UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"

ESCUELA DE POSTGRADO

MAESTRIA EN INGENIERÍA DE SISTEMAS

"MODELO DE GESTIÓN DE RIESGOS DE TI BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA – CHACHAPOYAS PERÚ"

TESIS

PRESENTADA PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE

AUTOR:

Ing. OSCAR ÑAÑEZ CAMPOS

ASESOR:

Dr. ERNESTO KARLO CELI ARÉVALO

LAMBAYEQUE – PERÚ

2019

DATOS INFORMATIVOS

Título del proyecto

Modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú

Autor

Oscar Ñañez Campos

email: oscar_nanez@hotmail.com

Asesor

Dr. Ing. Ernesto Karlo Celi Arévalo

Fecha de presentación

Junio del 2019

Presentado por

Ing. Oscar Ñañez Campos	Dr. Ernesto Karlo Celi Arévalo
Autor	Asesor

JURADO EVALUADOR

_____

Dra. JESSIE BRAVO JAICO
Presidente del Jurado

_____

M.Sc. PEDRO FIESTAS RODRÍGUEZ
Secretario

_____

M.Sc. ROBERTO ARTEAGA LORA
Vocal

DEDICATORIA

A Dios, por darme la oportunidad de vivir y estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante el periodo de estudios.

A mis padres: **MANUEL ÑAÑEZ CHANCAFE** y **MARGARITA CAMPOS MORALES**, por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académico, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo. Todo este trabajo ha sido posible gracias a ellos.

A mis hermanos, amigos, colegas y a todos aquellos que participaron directa e indirectamente en la elaboración de esta tesis. ¡Gracias a ustedes!

AGRADECIMIENTOS

A Dios por bendecirme para llegar hasta donde he llegado, por hacer realidad una de mis metas anheladas.

A la UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO por darme la oportunidad de estudiar la Maestría en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de Información y Gestión del Software.

Mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización de la presente tesis, en especial al **Dr. Ing. Ernesto Karlo Celi Arévalo,** por su permanente colaboración y apoyo incondicional en el desarrollo y culminación de mi Proyecto e informe de tesis.

En general a la dirección de Tecnologías de Información y Comunicaciones de la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas por facilitarme el acceso a la información requerida para alcanzar los objetivos trazados en la presente tesis.
En especial, a mis padres y hermanos, de los cuales siempre recibí su apoyo.

Finalmente, a todas aquellas personas, colegas y amigos que me brindaron su apoyo, tiempo e información para el logro de mis objetivos.

A todos ellos muchas gracias.

RESUMEN

Uno de los aspectos más críticos de la administración de una organización es la gestión de sus activos que generan valor a los procesos del negocio. La información, puede considerarse como uno de los activos más críticos que hay que proteger, porque su disponibilidad e integridad, no solo se utiliza como insumo para la toma de decisiones, si no también asegura la continuidad de los procesos.

La gestión de la información no solo implica incorporar tecnologías que le den soporte a su captura, almacenamiento, procesamiento y comunicación; si no también se debe implementar procesos y sistemas que gestionen este recurso para lograr su seguridad. La implementación de sistemas de gestión de la seguridad de la información (SGSI) permite que ésta logre niveles aceptables de confidencialidad, integridad y disponibilidad.

Un proceso de implementación de un SGSI, metodológicamente hablando, implica una serie de actividades y tareas, que van desde la planificación de su alcance hasta la planificación de los planes de mejora continua. Sin embargo, el aspecto más crítico que debe considerarse en la implementación de un SGSI es la gestión de los riesgos. La gestión de los riesgos es una estrategia preventiva que permite identificar y evaluar los diferentes escenarios de riesgo a los que está expuesta la información, en sus diferentes formas de expresión, y las tecnologías que le dan soporte a lo largo de su ciclo de vida. Con esta información, se podrá implantar los controles y salvaguardas necesarias para la mitigación de aquellos niveles de exposición al riesgo que la organización considere no aceptables.

El propósito de este trabajo de investigación se centró en el desarrollo de un Modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza (UNTRM) – Chachapoyas Perú.

Esta propuesta permitió el aumento significativo de la satisfacción de los usuarios de TI en relación a la gestión de los servicios de TI en la UNTRM, que garantiza que los riesgos de TI sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Palabras clave: sistema de gestión de riesgos de TI, análisis y evaluación de riesgos, activo de TI.

ABTRACT

One of the most critical aspects of managing an organization is the management of its assets that generate value to business processes. Information can be considered as one of the most critical assets that must be protected, because its availability and integrity is not only used as input for decision making, but also ensures the continuity of processes.

Information management does not only involve incorporating technologies that support its capture, storage, processing and communication; If not, you must also implement processes and systems that manage this resource to achieve your security. The implementation of information security management systems (ISMS) allows it to achieve acceptable levels of confidentiality, integrity and availability.

A process of implementation of an ISMS, methodologically speaking, involves a series of activities and tasks, ranging from the planning of its scope to the planning of continuous improvement plans. However, the most critical aspect that should be considered in the implementation of an ISMS is risk management. Risk management is a preventive strategy that allows identifying and evaluating the different risk scenarios to which the information is exposed, in its different forms of expression, and the technologies that support it throughout its life cycle. With this information, the necessary controls and safeguards can be implemented to mitigate those levels of risk exposure that the organization considers not acceptable.

The purpose of this research work was focused on the development of an IT risk management model based on the ISO / IEC 27005 standard and the Magerit methodology to improve information security management at the Toribio Rodríguez de Mendoza National University (UNTRM) - Chachapoyas Peru.

This proposal allowed the significant increase in the satisfaction of IT users in relation to the management of IT services in the UNTRM, which guarantees that IT risks are known, assumed, managed and minimized in a documented, systematic way, structured, repeatable, efficient and adaptable to changes that occur in risks, the environment and technologies.

Key words: IT risk management system, risk analysis and evaluation, IT asset.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE GRÁFICOS

INTRODUCCION

En la presente tesis, se diseña y desarrolla el modelo para implementar un sistema de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza (UNTRM) – Chachapoyas Perú.

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 permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad.

La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en la UNTRM; lo cual 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.

La problemática principal actual de las organizaciones que están en franco desarrollo y que soportan sus procesos de negocio sobre TI, es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la empresa a pérdidas no solo de información, sino también económica.

Es por ello, que la UNTRM se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

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 riesgos 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 los materiales, métodos y herramientas utilizadas para el desarrollo del trabajo de investigación. También se define la metodología empleada, la cual es la resultante de un estudio de distintas metodologías y de la investigación y aporte de los autores de este trabajo de investigación. Adicionalmente este capítulo también contiene la etapa de desarrollo del proyecto, en la cual se muestra el proceso seguido para la realización del mismo.

- El capítulo IV está destinado a la presentación de las pruebas y resultados del trabajo de investigación. Así mismo, se aborda la discusión de los resultados a manera de explicación de los mismos, teniendo en cuenta las variables expuestas en los capítulos anteriores.

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

CAPÍTULO I. EL PROBLEMA

1.1. Descripción de la problemática

La importancia de la incorporación de los Sistemas y Tecnologías de Información (TSI) en los procesos de negocio de las organizaciones son cada vez justificables, pero también cada vez más complejas, sustentada básicamente, en lograr diferenciación con respecto a la competencia u obtener mejoras en los procesos: tiempos de respuesta, integración de áreas y usuarios, reducción de costos, etcétera. No interesa el tipo y tamaño de la entidad, sólo basta que los procesos del negocio sean soportados por TSI.

Entre las situaciones que las organizaciones deben gestionar, están los entornos dinámicos y cambiantes a los que se enfrenta la infraestructura tecnológica; así como las inversiones necesarias para mantener operativos los diferentes servicios que presta el área de TI. Los especialistas de TI han comprobado que la ausencia o carencia de procedimientos ordenados que brinden una línea de servicios de soporte técnico (baseline) de las TI que se encuentran en la organización impacta en su rendimiento, lo que conlleva a:

- Costos mayores.
- Tiempos de paro continuos.
- Pérdidas de información.
- Mal uso de las TI que se encuentran en la organización.
- Insatisfacción de los usuarios.

El uso de las tecnologías de la información (de ahora en adelante TI) se ha intensificado en las organizaciones independiente de la naturaleza y actividad de las mismas, estás se encuentran en constante evolución adaptándose a las nuevas necesidades de las organizaciones y así mismo dando lugar a otras relacionadas con su operación diaria. Adicionalmente su masificación las han convertido en blanco de ataques y vías para los mismos; los riesgos asociados a estas se intensifican y transforman y por ello se hace necesario crear y adaptar constantemente los medios y métodos utilizados para conservar la seguridad de la información que las organizaciones quieren proteger.

En este punto el desarrollo y uso de metodologías integradas y ágiles para gestionar riesgos y en especial el tecnológico es importante con el fin de minimizar el impacto que pueda causar la violación de alguna de las dimensiones de la seguridad (esto corresponde a la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad). Hasta el momento el marco existente para gestión de riesgos lo conforman los estándares ISO 31000 (Risk management) e ISO/IEC 27005 (Information security risk management). Estos proveen lineamientos generales pero hace falta una guía más precisa que ofrezca pautas sobre la forma de lograr los aspectos de seguridad requeridos; adicionalmente este marco hace referencia a la gestión sobre los riesgos como concepto global y deja de lado el análisis de riesgos específicos como el tecnológico, lo más cercano es la administración del riesgo operativo en el que se relaciona de forma tangencial el riesgo tecnológico.

El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico.

Este contexto motiva el desarrollo de una metodología, que permite la gestión de riesgos de origen tecnológico cuya base son los estándares ISO 31000 e ISO/IEC 27005 de los cuales se realizaron las adaptaciones y especificaciones requeridas para este tipo de riesgo. Además se puede adoptar e incorporar recomendaciones y buenas prácticas de otras guías y metodologías para gestión de riesgos como MAGERIT , NIST SP 800-30, NTC 5254, ISO 27001 y lo correspondiente a seguridad en gestión de servicios de ITIL® v3. De igual forma se presenta una forma de ajustar esta metodología a la gestión de continuidad de negocios en lo respectivo a la definición de planes de gestión de incidentes tecnológicos.

La UNTRM en su función de formar nuevos profesionales, no escapa a este tipo de problemas. Sus procesos académicos y administrativos funcionan bajo el soporte de aplicaciones informáticas y de una infraestructura de tecnologías de información en constante crecimiento. Surge entonces, la necesidad de establecer

una línea de soporte técnico basada en alguna metodología que permita identificar, evaluar y tratar los riesgos de TI, y de esta manera realizar una gestión eficiente de los controles necesarios para mitigar los potenciales escenarios de riesgo que podrían afectar o impactar negativamente en la continuidad del negocio.

1.2. Formulación del problema científico

¿Cuál es el impacto de la aplicación de un modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, sobre la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Elaborar un modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú

1.3.2. Objetivos específicos

Los objetivos específicos del estudio son:

a. Identificar y evaluar los escenarios de riesgo en la seguridad de la información en los procesos académicos y administrativos de la Universidad Nacional Toribio Rodríguez de Mendoza.
b. Elaborar el procedimiento de evaluación y tratamiento de riesgos en la seguridad de la información para los procesos académicos y administrativos.
c. Establecer el apetito y las tolerancias a los niveles de exposición al riesgo que permita evaluar las amenazas, vulnerabilidades, impactos y frecuencias de ocurrencia de las amenazas.
d. Determinar los niveles de exposición a los riesgos de TI con la finalidad de identificar los controles necesarios para aquellos niveles no tolerables por la UNTRM.
e. Obtener brechas de seguridad para determinar la efectividad de los controles.

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 del Modelo de Gestión de Riesgos de TI.

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 gráfico siguiente:

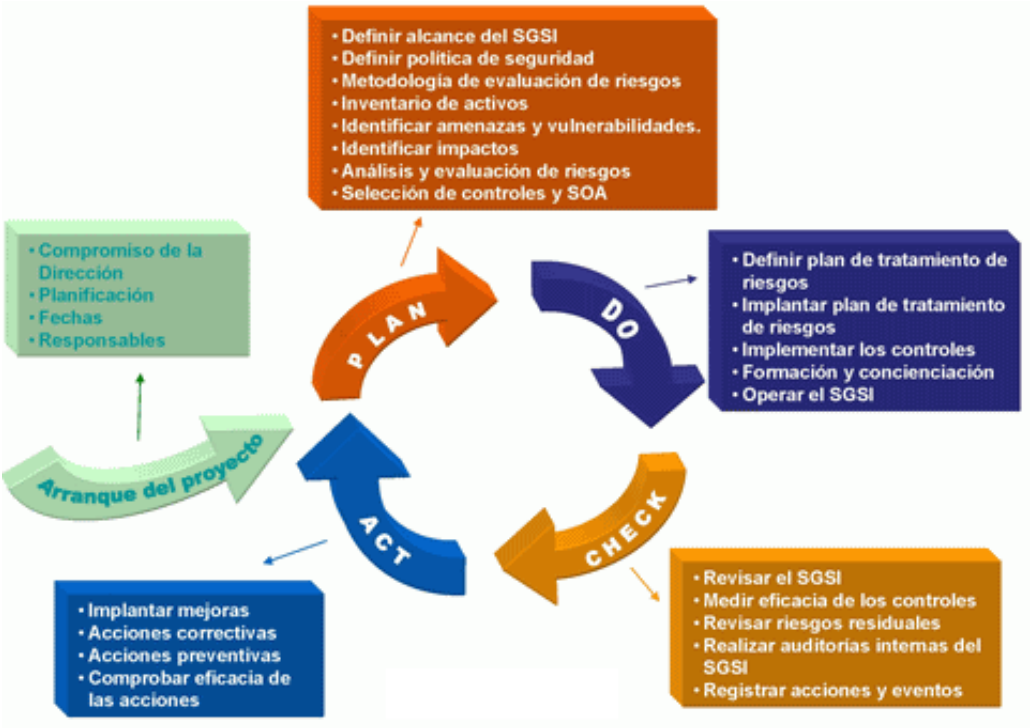

Gráfico N° 1. Etapas de un SGSI

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. Elemento de un SGSI

La ISO 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.

2.7. Gestión de Riesgos de TI

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 garantizará 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)

2.8. Elementos evaluados en la Gestión de Riesgo de TI

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?)

2.9. Proceso de Gestión de Riesgos

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.

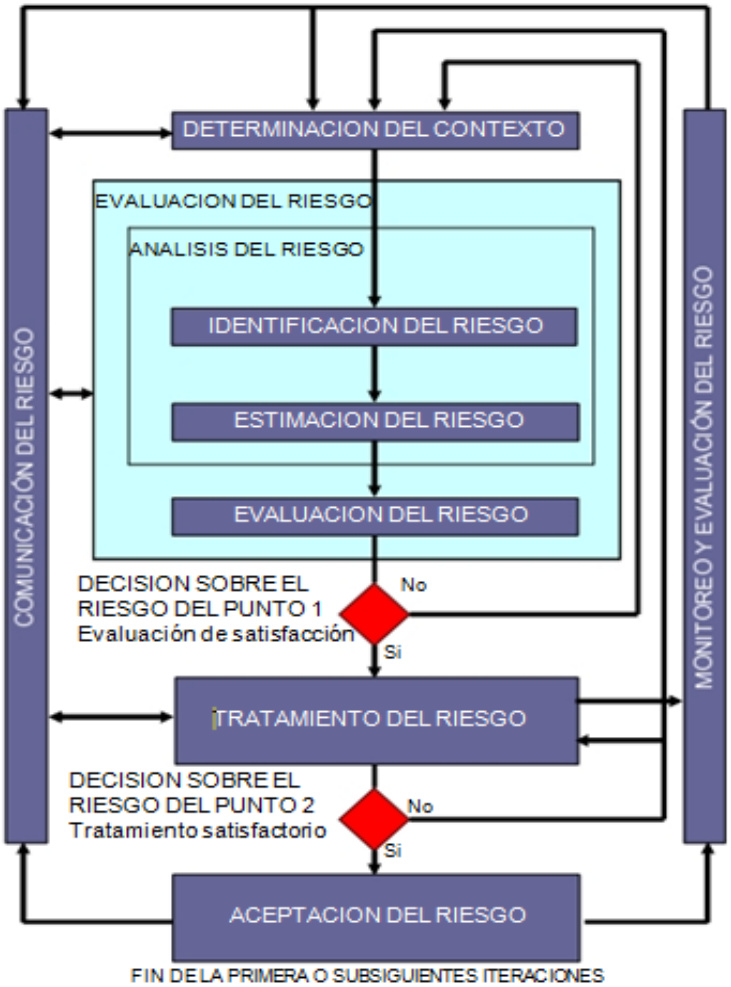

Gráfico N° 3. Proceso de gestión del riesgo según la ISO 31000
Fuente: (Magerit, 2012)

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 gráfica 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 de área 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° 1. Alineamiento del SGSI y del Proceso de Gestión del Riesgo en Seguridad de la Información

Proceso Sistema de Gestión de Seguridad de la información	Proceso de Gestión del Riesgo en Seguridad de la Información
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)

2.10. Metodología para la Gestión de Riesgos de TI Magerit

Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", dentro del "**Ma**rco de **Ge**stión de **Ri**esgos de **T**ecnologías de la Información". 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 - Libro 1, 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). Para ello Magerit propone el siguiente modelo:

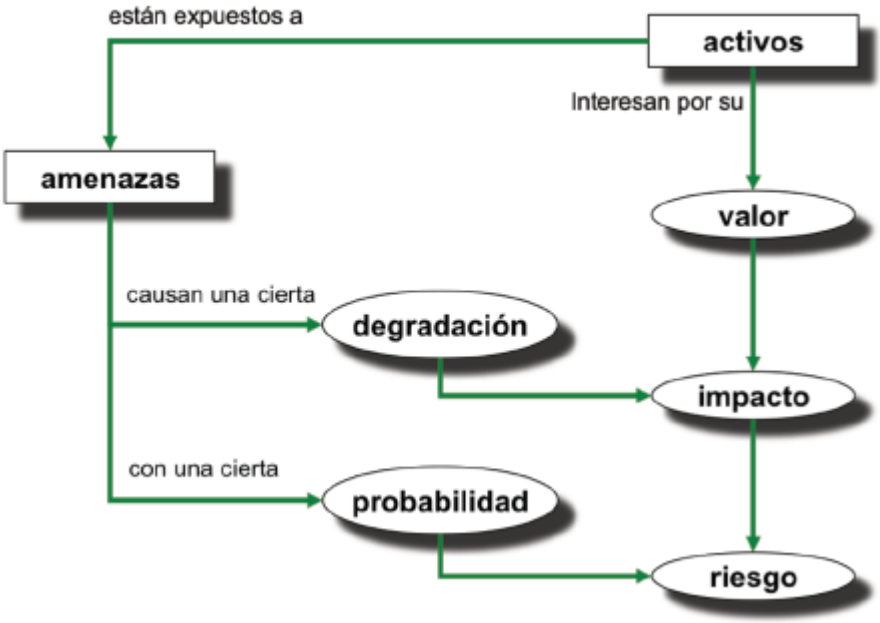

Gráfico N° 4. Elementos del análisis de riesgos potenciales
Fuente: (Magerit - Libro 1, 2012)

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.

