firmada del compromiso será retenida en forma segura por la UNC.

Mediante este documento el trabajador se comprometerá a utilizar la información solamente para uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, empresa o tercera persona, salvo autorización previa y escrita del jefe de la Oficina General de TI y de la Oficial de Seguridad de la Información.

Cumplimiento de la Política de Seguridad

Cada jefe de área o unidad organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Oficial de la Seguridad de la información, realizará revisiones periódicas de todas las áreas de la UNC a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen los siguientes:

a) Sistemas de información.
b) Propietarios de información.
c) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

Sanciones

a) Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento Interno de la UNC.

b) Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión, dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

c) Al margen de la aplicación del reglamento interno por incumplimiento de las políticas de seguridad, la UNC, está en la potestad de iniciar acción penal (de acuerdo a las normas legales vigentes) contra el empleado infractor.

d) Corresponderá a la Oficina General de Administración, hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la UNC.

4.6. Validación del SGSI propuesto

4.6.1. Preguntas de la investigación

La investigación es del tipo descriptivo no experimental, por tanto, no se plantea hipótesis. Sin embargo, se plantean las siguientes preguntas de investigación:

a. ¿En qué medida el SGSI propuesto se adecúa al contexto de los procesos académicos de la Universidad Nacional de Cajamarca?
b. ¿En qué medida el SGSI propuesto permite un liderazgo para su implementación en la Universidad Nacional de Cajamarca?
c. ¿En qué medida se ha desarrollado un SGSI que permita la adecuada planificación de los controles y salvaguardas en base a la gestión de riesgos de TI que se propone?

4.6.2. Operacionalización de las variables de la investigación

La tabla siguiente muestra los indicadores que se obtendrán para cada uno de las dimensiones consideradas en la evaluación de la variable independiente, que es la variable que se va a manipular.

Tabla N° 29. Operacionalización de las variables de la investigación

Variable	Dimensión	Indicador	Instrumento para la evaluación	Escala
Sistema de Gestión de la Seguridad de la Información, basado en la ISO/IEC 27003	Contexto de la organización	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos académicos de la UNC	Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"
		Nivel de satisfacción de las necesidades y expectativas de las partes interesadas		
		Nivel de conformidad del alcance del SGSI		
		Nivel de cumplimiento de los requisitos de la Norma ISO/IEC 27003		
	Liderazgo	Nivel de compromiso de la alta dirección	Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"
		Nivel Efectividad de las políticas de TI		
		Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.		
	Planificación	Nivel de efectividad de las acciones para tratar los riesgos de TI	Cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"
		Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.		
Gestión de riesgos de TI	Grado de satisfacción de la identificación, análisis y tratamiento de los riesgos identificados		cuestionario	Escala Likert: (1) "muy en desacuerdo" - (5) "fuertemente de acuerdo"

4.6.3. Población y muestra de estudio

Unidad de Análisis: Usuarios de los servicios académicos de TI ofrecidos por la Oficina General de TI de la Universidad Nacional de Cajamarca.

Población: La población de la investigación está conformada por 31 usuarios.

Muestra: La muestra es la población.

4.6.4. Técnica de recopilación de los datos

Se aplicó una encuesta de satisfacción sobre el Sistema de Gestión de la Seguridad de la Información propuesto a la población indicada. Esta encuesta fue diseñada de tal

forma que sea compatible con los indicadores que se desean evaluar en esta investigación.

Para ello se elaboró la siguiente tabla que muestra la relación de las preguntas diseñadas en la encuesta con los correspondientes indicadores que permiten medirlo con la información recopilada.

Tabla N° 30. Matriz de consistencia entre los indicadores y las preguntas de la encuesta

