Universidad Católica de Santa María

Facultad de Ciencias e Ingenierías Físicas y Formales

Escuela Profesional de Ingeniería de Sistemas

"DISEÑO DE UN MODELO SISTÉMICO DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN, INTEGRANDO LA METODOLOGÍA MAGERIT Y LA NORMA ISO 27002:2013 EN EMPRESAS FINANCIERAS"

Presentado por los Bachilleres:
Fernández Vargas, Alberto Junior
Mayta Aguilar, Joel Ricardo

Para optar el Título Profesional de:
Ingeniero de Sistemas

Asesor:
Mg. Rosas Paredes, Karina

AREQUIPA – PERÚ
2017

PRESENTACIÓN

Sr. Director de la Escuela Profesional de Ingeniería de Sistemas.

Sres. Miembros del Jurado.

De conformidad con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniera de Sistemas, pongo a vuestra consideración el presente trabajo de investigación titulado:

“Diseño de un modelo sistémico de gestión de riesgos de la seguridad de la información, integrando la metodología Magerit y la norma ISO 27002:2013 en empresas financieras”, el mismo que de ser aprobado nos permitirá optar el título Profesional de Ingeniero de Sistemas.

Fernández Vargas, Alberto Junior

Mayta Aguilar, Joel Ricardo

AGRADECIMIENTOS

A nuestra asesora Ing. Karina Rosas Paredes, por su incondicional apoyo en el desarrollo de este trabajo.

Al Ing. Fernando Paredes Marchena por sus consejos brindados durante el desarrollo de la tesis.

DEDICATORIA

A Dios que me lo ha dado todo.

A mi papá por ser mi ejemplo a seguir por su inteligencia, perseverancia y por enseñarme el valor de las cosas, a mi mamá por enseñarme el valor de la generosidad, el amor y la humildad, a los dos gracias por su cariño y apoyo, a mis padres, Alberto y Rosa.

A mis hermanas Julissa y Ana Sofía, por su comprensión y apoyo durante todo este tiempo en los momentos buenos y malos.

A mis tíos Mario, Cesar, Victor y Mañuco, por haberme brindado la fuerza necesaria para salir adelante.

Junior.

A mi madre Victoria, por haberme inculcado la lealtad, humildad, responsabilidad y esas ganas de sacar a delante a su familia a pesar de las vicisitudes. Sé que siempre fuiste orgullosa de tus hijos madre linda y sé que lo estás allá en lo alto del cielo.

A mi padre Andrés, por haberme enseñado el valor de la perseverancia y fortaleza para poder salir adelante en los malos momentos y disfrutar mucho de los buenos que tiene la vida.

A mi tía Ana, por haberme apoyado en el momento más difícil de mi vida brindándome el cobijo de una madre.

A mi tío Raúl, por haberme apoyado en el momento en que más lo necesité brindándome los consejos para ir por el camino adecuado.

A mi hermano Eder, por haber compartido todas estas ganas de salir adelante a pesar de los obstáculos que nos puso la vida.

A mi esposa Shiomara, por haberme enseñado el significado de familia y el sentir de la felicidad en la vida.

A mi hija Leonela y a mi hijo Isaac, por ser fuentes de mi inspiración para seguir adelante y luchar contra viento y marea.

A toda mi familia, por su apoyo y compañía.

Siempre para adelante como gallo fino.

***Joel**.*

INDICE

LISTA DE TABLAS

LISTA DE FIGURAS

ANEXOS

RESUMEN

El siguiente trabajo ha sido desarrollado con el fin de proporcionar un modelo de gestión de riesgos de la seguridad de la información, aplicando la metodología MAGERIT y la norma internacional ISO 27002:2013, el cual permite identificar los principales activos de una forma rápida y sencilla dentro del área de Tecnologías de Información en el rubro de las empresas financieras, facilitando el reconocimiento de las amenazas a las cuales están expuestos y el daño que puedan causar mediante la degradación que estas puedan producir en caso de que estas se materialicen, hallando el impacto y riesgo a los cuales están sometidos los activos con el fin de dar un correcto tratamiento a los riesgos y aplicando controles estandarizados para minimizar el daño que puedan generar actuando como salvaguardas.