2.11. 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 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.

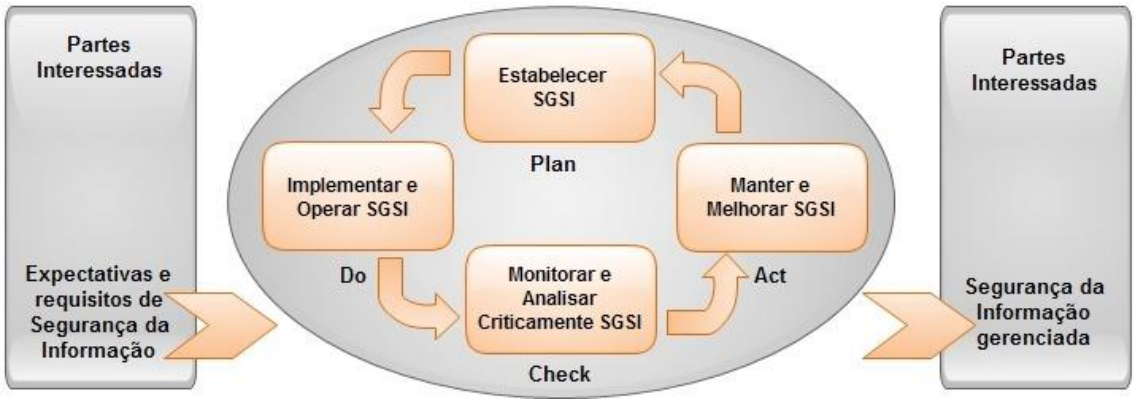

Gráfico N° 5. Modelo PDCA aplicado a los procesos de un SGSI
Fuente: (ISO/IEC 27001, 2005)

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.

Estructura de la ISO/IEC 27001:2013

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

Tabla N° 2. 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)

2.12. 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. ISO/IEC 27005 EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información

ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001 (ISOTools Excellence, 2014).

ISO 27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia organización. Los usuarios elijen el método que mejor se adapte para, por ejemplo, una evaluación de riesgos de alto nivel seguido de un análisis de riesgos en profundidad sobre las zonas de alto riesgo (ISOTools Excellence, 2014).

Las secciones de contenido son:

1. Prefacio.
2. Introducción.
3. Referencias normativas.
4. Términos y definiciones.
5. Estructura.
6. Fondo.
7. Descripción del proceso de ISRM.
8. Establecimiento Contexto.
9. Información sobre la evaluación de riesgos de seguridad (ISRA).
10. Tratamiento de Riesgos Seguridad de la Información.
11. Admisión de Riesgos Seguridad de la información.
12. Comunicación de riesgos de seguridad de información.
13. Información de seguridad Seguimiento de Riesgos y Revisión.

    Anexo A: Definición del alcance del proceso.

    Anexo B: Valoración de activos y evaluación de impacto.

    Anexo C: Ejemplos de amenazas típicas.

    Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.

Anexo E: Enfoques de evaluación del riesgo en seguridad de la información

En el Anexo E: Enfoques de evaluación del riesgo en seguridad de la información, la NTP-ISO/IEC 27005 (2009) muestra dos enfoques:

a. E.1 Evaluación del riesgo en seguridad de la información de alto nivel (NTP-ISO/IEC 27005, 2009)

   Las características de la iteración de la evaluación del riesgo del alto nivel pueden incluir las siguientes:

   - La evaluación del riesgo de alto nivel puede dirigirse a una visión más global de la organización y de sus sistemas de información, considerando los aspectos de la tecnología como independientes de las cuestiones empresariales. Al hacer esto, el análisis del contexto se concentra más en el negocio y el entorno operativo que en los elementos tecnológicos.
   - La evaluación del riesgo de alto nivel puede resolver una lista más limitada de amenazas y vulnerabilidades agrupadas en dominios definidos o para hacer el proceso más expeditivo, puede centrarse en los escenarios de riesgo o ataque en vez de sus elementos.
   - Los riesgos que se presentan en una evaluación del riesgo de alto nivel frecuentemente son dominios de riesgo más generales que los riesgos específicos identificados.

b. E.2 Evaluación detallada del riesgo en seguridad de la información (NTP-ISO/IEC 27005, 2009)

   El proceso de evaluación detallada del riesgo en seguridad de la información incluye una identificación y valorización profunda de los activos, la evaluación de amenazas a esos activos y la evaluación de vulnerabilidades. Los resultados de esas actividades se utilizan entonces para evaluar los riesgos y luego identificar el tratamiento del riesgo.

   Se puede evaluar las consecuencias de varias maneras, incluyendo el uso de medidas cuantitativas, por ejemplo, monetarias, y cualitativas (las que se pueden basar en el uso de adjetivos como moderado o grave), o una combinación de ambas.

2.14. Definición de la terminología técnica básica

- **Aceptación del riesgo:** Decisión de aceptar el riesgo
- **Activo:** Recursos relacionados con el sistema de información o relacionado con éste, necesario para el correcto funcionamiento de la organización
- **Amenaza:** Una causa potencial de un incidente no-deseado, el cual puede resultar dañando a un sistema o activo de TI
- **Análisis de riesgo:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo. Identifica los activos a proteger o evaluar.
- **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.
- **Declaración de aplicabilidad (SOA):** Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del SGSI.
- **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.
- **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.
- **Frecuencia (probabilidad de ocurrencia):** Posibilidad de que una amenaza se materialice, independientemente de las salvaguardas que existan para contrarrestarla.
- **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.
- **Impacto:** Medida del daño sobre el activo derivado de la materialización de una amenaza
- **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.

- **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.
- **Riesgo residual:** El riesgo remanente después del tratamiento del riesgo
- **Riesgo:** Es la combinación de la probabilidad de un evento y su ocurrencia.
- **Salvaguardas** o contra medidas: Son aquellos procedimientos o mecanismos tecnológicos o administrativos que reducen el nivel de riesgo.
- **Tratamiento del riesgo:** Proceso de tratamiento de la selección e implementación de salvaguardas y controles para modificar el riesgo.
- **Vulnerabilidad:** Son ciertas condiciones inherentes a los activos que facilitan que las amenazas se materialicen y llevan a esos activos a ser vulnerables.

CAPÍTULO III. DESARROLLO DE LA PROPUESTA

3.1. Definición de la metodología para la implementación

Tomando como referencia la ISO 27005, que es el estándar internacional que sirve de guía para la implantación de un Sistema de Gestión de Riesgos de TI y la metodología española Magerit v3, se plantea la siguiente metodología para el desarrollo de la propuesta de un Sistema de Gestión de Riesgos:

Fase 1: Definición del alcance del Sistema de Gestión de Riesgos
Fase 2: Evaluación de riesgos de TI
Fase 3: Tratamiento y administración del riesgo de TI
Fase 4: Propuesta de políticas de seguridad de la información

3.1.1. Actividades para la Fase 1: Definición del alcance del SGR

La cláusula 4.2.1 del estándar ISO 27001, en relación con el alcance del modelo de SGSI, refiere la siguiente obligación: “Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance“ (NTP-ISO/IEC 27001, 2014).

Al definir el alcance del SGR, se busca **clarificar cual es la información a la que se quiere dar protección**, con independencia de dónde se halle, cómo se almacene o quién pueda acceder a la misma.

Para ello se debe analizar los aspectos tanto internos como externos de la entidad en análisis, para lograr un entendimiento de la organización, identificando partes interesadas y las interrelaciones entre los procesos involucrados y su entorno.

Para lograr este propósito se desarrollan las siguientes tareas:

a. **Identificación de procesos y activos críticos:** Se identifican primero los procesos que son considerados dentro del alcance del SGSI, describiendo el flujo de trabajo para identificar las áreas y usuarios intervinientes y sus interrelaciones. Para ello se modelan los procesos seleccionados mediante la perspectiva BPM.

Finalmente se identifican los activos de la información y de TI que se deben proteger en los procesos analizados.

Esta actividad también debe incluir el modelado de los procesos seleccionados con la finalidad de identificar el flujo de la información a través de las diferentes áreas y dependencias administrativas.

b. **Definición de la política general del SGSI:** Para definir la política general del SGSI se debe tener en consideración lo siguiente:
   - Debe incluir el marco referencial para establecer los objetivos,
   - Debe tomar en cuenta los requerimientos comerciales, legales, reguladores, y las obligaciones de la seguridad contractual,
   - Debe estar alineada con el contexto de la gestión del riesgo estratégico de la gerencia,
   - Debe establecer el criterio con el que se evalúa el riesgo,
   - Debe ser revisada y aprobada por la gerencia.

c. **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 27001.

   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 27001.

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

Tabla N° 3. Formato para la evaluación de brechas de seguridad de la información

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

3.1.2. Actividades para la Fase 2: Evaluación de riesgos de TI

Las actividades de la Fase 2 se plantearon en base a la ISO 27005. Para determinar las actividades de esta fase, primero se identificaron los componentes que deberán ser considerados para la evaluación de los riesgos. Para ello se tomó como referencia el modelo de la ISO 27005.

En la gráfica siguiente se puede apreciar, que los elementos o componentes que deben ser considerados para la evaluación de los riesgos de TI son:

- Los activos de información y de TI
- El valor de los activos de TI (criticidad del activo)
- Las amenazas
- El impacto (de la materialización de una amenaza)
- La frecuencia (o probabilidad de ocurrencia de la materialización de una amenaza)

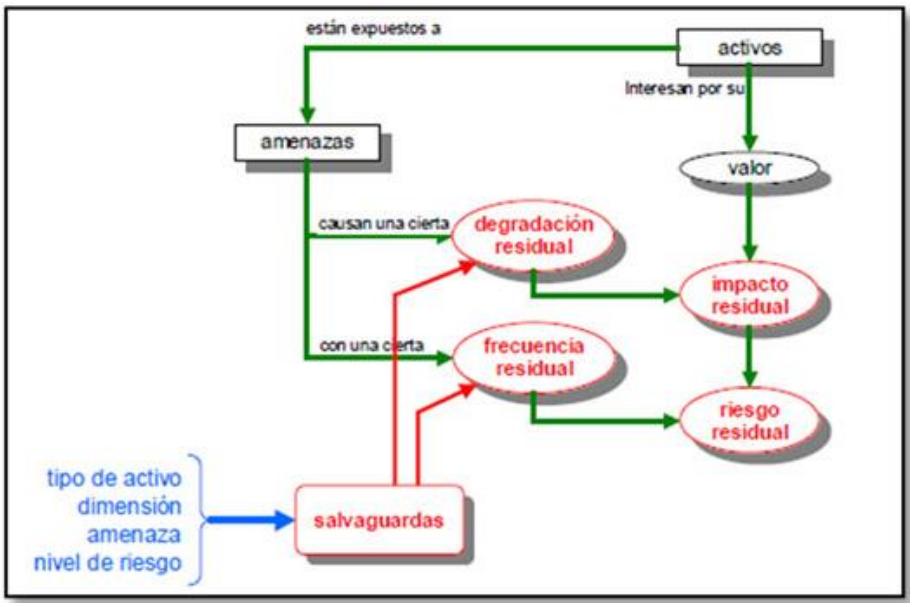

Gráfico N° 6. Elementos y sus relaciones de un modelo de gestión de riesgos de TI
Fuente: (Magerit - Libro 1, 2012)

En base al modelo de gestión de riesgos de TI utilizado para esta investigación, las actividades consideradas para la fase de valoración de los riesgos, fueron:

a. **Definición del inventario de activos de información y de TI relevantes**

   En esta tarea se identificarán los activos que dan soporte a los procesos del alcance del SGR. Para ello, se utilizará la clasificación propuesta por la Metodología Magerit; específicamente la clasificación propuesta para activos de soporte de los activos primarios (procesos e información). Se clasificarán los activos de TI, según sus características, en los siguientes tipos:

Tabla N° 4. Clasificación de activos de TI

Tipo de activo	Descripción del tipo de activo
Dato	Información que se genera, envía, recibe y gestionan dentro de la organización. Incluye los documentos que se gestionan dentro de sus procesos.
Aplicación	Software que se utilice como soporte en los procesos
Personal	Actores que tienen posibilidades de acceso y manejo, de una u otra manera, de los activos de información
Servicio	Servicios que alguna área de la organización suministra a otra área o entidades externas a la misma
Tecnología	Hardware donde se procesa, almacena o transmite la información
Instalación	Lugar donde se alojan los activos de información. Puede estar ubicado dentro de la entidad o fuera de ella
Equipamiento auxiliar	Activos que no se hallan definidos en ninguno de los anteriores tipos

Fuente: Elaboración propia, adaptado de (Magerit, 2012)

b. Determinación de la criticidad de los activos de información y de TI

Una vez inventariados los activos de TI es necesario identificar y documentar el valor que su seguridad representa para la entidad. Para ello, se asignará un conjunto de valores a cada activo teniendo en cuenta los diferentes requerimientos de seguridad que se consideren relevantes.

El valor que tienen los activos de información en el ámbito de la seguridad puede medirse desde diversos puntos de vista. Estos puntos de vista se denominan, en el marco de este modelo, requerimientos de seguridad o dimensiones de la seguridad, los cuales están definidos en el Anexo N° 1.

La valoración se deberá realizar mediante la ponderación de las pérdidas ocasionadas para la entidad en caso de que falle o caiga el activo, debido a la materialización de una amenaza, de cada uno de los requerimientos de seguridad definidos para los diferentes activos de información, según las tablas de referencia del Anexo N° 4 en relación a: disponibilidad, integridad y confidencialidad.

Las escalas y criterios que se utilizarán para calificar cada una de las dimensiones de seguridad de TI de cada activo, se muestran en la tabla N° 5.

Tabla N° 5. Escalas propuestas para la valoración de los criterios de seguridad de la información para determinar la criticidad de los activos

Criterio	Valor en escala	Descripción
Disponibilidad	1	El activo debe estar disponible por lo menos 25% del tiempo que se necesite. No existe riesgo operacional, reputacional, ni legal si el activo de información se ha eliminado o no está disponible.
	2	El activo debe estar disponible por lo menos 50% del tiempo que se necesite. Si no lo estuviera o si fuese destruido puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe estar disponible el 100% del tiempo que se necesite. Si no lo estuviera o si fuese destruido ocasionará daños graves o hasta catastróficos para la organización, afectarán los intereses legales, operacionales o reputacionales, y causarán pérdidas económicas.
Integridad	1	El activo debe estar correcto y completo por lo menos el 25% de las veces que se necesite. No existe pérdidas económicas, ni riesgo operacional, reputacional, ni legal.
	2	El activo debe ser correcto y completo al menos el 50% de las veces que se necesita. Puede ocasionar daños leves en la organización, que afecten los intereses legales, operacionales y reputacionales.
	3	El activo debe ser correcto y completo el 100% de las veces utilizadas. De no cumplir con lo anterior, puede causar daños graves o hasta catastróficos para la organización, y afectará los intereses legales, operacionales o reputacionales, además de pérdidas económicas significativas.
Confidencialidad	1	El activo es de conocimiento del público, por lo tanto, no existe ningún riesgo legal, reputacional, operacional, ni económico.
	2	El activo podrá ser divulgado hacia los colaboradores. Si se cumple con lo anterior no será perjudicial para los intereses legales, reputacional, operacional, ni económico.
	3	El activo contiene información altamente sensible. Su divulgación puede causar daños graves o hasta catastróficos, afectando los intereses legales, reputacionales, y económicos.

Fuente: Desarrollo propio, tomando como referencia los criterios de valoración de la metodología Magerit (Magerit, 2012)

Para determinar la criticidad de los activos se utilizará el siguiente formato:

Tabla N° 6. Plantilla para la calificación de la criticidad de los activos de TI

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		Confidencialidad	Integridad	Disponibilidad		
1						
2						
3						

Fuente: Desarrollo propio

Los niveles de criticidad de los activos de TI se obtendrán del producto de las calificaciones realizadas para cada criterio de seguridad y se clasificarán de la siguiente manera:

Tabla N° 7. Niveles de valoración de la criticidad de los activos de TI

Rango	Nivel de criticidad	Descripción
1 – 5	1	Muy bajo
6 – 10	2	Bajo
11 – 15	3	Medio
16 – 20	4	Alto
21 – 25	5	Muy alto

Fuente: Desarrollo propio

c. Identificación de las amenazas y vulnerabilidades

En esta actividad caracteriza el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cuán probable es que pase. Es decir, describe las amenazas a los que cada uno de los activos está expuesto.

Para la identificación de las amenazas significativas de cada activo de TI identificado, se tomará en consideración lo siguiente:

- El tipo de activo
- Las dimensiones de seguridad con las que cada activo está relacionado
- La experiencia de la organización
- Los reportes de incidentes de seguridad

Tomando como referencia la tabla de inventario de las amenazas por activo y dimensión de seguridad de la información del Anexo N° 2 y el informe de valor de los activos de la actividad anterior, se debe obtener la relación de amenazas por cada activo de TI. Se utilizará el siguiente formato:

Tabla N° 8. Plantilla para la identificación de amenazas por activo

N°	Activo	Amenaza
1		
2		
3		

Fuente: Desarrollo propio

Las amenazas se materializan por la existencia de debilidades en los mecanismos de seguridad de los activos. Por tanto, en esta actividad

también se deben identificar las vulnerabilidades existentes asociadas a cada uno de los activos de información y de TI.

En esta actividad se realiza el análisis de las deficiencias, debilidades y carencias que tiene la organización en los diferentes procesos de TI relacionados a la protección de los activos que han sido identificados. El resultado de esta actividad permitirá determinar cuáles son las debilidades internas que pueden ser aprovechadas por las amenazas para materializarse y hacer fallar o atacar a los activos de TI.