Dim.	Indicador	Pregunta	
Contexto de la organización	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos académicos	P1	¿Usted considera que el Sistema de Gestión de Seguridad de la Información se adecuada a la estructura organizativa, a la normativa interna y a los procesos académicos de la UNC?
	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	P2	¿El SGSI propuesto permite satisfacer las necesidades y expectativas de las partes interesadas en la gestión de la seguridad de la información?
	Nivel de conformidad del alcance del SGSI	P3	¿Usted está conforme del modo como se determinó el alcance del Sistema de Gestión de Seguridad de la Información propuesto?
	Nivel de cumplimiento de los requisitos de la Norma 27003	P4	¿En qué grado usted cree que el SGSI propuesto cumple con las exigencias o los requisitos de la ISO/IEC 27003?
Liderazgo	Nivel de compromiso de la alta dirección	P5	¿Cree usted que en el SGSI propuesto se han establecido con claridad los liderazgos y compromisos para un adecuado gobierno de la seguridad de la información en la UNC?
	Nivel Efectividad de las políticas de TI	P6	¿Usted cree que la declaración de las políticas de seguridad en el SGSI permite establecer los objetivos de seguridad y permite la mejora continua del mismo?
	Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.	P7	¿Usted cree que los roles, responsabilidades y autoridades organizacionales del SGSI son adecuadas para la gestión de la seguridad de la información en la UNC?
Planificación	Nivel de efectividad de las acciones para tratar los riesgos de TI	P8	¿Considera usted que se definió y aplico adecuadamente un proceso de estimación de los riesgos de TI?
	Nivel de efectividad de las acciones para tratar los riesgos	P9	¿Considera usted que se definió y aplico adecuadamente un proceso de tratamiento de riesgo de TI?
	Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.	P10	¿Usted cree que los objetivos de seguridad de la información y su plan de ejecución planteados en el SGSI son adecuados para la gestión de la seguridad de la información en la UNC?
Grado de satisfacción de la identificación, análisis y tratamiento de los riesgos identificados		P11	¿Según usted cuál es su nivel de satisfacción de que el SGSI propuesto logra gestionar los riesgos reales y potenciales de TI?

4.6.5. Tratamiento de los datos y discusión de resultados

Para el tratamiento de los datos, se utilizó el aplicativo SPSS v 21, obteniéndose los siguientes resultados:

a. Fiabilidad del instrumento (encuesta)

Se determinó el nivel de fiabilidad del instrumento (la encuesta) utilizando el estadístico Alfa de Cronbach. El método de consistencia interna basado en el alfa

de Cronbach permite estimar la fiabilidad de un instrumento de medida a través de un conjunto de ítems que se espera que midan el mismo constructo o dimensión teórica. La validez de un instrumento se refiere al grado en que el instrumento mide aquello que pretende medir. Y la fiabilidad de la consistencia interna del instrumento se puede estimar con el alfa de Cronbach. La medida de la fiabilidad mediante el alfa de Cronbach asume que los ítems (medidos en escala tipo Likert) miden un mismo constructo y que están altamente correlacionados (Welch & Comer, 1988). Cuanto más cerca se encuentre el valor del alfa a 1 mayor es la consistencia interna de los ítems analizados. La fiabilidad de la escala debe obtenerse siempre con los datos de cada muestra para garantizar la medida fiable del constructo en la muestra concreta de investigación.

Procesados los datos se obtuvo lo siguiente:

Tabla N° 31. Resultados de la evaluación de la fiabilidad del instrumento

Alfa de Cronbach	N de elementos
,833	11

		N	%
Casos	Válidos	31	100,0
	Excluidos[a]	0	,0
	Total	31	100,0

Como criterio general, George & Mallery (2003) sugieren las recomendaciones siguientes para evaluar los coeficientes de Alfa de Cronbach:

- Coeficiente alfa >0.9 es excelente
- Coeficiente alfa >0.8 es bueno
- Coeficiente alfa >0.7 es aceptable
- Coeficiente alfa >0.6 es cuestionable
- Coeficiente alfa >0.5 es pobre
- Coeficiente alfa <0.5 es inaceptable

Es este caso se ha alcanzado 0.833, confirmándose que la encuesta aplicada es buena.

b. Análisis de la regresión múltiple

Utilizamos regresión múltiple porque nuestra hipótesis pretende estudiar la posible relación entre las variables independientes (predictoras o explicativas) y la variable dependiente (criterio, explicada, respuesta). En este caso, nuestras variables son:

- Variable Independiente (X_i): Sistema de Gestión de la Seguridad de la Información, basado en la ISO/IEC 27003, descrita a través de las dimensiones de Contexto de la organización (X_1), Liderazgo (X_2) y Planificación (X_3)
- Variable dependiente (Y): Gestión de riesgos de TI

Por tanto, el modelo a evaluar es un modelo de regresión múltiple de la forma:

$$Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + e$$

c. Reducción de ítems de cada dimensión evaluada

Dado que cada una de las dimensiones tiene más de un ítem a evaluar, de acuerdo a la estructura de la encuesta, se tuvo que reducir a un solo ítem, de la siguiente manera:

Tabla N° 32. Matriz de reducción de ítems evaluados

Dimensión	Ítem		Ítem reducido
Contexto de la organización(X_1)	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos académicos	P1	Dim_contexto = (P1 + P2 + P3 + P4)/4
	Nivel de satisfacción de las necesidades y expectativas de las partes interesadas	P2	
	Nivel de conformidad del alcance del SGSI	P3	
	Nivel de cumplimiento de los requisitos de la Norma 27003	P4	
Liderazgo(X_2)	Nivel de compromiso de la alta dirección	P5	Dim_liderazgo = (P5 + P6 + P7)/3
	Nivel Efectividad de las políticas de TI	P6	
	Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.	P7	
Planificación(X_3)	Nivel de efectividad de las acciones para tratar los riesgos de TI	P8	Dim_planificacion = (P8 + P9 + P10)/3
	Nivel de efectividad de las acciones para tratar los riesgos	P9	
	Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.	P10	

d. Procesamiento de datos

Para nuestro análisis se aplicará la metodología de regresión múltiple jerárquica con tres bloques, donde se fueron tomando variable por variable independiente con las que estamos trabajando, con la finalidad de generar diferentes modelos. Los modelos que esperamos generar son los siguientes:

- Modelo 1: sólo con la variable Contexto de la organización(X_1)
- Modelo 2: sólo con las variables Contexto de la organización (X_1) y Liderazgo (X_2)
- Modelo 3: con las tres variables Contexto de la organización (X_1), Liderazgo (X_2) y Planificación (X_3)

Esto nos permitirá identificar mayor información de las variables independientes con las que estamos trabajando; así como también nos permite identificar si alguna de esas variables independientes no aporta al modelo, por tanto, puede ser excluida del modelo.

Los resultados obtenidos se muestran a continuación:

Tabla N° 33. Resultados del procesamiento de datos por regresión lineal

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Durbin-Watson
1	,598[a]	,357	,335	,468	
2	,632[b]	,399	,356	,460	
3	,728[c]	,530	,478	,415	1,645
a. Variables predictoras: (Constante), Dim_contexto					
b. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo					
c. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo, Dim_planificacion					
d. Variable dependiente: P11					

Del cuadro se deduce que:

- El Modelo 1 (sólo con la variable Contexto de la organización (X_1)) explica el 35.7% de la varianza de la variable dependiente.
- El Modelo 2 (sólo con las variables Contexto de la organización (X_1) y Liderazgo (X_2)) explica el 39.9% de la varianza de la variable dependiente.

- El Modelo 3 (con las tres variables Contexto de la organización (X_1), Liderazgo (X_2) y Planificación (X_3)) explica el 53.0% de la varianza de la variable dependiente.

Para efectos de la demostración de la hipótesis seleccionamos el Modelo 3 donde se incluyen las tres variables independientes. Por otro lado, en el mismo cuadro observamos el resultado de la prueba de Durbin-Watson que nos da un valor para determinar la independencia de errores, pero no una significancia; por lo que tenemos que tener algunos criterios de identificación de cuando este valor es bueno o no bueno. El valor esperado de la prueba Durbin-Watson es que sea lo más cercano a 2, en este caso tenemos un valor de 1.645 que es bueno. El rango que se debe tener en cuenta para aceptar el resultado de la prueba de Durbin- Watson es 1 ± 2, es decir entre 1 y 3.

La interpretación de este resultado es que no existe dependencia de las observaciones recogidas, por lo tanto, se demuestra que la recogida de la información ha sido aleatoria, evitando así invalidar por completo las conclusiones del análisis estadístico.

e. Análisis de varianza (ANOVA)

Los resultados del ANOVA se muestran en la siguiente tabla:

Tabla N° 34. Resultados del análisis de varianza (ANOVA)

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	3,524	1	3,524	16,104	,000[b]
	Residual	6,347	29	,219		
	Total	9,871	30			
2	Regresión	3,942	2	1,971	9,309	,001[c]
	Residual	5,929	28	,212		
	Total	9,871	30			
3	Regresión	5,232	3	1,744	10,151	,000[d]
	Residual	4,639	27	,172		
	Total	9,871	30			
a. Variable dependiente: P11						
b. Variables predictoras: (Constante), Dim_contexto						
c. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo						
d. Variables predictoras: (Constante), Dim_contexto, Dim_liderazgo, Dim_planificacion						

Como el modelo de regresión que estamos trabajando es saber si las tres variables independientes están prediciendo la variable dependiente, entonces nos quedamos con los resultados del último modelo (Modelo 3) que se muestra en la tabla ANOVA.