Se realiza un análisis que permite valorizar de manera cualitativa los activos con el fin de hallar los riesgos a que estos están expuestos en base a la probabilidad de ocurrencia.

El modelo propuesto permite a su vez la determinación del nivel de madurez de implementación de la ISO 27002:2013, permitiendo llevar un seguimiento de los controles ya implementados y mejora de los existentes, permitiendo optar por una certificación de la norma ISO 27001:2013; así mismo se desarrolló una herramienta que permite automatizar el modelo propuesto, lo que facilitara su aplicación en cualquier empresa del ámbito financiero.

Palabras Clave: Modelo, Gestión de Riesgos, Seguridad, MAGERIT, ISO.

ABSTRACT

The following work has been developed to provide information security risk management model, applying the MAGERIT methodology and the international standard ISO 27002:2013, which allows identifying the main assets in a fast and simple way within the area of Information Technologies in financial companies, facilitating the recognition of the threats to which they are exposed and the damage they can cause through the degradation that these can produce in case they materialize, finding the impact and risk to which these assets are subject in order to give a correct treatment to the risks and applying standardized controls to minimize the damage they can generate acting as safeguards.

An analysis is performed that allows qualitative valuation of the assets in order to find the risks to which they are exposed based on the probability of occurrence.

The proposed methodology allows the determination of the level of maturity of implementation of ISO 27002:2013, allowing monitoring of the already implemented controls and improvement of existing ones, enabling the Company to opt for a certification of ISO 27001:2013 in the information security management system.

Likewise, a tool was developed to automate the proposed methodology, which will facilitate its application in any company in the financial field.

Key Words: Model, Risk Management, Security, MAGERIT, ISO.

INTRODUCCIÓN

Actualmente se cuenta con una gran variedad de normas dadas por órganos supervisores como la SBS y la Contraloría General de la Republica, así como también existen diversos estándares que han sido propuestas por diversas entidades a nivel mundial. Estas normas nos describen de manera general los elementos a tener en cuenta para un adecuado análisis y gestión de riesgos de seguridad de información, sin embargo no nos indican de una manera precisa sobre los pasos y procedimientos a seguir para el adecuado uso de la misma.

“Financiera Arequipa” se encuentra en una etapa de crecimiento a nivel nacional y es necesario contar con una metodología que optímese el análisis y la gestión de riesgos de la seguridad de información de una forma eficaz y sencilla, lo cual permitirá identificar las posibles amenazas y riesgos que puedan existir. El trabajo se ha desarrollado de la siguiente forma:

El capítulo I trata sobre las generalidades del planteamiento del problema del presente proyecto de tesis. En el capítulo II se exponen los fundamentos teóricos sobre la gestión de riesgos.

En el capítulo III se establecen los lineamientos para la justificación de la metodología propuesta, mientras que en el Capítulo IV describe el desarrollo y aplicabilidad de la metodología.

En el capítulo V se desarrolló el software que permitirá la aplicabilidad del modelo y en el capítulo VI se hace la validación de la metodología, terminando con las conclusiones a las que se llegó y las recomendaciones propuestas.

CAPÍTULO I

DESCRIPCIÓN DEL PROYECTO

1.1 Planteamiento del Problema

1.1.1 Título Descriptivo

DISEÑO DE UN MODELO SISTÉMICO DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN, INTEGRANDO LA METODOLOGÍA MAGERIT Y LA NORMA ISO 27002:2013 EN EMPRESAS FINANCIERAS.

1.1.2 Caracterización del Problema

Las organizaciones empresariales soportan su actividad de negocio en tecnologías de la información por lo que necesitan dotar a sus sistemas e infraestructura informática de políticas y medidas de protección que garanticen el desarrollo y sostenibilidad de sus actividades de negocio. Mantener la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tiene mucha importancia y plantea la necesidad de disponer de profesionales capaces de asegurar, gestionar y mantener la seguridad de la información en sus sistemas ante la aparición de amenazas presentes y futuras.

Es así que se identificaron actividades las cuales no cuentan con una adecuada gestión, que permita aplicar estándares y brindar un control oportuno de los riesgos.