Para realizar esta tarea se analizaron los siguientes tipos de vulnerabilidades:

- Vulnerabilidades en la seguridad lógica
- Vulnerabilidades en la seguridad de recursos humanos
- Vulnerabilidades en la seguridad física y ambiental
- Vulnerabilidades en la seguridad gestión de operaciones y comunicaciones
- Vulnerabilidades en el mantenimiento, desarrollo y adquisición de sistemas de información

La identificación de las vulnerabilidades se realiza en un trabajo colaborativo con el personal que conoce y participa en los procesos seleccionados dentro del alcance del SGR.

Tabla N° 9. Plantilla para la identificación de las vulnerabilidades por cada Activo-Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Activo 1	Amenaza 1.1	Vulnerabilidad 1.1.1
			Vulnerabilidad 1.1.2
		Amenaza 1.2	Vulnerabilidad 1.2.1
			Vulnerabilidad 1.2.2
2	Activo 2	Amenaza 2.1	Vulnerabilidad 2.1.1
			Vulnerabilidad 2.1.2
		Amenaza 2.2	Vulnerabilidad 2.2.1
			Vulnerabilidad 2.2.2
			Vulnerabilidad 2.2.3

Fuente: Desarrollo propio

d. Estimación del impacto de la materialización de las amenazas

Para esta investigación, se considera impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

Para la estimación del impacto que ocasiona una amenaza al materializarse, se utilizó una escala de cinco niveles, para valorar los siguientes criterios propuestos por la metodología Magerit (Magerit - Libro 1, 2012): (1) Operación o interrupción de los servicios, (2) Intereses económicos y (3) Seguridad, como se muestra en la siguiente tabla.

Tabla N° 10. Escala de valoración propuesta para el impacto que ocasiona una amenaza al materializarse

Nivel de degradación	Operación o interrupción de los servicios	Intereses económicos	Seguridad
5: Catastrófico	Probablemente cause una interrupción excepcionalmente seria de las actividades propias del proceso con un serio impacto en los usuarios. Destrucción de equipamiento/instalaciones	Costos económicos de recuperación excepcionalmente elevados. Constituye un incumplimiento excepcionalmente grave de las obligaciones, cronogramas y planes	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
4: Mayor	Probablemente tenga un serio impacto en las operaciones y servicios	Genera costos de recuperación graves. Causa merma de ingresos.	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
3: Moderado	Causa la interrupción de actividades propias de los procesos ocasionando condiciones operativas adversas como resultado del incremento de la carga de trabajo o como resultado de condiciones que impiden su eficiencia. Ocasionan incidentes serios		Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
2: Menor	Probablemente cause la interrupción de actividades propias de los procesos con interferencia en los servicios, y se requiera utilizar procedimientos de emergencia.	Supondría costos de recuperación menores. Constituye un incumplimiento leve de obligaciones, cronogramas y planes	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
1: Insignificante	Probablemente cause la interrupción de actividades propias de los procesos	Supondría costos de recuperación mínimos. Causa incidencias de pequeño valor económico	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente.

Fuente: Elaboración propia, adecuando la propuesta de Magerit

e. Estimación de la frecuencia de la materialización de las amenazas

Para esta investigación, se considera frecuencia como la posibilidad de que una amenaza se materialice.

Para la estimación de la frecuencia de la materialización de una amenaza se utilizó una escala de cinco niveles, como se muestra en la siguiente tabla:

Tabla N° 11. Escala de valoración propuesta para el impacto que ocasiona una amenaza al materializarse

Nivel / clasificación	Descripción del nivel
5: Casi seguro	Ocurrencia diaria La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.
4: Altamente posible	Ocurrencia semanal La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.
3: Posible	Ocurrencia mensual La fuente de amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda.
2: Raro	Ocurrencia anual La fuente de amenaza carece de motivación. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda.
1: Improbable	Ocurrencia más de una vez al año La fuente de amenaza carece de motivación. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda.

Fuente: Elaboración propia

f. Valoración del riesgo

El objetivo del análisis del riesgo es identificar los escenarios de riesgo y calcular los niveles de exposición riesgos a dichos escenarios de riesgo en cada uno de los activos, en base a las condiciones encontradas en la identificación de las amenazas y vulnerabilidades.

El cálculo del nivel de riesgos de cada una de las amenazas identificadas para cada activo, estará en función de la valoración y clasificación del impacto y la probabilidad de su ocurrencia. Se utilizará la siguiente relación:

NRI = Probabilidad de ocurrencia x Impacto (fórmula N° 1)

El producto de esta relación se ubicará en el siguiente mapa de calor, tomando como referencia los niveles de riesgo definidos anteriormente.

Tabla N° 12. Matriz de calor para la valoración del impacto y probabilidad de las amenazas

Impacto en los procesos	Probabilidad de ocurrencia				
	Raro	Improbable	Posible	Probable	Casi seguro
Catastrófico	Bajo	Medio	Alto	Muy alto	Muy alto
Mayor	Bajo	Bajo	Medio	Alto	Muy alto
Moderado	Muy bajo	Bajo	Medio	Medio	Alto
Mínimo	Muy bajo	Bajo	Bajo	Bajo	Medio
Insignificante	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

Fuente: Elaboración propia

3.1.3. Actividades para la Fase 3: Tratamiento y administración del riesgo de TI

En esta actividad se definirá e implementará los controles o salvaguardas necesarias para tratar cada una de las amenazas en cuya evaluación se haya obtenido niveles de riesgos no tolerantes, es decir, con el calificativo de “Alto” o “Muy Alto”.

Esta fase contempla las siguientes actividades y tareas:

a. Plan de tratamiento de los riesgos no tolerables
b. Implementación de las medidas de seguridad
c. Identificación de la estrategia de implementación de controles

a. Plan de tratamiento de los riesgos no tolerables

Luego de definir los niveles de riesgos (NR) en cada escenario de riesgo evaluado (Activo-Amenaza-Vulnerabilidad) que puedan afectar la integridad, confidencialidad o disponibilidad de la información; se debe definir el criterio de aceptación del riesgo, el cual determina si el riesgo es aceptable o si requiere de algún tratamiento. Esto se determina como el Apetito del Riesgo de TI.

Los NR cuya valoración sea “Muy Alta” o “Alta” son los que se tratarán mediante controles o salvaguardas para reducir la probabilidad que dichos riesgos identificados se materialicen o para reducir su impacto. Para las amenazas con NR “Medio”, “Baja” o “Muy Baja” se aplicará la estrategia de convivir con el riesgo.

A continuación, se presenta los criterios de aceptación o no aceptación para dada uno de los niveles de los riesgos:

Tabla N° 13. Apetito al riesgo de TI según el nivel de exposición al riesgo

Nivel de Riesgo	Política para la toma de Acciones
Muy alto	Riesgo no aceptable
Alto	Riesgo no aceptable
Medio	Riesgo aceptable
Bajo	Riesgo aceptable
Muy bajo	Riesgo aceptable

Fuente: Elaboración propia

Luego, se determina el plan de tratamiento para cada uno de los riesgos encontrados no aceptables.

b. Implementación de las medidas de seguridad

Los controles que se seleccionarán para el tratamiento de los riesgos no aceptables, se obtendrán del Catálogo de la ISO/IEC 27002, el cual contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general.

Para determinar los controles que se van a implementar se desarrollará la Declaración de la Aplicabilidad, donde se mostrarán los controles que se implementarán, adaptados a la realidad organizacional y capacidad instalada de UNTRM.

c. Identificación de la estrategia de implementación de controles

Seleccionado el control, con su correspondiente objetivo de control, para cada NR no aceptable, se debe definir la estrategia de implementación del control, que puede ser:

- Aceptar el riesgo
- Elección de controles para mitigar los riesgos
- Transferencia del riesgo a terceros
- Evitar aumento del riesgo

3.2. Desarrollo del Modelo de Gestión del Riesgo de TI propuesto

3.2.1. Definición del alcance del Sistema de Gestión de Riesgos

Para determinar el alcance del SGR, se realizó un análisis de los procesos académicos y administrativos que gestionan los diferentes servicios que se brindad a los estudiantes en la UNTRM, con la finalidad de identificar aquellos procesos que están directamente relacionados con los servicios que se gestionan en las facultades, que es el propósito de esta investigación. A partir de este análisis, se seleccionó aquellos procesos que se consideran como críticos en base a la cantidad de trámites que se gestionan en un periodo determinado.

Posteriormente, se realizó el mapeado de los procesos seleccionados para identificar el flujo de trabajo y las áreas/usuarios involucradas. Esta información será utilizada como insumo para la identificación de los activos de TI que serán considerados en la evaluación de riesgos de TI con el modelo propuesto.

a. Identificación y selección de procesos críticos

La primera tarea de para determinar el alcance del SGR, fue el análisis de la gestión de trámite documentario que actualmente se desarrolla en la UNTRM para identificar y seleccionar los principales procesos que gestionan los diferentes servicios.

De acuerdo al Texto Único de Procesos Administrativos (TUPA) vigente (2018), los procesos de la UNTRM que requieren trámite académico/administrativo, son los que se muestran en el Anexo N° 1, los cuales se resumen a continuación:

Tabla N° 14. Procesos de la UNTRM, según el TUPA vigente

N°	Unidad orgánica	Nro. de procesos	Observación
1	Oficina General de Admisión	14	
2	Facultades	39	
3	Oficina General de Asuntos Académicos	8	
4	Oficina General de Biblioteca	6	Los procesos son los mismos en la Biblioteca Central como en las bibliotecas especializadas
5	Oficina General de Bienestar Universitario	7	
6	Oficina General de Tecnologías de Información Administrativos	2	
7	Oficina General de Responsabilidad Social Universitaria	7	Los procesos son los mismos en la Oficina Central como en las oficinas de cada Facultad
8	Oficinas de Investigación – Facultades	3	Los procesos que figuran en el TUPA son 3, pero durante la ejecución de la presente tesis, se aprobó un nuevo reglamento con nuevos procesos de acuerdo a la nueva ley universitaria
9	Dirección General de Administración	5	
10	Secretaria general	14	
11	Oficina General de Recursos Humanos	10	
12	Escuela de Postgrado	17	

Fuente: TUPA 2018 - UNTRM

Para la selección de los procesos que se tomaron como casos de análisis se utilizaron los siguientes criterios:

- posibilidad de acceso a la información
- mayor demanda

En el caso de los procesos que tienen mayor demanda, la siguiente tabla muestra los resultados del análisis cuantitativo que se realizó, a partir de la información registrada en los cuadernos de registro de trámite documentario en las diferentes oficinas de la UNTRM, durante el periodo del 22 de agosto al 30 de noviembre del 2018. No se consideraron los trámites requeridos que no figuran como proceso en el TUPA vigente. Adicionalmente se observó que los procesos que son los más requeridos (mayor demanda), son los realizados por los estudiantes como parte de los trámites que realizan durante toda su vida universitaria, desde su admisión a la universidad hasta la obtención del título profesional.

Tabla N° 15. Número de trámites registrados por tipo de proceso

N°	Denominación del proceso	Nro. de trámites registrados	Observación
1	Matricula	---	No se consideró porque no requiere de trámite administrativo. Los llamados matrículas por casos especiales no están formalmente procedimentados como procesos
2	Adicional por asignatura desaprobada	---	Proceso obsoleto, por cuanto está considerado como parte del proceso de matrícula
3	Matricula de ingresantes	---	No se consideró porque no requiere de trámite administrativo
4	Matricula extemporánea	---	Proceso incluido como parte del proceso de matrícula
5	Reactualización de matricula	17	En el periodo de recopilación de la información, sólo se abarcó el proceso de matrícula 2018- II
6	Reserva de matricula	11	
7	Matricula por traslado interno	7	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
8	Matricula de ingresantes por traslado externo - cambio de universidad	3	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
9	Carnet de biblioteca especializada	1	
10	Duplicado de carnet	0	
11	Carnet de biblioteca a terceros	0	
12	Multas por día y por libro	13	
13	Constancias académicas de cualquier tipo	187	
14	Certificado de estudios	321	
15	Expedición y Visación de sílabos	13	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
16	Convalidación y equivalencia de asignatura	22	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
17	Curso dirigido	51	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
18	Examen extraordinario	39	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
19	Traslado interno	16	Incluye a las Escuelas Profesionales de Ingeniería de Sistemas y Mecánica Eléctrica
20	Carta de presentación practicas pre profesionales	112	No se consideró porque solo requiere de ingresar una solicitud y la espera de la respuesta como parte del trámite
21	Grado académico	97	
22	Presentación del proyecto de tesis	---	No se incluyó a las Oficinas de Investigación por no tener la posibilidad de acceso a la información
23	Anulación o cambio del proyecto de tesis	---	No se incluyó a las Oficinas de Investigación, por no tener la posibilidad de acceso a la información
24	Modalidad de obtener título - Con sustentación de tesis	---	No se incluyó a las Oficinas de Investigación, por no tener la posibilidad de acceso a la información
25	Modalidad de obtener título - Experiencia profesional	---	No se incluyó a las Oficinas de Investigación, por no tener la posibilidad de acceso a la información

26	Modalidad de obtener título - Examen de suficiencia profesional	---	No se incluyó a las Oficinas de Investigación, por no tener la posibilidad de acceso a la información
27	Título profesional	87	
28	Concurso de admisión residentado médico	---	Este proceso solo se realiza en la Escuela Profesional de Medicina Humana.
29	Matricula residentado médico y titulación	---	Este proceso solo se realiza en la Escuela Profesional de Medicina Humana.
30	Rectificación de nombres y apellidos	2	
31	Revalidaciones de grados y títulos provenientes del extranjero	2	

Fuente: Desarrollo propio, tomando como referencia cuaderno de registro de trámites de las diferentes oficinas de la UNTRM

Los procesos seleccionados fueron:

1. Emisión de Constancias académicas de cualquier tipo
2. Emisión de Certificado de estudios
3. Convalidación y equivalencia de asignatura
4. Atención a solicitudes de curso dirigido
5. Atención a solicitudes de examen extraordinario
6. Evaluación de solicitudes de Traslado interno
7. Otorgamiento de Grado académico de bachiller o Título profesional

b. Identificación de los procesos de TI de soporte a los procesos académicos/administrativos

Los procesos de TI considerados son los que dan soporte a los procesos académicos/administrativos seleccionados para garantizar su capacidad, seguridad, continuidad y disponibilidad.

Los procesos de TI identificados son los siguientes:

- Procesos para las funciones de Desarrollo de software
- Procesos para la función de Producción y Soporte de TI
- Procesos para la función de Gestión de Centros de Cómputo

Dado que estos procesos de TI no están formalmente establecidos y documentados, para el propósito de la investigación se tomaron como funciones que realiza la Oficina General de Tecnologías de Información y la Oficina General de Asuntos Académicos, para el

caso de los procesos de Desarrollo de software y, Producción y Soporte de TI.

c. Definición de la política general del SGSI

La OGTI, consciente de la importancia que la seguridad de la información en los procesos académicos/administrativos de la UNTRM, suscribe en la presente política general de seguridad de la información.

- La OGTI 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 de servicios que le sean de aplicación, que incrementa de esta manera, la confianza de nuestros usuarios y otras partes interesadas.

- 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.

- La OGTI establece los criterios de evaluación del riesgo de manera que todos aquellos escenarios que impliquen un nivel de riesgo inaceptable sean tratados adecuadamente.

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

- La Jefatura de la OGTI se compromete con la implantación, mantenimiento y mejora del SGSI facilitando los medios y recursos que sean necesarios.

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

- 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.

d. Análisis de brechas de 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 27001, con la finalidad de determinar el Nivel de aplicabilidad de la norma (SOA) en la UNTRM. La evaluación del cumplimiento de los controles se realizó tomando como base los resultados del análisis de potenciales riesgos de los principales activos de la empresa que se muestra en el anexo N° 01. Los controles que no han sido evaluados se deben a que la UNTRM no los aplica.

La tabla siguiente muestra los resultados de ese análisis:

Tabla N° 16. Análisis de brechas de cumplimiento de los controles de la ISO 27001/ISO 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.	NO	
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 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	45%
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	SI	50%
6.1.3	Asignación de responsabilidades sobre la seguridad de la información	Debería definirse claramente todas las responsabilidades de seguridad de la información	SI	40%
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	SI	35%
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 y 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.	SI	40%
6.2.2	Consideraciones de seguridad en contratos con clientes/usuarios	Todos los requisitos de seguridad que se hayan identificado deberían ser dirigidos antes de dar acceso a los clientes/usuarios a los activos o a la información de la seguridad.	SI	60%

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	SI	40%
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	30%
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	NO	
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	NO	
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	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	30%
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	40%
9.1.3	Aseguramiento de oficinas, cuartos e instalaciones	Se debería diseñar y aplicar la seguridad física para las oficinas, despachos y recursos	SI	70%
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	40%
9.1.5	Trabajo en áreas restringidas	Se debería diseñar e implantar la protección física y las directrices para trabajar en las áreas seguras.	NO	
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	70%
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	SI	60%
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	60%
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	50%
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	60%
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	60%
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	70%
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	SI	60%

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	SI	60%
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	SI	40%
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	70%
11.2.2	Administración de privilegios	La asignación y el uso de privilegios deberían estar restringidos y controlados	SI	70%
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	NO	
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	50%
11.3.2	Equipos desatendidos	Los usuarios deberían asegurarse que el equipo desatendido tiene la protección adecuada	NO	
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	NO	
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	80%
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	80%
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	SI	40%

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	70%
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	SI	40%
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	SI	50%
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	NO	
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	NO	
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	NO	
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	SI	80%
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	SI	70%
12.4.2	Protección de los datos en sistemas de prueba	Los datos de prueba deberían seleccionarse atentamente, protegerse y controlarse	NO	
12.4.3	Control de acceso a las librerías de código fuente	Debería restringirse el acceso al código fuente de los programas	SI	70%
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	NO	
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	NO	
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	50%
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	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	SI	40%
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	50%
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	

3.2.2. Identificación y evaluación de riesgos de TI

Para el análisis y evaluación de los riesgos de TI se aplicó la metodología de gestión de riesgos descrita en el ítem 3.1.2.

a. Inventario de activos de TI

El inventario de los activos de TI relacionados con los procesos académicos/administrativos analizados se muestra a continuación:

Tabla N° 17. Inventario de activos de TI de los procesos académicos/administrativos

N°	ACTIVO
1	Servidor de dominio (DNS)
2	Servidores: base de datos y aplicaciones
3	Red de comunicaciones Incluye: Firewall, gabinetes de comunicación, switch central, switchs de borde
4	Sala de servidores
5	Bases de Datos (de las diferentes aplicaciones)
6	Personal de TI. Incluye: Jefatura de Oficina General de Tecnologías de Información (OGTI), Personal especialista en desarrollo y producción que labora en la OGTI
7	Aplicaciones informáticas: Sistema de Matrícula y Control de Notas, Sistema de Calificación Admisión
8	Correo electrónico institucional
9	Equipos de cómputo terminales en las diferentes oficinas y dependencias que participan en los procesos académicos/administrativos evaluados
10	Equipos de cómputo del Área de Desarrollo (Ubicados en OGTI)
11	Código fuente de aplicaciones Incluye: biblioteca de versiones, librerías
12	Backups o respaldos de base de datos y aplicaciones Incluye: código fuente, librerías
13	Herramientas de desarrollo Incluye: base de datos, software de desarrollo
14	Herramientas de ofimática Incluye: Licencias Campus Agreement
15	Registros de control de cambios de las aplicaciones. Incluye: scripts, cambios en estructuras de datos, carga de datos, manuales de usuario, pruebas realizadas
16	Documentos de gestión Incluye: oficios, actas, certificados, solicitudes, reglamentaciones y procedimientos, etc.