Aquí se observa que hay una significancia menor al 0.05 (0.00 ≤ 0.05) y la interpretación en términos de hipótesis es que el modelo que estamos probando mejora significativamente la predicción de la variable dependiente.

f. Análisis de coeficiente de la ecuación de regresión

Tabla N° 35. Análisis de coeficientes

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Estadísticos de colinealidad	
		B	Error típ.	Beta			Tolerancia	FIV
1	(Constante)	,826	,779		1,059	,298		
	Dim_contexto	,829	,207	,598	4,013	,000	1,000	1,000
2	(Constante)	,534	,794		,672	,507		
	Dim_contexto	,550	,284	,396	1,933	,063	,511	1,958
	Dim_liderazgo	,358	,255	,288	1,405	,171	,511	1,958
3	(Constante)	,733	,719		1,019	,317		
	Dim_contexto	-,025	,331	-,018	-,075	,941	,306	3,270
	Dim_liderazgo	,277	,232	,223	1,199	,241	,502	1,990
	Dim_planificacion	,632	,231	,586	2,740	,011	,380	2,631

En la tabla de coeficientes siguientes se observa que nuestro modelo de regresión es:

$$Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + E$$

$$Y = .733 - .025X_1 + .277X_2 + .632X_3 + E$$

De los coeficientes obtenidos concluimos que solo la variable Contexto de la Organización (X_1) no aporta en la explicación del modelo propuesto, porque su coeficiente es -.025.

De la misma tabla, también podemos observar los valores t y su significancia, que son valores que nos demuestran que tanto podemos generalizar el modelo de predicción a la población, son: t = -0.75, 1.199 y 2,740. La cual nos confirma que

el modelo puede generalizarse a toda la población solo con las variables de Liderazgo (X_2) y de la variable de Planificación (X_3).

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se realizó un análisis de brechas de cumplimiento de los controles de la ISO/IEC 27002 para determinar la situación actual de la seguridad de la información en la Universidad Nacional de Cajamarca, y determinar el alcance que tendría la propuesta de un SGSI; encontrándose que existen incumplimientos significativos con respecto a la norma de referencia, sobre todo en los dominios de Organización de la seguridad de la información, Gestión de activos, Seguridad física y ambiental, Gestión de las comunicaciones y las operaciones, Gestión de incidentes de seguridad de la información y Cumplimiento.

2. Aplicando la metodología española MagerIT se desarrolló un procedimiento para identificar y analizar los riesgos de seguridad de información en los procesos académicos de la Universidad Nacional de Cajamarca. Este procedimiento evalúa la importancia de los activos de TI que han sido identificados en el alcance del SGSI definido en la etapa anterior, las amenazas asociadas a cada uno de ellos, se valora los impactos en los procesos y la probabilidad de su ocurrencia y finalmente se estima de los niveles de riesgo de TI. La aplicación de este procedimiento nos arrojó como resultado que existen niveles de riesgos importante y críticos en (1) interrupción de otros servicios y suministros esenciales, (2) caída del sistema por agotamiento de recursos, (3) avería de origen físico o lógico, (4) Condiciones ambientales inadecuadas de los equipos críticos.

3. De la misma manera, aplicando la metodología MagerIT se desarrolló un procedimiento para el tratamiento de los niveles de riesgo no tolerables, a través de salvaguardas, seleccionadas del catálogo de la metodología tomada como referencia, pero contextualizadas al entorno de la UNC. Aplicando el procedimiento establecido, se definieron un conjunto de salvaguardas para los activos, entre los más importantes destacan: (1) Servicios, (2) Aplicaciones, (3) Equipos informáticos, (4) Redes y comunicaciones, (5) Instalaciones y (6) Personal.

4. De acuerdo a la estructura organizativa de la UNC y del personal con que cuenta la Oficina General de TI, órgano encargado de la gestión de las TI, se identificó los principales roles y sus correspondientes funciones de la estructura organizativa de la seguridad de la información propuesta para la UNC. Se definieron los roles y funciones de: (1) Comité de Seguridad de la Información, (2) Comité Operativo de Seguridad de la Información, (3) Oficial de Seguridad de la Información, (4) Oficina General de TI, (5) Áreas académicas y (6) Propietario de los activos de seguridad de información.