Se tienen definidos algunos controles basados en la norma ISO 27002:2005 con el fin de mitigar los riesgos a los cuales están expuestos los activos de

información; sin embargo no se cuenta con un control del nivel de madurez de los mismos, siendo complejos de aplicar por usuarios relacionados a la gestión de activos informáticos.

1.1.3 Línea y Sub-línea de Investigación

Línea de Investigación: Sistemas de Información y Bases de Datos

Sub-línea: Seguridad de información

1.2 Objetivos

1.2.1 Objetivo General

Diseñar un modelo de gestión de riesgos de la seguridad de información, integrando la metodología Magerit y la norma ISO 27002, a partir del diagnóstico de la situación actual de la organización, que permita asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

1.2.2 Objetivos Específicos

1. Identificar y analizar los factores internos y externos que motivan y justifican la incorporación de prácticas/estándares de seguridad en Tecnologías de Información.
2. Reducir el riesgo de pérdida y fuga de información en la Financiera mediante controles que aseguren la seguridad de información.
3. Cumplir con el mínimo de exigencias de la normativa de la SBS, en relación a la gestión de riesgos y seguridad de la información,

mejorando los procedimientos para identificar y definir los riesgos de TI.

4. Incrementar el nivel de concientización del personal en relación a la aplicabilidad de los controles/salvaguardas de TI en base a la ISO 27002.
5. Mejorar los procedimientos para identificar y evaluar los activos, determinando las amenazas, vulnerabilidades, salvaguardas, impactos y riesgos.
6. Elaborar el plan de seguridad basado en el estándar ISO 27002:2013, que permita a la entidad asegurar su gestión de riesgos.
7. Facilitar la aplicación del modelo propuesto, a personas que no necesariamente sean expertas en la gestión de riesgos de la seguridad de la información.
8. Desarrollar un software para la utilización del modelo implementado.

1.3 Justificación

El siguiente proyecto de tesis traerá consigo una serie de beneficios a la empresa, tal como que los responsables de los sistemas de información comprendan la existencia de riesgos y la necesidad de mitigarlos a tiempo, así mismo proporcionar un método para analizar los riesgos que se presenten y apoyar en la identificación y planificación de medidas oportunas para mantener los riegos controlados basándose en la norma ISO 27002:2013

Para el proyecto de Tesis se optó por trabajar con la metodología Magerit la cual permite el análisis y gestión de riesgos de los sistemas de información y al estar alineada con los estándares ISO es que se convierte en base para optar por una certificación y poder mejorar los sistemas de gestión; además Magerit a diferencia de otras metodologías tiene la capacidad de poder realizar un análisis cualitativo como cuantitativo de los riesgos, este último con el fin de realizar un cálculo financiero acerca de las posibles pérdidas al materializarse los riesgos. Esta metodología se basa en un análisis de dependencias lo que es fundamental para determinar la importancia de los activos frente a otros. Así mismo nos proporciona catálogos de elementos ya identificados, lo cual permite disminuir el tiempo de implementación ya que es aplicable en organizaciones grandes, medianas empresas y Pymes.

Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Existen recomendaciones de aplicación de calidad orientados a todo tipo de actividades, y por tanto proponer esta aplicación a la gestión de riesgos no sería la excepción, para lo cual el propósito de este trabajo es proponer un modelo práctico, que explique paso a paso cómo implantar un sistema de gestión aplicado a la gestión de riegos.

1.4 Alcances y Limitaciones de la investigación

1.4.1 Alcances

El desarrollo de la metodología y su implementación se circunscribe en la Financiera Arequipa S.A, ubicada en la provincia de Arequipa. Sin embargo, por tratarse de un modelo propuesto en base a normas, parte de este estudio podrá ser aplicable en otras organizaciones financieras.

El proceso de investigación utiliza recolección de datos de fuentes primarias (documentos de gestión que actualmente se utilizan en la Financiera), fuente secundarias (textos, documentos de gestión, revistas, publicaciones). Así como la realización y análisis de encuestas a los diferentes grupos de interés que estén involucrados en el proyecto.