Fuente: Desarrollo propio

Utilizando la clasificación propuesta por la ISO 27005:2008, se tiene el siguiente resultado:

Tabla N° 18. Clasificación de los activos de TI identificados

N°	Tipo de activo	Activo
1	Aplicaciones	Aplicaciones informáticas: sistema de matrícula y control de notas, Admisión
2	Aplicaciones	Herramientas de desarrollo
3	Aplicaciones	Herramientas de ofimática
4	Comunicaciones	Red de comunicaciones
5	Datos o documentos	Código fuente de aplicaciones
6	Datos o documentos	Registros de control de cambios de las aplicaciones
7	Equipos informáticos	Equipos de cómputo terminales en las diferentes oficinas y dependencias que participan en los procesos académicos/administrativos evaluados
8	Equipos informáticos	Equipos de cómputo del Área de Desarrollo
9	Información	Bases de Datos
10	Información	Backups de documentos de gestión
11	Instalaciones	Sala de servidores
12	Personal	Personal de área de TI
13	Servicios	Servidor de dominio
14	Servicios	Servidores: de base de datos y aplicaciones
15	Servicios	Correo electrónico institucional
16	Soporte de información	Backups o respaldos de desarrollo y mantenimiento

Fuente: Desarrollo propio

b. Definición de la criticidad de los activos de TI identificados

Una vez inventariados los activos de TI se ha valorado y clasificado su nivel de importancia o criticidad, tomando como base la calificación dada a cada característica o dimensión de seguridad de la información, de acuerdo a las escalas de valoración propuestas, obteniéndose los siguientes resultados:

Tabla N° 19. Valoración del nivel de criticidad de los activos de TI identificados

N°	Activo	Criterios de seguridad			Total	Nivel de criticidad
		C	I	D		
1	Servidor de dominio (DNS)	4	5	5	4	Alto
2	Servidores: base de datos y aplicaciones	5	5	5	5	Muy Alto
3	Red de comunicaciones	4	1	5	3	Medio
4	Sala de servidores	4	1	5	3	Medio
5	Bases de Datos (de las diferentes aplicaciones)	5	5	5	5	Muy Alto
6	Personal de TI	4	1	5	3	Medio
7	Aplicaciones informáticas: sistema de matrícula y control de notas, Admisión	4	4	5	4	Alto
8	Correo electrónico institucional	4	4	5	4	Alto
9	Equipos de cómputo terminales en las diferentes oficinas y dependencias que participan en los procesos académicos/administrativos evaluados	5	5	5	5	Muy Alto
10	Equipos de cómputo del Área de Desarrollo (Ubicados en OGTI)	4	5	5	4	Alto
11	Código fuente de aplicaciones	4	5	5	4	Alto
12	Backups o respaldos de base de datos y aplicaciones	4	5	5	4	Alto
13	Herramientas de desarrollo	4	4	4	4	Alto
14	Herramientas de ofimática	4	4	4	4	Alto
15	Registros de control de cambios de las aplicaciones	3	3	5	3	Medio
16	Documentos de gestión	3	3	5	3	Medio

Fuente: Desarrollo propio

c. Identificación de las amenazas de los Activos de TI

Para cada activo de TI se han identificado las siguientes amenazas:

Tabla N° 20. Listado de amenazas por Activo de TI

N°	Activo	Amenaza
1	Servidor de dominio (DNS)	Paralización parcial o total de los procesos académicos/ administrativos. No se accede a los servicios y recursos de red
2	Servidores: base de datos y aplicaciones	Paralización parcial o total de los sistemas o aplicaciones informáticas. No se accede a los sistemas.
3	Red de comunicaciones	Paralización de servicios de comunicación
4	Sala de servidores	Sabotaje a las instalaciones
		Pérdida de Activos de TI en la sala de servidores y paralización de Operaciones

Continúa Tabla N° 20

N°	Activo	Amenaza
5	Bases de Datos (de las diferentes aplicaciones)	Perdida o modificación de información sensible de los procesos académicos/ administrativos debido a accesos no autorizados
		Falta de espacio de almacenamiento
6	Personal de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos
		Modificación, divulgación y destrucción de la información
7	Aplicaciones informáticas: sistema de matrícula y control de notas, Admisión	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente o en la conectividad a la base de datos.
		Información brindada por los sistemas o aplicaciones informáticas es inexacta debido errores en la integridad de los datos
8	Correo electrónico institucional	Retraso de actividades debido a caídas del servicio de correo electrónico
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico
9	Equipos de cómputo terminales en las diferentes oficinas y dependencias que participan en los procesos académicos/administrativos evaluados	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio Paralización parcial o total de las operaciones en puesto de trabajo
10	Equipos de cómputo del Área de Desarrollo (Ubicados en OGTI)	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las tareas de desarrollo
11	Código fuente de aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción
		Perdida o modificación de código fuente por acciones mal intencionadas de usuarios
12	Backups o respaldos de base de datos y aplicaciones	No continuidad de los procesos por imposibilidad de recuperación de la información y/o aplicaciones ante la caída o pérdida de la base de datos o aplicaciones en producción
13	Herramientas de desarrollo	Paralización de las actividades de desarrollo o falta de atención oportuna de las solicitudes de requerimientos de cambio
14	Herramientas de ofimática	Paralización de continuidad de tareas en procesos académicos/administrativos
15	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente
16	Documentos de gestión	Pérdida de información por no cumplir con el requerimiento de información histórica por parte de ente supervisor

Fuente: Desarrollo propio

d. Identificación de las vulnerabilidades de los Activos de TI

Para cada relación de activo de TI - amenaza se han identificado las siguientes vulnerabilidades, el cual es el resultado del análisis de los datos recopilados en el levantamiento de la información de las brechas de seguridad.

Tabla N° 21. Listado de vulnerabilidades por Activo de TI – Amenaza

N°	Activo	Amenaza	Vulnerabilidad
1	Servidor de dominio (DNS)	Paralización parcial o total de los procesos académicos/ administrativos. No se accede a los servicios y recursos de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio
			Falla en los componentes físicos
			Fallas en el sistema operativo, falta de actualización de parches
			No se cuenta con un plan de mantenimiento de los servidores
			Sistema antivirus deficiente en la actualización de firmas
2	Servidores: base de datos y aplicaciones	Paralización parcial o total de los sistemas o aplicaciones informáticas. No se accede a los sistemas.	Administrador tiene acceso total a la base de datos y puede realizar modificaciones
			Deficiencia en el diseño de base datos (normalización de BD).
			Usuarios acceden a servidor de base de datos por canales no autorizados
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones
			Falla de la red de comunicaciones con otras agencias
			Fallas eléctricas que generen la interrupción de los procesos y servicios
			No se cuenta con servidor de firewall a nivel de hardware

Continúa Tabla N° 21

N°	Activo	Amenaza	Vulnerabilidad
4	Sala de servidores	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores.
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.
		Pérdida de Activos de TI en la sala de servidores y paralización de Operaciones	No se mantiene un control o registro de acceso a las áreas restringidas
			Falta de un registro de acceso a la sala de servidores
			No se tiene una política y procedimiento para el personal que realiza mantenimiento en la institución
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento) y revisión de maletines.
5	Bases de Datos (de las diferentes aplicaciones)	Perdida o modificación de información sensible de los procesos académicos/ administrativos debido a accesos no autorizados	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD
			Existencia de password no adecuados para usuarios locales y de red
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente
			Acceso a la BD desde otras aplicaciones
			Sistema antimalware obsoleto o deficiente
			Realización de copias no autorizadas de la Base de Datos
			Modificación no autorizada de BD
		Falta de espacio de almacenamiento	Falta de monitoreo de incremento de transacciones
			No existe un procedimiento de mantenimiento de a BD
			Sistema antimalware deficiente para monitorear incremento de espacio por virus.

Continúa Tabla N° 21

N°	Activo	Amenaza	Vulnerabilidad
6	Personal de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos	Inadecuada segregación de funciones
			No existe un plan de capacitación adecuado
			Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos
			Falta de control y seguimiento de accesos
			Falta de acuerdos de confidencialidad
			Acciones mal intencionadas de los usuarios de TI
			Falta de procedimiento de mantenimiento de usuarios
7	Aplicaciones informáticas: sistema de matrícula y control de notas, Admisión	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente o en la conectividad a la base de datos.	Errores operativos por parte del usuario (registro de información errada)
			Fallas en las conexiones de red o en equipo de computo
			Fallas eléctricas (a partir de 2 horas).
		Información brindada por los sistemas o aplicaciones informáticas es inexacta debido a errores en la integridad de los datos	Falta de soporte y mantenimiento de los sistemas y aplicaciones informáticas en producción
			No llevar un control de la historia del código fuente
8	Correo electrónico institucional	Retraso de actividades debido a caídas del servicio de correo electrónico	Problemas de conexión o servidor del servicio que brinda el proveedor
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico	No generación de copias de respaldo (cuentas creadas, permisos y configuración)
			Capacidad de almacenamiento limitada
			Borrado de cuentas por accesos no autorizados por personal que administra el correo
			Bajo nivel de complejidad de las contraseñas de correo vía acceso-página web

Continúa Tabla N° 21

N°	Activo	Amenaza	Vulnerabilidad
9	Equipos de cómputo terminales en las diferentes oficinas y dependencias que participan en los procesos académicos/administrativos evaluados	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio Paralización parcial o total de las operaciones en puesto de trabajo	Personal no capacitado para el mantenimiento de equipos de computo
			No se ha determinado la vida útil de los equipos
			Incumplimiento del plan de mantenimiento de equipos
			Fallas en sistema de alimentación eléctrica
			Errores de configuración de los equipos
			Mal uso del equipo por parte del usuario
			Condiciones de ambientes inadecuadas
			No se tienen identificados los equipos críticos en caso de incidentes
			El personal guarda información sensible en sus equipos y genera respaldos
10	Equipos de cómputo del Área de Desarrollo (Ubicados en OGTI)	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las tareas de desarrollo	Incumplimiento del plan de mantenimiento de equipos
			Fallas en sistema de alimentación eléctrica
			Errores de configuración de los equipos
			Mal uso del equipo por parte del usuario
			El personal guarda información sensible en sus equipos y genera respaldos
11	Código fuente de aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción	No se realizan copias de seguridad
			Falta de control para accesos no autorizado a la PC de integración de Software
		Perdida o modificación de código fuente por acciones mal intencionadas de usuarios	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema
			No complejidad de contraseñas en el respaldo de código fuente
			Falta de control para la manipulación del código fuente que puede alterar el desarrollo normal de un proceso

Continúa Tabla N° 21

Nº	Activo	Amenaza	Vulnerabilidad
12	Backups o respaldos de base de datos y aplicaciones	No continuidad de los procesos por imposibilidad de recuperación de la información y/o aplicaciones ante la caída o pérdida de la base de datos o aplicaciones en producción	Fallas en los dispositivos de almacenamiento (disco duro del servidor)
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo
			Errores en el proceso de generación de backups
			No se lleva un registro de la generación de backups
13	Herramientas de desarrollo	Paralización de las actividades de desarrollo o falta de atención oportuna de las solicitudes de requerimientos de cambio	No se cuenta con copias en sitios alternos seguros
14	Herramientas de ofimática	Paralización de continuidad de tareas en procesos académicos/administrativos	No se cuenta con copias en sitios alternos seguros
			Personal mal capacitado
15	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente	No se cuenta con un mecanismo de control de cambios
16	Documentos de gestión	Pérdida de información por no cumplir con el requerimiento de información histórica por parte de ente supervisor	No se ha establecido la periodicidad para la generación de backups de la documentación histórica
			No se ha identificado un lugar adecuado para el resguardo de los respaldos de la documentación de gestión.

Fuente: Desarrollo propio

e. Valoración del impacto y probabilidad de ocurrencia de las amenazas; y la estimación del nivel de riesgo

Para la valoración del impacto y probabilidad de ocurrencia, y en consecuencia, para obtener el nivel de riesgo al que está expuesto cada activo de TI de los procesos académicos/administrativos, se realizó un levantamiento de información para evaluar los controles existentes actualmente y la efectividad de su implementación. Esta información se registra en el Anexo N° 04 y fue obtenida a través de entrevistas (en la medida que fue permitido).

Los resultados de las valoraciones para los impactos y probabilidad de ocurrencia de cada amenaza para cada activo de TI; así como la obtención del nivel de riesgo intrínseco (usando los formatos y niveles de valoración de las tablas N° 10, 11, 12, 13), se muestran en la siguiente tabla:

Tabla N° 22 Valoración del Nivel de Riesgo (NR)

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
1	Servidor de dominio (DNS)	Paralización parcial o total de los procesos académicos/ administrativos. No se accede a los servicios y recursos de red	Falta de personal especializado, para dar el mantenimiento necesario al servidor de dominio	3	Moderado	2	Improbable	R1	2	Bajo
			Falla en los componentes físicos	4	Mayor	3	Posible	R2	3	Medio
			Fallas en el sistema operativo, falta de actualización de parches	5	Catastrófico	4	Probable	R3	5	Muy alto
			No se cuenta con un plan de mantenimiento de los servidores	3	Moderado	2	Improbable	R4	2	Bajo
			Sistema antivirus deficiente en la actualización de firmas	2	Menor	2	Improbable	R5	2	Bajo
2	Servidores: base de datos y aplicaciones	Paralización parcial o total de los sistemas o aplicaciones informáticas. No se accede a los sistemas.	Administrador tiene acceso total a la base de datos y puede realizar modificaciones	4	Mayor	4	Probable	R6	4	Alto
			Deficiencia en el diseño de base datos (normalización de BD).	2	Menor	3	Posible	R7	2	Bajo
			Usuarios acceden a servidor de base de datos por canales no autorizados	5	Catastrófico	4	Probable	R8	5	Muy alto

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
3	Red de comunicaciones	Paralización de servicios de comunicación	Falla de la línea principal de comunicaciones	5	Catastrófico	3	Posible	R9	4	Alto
			Falla de la red de comunicaciones	4	Mayor	4	Probable	R10	4	Alto
			Fallas eléctricas que generen la interrupción de los procesos y servicios	4	Mayor	3	Posible	R11	3	Medio
			Debilidades en el servidor de firewall	3	Moderado	2	Improbable	R12	2	Bajo
4	Sala de servidores	Sabotaje a las instalaciones	Acceso de Personal no autorizado (interno/externo) a la sala de servidores.	5	Catastrófico	2	Improbable	R13	3	Medio
			Falta de un sistema de vigilancia y de seguridad del equipamiento en la sala de servidores.	2	Menor	3	Posible	R14	2	Bajo
		Pérdida de Activos de TI en la sala de servidores y paralización de Operaciones	No se mantiene un control o registro de acceso a las áreas restringidas	2	Menor	2	Improbable	R15	2	Bajo
			Falta de un registro de acceso a la sala de servidores	3	Moderado	2	Improbable	R16	2	Bajo

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
4	Sala de servidores	Pérdida de Activos de TI en la sala de servidores y paralización de Operaciones	No se tiene una política y procedimiento para el personal que realiza mantenimiento en la UNTRM	2	Menor	3	Posible	R17	2	Bajo
			Personal de vigilancia no lleva un control de los equipos de entrada / salida (personal de mantenimiento) y revisión de maletines.	4	Mayor	3	Posible	R18	3	Medio
5	Bases de Datos (de las diferentes aplicaciones)	Perdida o modificación de información sensible de los procesos académicos/ administrativos debido a accesos no autorizados	Falta de un adecuado procedimiento para la asignación de perfiles para accesos a la BD	4	Mayor	3	Posible	R19	3	Medio
			Existencia de password no adecuados para usuarios locales y de red	3	Moderado	2	Improbable	R20	2	Bajo
			Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente	3	Moderado	2	Improbable	R21	2	Bajo
			Acceso a la BD desde otras aplicaciones	4	Mayor	3	Posible	R22	3	Medio
			Sistema antimalware obsoleto o deficiente	3	Moderado	3	Posible	R23	3	Medio
			Realización de copias no autorizadas de la Base de Datos	4	Mayor	3	Posible	R24	3	Medio
			Modificación no autorizada de BD	5	Catastrófico	4	Probable	R25	5	Muy alto