5. Se definieron las políticas de seguridad de la información, para cada uno de los siguientes dominios de la seguridad de la información: (1) Gestión de activos de información, (2) Seguridad física y del entorno, (3) Gestión de comunicaciones y operaciones, (4) Control de acceso, (5) Adquisición, desarrollo y mantenimiento de sistemas y (6) Cumplimiento.

6. El Sistema de Gestión de la Seguridad de Información propuesto fue valorada desde 3 dimensiones: Contextualización en la organización, Liderazgo y Planificación de la seguridad de la información, a través de una encuesta de opinión a 31 usuarios de TI que contestaron oportuna y correctamente. Aplicando la técnica de la regresión múltiple jerarquizada, se obtuvo que la dimensión Contexto de la organización aporta con un 35.7% al SGSI propuesto, esto quiere decir, que la propuesta está bastante aceptable en relación a su adecuación al contexto de los procesos y procedimientos que se realizan en la UNC, la dimensión Liderazgo aporta con casi 4%, lo cual significa que los usuarios no le dan mucha importancia a esta dimensión y finalmente en la dimensión Planificación, se obtuvo que aporta con el 13% al SGSI. En resumen, las dimensiones Contexto de la organización y Planificación de la seguridad de la información son las dimensiones mejor valoradas en el SGSI propuesto, por los usuarios de TI de la UNC.

Recomendaciones

1. Se recomienda mantener una constante revisión de la política del SGSI y verificar el cumplimiento de la misma por parte de los empleados de la organización.

2. Se recomienda establecer los mecanismos que permitan la identificación de nuevos activos de información, y también la cultura organizacional para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos detectados; y con base en esa información tomar acciones preventivas

3. Se recomienda seguir con la utilización de una metodología para gestionar los riesgos; ya que, de esta manera se puede lograr una reducción en los riesgos a los cuales son sometidos los activos de información y también se puede hacer lo mismo para nuevos riesgos que aparezcan.

4. Se recomienda formar y capacitar de manera periódica al personal en temas de seguridad de la información y así lograr que todos los involucrados o relacionados con los activos de información tengan los alcances de la implementación claros.

5. Se recomienda la revisión periódica de los procedimientos de gestión de riesgos de TI para verificar si existen cambios en los escenarios de riesgo que impacten en el SGSI.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre Freire, D. S., & Palacios Cruz, J. C. (2014). *Evaluación técnica de seguridades del data center del municipio de Quito según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005.* Ecuador: Universidad de las fuerzas armadas ESPE, Sede SANGOLQUI.

Aguirre Mollehuanca, D. A. (2014). Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S:A. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Alcántara Torres, J. C. (2015). Guía de implementación de La seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte PNP en la ciudad de Chiclayo. Universidad Catolica Santo Toribio de Mogrovejo.

Alexander, A. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información. Optica ISO/IEC 27001:2005.* Bogotá, Colombia: Alfaomega.

BSI Group México . (s/a). Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013. *ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición*.

Carrasco, C. A. (2010). *Impacto del riesgo en el gobierno de las tecnologias de Información y comunicación en la gestión empresarial industrial del sigo XXI.* Lima-Perú.

Caviedes Sanabria, F., & Prado Urrego, B. A. (2012). *Modelo unificado para identificación y valoración de los riesgos de los activos de información en una organización.* Santiago de Cali.

Concha Huacoto, N. E. (2005). Propuesta para implantar CMMI en una empresa con multiples unidades desarrolladoras de software. *Tesis pregrado*. Lima: Universidad Nacioanl Mayor de San Marcos.

Condori Alejo, H. I. (2012). Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario. *tesis postgrado*. Lima: Universidad Inca Garcilaso de la Vega.

De la Cruz Guerrero, C. W., & Vasquez Montenegro, J. C. (2008). Elaboración y aplicación de un Sistema de Gestión de la Seguridad de la Información(SGSI) para la realidad Tecnólogica de la USAT. *tesis pregrado*. Chiclayo: Universidad Catolica Santo Toribio de Mogrovejo.

Eleven Paths. (23 de febrero de 2016). *Gestión de Incidentes* . Obtenido de http://blog.elevenpaths.com/2016/02/gestion-de-incidentes-i.html

Enriquez Espinosa, P. R. (2013). *Implementación de los controles asignados al dominio "Gestión De Activos", bajo los lineamientos establecidos por la norma ISO/IEC 27001 anexo a, para las empresas Municipales de Cali, Emcali E.I.C.E-ESP.* Colombia: Universidad Autónoma de Occidente.

Espinoza Aguinaga, H. R. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Espinoza, A. H. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *Tesis PreGrado*. Lima: Pontificia Universidad Católica del Peru.