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
5	Bases de Datos (de las diferentes aplicaciones)	Falta de espacio de almacenamiento	Falta de monitoreo de incremento de transacciones	3	Moderado	3	Posible	R26	3	Medio
			No existe un procedimiento de mantenimiento de a BD	3	Moderado	2	Improbable	R27	2	Bajo
			Sistema antimalware deficiente para monitorear incremento de espacio por virus.	3	Moderado	1	Raro	R28	1	Muy bajo
6	Backups o respaldos de base de datos y aplicaciones	No continuidad de los procesos por imposibilidad de recuperación de la información y/o aplicaciones ante la caída o pérdida de la base de datos o aplicaciones en producción	Fallas en los dispositivos de almacenamiento (disco duro del servidor)	4	Mayor	3	Posible	R29	3	Medio
			Falta de un lugar adecuado para su resguardo y protección de las copias de respaldo	2	Menor	2	Improbable	R30	2	Bajo
			Errores en el proceso de generación de backups	5	Catastrófico	4	Probable	R31	5	Muy alto
			No se lleva un registro de la generación de backups	3	Moderado	3	Posible	R32	3	Medio
7	Personal de TI	Retraso en las actividades, paralización de procesos, pérdida de información debido a fuga de talentos	Inadecuada segregación de funciones	3	Moderado	2	Improbable	R33	2	Bajo
			No existe un plan de capacitación adecuado	2	Menor	3	Posible	R34	2	Bajo
			Indisponibilidad del personal (enfermedad, accidente y/o otros actos que impiden al personal realizar sus actividades)	2	Menor	3	Posible	R35	2	Bajo

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
7	Personal de TI	Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos	4	Mayor	3	Posible	R36	3	Medio
			Falta de control y seguimiento de accesos	5	Catastrófico	3	Posible	R37	4	Alto
			Falta de acuerdos de confidencialidad	4	Mayor	3	Posible	R38	3	Medio
			Acciones mal intencionadas de los usuarios de TI	3	Moderado	3	Posible	R39	3	Medio
			Falta de procedimiento de mantenimiento de cuentas de usuarios	3	Moderado	2	Improbable	R40	2	Bajo
8	Aplicaciones informáticas: sistema de matrícula y control de notas, Admisión	Paralización de procesos debido a problemas en el procesamiento de transacciones a nivel de usuario/cliente o en la conectividad a la base de datos.	Errores operativos por parte del usuario (registro de información errada)	3	Moderado	3	Posible	R41	3	Medio
			Fallas en las conexiones de red o en equipo de computo	3	Moderado	3	Posible	R42	3	Medio
			Fallas eléctricas (a partir de 2 horas).	4	Mayor	3	Posible	R43	3	Medio
		Información brindada por los sistemas o aplicaciones informáticas es inexacta debido a errores en la integridad de los datos	Falta de soporte y mantenimiento de los sistemas y aplicaciones informáticas en producción	3	Moderado	2	Improbable	R44	2	Bajo
			No llevar un control de la historia del código fuente	4	Mayor	3	Posible	R45	3	Medio

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
9	Correo electrónico institucional	Retraso de actividades debido a caídas del servicio de correo electrónico	Problemas de conexión o servidor del servicio que brinda el proveedor	3	Moderado	3	Posible	R46	3	Medio
		Pérdida de datos por gestión inadecuada del servidor de correo electrónico	No generación de copias de respaldo (cuentas creadas, permisos y configuración)	3	Moderado	3	Posible	R47	3	Medio
			Capacidad de almacenamiento limitada	2	Menor	2	Improbable	R48	2	Bajo
			Borrado de cuentas por accesos no autorizados por personal que administra el correo	3	Moderado	2	Improbable	R49	2	Bajo
			Bajo nivel de complejidad de las contraseñas de correo vía acceso-página web	3	Moderado	3	Posible	R50	3	Medio
10	Equipos de cómputo terminales de oficinas	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio Paralización parcial o total de las operaciones en puesto de trabajo	Personal no capacitado para el mantenimiento de equipos de computo	4	Mayor	2	Improbable	R51	2	Bajo
			No se ha determinado la vida útil de los equipos	2	Menor	2	Improbable	R52	2	Bajo
			Incumplimiento del plan de mantenimiento de equipos	2	Menor	3	Posible	R53	2	Bajo
			Fallas en sistema de alimentación eléctrica	3	Moderado	3	Posible	R54	3	Medio

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
10	Equipos de cómputo terminales de oficinas	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio Paralización parcial o total de las operaciones en puesto de trabajo	Errores de configuración de los equipos	2	Menor	3	Posible	R55	2	Bajo
			Mal uso del equipo por parte del usuario	3	Moderado	4	Probable	R56	3	Medio
			Condiciones de ambientes inadecuadas	2	Menor	3	Posible	R57	2	Bajo
			No se tienen identificados los equipos críticos en caso de evacuación	3	Moderado	2	Improbable	R58	2	Bajo
			El personal guarda información sensible en sus equipos y no las guarda en el servidor	4	Mayor	4	Probable	R59	4	Alto
11	Código fuente de aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción	No se realizan copias de seguridad	4	Mayor	2	Improbable	R60	2	Bajo
			Falta de control para accesos no autorizado a la PC de integración de Software	4	Mayor	2	Improbable	R61	2	Bajo
		Perdida o modificación de código fuente por acciones mal intencionadas de usuarios	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).	4	Mayor	3	Posible	R62	3	Medio
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema	4	Mayor	3	Posible	R63	3	Medio
			No complejidad de contraseñas en el respaldo de código fuente	3	Moderado	3	Posible	R64	3	Medio
			Falta de control para la manipulación del código fuente que puede alterar el desarrollo normal de un proceso	5	Catastrófico	4	Probable	R65	5	Muy alto

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
11	Backups o respaldos de desarrollo y mantenimiento	Reversión de adecuaciones a los sistemas, no es posible	No se trasladan copias de respaldo en sitios alternos	5	Catastrófico	3	Posible	R74	4	Alto
12	Herramientas de desarrollo	Paralización de las actividades de desarrollo o falta de atención oportuna de las solicitudes de requerimientos de cambio	No se cuenta con copias en sitios alternos seguros	3	Moderado	3	Posible	R75	3	Medio
13	Registros de control de cambios de las aplicaciones	No poder determinar el origen de los cambios en código Fuente	No se cuenta con un mecanismo de control de cambios	3	Moderado	3	Posible	R76	3	Medio
14	Documentos de gestión	Pérdida de información por no cumplir con el requerimiento de información histórica por parte de ente supervisor	No se ha establecido la periodicidad para la generación de backups de la documentación histórica	3	Moderado	2	Improbable	R77	2	Bajo
			No se ha identificado un lugar adecuado para el resguardo de los backups	2	Menor	2	Improbable	R78	2	Bajo

Fuente: Desarrollo propio

3.2.3. Tratamiento y administración del riesgo de TI

Luego de haber evaluado los diferentes escenarios de riesgo y determinado los niveles de exposición al riesgo efectivo, se procedió a definir los las medidas de seguridad necesarias para el tratamiento de los diversos riesgos no tolerables (controles y salvaguardas), identificando la estrategia de su implementación.

Los resultados de esta actividad se muestran en el cuadro siguiente:

Tabla N° 23 Propuesta de medidas de seguridad para cada escenario de riesgo

Nivel de Riesgo Intrínseco (NRI)			Medidas de seguridad (controles y salvaguardas)		Estrategia de implementación
ID riesgo	Nivel	Categoría	ID Control	Descripción	
R1	2	Bajo	C1	Plan de mantenimiento preventivo y procedimientos establecidos y documentados para mantenimiento correctivo de servidores	Evitar aumento del riesgo
R2	3	Medio	C2	Contratos de servicio de mantenimiento	Transferencia del riesgo a terceros
			C3	Sala de servidores con controles ambientales	Evitar aumento del riesgo
R3	5	Muy alto	C4	Personal capacitado en administración de sistema operativos	Mitigar el riesgo
R4	2	Bajo	C5	Plan de mantenimiento preventivo y procedimientos establecidos y documentados para mantenimiento correctivo de servidores	Evitar aumento del riesgo
R5	2	Bajo	C6	Licenciamiento de un sistema antimalware administrable a través de un servicio para toda la red, con actualizaciones en línea	Evitar aumento del riesgo
			C7	Copias de seguridad de la BD	Evitar aumento del riesgo
			C8	Implementar un servidor de backup de respaldo, configurado y listo para puesta en producción	Evitar aumento del riesgo
			C9	Implementar un centro alterno de procesamiento básico	Evitar aumento del riesgo
R6	4	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera bimensual las pistas de auditoría al administrador de la BD, así como también las operaciones que realiza en la arquitectura de la BD	Elección de controles

R7	2	Bajo	C11	Implementar procedimientos de gestión de cambios y versiones	Evitar aumento del riesgo
			C12	Implementar procedimientos documentados para las pruebas de cambios antes de puesta en producción	Evitar aumento del riesgo
R8	5	Muy alto	C13	Desactivar herramientas adicionales que permiten acceder a la base de datos	Mitigar el riesgo
			C14	Implementar protocolos de fijación de contraseña de acceso a la base de datos con un nivel de complejidad distinta a las contraseñas que manejan los usuarios locales	Mitigar el riesgo
			C15	Implementar procedimientos de gestión de perfiles de usuario y Gestión de latas, bajas y modificaciones de cuentas de usuarios	Mitigar el riesgo
R9	4	Alto	C16	Implementar una línea de contingencia para comunicaciones	Transferencia del riesgo a terceros
			C17	Reporte de averías e incidentes en la red mediante un sistema de escaneo y monitoreo de la red	Evitar aumento del riesgo
R10	4	Alto	C18	Implementar un procedimiento documentado para la gestión de incidentes en la red	Evitar aumento del riesgo
R11	4	Medio	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos Core ante una posible interrupción del corte de energía eléctrica	Elección de controles
			C20	Plan de pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento	Evitar aumento del riesgo
			C21	Plan de mantenimiento al sistema eléctrico	Evitar aumento del riesgo
R12	2	Bajo	C22	Se cuenta con firewall a nivel de software	Elección de controles
R13	3	Medio	C23	Implementar políticas y procedimientos de control de acceso físico a ambientes restringidos	Evitar aumento del riesgo
			C24	Registrar los accesos a sala de servidores y el área de TI, mediante una bitácora de acceso	Evitar aumento del riesgo
			C25	Los accesos por parte de personal a realizar mantenimiento, se realiza acompañado de personal del área	Elección de controles
			C26	El acceso al ambiente de la sala de servidores, tiene acceso restringido mediante una puerta con llave. La llave la maneja únicamente el responsable de la	Elección de controles
			C27	Sala de servidores se encuentra en un ambiente aislado al ambiente de producción y de desarrollo	Elección de controles

			C28	Implementar un sistema de cámara de vigilancia que monitorea el ingreso de personas internas como externas a los ambientes de la	Evitar aumento del riesgo
R14	2	Bajo	C29	Instalar extintores y sensores de humo	Evitar aumento del riesgo
			C30	Instalar luces de emergencia	Evitar aumento del riesgo
			C32	Sala de servidores se encuentra en un ambiente aislado al ambiente de producción y de desarrollo	Elección de controles
			C33	Registrar los accesos a sala de servidores, mediante una bitácora	Evitar aumento del riesgo
			C34	Implementar un sistema de cámara de vigilancia que monitorea el ingreso de personas internas como externas a los ambientes de la Sala de Servidores	Evitar aumento del riesgo
			C35	Segregar funciones para la designación del personal para el manejo de llaves	Evitar aumento del riesgo
			C36	Implementar Sala de servidor alterno	Evitar aumento del riesgo
			C37	Plan de mantenimiento de los equipos de seguridad	Evitar aumento del riesgo
			C38	Capacitar al personal en uso de extintores	Evitar aumento del riesgo
R15	2	Bajo	C39	Implementar un registro de acceso a las áreas restringidas	Evitar aumento del riesgo
R16	2	Bajo	C40	Implementar un registro de acceso a la Sala de Servidores	Evitar aumento del riesgo
R17	2	Bajo	C41	Implementar políticas y procedimientos para el mantenimiento de equipos	Evitar aumento del riesgo
R18	3	Medio	C42	Reforzar el control de registro de de entrada / salida de equipos y revisión de maletines	Evitar aumento del riesgo
R19	4	Medio	C43	Implementar un reglamento de administración de usuarios a los sistemas, en el que incluye las opciones para la asignación de perfiles por usuarios	Evitar aumento del riesgo
R20	2	Bajo	C44	Implementar procedimiento para la generación de contraseñas con un nivel de seguridad y complejidad por primera vez, teniendo en cuenta caracteres numéricos y alfanuméricos.	Evitar aumento del riesgo
R21	2	Bajo	C45	Implementar un reglamento de administración de usuarios a los sistemas, en el que incluye la periodicidad de las revisiones de los perfiles	Evitar aumento del riesgo
R22	4	Medio	C46	Deshabilitar aplicaciones de acceso a base de datos en terminales informáticos de usuarios	Evitar aumento del riesgo

			C47	Acceso a la BD protegida por un password	Elección de controles
R23	3	Medio	C48	Licenciamiento de un sistema antimalware administrable a través de un servicio para toda la red, con actualizaciones en línea	Evitar aumento del riesgo
R24	3	Medio	C49	BD protegidos con clave únicamente	Evitar aumento del riesgo
			C50	Implementar procesos de uso de carpetas compartidas para la trasferencia de archivos	Evitar aumento del riesgo
R25	5	Muy alto	C51	Implementar un procedimiento de gestión de cambios en el que se incluya las modificaciones a la base de datos	Evitar aumento del riesgo
R26	3	Medio	C52	Monitoreo mediante software de la capacidad del disco de los servidores	Evitar aumento del riesgo
R27	2	Bajo	C53	Se realiza un mantenimiento de la BD, pero no está documentado	Evitar aumento del riesgo
R28	1	Muy bajo	C54	Licenciamiento de un sistema antimalware administrable a través de un servicio para toda la red, con actualizaciones en línea	Elección de controles
			C55	Administración de puertos para el control de acceso al servidor	Evitar aumento del riesgo
R29	4	Medio	C56	Se cuenta con políticas y procedimientos de generación de backups	Elección de controles
			C57	Implementar y probar procedimientos de restore	Evitar aumento del riesgo
			C58	Implementar un control trimestral del estado de almacenamiento de los medios de respaldo	Evitar aumento del riesgo
			C59	Se realiza un monitoreo del procedimiento de respaldo de los backups	Elección de controles
			C60	Implementar un centro alterno de procesamiento de datos básico	Evitar aumento del riesgo
R30	2	Bajo	C61	Reforzar el procedimiento de verificación de estado de almacenamiento y resguardo de los medios de respaldo.	Evitar aumento del riesgo
R31	5	Muy alto	C62	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos	Elección de controles
			C63	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación	Elección de controles

			C64	Reforzar el procedimiento de verificación de estado de almacenamiento y resguardo de los medios de respaldo.	Evitar aumento del riesgo
R32	3	Medio	C65	Implementar un procedimiento operativo para la generación de backups de la base de datos y aplicaciones.	Evitar aumento del riesgo
R33	2	Bajo	C66	Elaborar el manual de organización y funciones en el que se tiene establecido las responsabilidades que debe cumplir el personal en la operativa diaria	Evitar aumento del riesgo
R34	2	Bajo	C67	Desarrollar un plan de capacitación presentado por el jefe de la OGTI	Evitar aumento del riesgo
R35	2	Bajo	C68		Aceptar el riesgo
R36	4	Medio	C69	Continuar con la asignación perfiles de usuario de acuerdo a la función y puesto trabajo del usuario. Sin embargo, debe documentarse un procedimiento de administración de perfiles de usuario	Elección de controles
			C70	Generar pistas de auditoria de las transacciones realizadas por los usuarios	Evitar aumento del riesgo
R37	4	Alto	C71	Procedimentar la revisión periódica de las pistas de auditoria de las transacciones realizadas por los usuarios	Evitar aumento del riesgo
R38	4	Medio	C72	Implementar el procedimiento de firma de acuerdos de confidencialidad con todos los usuarios de TI y revisar periódicamente su cumplimiento	Evitar aumento del riesgo
R39	3	Medio	C73	Generar reportes de intentos de accesos no autorizados	Evitar aumento del riesgo
			C74	Implementar políticas de seguridad y reglamentos internos que establecen sanciones por incumplimiento de políticas de seguridad de la información	Evitar aumento del riesgo
R40	2	Bajo	C75	Implementar un procedimiento para administrar altas, bajas, modificaciones de cuentas de usuario congruente con los perfiles de usuario	Evitar aumento del riesgo
R41	3	Medio	C76	Generar pistas de auditoria que deben ser revisadas periódicamente con posibilidades de recuperación	Evitar aumento del riesgo
			C77	Desarrollar planes de entrenamiento y capacitación de los usuarios de TI y realizar evaluaciones periódicas mediante casuísticas	Evitar aumento del riesgo
R42	3	Medio	C78	Identificar y clasificar los equipos críticos y monitorear su operación, registrando los incidentes técnicos y de seguridad que ocurran sobre ellos	Evitar aumento del riesgo
			C79	Contar con una cartera de proveedores de mantenimiento correctivo para los equipos críticos	Evitar aumento del riesgo

			C80	Capacitar al personal técnico de la OGTI para respuestas rápidas en escenarios de Fallas en las conexiones de red o en equipo de computo	Evitar aumento del riesgo
R43	3	Medio	C81	Se cuenta con grupo electrógeno operativo como contingencia; así como con un sistema de alimentación ininterrumpida (UPS) para abastecer de energía a los equipos de Core	Elección de controles
R44	2	Bajo	C82	Se da soporte de mantenimiento basado en requerimientos de los usuarios y mejoras de los procesos existentes de manera continua	Elección de controles
R45	3	Medio	C83	Implementar procedimientos de control de cambios sobre los sistemas y aplicaciones informáticas en producción; así como llevar un control de versiones con su correspondiente documentación de respaldo	Evitar aumento del riesgo
R46	3	Medio	C84	Se utiliza una plataforma abierta para la generación y administración de correo institucional (Gmail.com)	Elección de controles
R47	3	Medio	C85	La plataforma utilizada para la generación y administración de correo institucional genera copias de respaldo de los correos	Elección de controles
R48	2	Bajo	C86	La plataforma utilizada para la generación y administración de correo institucional permite almacenamiento ilimitado	Elección de controles
R49	2	Bajo	C87	La administración de la plataforma utilizada para la generación de correo institucional solo tiene el perfil de creación de cuentas. Luego del cambio de la clave el administrador no puede acceder a las cuentas	Elección de controles
			C88	Se debe generar un procedimiento para el cambio automático de las cuentas de usuario generadas por primera vez, con claves robustas	Evitar aumento del riesgo
R50	3	Medio	C89	Implementar un procedimiento y reglamento operativo sobre el uso de correo institucional, donde se establecen indicaciones para la creación de contraseñas robustas y seguras	Evitar aumento del riesgo
R51	2	Bajo	C90	Gestionar el contrato permanente de personal técnico para el mantenimiento de equipos de computo	Evitar aumento del riesgo
			C91	Contar con un catálogo de proveedores del servicio de mantenimiento	Evitar aumento del riesgo
			C92	Implementar cursos permanentes de capacitación para practicantes en materia de mantenimiento de computadoras, como una estrategia de motivación	Evitar aumento del riesgo
R52	2	Bajo	C93	Elaborar y mantener un inventario de activos de TI actualizado, revisado periódicamente para identificar la operatividad de los equipos y su tiempo de uso	Evitar aumento del riesgo

R53	2	Bajo	C94	Elaborar un Plan de mantenimiento preventivo de cumplimiento obligatorio de manera anual como parte de un Plan de Continuidad	Evitar aumento del riesgo
R54	3	Medio	C95	Coordinar con la Oficina General de Obras para incorporar en un Plan de mantenimiento preventivo de equipos de TI, el sistema eléctrico, sobre todo en las áreas críticas	Evitar aumento del riesgo
			C96	Se cuenta con una red eléctrica estabilizada	Elección de controles
			C97	Las PCs de misión crítica están conectadas a UPS	Elección de controles
			C98	Realizar pruebas periódicas del sistema de respaldo eléctrico (UPS, Grupo electrógeno y motor). Incorporarlo dentro de un Plan de Mantenimiento preventivo	Evitar aumento del riesgo
			C99	Incorporar en un Plan de Mantenimiento preventivo la revisión de las conexiones eléctricas y acometidas	Evitar aumento del riesgo
R55	2	Bajo	C100	Definir las configuraciones básicas que deben tener los diferentes equipos terminales informáticos en toda la Universidad para evitar backdoors	Evitar aumento del riesgo
R56	3	Medio	C101	Desarrollar mensajerías en línea para concientizar a los usuarios de TI sobre el buen uso de los equipos terminales informáticos (encendido, apagado, comunicación de incidentes, etc.)	Evitar aumento del riesgo
R57	2	Bajo	C102	En el inventario de activos debe asignarse las responsabilidades de uso y mantenimiento. Cada dependencia debe asegurar condiciones ambientales y ergonómicas adecuadas para cada terminal informático.	Aceptar el riesgo
R58	2	Bajo	C103	En un inventario de activos de TI, la OGTI debe identificar los activos críticos, con sus correspondientes controles y salvaguardas específicas para asegurar la continuidad de su operación	Evitar aumento del riesgo
			C104	Los equipos considerados como críticos en el inventario de activos de TI deben generar respaldos de la información que procesan, almacenan o de su configuración	Evitar aumento del riesgo
R59	4	Alto	C105	Realizar actividades de concientización de usuarios de TI para la generación de respaldos periódicos en dispositivos secundarios externos de la información y archivos más críticos	Evitar aumento del riesgo
R60	2	Bajo	C106	Los procesos de desarrollo de software deben ser controlados mediante la asignación de código fuente y base de datos, de acuerdo al requerimiento que se está atendiendo	Evitar aumento del riesgo

			C107	Implementar un procedimiento y un reglamento operativo para la generación de respaldos y backups de la información almacenada en los terminales de desarrollo, controlando las versiones.	Evitar aumento del riesgo
R61	2	Bajo	C108	Las pruebas de los cambios en los módulos y/o aplicaciones deben ser controladas en ambientes apropiadas para dicha actividad.	Evitar aumento del riesgo
			C109	La pc de integración de desarrollo deben estar separadas de la red de producción	Evitar aumento del riesgo
			C110	Generar de seguridad del código fuentes después de cada cambio realizado	Evitar aumento del riesgo
R62	4	Medio	C111	Los procesos de desarrollo de software deben ser controlados mediante la asignación de código fuente y base de datos, de acuerdo al requerimiento que se está atendiendo	Evitar aumento del riesgo
R63	4	Medio	C112	Documentar de control de cambios, donde se detalle todo lo que se modifica a nivel de código fuente, base de datos y alta de datos en la base de datos	Evitar aumento del riesgo
			C113	Generar y documentar pruebas de integración y pruebas unitarias para asegurar la calidad del software antes de puesta en producción	Evitar aumento del riesgo
			C114	Debe incorporarse como parte del testeo del software antes de puesta en producción la intervención de usuarios finales, como procedimientos de certificación de módulos	Evitar aumento del riesgo
R64	3	Medio	C115	Las copias de seguridad de los códigos fuentes de las aplicaciones en producción deben tener una clave de acceso robusta	Evitar aumento del riesgo
R65	5	Muy alto	C116	Implementar la política de que los desarrollo y cambios en las aplicaciones deben realizarlo los analistas desarrolladores y las pruebas antes de puesta en producción, debe realizarlo un personal de testeo diferente.	Evitar aumento del riesgo
			C117	Documentar de control de cambios, donde se detalle todo lo que se modifica a nivel de código fuente, base de datos y alta de datos en la base de datos	Evitar aumento del riesgo
			C118	Realizar revisiones del código generado para verificar la incorporación de código malicioso	Evitar aumento del riesgo
R74	4	Alto	C127	Definir dentro de un reglamento operativo para la generación de respaldos y backups los procedimientos para el etiquetado, traslado, almacenamiento y resguardo de los dispositivos de respaldo en ambientes externos alternos	Evitar aumento del riesgo
R75	3	Medio	C128	Definir dentro de un reglamento operativo para la generación de respaldos y backups los procedimientos para el etiquetado, traslado, almacenamiento y	Evitar aumento del riesgo

				resguardo de los dispositivos de respaldo en ambientes externos alternos	
R76	3	Medio	C129	En la implementación del procedimiento para la gestión de cambios en el software debe generarse registros de los cambios ocurridos. En el software debe registrarse los cambios en los scripts, base de datos y carga de datos; en el los cambios de harware debe actualizarse el inventario de TI y los registros de configuraciones	Evitar aumento del riesgo
R77	2	Bajo	C130	Definir dentro de un reglamento operativo para la generación de respaldos y backups la periodicidad y el tipo de respaldos y backups que deben generarse	Evitar aumento del riesgo
R78	2	Bajo	C131	Definir dentro de un reglamento operativo para la generación de respaldos y backups el lugar de almacenamiento y los mecanismos de resguardo. También deben definirse el ciclo de vida útil de las copias, estableciendo el mecanismo de su destrucción.	Evitar aumento del riesgo

Fuente: Desarrollo propio

CAPÍTULO IV. RESULTADOS

4.1. Análisis de brechas POST

El siguiente cuadro muestra el análisis de brechas realizado después de la implementación de controles de análisis de riesgos.

Tabla N° 24. Análisis de brechas POST

Ítem	Requisitos de la ISO 27001	Cumple	Nivel de cumplimiento	Total
Generalidades				
1	Definición y difusión de una política	**SI**	50%	60%
2	Metodología de gestión de riesgos	**SI**	80%	
3	Mantenimiento de registros	**SI**	50%	
4	Estructura organizacional definida y difundida	**SI**	100%	
5	Asegurar el cumplimiento de la política	**NO**	0%	
6	Monitoreo de la implementación de controles	**SI**	50%	
7	Método para la concientización y entrenamiento del personal	**SI**	50%	
8	Método para la evaluación de incidentes de seguridad / acciones	**NO**	0%	
Seguridad lógica				
9	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios	**SI**	50%	42%
10	Revisiones periódicas sobre los derechos concedidos a los usuarios	**SI**	50%	
11	Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas	**SI**	100%	
12	Controles especiales sobre utilidades del sistema y herramientas de auditoría	**NO**	0%	
13	Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas	**NO**	0%	
14	Controles especiales sobre usuarios remotos y computación móvil	**SI**	50%	
Seguridad de personal				
15	Definición de roles y responsabilidades establecidos sobre la seguridad de información	**SI**	100%	66%
16	Verificación de antecedentes, de conformidad con la legislación laboral vigente	**SI**	100%	
17	Concientización y entrenamiento	**SI**	100%	
18	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente	**NO**	0%	
19	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como	**NO**	0%	

	la revocación de los derechos de acceso y la devolución de activos			
Seguridad física y ambiental				
20	Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa	**SI**	80%	80%
21	Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales	**SI**	80%	
Inventario de activos y clasificación de la información				
22	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos	**SI**	80%	80%
23	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones	**SI**	80%	
Inventario de activos y clasificación de la información				
24	Procedimientos documentados para la operación de los sistemas	**SI**	80%	58%
25	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos	**NO**	0%	
26	Separación de funciones para reducir el riesgo de error o fraude	**SI**	80%	
27	Separación de los ambientes de desarrollo, pruebas y producción	**SI**	100%	
28	Monitoreo del servicio dado por terceras partes	**SI**	100%	
29	Administración de la capacidad de procesamiento	**SI**	70%	
30	Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares	**SI**	100%	
31	Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas	**SI**	30%	
32	Seguridad sobre el intercambio de la información, incluido el correo electrónico	**SI**	25%	
33	Seguridad sobre canales electrónicos	**SI**	50%	
34	Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas	**NO**	0%	
Adquisición, desarrollo y mantenimiento de sistemas informáticos				
35	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida	**SI**	100%	75%
36	Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida	**SI**	100%	
37	Definir controles sobre la implementación de aplicaciones antes del ingreso a producción	**SI**	100%	
38	Controlar el acceso a las librerías de programas fuente	**SI**	100%	

39	Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios	**SI**	50%	
40	Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa	**NO**	0%	
Procedimientos de respaldo				
41	Procedimientos de respaldo regular y periódicamente validado. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa	**SI**	100%	100%
42	Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento	**SI**	100%	
Gestión de incidentes de seguridad de información				
43	Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información	**NO**	0%	40%
44	Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas	**SI**	80%	

Fuente: Desarrollo propio

4.2. Indicadores versus objetivos de seguridad

A continuación, se muestran los resultados obtenidos en cada uno de los indicadores en relación con los objetivos de seguridad

Tabla N° 25. Objetivos de seguridad vs indicadores

Objetivos	Indicadores	Fórmula	Meta
Implementar una política de seguridad de información que sea desplegada a todos los colaboradores, proveedores y terceros involucrados en los procesos de tecnología	Colaboradores que conocen la política de seguridad de información	$\frac{Nro\ colaboradores\ conocen}{Nro\ total\ de\ colaboradores}$	100%
	Colaboradores que cumplen de la política de seguridad de información	$\frac{Nro\ colaboradores\ cumplen}{Nro\ total\ de\ colaboradores}$	80%
Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de información, para reducirlos en un 80%.	Incidentes reportados adecuadamente	$\frac{Nro\ de\ incidentes\ reportados\ adecuadamente}{Nro\ total\ de\ incidentes}$	80%
	Vulnerabilidades reportadas adecuadamente	$\frac{Nro\ de\ vulnerabilidades\ reportadas\ adecuadamente}{Nro\ total\ de\ vulnerabilidades}$	80%
	Incidentes atendidos oportunamente	$\frac{Nro\ de\ incidentes\ atendidos}{Nro\ total\ de\ incidentes}$	95%
	Vulnerabilidades atendidas oportunamente	$\frac{Nro\ de\ vulnerabilidades\ superadas}{Nro\ total\ de\ vulnerabilidades}$	85%
Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos, para reducir el 90% de los riesgos a niveles aceptables	Activos de información sin mecanismos de control	$\frac{Nro\ de\ activos\ \text{sin}\ control}{Nro\ total\ de\ activos}$	0%
	Riesgos con nivel de tolerancia "No tolerables"	$\frac{Nro\ de\ riesgos\ no\ tolerables}{Nro\ total\ de\ riesgos}$	0%
	Riesgos con nivel de tolerancia "Totalmente tolerables"	$\frac{Nro\ de\ riesgos\ totalmente\ tolerables}{Nro\ total\ de\ riesgos}$	65%
Formación y concientización al 100% de los colaboradores involucrados en los procesos	Colaboradores capacitados/concientizados	$\frac{Nro\ colaboradores\ capacitados}{Nro\ total\ de\ colaboradores}$	100%

de tecnología, en temas de seguridad de información.	Colaboradores capacitados/concientizados aprobados > 13	$\frac{Nro\ colaboradores\ aprobados > 13}{Nro\ total\ de\ capacitados}$	90%
Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras.	Cumplimiento de requisitos reglamentarios	$Análisis\ de\ brechas$	90%
Gestionar y controlar el 100% de los documentos del SGSI.	Procedimientos necesarios SGSI Documentados/ Estandarizados/ Difundidos	$\frac{Nro\ de\ procedimientos\ DED}{Nro\ total\ de\ requisitos}$	90%
	Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ Difundidos	$\frac{Nro\ cumplimiento\ de\ procedimientos\ DED}{Nro\ total\ de\ procedimientos}$	90%

Fuente: Desarrollo propio

4.3. Resultados de indicadores PRE y POST

Tabla N° 26. Resultado de indicadores antes VS después

Indicadores	PRE (antes)		POST (ahora)	
Colaboradores que conocen la política de seguridad de información	$\frac{5}{52}$	10%	$\frac{52}{52}$	100%
Colaboradores que cumplen de la política de seguridad de información	$\frac{5}{52}$	10%	$\frac{40}{52}$	77%
Incidentes reportados adecuadamente	$\frac{494}{918}$	54%	$\frac{756}{871}$	87%
Vulnerabilidades reportadas adecuadamente	$\frac{15}{67}$	22%	$\frac{18}{23}$	78%
Incidentes atendidos oportunamente	$\frac{813}{918}$	88%	$\frac{852}{871}$	98%
Vulnerabilidades atendidas oportunamente	$\frac{50}{67}$	75%	$\frac{18}{23}$	78%
Activos de información sin mecanismos de control	$\frac{39}{88}$	44%	$\frac{88}{88}$	0%
Riesgos con nivel de tolerancia "No tolerables"	$\frac{12}{268}$	4.5%	$\frac{0}{268}$	0%
Riesgos con nivel de tolerancia "Totalmente tolerables"	$\frac{87}{268}$	32.5%	$\frac{207}{268}$	77%
Colaboradores capacitados/concientizados	$\frac{5}{52}$	10%	$\frac{52}{52}$	100%
Colaboradores capacitados/concientizados aprobados > 13	$\frac{5}{52}$	10%	$\frac{38}{52}$	73%
Cumplimiento de requisitos reglamentarios	$Brecha\ PRE$	34%	$Brecha\ POST$	86%
Procedimientos necesarios SGSI Documentados/ Estandarizados/ Difundidos (1)	$\frac{3}{15}$	20%	$\frac{15}{15}$	100%
Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ Difundidos	$\frac{2}{3}$	67%	$\frac{12}{15}$	80%

Fuente: Desarrollo propio

(1) Los documentos necesarios SGSI son: política SGSI, manual SGSI, procedimiento de gestión de riesgos, procedimiento de gestión de incidentes y vulnerabilidades, procedimiento de gestión de usuarios, procedimiento de control de accesos, procedimientos disciplinarios de seguridad, procedimiento para cese de personal, procedimiento para ingreso de personal, política sobre seguridad física y ambiental, procedimientos de la operación de sistemas, procedimientos para el monitoreo del trabajo de terceros, políticas sobre la gestión de la capacidad de procesamiento, procedimiento para la adquisición, desarrollo y mantenimiento de sistemas, procedimientos de respaldo.

4.4. Análisis por indicadores

Objetivo 1: Implementar una política de seguridad de información que sea entendida, cumplida e interiorizada por el 100% de los colaboradores involucrado en los procesos de Tecnología

Indicadores	Meta	Antes	Después
Colaboradores que conocen la política de seguridad de información	100%	10%	100%
Colaboradores que cumplen de la política de seguridad de información	80%	10%	77%

Interpretación:

Al iniciar el proyecto no existía una política de seguridad de información y mucho menos la cultura para proteger los activos de información. Se puede observar una mejoría de 88.5% en promedio de los dos indicadores. Actualmente los colaboradores de la gerencia de tecnología conocen como sus funciones cotidianas aportan al mantenimiento y mejora continua del SGSI implementado

Objetivo 2: Gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de información para reducir los impactos en un 80%.

Indicadores	Meta	Antes	Después
Incidentes reportados adecuadamente	80%	54%	87%
Vulnerabilidades reportadas adecuadamente	80%	22%	78%
Incidentes atendidos oportunamente	95%	88%	98%
Vulnerabilidades atendidas oportunamente	85%	75%	78%

Interpretación:

Con los resultados obtenidos después de la implementación del SGSI, se lograron detectar de manera preventiva las vulnerabilidades, mitigando así los futuros riesgos. De igual manera, se logró implementar procesos de atención inmediata para las vulnerabilidades e incidentes reportados

Objetivo 3: Desplegar las medidas de seguridad para gestionar los riesgos y ejecutar el plan de tratamiento de riesgos planteado para reducir el 90% de los riesgos a niveles aceptables

Indicadores	Meta	Antes	Después
Colaboradores capacitados/concientizados	100%	10%	100%
Colaboradores capacitados/concientizados aprobados > 13	90%	10%	73%

Interpretación:

Al iniciar el proyecto, se detectó:

- Activos de información sin controles para los cuales se implementaron diferentes tipos de controles preventivos, correctivos y detectivos.
- Muchos riesgos con calificativo no tolerables, los cuales se lograron minimizar a un 0 %.

Objetivo 4: Formación y concientización al 100% de los colaboradores involucrados en los procesos de tecnología en temas de seguridad de información

Indicadores	Meta	Antes	Después
Cumplimiento de requisitos reglamentarios	90%	34%	86%
Procedimientos necesarios SGSI Documentados/ Estandarizados/ Difundidos	90%	20%	100%
Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ Difundidos	90%	67%	80%

Interpretación:

Si bien todos los colaboradores involucrados en los procesos de tecnología están muy bien entrenados para el cumplimiento de sus labores, no contaban con una formación y concientización sobre la seguridad de información y protección de los activos de información.

Se puede observar que después de la implementación del SGSI, los colaboradores incrementaron notablemente su compromiso con la seguridad de los activos de información.

Objetivo 5: Cumplimiento de la legislación vigente sobre información personal, propiedad intelectual y otras

Indicadores	Meta	Antes	Después
Cumplimiento de requisitos reglamentarios	90%	34%	86%

Interpretación:

Después de los análisis de brechas PRE y POST, se observa que el cumplimiento de las normas ISO 27001 e ISO 27002 mejora en un 52%. Aun así, existe una pequeña brecha por cumplir, en la cual la empresa deberá seguir trabajando para cubrirla

Objetivo 6: Gestionar y controlar el 100% de los documentos del SGSI.