Hernández Pinto, M. G. (2006). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. *tesis pregrado*. Guayaquil - Ecuador: Escuela Superior Politécnica del Litoral.

Huamán Monzón, F. M. (2014). Diseño De Procedimientos De Auditoría De Cumplimiento De La Norma NTP-ISO/IEC 17799:2007 Como Parte Del Proceso De Implantación De La Norma Técnica NTP-ISO/IEC 27001:2008 En Instituciones Del Estado Peruano. *tesis pregrado*. Lima: Pontificia Universidad Católica del Perú.

Inteco. (s/a). Implantación de un SGSI en la empresa. *SGSI*, 22.

ISO 27000.es. (2005). *ISO 27000*. Recuperado el 15 de 03 de 2017, de ISO 27000: www.iso27000.es

ISO/IEC 27001. (2005). *Tecnologia de la información - Tecnicas de seguridad - Sistemas de Gestion de seguridad de la información - Requerimientos.*

ISO/IEC 27001. (2005). *Tecnología de la Informacion-Tecnicas de Seguridad-Sistemas de gestión de seguridad de la Información - Requerimientos.* Primera edicion 2005-10-15.

ISO/IEC 27002. (2013). *Information technology - Security techniques - Code of practice for information security management.* EEUU.

ISOTools Excellence. (17 de 01 de 2014). *http://www.pmg-ssi.com*. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

ISOTools Excellence. (31 de 01 de 2014). *http://www.pmg-ssi.com/*. Obtenido de http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

Ladino A., M. I., Villa S., P. A., & López E., A. M. (2011). Fundamentos de ISO/IEC 27001 y su aplicación en las empresas. *Scientia et Technica Año XVII*, 334.

López M., A. A. (2011). *Diseño de un Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara.* Venezuela: Universidad Centoccidental "Lisandro Alvarado".

Magerit. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciónes Públicas.

Mancera, S. (. (2011). Perspectivas sobre los riesgos de TI. *Seguridad de la información en un mundo sin fronteras*, 15.

Mega, I. G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Montevideo, Uruguay.

Montesino Perurena, R., Baluja Garcia, W., & Porven Rubier, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista de Ingenieria Electrónica Automática y Comunicaciones*.

NTP ISO/IEC 17799. (2007). *EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.* Lima.

NTP ISO/IEC 27001. (2016). *EDI Tecnologia de la Información. Tecnicas de seguridad. Sistemas de gestión de seguridad de la información.* Lima.

NTP-ISO/IEC 27001. (2014). *EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.* Lima.

NTP-ISO/IEC 27005. (2009). *EDI. Tecnologia de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información.* Lima.

Ozier, W. (2004). *Risk Analysis and Assessment" Information Security Management Handbook. 5th edition.* USA: Auerbach Publications.

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals.* USA: Auerbach Publications.

Portal Oficial de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI. (NTP ISO/IEC 27001:2008). Obtenido de http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552

Poveda, J. M. (s/a). *Auditoría Informática.* UNI-NORTE.

Reina García, E., & Morales Ramírez , J. R. (2014). Modelamiento de procesos basados en el grupo de normas internacionales ISO/IEC 27000 para gestionar el riesgo y seleccionar controles en la implementación del sistema de gestión de seguridad de la información. *tesis pregrado*. Universidad tecnológica de Pereira Facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación.

Robles , R., & Rodriguez de Roa, Á. (2006). La gestión de la seguridad en la empresa. *Comite de Entidades de Certificación de la AEC*, 14-18.

Talavera Álvarez, V. R. (2015). *Diseño de un Sistema de Gestión De Seguridad de la Información para una entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013.* Lima-Perú: Pontificia Universidad Católica del Perú.

Tupia Anticona, M. F. (2011). *Gobierno de las tecnologías de información bajo la óptica de COBIT.* Perú: Tupia Consultores y Auditores S.A.C. Perú.

Universidad Distrital Franscisco José de Caldas. (s/a). Gestión del riesgo. En *Proceso de desarrollo Open UP/OAS* (pág. Cap. 5).

Villalón Huerta, A. (2002). *SEGURIDAD EN UNIX Y REDES Version 2.1.*

Welch, S., & Comer, J. (1988). *Quantitative methods for public administration: techniques and applications* (2, reimpresa ed.). (1. Brooks/Cole Pub. Co., Ed.) la Universidad de Virginia.