Indicadores	Meta	Antes	Después
Procedimientos necesarios SGSI Documentados/ Estandarizados/ Difundidos	90%	20%	100%
Cumplimiento de los procedimientos SGSI documentados/ estandarizados/ Difundidos	90%	67%	80%

Interpretación:

La UNTRM no contaba con la documentación mínima necesaria para soportar un SGSI. Se puede observar que al final de la implementación se logró contar con toda la documentación necesaria

4.5. Beneficios obtenidos

Los beneficios obtenidos con la propuesta fueron:

1. Provee a la gerencia dirección y apoyo para la seguridad de la información.
2. Ayuda a identificar los activos de información y a protegerlos adecuadamente.
3. Enfoque sistemático para el análisis y evaluación del riesgo de información de la UNTRM.
4. Asegura una correcta y segura operación de información de la UNTRM, reduciendo el riesgo del error humano.
5. Incrementa sustancialmente los controles de acceso a la información.
6. Minimiza la interrupción en el funcionamiento de las actividades del negocio y lo protege de desastres y fallas mayores.

7. Mayor confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

4.6. Validación del modelo de gestión de riesgos de TI propuesto

Para la validación del modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, sobre la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú propuesto, se realizó una valoración por juicio de expertos.

Los expertos que fueron considerados para dicha evaluación fueron los siguientes:

Tabla N° 27. Identificación de expertos para la valoración del modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit propuesto

	Experto 1	**Experto 2**	**Experto 3**
Nombres y Apellidos	Erwin Mac Dowall Reynoso	Pedro Segundo Castañeda Vargas	Oscar Zocón Alva
Formación académica	- Licenciado en Computación - Maestro en Computación	- Ingeniero de Sistemas - Maestría en Administración de Negocios – MBA - Maestría en Dirección y Gestión de Tecnologías de Información	- Ingeniero de Computación y Sistemas - Magister en Ingeniería de Sistemas
Área de experiencia profesional	- Especialización en Sistemas de Gestión de la Seguridad de la Información ISO 27001 - Certificación ITIL Fundation	- Process Consulting, Aplicación del Modelo CMMI V1.2 - Despliegue de CMMI Nivel de Madurez 3. - Inducción a Metodologías y Pruebas de Testing	- Certificación Internacional ITIL en Gestión de Servicios de Tecnologías de Información - Certificación en Gestión y Desarrollo de Proyectos Agiles Certified Scrum Developer - Auditor Interno ISO 27001:2007
Tiempo de experiencia	31 años	14 años	23 años
Cargo actual	- Consultor de TI - Docente Universitario	- Jefe de Proyectos - Mejora de Procesos bajo enfoque CMMI - Docente Universitario	- Docente Universitario
Institución	- Independiente	- GMD S.A.	- Universidad Nacional de Cajamarca

Los objetivos perseguidos con la valoración del modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit propuesto, fueron:

a. Objetivo de la investigación

Elaborar un modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú.

b. Objetivo del juicio de expertos

Validar el modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

c. Objetivo de la prueba

Determinar la utilidad del modelo propuesto para la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas.

Los criterios y el sistema de valoración del modelo de gestión de riesgos de TI basado en la norma ISO/IEC 27005 y metodología Magerit propuesto, fueron:

Tabla N° 28. Criterios y sistema de valoración del modelo de gestión de riesgos de TI basado en la norma ISO/IEC 27005 y metodología Magerit propuesto por juicio de expertos

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA La cantidad y calidad de los elementos presentados en el contenido son suficientes para la aplicación del modelo.	1. No cumple con el criterio	Los aspectos considerados en la actividad o tarea no son suficientes para medir ésta.
	2. Bajo Nivel	Los aspectos considerados en la actividad o tarea permiten medir algún aspecto de ésta, pero no corresponden con la totalidad de la actividad o tarea.
	3. Moderado nivel	Se deben incrementar algunos aspectos para poder evaluar la actividad o tarea completamente.
	4. Alto nivel	Los aspectos considerados en la actividad o tarea son suficientes.
CLARIDAD El contenido se presenta utilizando un lenguaje apropiado que facilita su comprensión del modelo.	1. No cumple con el criterio	La actividad o tarea no es clara.
	2. Bajo Nivel	La actividad o tarea requiere bastantes modificaciones o una modificación muy significativa en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos de la actividad o tarea.
	4. Alto nivel	La actividad o tarea es clara, tiene semántica y sintaxis adecuada.

COHERENCIA Existe una correspondencia lógica entre el contenido presentado y la teoría utilizada para el desarrollo del modelo.	1. No cumple con el criterio	La actividad o tarea no tiene relación lógica con el objetivo perseguido.
	2. Bajo Nivel	La actividad o tarea tiene una relación tangencial con el objetivo perseguido.
	3. Moderado nivel	La actividad o tarea tiene una relación moderada con el objetivo que está midiendo.
	4. Alto nivel	La actividad o tarea se encuentra completamente relacionada con el objetivo que está midiendo.
RELEVANCIA El contenido presentado es importante y determinante para lograr el entendimiento del modelo.	1. No cumple con el criterio	La actividad o tarea puede ser eliminado sin que se vea afectada la medición del objetivo perseguido.
	2. Bajo Nivel	La actividad o tarea tiene alguna relevancia, pero otra actividad o tarea puede estar incluyendo lo que mide ésta.
	3. Moderado nivel	La actividad o tarea es relativamente importante para el modelo.
	4. Alto nivel	La actividad o tarea es muy relevante y debe ser incluido en el modelo.

Aplicando el formato de encuesta que se muestra en el Anexo N° 4, se obtuvieron las valoraciones de cada uno de los expertos para cada uno de los criterios considerados para validar el modelo de gestión de riesgos de TI basado en la norma ISO/IEC 27005 y metodología Magerit propuesto, cuyos resultados se muestran a continuación:

Tabla N° 29. Resultados de la validación de expertos del modelo de gestión de riesgos de TI basado en la norma ISO/IEC 27005 y metodología Magerit propuesto por juicio de expertos

ETAPA	ACTIVIDAD	EXPERTO 1				EXPERTO 2				EXPERTO 3							
		SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE	SU	CL	CO	RE
FASE I. Definición del alcance del SGR	Identificación de los procesos y activos críticos	4	4	4	4	4	3	4	3	4	4	4	4	3.67	3.44	3.67	3.56
	Definición de la política general del SGSI	3	3	4	3	3	3	3	3	3	4	4	4				
	Análisis de las brechas de seguridad de la información	4	3	3	3	4	4	3	4	4	3	4	4				
FASE II. Evaluación del riesgo de TI	Definición del inventario de activos de información y de TI relevantes	4	4	4	3	4	4	4	4	4	4	4	4	4.61	4.56	4.61	4.06
	Determinación de la criticidad de los activos de información y de TI	5	4	5	4	5	5	4	4	5	5	5	4				
	Identificación de amenazas y vulnerabilidades	5	4	5	4	5	5	4	4	5	5	5	4				
	Estimación del impacto de la materialización de las amenazas	4	4	4	5	4	5	5	4	5	5	5	4				
	Estimación de la frecuencia de la materialización de las amenazas	4	4	5	5	5	5	5	4	5	5	5	4				
	Valoración del riesgo	5	4	5	4	4	5	4	4	5	5	5	4				
FASE III Tratamiento y administración del riesgo de TI	Plan de tratamiento de los riesgos no tolerables	4	4	4	4	3	4	4	4	4	4	4	4	3.44	3.78	3.78	3.67
	Implementación de las medidas de seguridad	4	4	4	4	3	3	4	3	4	4	3	3				
	Identificación de la estrategia de implementación de controles	3	4	4	3	3	3	3	4	3	4	4	4				

De las calificaciones, que los expertos dieron en su valoración del modelo de gestión de riesgos de TI propuesto, se realizaron las siguientes interpretaciones:

a. En relación a la Etapa 1: Definición del alcance del SGR
   - Las actividades y tareas desarrolladas son suficientes para lograr los objetivos o resultados esperados, pero falta reforzar la definición de la política general del SGSI.
   - La descripción de las actividades y tareas son claras y comprensibles en su explicación para su ejecución dentro del modelo, pero falta aclarar la definición de la política general del SGSI.
   - Las actividades y tareas desarrolladas son coherentes y hay una lógica para su ejecución en el modelo. Se requiere mejorar aspectos en el análisis de brechas de seguridad.
   - Las actividades o tareas desarrolladas son muy relevante y debe ser incluido en el modelo. Se debe mejorar la definición de la política general del SGSI y el análisis de brechas de seguridad.

b. En relación a la Etapa 2: Evaluación del riesgo de TI
   - Las actividades y tareas desarrolladas permiten cumplir con los objetivos o resultados esperados en esta etapa del modelo.
   - La descripción de las actividades y tareas son claras y comprensibles en su explicación para su ejecución dentro del modelo.
   - Las actividades y tareas desarrolladas son coherentes y hay una lógica para su ejecución en el modelo.
   - Las actividades o tareas desarrolladas son muy relevantes y deben ser incluidas en el modelo.

c. En relación a la Etapa 3: Tratamiento y administración del riesgo de TI
   - Las actividades y tareas desarrolladas son suficientes para lograr los objetivos o resultados esperados en esta etapa del modelo, pero debe reforzarse la propuesta de implementación de las medidas de seguridad eiIdentificación de la estrategia de implementación de controles
   - La descripción de las actividades y tareas son claras y comprensibles en su explicación para su ejecución dentro del modelo.
   - Las actividades y tareas desarrolladas son coherentes y hay una lógica para su ejecución en el modelo.
   - Las actividades o tareas desarrolladas son muy relevantes y deben ser incluidas en el modelo.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Para delimitar la aplicabilidad de un sistema de gestión de riesgos de TI, éste debe estar en concordancia con los objetivos del sistema de seguridad de la información de la institución. En el desarrollo del modelo de gestión de riesgos de TI propuesto se logró desarrollar un procedimiento sencillo que permitió identificar los procesos críticos sobre los cuales se realizó la evaluación de los escenarios de riesgos, obteniendo un listado de procesos académicos y administrativos críticos de la Universidad Nacional Toribio Rodríguez de Mendoza.

2. Se logró elaborar un procedimiento, adecuando el marco de referencia de la metodología MagerIT, para desarrollar las actividades y tareas de las dos principales fases de un sistema de gestión de riesgos de TI, como son: la evaluación de los riesgos y el tratamiento de los mismos; para cada uno de los activos de TI que se tenían que protegerse, con la finalidad de asegurar una gestión adecuada de la seguridad de la información en los procesos académicos y administrativos identificados como críticos.

3. El modelo de gestión de riesgos de TI propuesto permite, con coherencia, claridad y suficiencia, identificar para cada activo de TI, valorar su criticidad, identificar las amenazas y vulnerabilidades que conforman los escenarios de riesgos a los que están expuestos cada activo y finalmente valorar los niveles de exposición al riesgo, basado en el análisis de los impactos y frecuencias de ocurrencia de cada escenario de riesgo identificado.

4. Así mismo, el modelo de gestión de riesgos de TI propuesto, también permite con coherencia, claridad y suficiencia y pertinencia, elaborar estrategias de tratamiento de los escenarios de riesgos de TI que han sido valorados en niveles de exposición que están fuera de los rangos de tolerancia fijados por la universidad. Las estrategias de tratamiento contemplan las formas de implantación de los controles necesarios.

5. En un trabajo colaborativo con el personal responsable y con autoridad en la gestión de la seguridad de la información en la universidad, se elaboraron las tablas que permitieron definir el apetito de riesgo que tienen la institución. La propuesta de

apetito de riesgos está basada en la definición de tablas que determinan los niveles de impacto y frecuencia de exposición al riesgo. Estas tablas fueron utilizadas para determinar los niveles de exposición al riesgo tolerable y no tolerable.

6. En base a indicadores KRI (indicadores claves de riesgo) se logró determinar la mejora en la gestión de los riesgos, en base a los resultados obtenidos en las fases de análisis y tratamiento de los riesgos que están propuestos en el modelo. A través de estos indicadores se identificó las brechas de seguridad, llegando a concluir que el modelo, permite disminuir estas brechas.

7. El modelo de gestión de riesgos de TI propuesto fue validado a través de un procedimiento de valoración por el juicio de tres expertos, calificando la coherencia, claridad, pertinencia y suficiencia del modelo, llegando a obtener, en cada uno de las categorías mencionadas, valores que sobrepasan la media en una escala de cinco niveles. Por tanto, el modelo es calificado como favorable para la gestión de riesgos de TI en la universidad.

RECOMENDACIONES

1. Se recomienda mantener una constante revisión de la política del SGSI y verificar el cumplimiento de la misma por parte de los responsables de la seguridad de la información en la universidad. La finalidad es que los controles que se identifiquen como necesarios después de la evaluación de riesgos de TI, sean implementados como parte del SGSI y se evalúe la efectividad de los mismos.

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 de TI; 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 realizar una documentación de procesos para poder gestionar los riesgos de TI, para asegurar su formal implementación y su cumplimiento.

REFERENCIAS CONSULTADAS

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 27001:2005. Bogotá, Colombia: Alfaomega.

Alexander, A. (2011). Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca. CENTRUM - Centro de Negocios, Pontificia Universidad Católica del Perú.

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 2016, 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 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 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 - Libro 1. (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 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.

ANEXO N° 1

TABLAS DE REFERENCIA PARA LA VALORACIÓN DE LA CRITICIDAD DE LOS ACTIVOS DE TI

Para la valoración de los activos se tomarán en cuenta las siguientes dimensiones de seguridad:

Tabla N° 30. Descripción de las dimensiones de seguridad de la información que se tomarán en cuenta en la valoración de la criticidad de los activos de TI

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Fuente: (Magerit, 2012)

Tabla N° 31. Definición de escala de valoración de la criticidad de los activos de TI

[pi] Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7 – 8	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5 – 6	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3 – 4	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1 – 2	pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9 - 10	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7 - 8	probablemente cause un incumplimiento grave de una ley o regulación
5 - 6	probablemente sea causa de incumplimiento de una ley o regulación
3 – 4	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1 – 2	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9 - 10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7 - 8	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5 - 6	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

3 – 4	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1 – 2	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales económicos	
9 - 10	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7 - 8	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
5 - 6	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3 – 4	de bajo interés para la competencia de bajo valor comercial
1 – 2	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
[da] de interrupción del servicio	
9 - 10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7 - 8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5 - 6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3 – 4	Probablemente cause la interrupción de actividades propias de la Organización
1 – 2	Pudiera causar la interrupción de actividades propias de la Organización
[po] de orden público	
9 - 10	alteración seria del orden público
7 - 8	probablemente cause manifestaciones, o presiones significativas
3 - 6	causa de protestas puntuales
1 – 2	pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7 – 8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5 – 6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3 – 4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1 – 2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] administración y gestión	
9 - 10	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7 - 8	probablemente impediría la operación efectiva de la Organización
5 - 6	probablemente impediría la operación efectiva de más de una parte de la Organización
3 – 4	probablemente impediría la operación efectiva de una parte de la Organización

1 – 2	pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1 - 2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[pd] persecución de delitos	
6 - 10	Impida la investigación de delitos graves o facilite su comisión
1 – 5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9 –10	RTO < 4 horas
7 – 8	4 horas < RTO < 1 día
4 – 6	1 día < RTO < 5 días
1 – 3	5 días < RTO

Fuente: (Magerit, 2012)

ANEXO N° 2

CATÁLOGO DE AMENAZAS POR ACTIVO Y DIMENSIÓN DE SEGURIDAD DE LA INFORMACIÓN

Tabla N° 32. Catálogo de amenazas por activo y dimensión se seguridad de la información

[N]	Desastres naturales			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[N.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[N.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[N.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I]	**De origen industrial**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[I.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones

[I.*]	Desastres industriales	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas. Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[I.3]	Contaminación mecánica	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.4]	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.5]	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	[D] disponibilidad	[SW] aplicaciones (software) [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.6]	Corte del suministro eléctrico	Cese de la alimentación de potencia	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información (electrónicos) [AUX] equipamiento auxiliar
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[I.8]	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	[D] disponibilidad	[COM] redes de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante,	[D] disponibilidad	[AUX] equipamiento auxiliar

[I.10]	Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	Media] soportes de información
[I.11]	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación	[C] confidencialidad	[HW] equipos informáticos (hardware) [Media] media [AUX] equipamiento auxiliar [L] instalaciones
[E]	**Errores y fallos no intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[E.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información
[E.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información
[E.3]	Errores de monitorización *(log)*	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad (trazabilidad)	[D.log] registros de actividad
[E.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad	[D.conf] datos de configuración

[E.7]	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	[D] disponibilidad	[P] personal
[E.8]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	SW] aplicaciones (software)
[E.9]	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	[C] confidencialidad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[E.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[E.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	
[E.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[E.18]	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[D] disponibilidad	D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[E.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW)

				[COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones [P] personal (revelación)
[E.20]	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[I] integridad [D] disponibilidad [C] confidencialidad	[SW] aplicaciones (software)
[E.21]	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	[I] integridad [D] disponibilidad	[SW] aplicaciones (software)
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes electrónicos [AUX] equipamiento auxiliar
[E.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	[S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[E.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[E.28]	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	[P] personal interno
[A]	**Ataques intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[A.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	[D.log] registros de actividad
[A.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [A] disponibilidad	[D.log] registros de actividad

[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	[C] confidencialidad [A] autenticidad [I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.6]	Abuso de privilegios de acceso	Cada usuario utiliza un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, puede ocasionar problemas.	[C] confidencialidad [I] integridad [D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[A.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	[SW] aplicaciones (software)
[A.9]	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.10]	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	[I] integridad	[S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir	[C] confidencialidad	[COM] redes de comunicaciones

		del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.		
[A.13]	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	[I] integridad (trazabilidad)	S] servicios [D.log] registros de actividad
[A.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	[COM] redes de comunicaciones
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [Media] soportes de información [L] instalaciones
[A.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	[D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones
[A.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	[SW] aplicaciones (software)

[A.22]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	[HW] equipos [Media] soportes de información [AUX] equipamiento auxiliar
[A.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada (saturación del equipo informático)	[D] disponibilidad	[S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones
[A.25]	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar
[A.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)	[D] disponibilidad	[HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones
[A.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	[L] instalaciones
[A.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	[P] personal interno
[A.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	[P] personal interno
[A.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	[P] personal interno

Fuente: Elaboración propia, adecuado de (Magerit, 2012)

ANEXO N° 3

CUESTIONARIO PARA LA RECOPILACIÓN DE LA INFORMACIÓN PARA LA EVALUACIÓN DE LAS BRECHAS DE SEGURIDAD DE LA INFORMACIÓN

Tabla N° 33. Cuestionario para la evaluación de brechas de seguridad de la información

PREGUNTAS	SI	NO	COMENTARIOS
1. ¿Se lleva un registro detallado de los activos de información de la Unidad (inventario)?			
2. ¿El inventario de activos informáticos se encuentra actualizado?			
3. ¿Hay asignación de responsabilidades a los funcionarios sobre la custodia de los activos informáticos?			
4. ¿Existe un inventario de las configuraciones de los equipos (incluyendo componentes y software instalado)?			
5. ¿Se lleva control de licencias de software y sus costos de licenciamiento (en caso necesario)?			
6. ¿Se han identificado los activos o servicios más críticos para el cumplimiento de los objetivos del Área?			
7. ¿Se tiene un procedimiento para identificar amenazas?			
8. ¿se identifican los activos afectados por amenazas?			
9. ¿Cuenta con una escala de valoración de amenazas?			
10. ¿Se calcula la probabilidad de ocurrencia de las amenazas?			
11. ¿La oficina cuenta con un manual de políticas con respecto a amenazas?			
12. ¿Se encuentran documentados las políticas y procedimientos respecto a amenazas?			
13. ¿Se lleva un registro de las amenazas ocurridas?			
14. ¿Se tiene un procedimiento para identificar vulnerabilidades?			
15. ¿se identifican los activos afectados por vulnerabilidades?			
16. ¿Cuenta con una escala de valoración de vulnerabilidades?			
17. ¿La oficina cuenta con un manual de políticas con respecto a vulnerabilidades?			
18. ¿Se encuentran documentados las políticas y procedimientos respecto a vulnerabilidades?			
19. ¿Se lleva un registro de las vulnerabilidades detectadas?			
20. ¿Existe algún mecanismo que determine la magnitud del impacto?			

21. ¿Se cuenta con una escala de valorización de impactos?			
22. ¿Se han identificado los riesgos de TI asociados a la gestión y operación de la plataforma informática del Área?			
23. ¿Se han identificado los riesgos asociados a los recursos más críticos?			
24. ¿Se estiman los niveles necesarios de exposición al riesgo?			
25. ¿Se clasifican los riesgos según su criticidad?			
26. ¿Se han establecido controles para mitigar los riesgos de los recursos de información más críticos?			
27. ¿Se tienen definidas las estrategias de cómo implementar los controles?			
28. ¿Cuentan con procedimientos para identificar controles?			
29. ¿El Área cuenta con un manual de políticas, procedimientos y normativa relacionada a la seguridad de información?			
30. ¿El Área cuenta con un manual de políticas, procedimientos y normativa relacionada a la gestión de riesgos?			
31. ¿Se ha establecido un mecanismo para la atención y registro de incidentes?			
32. ¿Se utilizan claves seguras de acceso?			
33. ¿Se llevan a cabo políticas en lo referente a gestión de cuentas de usuario?			
34. ¿Se eliminan los derechos de acceso a funcionarios inactivos o que han dejado de laborar para la Unidad?			
35. ¿Se revisan periódicamente los registros de acceso a los sistemas?			
36. ¿La carga de los extintores de incendio se encuentra vigente?			
37. ¿Se conoce el mecanismo de operación de los diversos tipos de extintores de incendio?			
38. ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal del Área o por motivo de reparación?			
39. ¿Se tiene una clasificación de la información de la Unidad por nivel de sensibilidad o privacidad?			
40. ¿Se ha establecido una política de respaldos periódicos de la información en la Unidad?			
41. ¿La oficina cuenta con el personal y cantidad adecuada para la realización de las funciones?			
42. ¿El área se encuentra en un ambiente adecuado para la realización de sus funciones?			

43. ¿Se tienen identificados los servicios requeridos por la función de TI?			
44. ¿Se tiene información del nivel de satisfacción del usuario respecto a los servicios brindados?			
45. ¿Se lleva el control de la vida útil de los activos de información?			
46. ¿Se mantiene un registro auxiliar de los activos informáticos en desuso?			
47. ¿Se lleva control de los componentes recuperables de los activos en desuso (discos duros, memoria, tarjetas de video, etc)?			
48. ¿Se sigue algún procedimiento para borrar la información de los discos duros u otras unidades de almacenamiento, antes de su desecho?			
49. ¿Se mantiene un control de la salida de activos por parte de terceros?			

Fuente: Elaboración propia

ANEXO N° 4

RESULTADOS DEL ANÁLISIS DE RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMATICA

En el siguiente formato contiene el resumen del análisis y evaluación de los posibles riesgos relacionados con Tecnología de la Información que afectan directamente los activos tecnológicos de los procesos académicos/administrativos de la UNTRM.

I. SERVIDORES Y CONCENTRADORES CENTRALES

Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Servidores y concentradores centrales y de borde	Acceso no autorizado	Si	El acceso a los recursos críticos en los gabinetes de piso o de pared (servidores, switch, router, modem, ups, transformadores de aislamiento) del cuarto de comunicaciones en la agencia principal está protegido con un sistema de puertas con llave y tabiquería a los que sólo tiene acceso el personal autorizado.
	Corte de luz, Sistema ininterrumpido de energía (UPS) descargado o variaciones de voltaje	Si	Se cuenta con un sistema de red múltiple de alimentación de energía que evita el fallo de suministro. Así mismo, se cuenta con un sistema de alimentación ininterrumpido de energía para caso extremos de suministro de energía. Este sistema mantiene en forma autónoma, de ser el caso, durante 20 minutos aprox. funcionando los equipos centrales y los terminales del área de tecnologías de información.
	Destrucción o fallo de un componente crítico del equipo (microprocesador, memoria, fuente de poder, otros)	Se recomienda mejorar	La seguridad para la entrada y salida de paquetes a Internet está basada en un servidor ISA Server sin tolerancia a fallos por riesgos en fuente de poder, discos duros y procesador. No existen equipos de comunicación que toleren fallos este es el caso del switch core (aquí se conectan los servidores), y los switches ubicados en cada una de las facultades o dependencias administrativas. Lo cual paralizaría las operaciones en todas las áreas en caso de avería.
	Errores de configuración	Se recomienda mejorar	Se cuenta con servidor de respaldo donde se replica toda la configuración necesaria para reiniciar el sistema. El servidor activo tiene implementado políticas de acceso a ser mejoradas, y no se cuenta con redundancia para este equipo altamente importante
	Factores ambientales no adecuados. (ventilación, protección contra incendios, acondicionamiento racks, otros)	Se recomienda mejorar	Se cuenta con sistema de aire acondicionado con BTU/h no adecuado en la Sala de Servidores
	Límite de vida útil – Máquinas obsoletas (antigüedad del equipo, repotenciamiento de componentes)	Si	Se tiene pendiente un pedido para adquirir nuevos equipos centrales
	Mantenimiento	Si	Hay un plan de mantenimiento de equipos
	Robo	Si	Los equipos de cómputo de Core están ubicados en lugares seguros
	Afectación por virus	Si	Protegidos con sistema antivirus

II. BASE DE DATOS

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Base de Datos	Copia no autorizada de o a un medio de datos externos	Si	Se generan backup mensuales y son almacenados en un lugar seguro fuera de los ambientes de la , manejados y transportados por personal autorizado.
	Errores de software (motor y contenedor de base de datos)	Se recomienda mejorar	El servidor activo tiene implementado políticas de acceso a ser mejoradas, y no se cuenta con redundancia para este equipo altamente importante.
	Falta de espacio de almacenamiento	Se recomienda mejorar	Se estima que en un tiempo próximo la arquitectura de datos con la que actualmente se trabaja no va a ser funcional y bajará su performance de respuesta, debido a: (1) la capacidad instalada del servidor de base de datos será insuficiente, necesitándose más potencia y rendimiento y (2) al modelo de arquitectura de datos que se utiliza.
	Pérdida o falla de backups	Si	Se genera backup mensuales de la base datos completa.
	Pérdida de confidencialidad en datos privados y de sistema	Si	El acceso a la base de datos está controlado a través de perfiles de usuario con niveles de acceso autorizados, según el área y responsabilidad.
	Directorios compartidos	Si	Directorio de la base de datos solo esta compartido para usuarios autorizados.
	Sabotaje	Si	El área Sala de Servidores está ubicada en una zona con perímetro de acceso restringido a personal no autorizado claramente definido.
	Afectación de virus	Si	Servidor de base de datos protegido con antivirus

III. SOFTWARE DE OFIMÁTICA (SOFTWARE BACKOFFICE Y SISTEMAS OPERATIVOS)

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Software de BackOffice y sistemas operativos instalados en servidores y terminales	Aplicaciones sin licencias	Si	Software licenciado (Campus Agreement)
	Error de configuración	Si	Software licenciado, con evaluación y pruebas.
	Mala Administración de control de accesos	Si	Se controla el acceso a las estaciones mediante política de acceso: niveles de acceso por perfiles de usuario.
	Pérdida de datos	No	En las estaciones de trabajo de los usuarios no se generan respaldos de sus archivos
	Afectación de virus	Si	Protegidos con antivirus

IV. BACKUP (SISTEMA DE RESPALDO)

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Backup	Copia no autorizada del backup	Si	Solo personal autorizado tiene acceso a generar, copiar y trasladar backup de información.
	Errores de software para recuperación de información de backup (restore)	No	No se cuenta con procedimientos de restore formalmente establecidos y documentados
	Falla o deterioro del medio de almacenamiento externo del backup	Se recomienda mejorar	Los backup son almacenados en dispositivos de almacenamiento secundario portátiles. El ambiente de resguardo no está climatizado. Tampoco existe procedimiento de etiquetado.
	Falta de espacio de almacenamiento	Si	Los dispositivos de almacenamiento secundario portátiles donde se almacenan los backups tienen suficiente espacio
	Mala integridad de los datos resguardados al recuperar la información de un backup	No	No se cuenta con procedimientos de restore formalmente establecidos y documentados
	Medios de datos no están disponibles cuando son necesarios	Se recomienda mejorar	No existe un procedimiento establecido y documentado para realizar pruebas de recuperación de los backups
	Pérdida o robo de backups	Si	Solo personal autorizado tiene acceso a los backups
	Sabotaje	Si	Solo personal autorizado tiene acceso a los backups

V. CABLEADO Y CONCENTRADORES

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Cableado y concentradores	Conexión de cables inadmisible (modificación de conexiones y mal etiquetado)	Se recomienda mejorar	El sistema de cableado estructurado (fibra óptica u UTP) se encuentra en buenas condiciones hasta los switch de borde. A partir de allí, existen muchos lugares donde el cableado y canaleteado está deteriorado. No se cuenta con documentación de las pruebas de cableado No se cuenta con planos de distribución de cableado
	Daño o destrucción, de cables o equipamiento, inadvertido (mala ubicación, por limpieza, impedimento de libre tránsito, otros)	Si	El sistema de cableado de cableado de la red de datos es está canaleteado. La fibra óptica está tendida sobre postes. Se cumple con los requerimientos mínimos de las normas para cableado estructurado.
		Se recomienda mejorar	Los gabinetes de comunicaciones están ubicados en ambientes seguros y los responsables tienen llaves de acceso.
	Factores ambientales	Se recomienda mejorar	Se cuenta con sistema de aire acondicionado con BTU/h que no es suficiente para climatizar toda la Sala de Servidores.
	Accesos no autorizados.	Se recomienda mejorar	No es posible conectar equipos portátiles en puntos de acceso a la red de datos sin que se genere un registro.
	Longitud de los cables de red excedidos a las normas	Si	Longitud de cables cumple con las normas establecidas.

VI. RED DE COMPUTADORAS

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Red de computadoras	Mantenimiento no adecuado de puertos. (restricciones de acceso a ciertos puertos, perfiles de acceso)	Si	Se controla el acceso a través de puertos. Esto no hace posible que intrusos puedan escanear y vulnerar a la red de datos.
	Configuración inadecuada de componentes de red	Si	Usuarios no pueden acceder a las configuraciones de red – acceso restringido
	Errores de operación (mala estandarización de velocidades de transmisión y ancho de banda, otros)	Se recomienda mejorar	El sistema de cableado troncal es fibra óptica, por tanto su ancho de banda es suficiente para transmitir paquetes de información a nivel interno
	Mal uso de servicios de red (mal uso del netmeeting, transmisión de datos, otros)	Si	No es posible enviar paquetes icmp desde un equipo portátil conectado a un punto de acceso a la red de datos a los servidores. Las políticas para el acceso a Internet ya sea por dominios asegura que solo se pueda ingresar a dominios que generar tráfico de paquetes autorizados.

VII. USUARIOS

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Usuarios	Acceso no autorizado a datos	Si	Cada usuario tiene un perfil y opciones asignadas para el acceso al sistema
	Borrado, modificación o revelación de claves de acceso a la información y aplicaciones, desautorizada o inadvertida	Si	Cada usuario cuenta con una clave personal. Falta implementar procedimientos para asegurar claves complejas.
	Condiciones de trabajo adversas (ergonomía, ubicación de equipos, otros)	Se recomienda mejorar	Los terminales informáticos son variados en modelo y configuración. No están estandarizados los terminales informáticos.
	Destrucción negligente de datos por parte de los usuarios	Si	Acceso a la base de datos protegido con perfiles de acceso.
	Documentación deficiente (manual de usuario)	No	No se cuenta con manuales de usuario los sistemas en producción
	Entrada sin autorización a ambientes	Se recomienda mejorar	Solo personal autorizado tiene acceso a los ambientes donde se encuentran los equipos de Core
	Entrenamiento de usuarios inadecuado	Se recomienda mejorar	No existe Plan de capacita en materia de seguridad de la información
	Falta de controles y log de las transacciones realizadas por los usuarios.	Se recomienda mejorar	Las bitácoras para registrar las operaciones y transacciones realizadas por los usuarios todavía son deficientes
	No cumplimiento con las medidas de seguridad del sistema	Si	Cada usuario tiene un perfil y opciones asignadas para el acceso a los sistemas y cada usuario cuenta con una clave personal intransferible

VIII. DOCUMENTACIÓN DE LOS SISTEMAS EN PRODUCCIÓN

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Documentación de programas, hardware, procedimientos administrativos locales, manuales, etc.	Acceso no autorizado a datos de documentación	No	No existe documentación de los sistemas en producción
	Borrado, modificación o revelación desautorizada de información	No	No existe documentación de los sistemas en producción
	Copia no autorizada de un medio de documentación del sistema	No	No existe documentación de los sistemas en producción
	Descripción de archivos y programas inadecuado	No	No existen políticas ni procedimientos de control de cambios.
	Documentación insuficiente o faltante, en relación a seguridad de la información	No	No existe documentación en relación a la seguridad de la información
	Mantenimiento y actualización inadecuado o ausente de la documentación	No	No existe documentación de los sistemas en producción

X. SISTEMAS O APLICACIONES INFORMÁTICAS EN PRODUCCIÓN (SISTEMA DE MATRÍCULA Y CONTROL DE NOTAS, ADMISIÓN)

Nombre del Activo	Factor de Riesgo	Se protege?	Cómo? / Por qué?
Sistemas y aplicaciones informáticas en producción	Modificaciones inoportunas y no documentadas	No	No se lleva el control detallado del desarrollo y mantenimiento. No existen procedimientos establecidos y documentados de “Control de cambios”
	Funcionalidad del sistema (no atiende todos los requerimientos de los usuarios y áreas)	Se recomienda mejorar	Se reciben y analizan todos los requerimientos, los cuales son atendidos de acuerdo a las posibilidades y capacidades de personal de TI
	Acceso a los programas fuentes no controlado	Si	Sólo el personal de autorizado tiene acceso al código fuente de los sistemas en producción
	Validación en los procesos de captura y registro de transacciones	No	No existen procedimientos establecidos y documentados de gestión de la calidad del software.

ANEXO N° 4

FORMATO PARA LA EVALUACIÓN DEL MODELO POR OPINION DE EXPERTO

Objetivo

El objetivo del presente formato es utilizarlo como instrumento para la evaluación del modelo de gestión de riesgos de TI basados en la norma ISO/IEC 27005 y metodología Magerit, para mejorar la gestión de seguridad de la información en la Universidad Nacional Toribio Rodríguez de Mendoza – Chachapoyas Perú.

1. DATOS GENERALES DEL EXPERTO

Nombres y apellidos
Grado académico y profesión
Áreas de experiencia profesional
Institución donde labora
Tiempo de experiencia

2. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del modelo:

Indicador	Criterio	Valoración				
		Muy malo	Malo	Regular	Bueno	Muy bueno
SUFICIENCIA	La cantidad y calidad de los elementos presentados en el contenido son suficientes para la aplicación del modelo.	1	2	3	4	5
CLARIDAD	El contenido se presenta utilizando un lenguaje apropiado que facilita su comprensión del modelo.	1	2	3	4	5
COHERENCIA	Existe una correspondencia lógica entre el contenido presentado y la teoría utilizada para el desarrollo del modelo.	1	2	3	4	5
RELEVANCIA	El contenido presentado es importante y determinante para lograr el entendimiento del modelo.	1	2	3	4	5

3. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.

Fase	Actividad	Criterios				Observaciones
		Suficiencia	Claridad	Coherencia	Relevancia	
FASE I. Definición del alcance del SGR	Identificación de los procesos y activos críticos					
	Definición de la política general del SGSI					
	Análisis de las brechas de seguridad de la información					
FASE II. Evaluación del riesgo de TI	Definición del inventario de activos de información y de TI relevantes					
	Determinación de la criticidad de los activos de información y de TI					
	Identificación de amenazas y vulnerabilidades					
	Estimación del impacto de la materialización de las amenazas					
	Estimación de la frecuencia de la materialización de las amenazas					
	Valoración del riesgo					
FASE III Tratamiento y administración del riesgo de TI	Plan de tratamiento de los riesgos no tolerables					
	Implementación de las medidas de seguridad					
	Identificación de la estrategia de implementación de controles					
	TOTAL					

4. RESULTADO FINAL

	FAVORABLE		DEBE MEJORAR		DESFAVORABLE