El alcance del proyecto a desarrollar es:

- Elaboración y aplicación del modelo propuesto.
- Utilización del software desarrollado en base al modelo.
- Las empresas tomaran mejores decisiones respecto al tratamiento de los riesgos.

1.4.2 Limitaciones

- Que el personal no brinde información completa y veraz para el desarrollo del modelo.
- El modelo está diseñado para poder ser aplicado preferentemente en entidades financieras.
- Resistencia al cambio por parte del personal para el uso del software desarrollado.

CAPITULO II

FUNDAMENTOS TEÓRICOS

2.1 Estado del arte

En Lima, Perú en el año 2011 se llevó a cabo un proyecto donde se desarrolló un Sistema de Gestión de la Seguridad de la Información, el cual fue adaptado para poder ser implementado en instituciones financieras, con el fin de asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización. Se tomó como referencia el modelo de seguridad de información de Mc Cumber, este trabajo ayudo a la financiera donde se realizó el proyecto a contar con un sistema de gestión de la seguridad de la información que ayude a proteger la información que es el principal activo de toda organización. (Villena, 2011)

En la ciudad de México, en el año 2011, se desarrolló un proyecto de Tesis el cual estuvo centrado en la aplicación de la metodología Magerit basado en el análisis de riesgo del flujo de información para el área de gestión de una empresa dedicada a la aplicación de exámenes de control de confianza, lo que ayudo a la organización a saber cuáles son los riesgos a los que se encuentran expuestos sus principales activos y así protegerlos; mitigando los riesgos latentes, por medio de la aplicación de la metodología, y así poder seleccionar al personal adecuado que cumple con el perfil para poder realizar dichas labores. (Florentino, Morales, Peña, 2011).

En la ciudad de Cuenca, Ecuador se realizó un proyecto que consistió en realizar un análisis de riesgos de los sistemas de la cooperativa de ahorro y crédito de jardín azuayo, utilizando la metodología Magerit lo cual contribuyo a que la institución posea un conocimiento claro sobre los riesgos a los cuales están sometidos los sistemas de información y activos de la empresa, identificando las áreas críticas que requieran un mayor control, con el fin de mitigar el daño que puedan causar los factores internos o externos; lo cual ayudo a que la empresa esté preparada para poder tomar decisiones en relación a los riesgos a los que se encuentran expuestos en tiempos rápidos y oportunos. (Lucero, Valverde, 2011)

En la Ciudad de Guayaquil, Ecuador en el año 2015, se desarrolló un plan de gestión de riesgos de tecnología, que fue aplicado a la escuela superior politécnica del Litoral de Ecuador como proyecto de Tesis para obtener el título de Magister en la universidad politécnica de Madrid. Se aplicó la metodología Magerit, donde se procedió a describir la situación actual de la organización, luego a identificar los activos con sus respectivas amenazas, para proseguir a realizar la medición de riesgos existentes y sugerir las salvaguardas necesarias que podrían formar parte del plan de implantación. Se utilizó la herramienta PILAR, la cual soporta el análisis y gestión de los riesgos de sistemas de información aplicando la metodología Magerit, el trabajo tuvo como resultado mejoras en la gestión de riesgos y se mejoró la protección que tienen los activos frente a amenazas detectadas

En la ciudad de Lima, Perú en el año 2016 se desarrolló un sistema de gestión de la seguridad de la información basado en la ISO/IEC 27001:2013,

para una empresa de consultoría de software; la implementación del sistema permitió que los directivos y demás involucrados gestionen y tomen decisiones adecuadas respecto a la seguridad de información de la organización, con el fin de asegurar que se cuente con niveles adecuados y estandarizados respecto a la confidencialidad, integridad y disponibilidad de la información que se maneja como parte de las labores diarias de la organización , ayudando así a la mejora continua y propiciando un adecuado manejo de la seguridad de su información. (Santos, 2016).

En conclusión de los trabajos revisados sobre la implementación de la metodología Magerit y el manejo de sistemas de gestión de la seguridad de la información; se identificó que se aplica la metodología Magerit en diferentes instituciones y en el caso de instituciones financieras no se han considerado los requerimientos de la SBS (entidad reguladora de las empresas financieras). A su vez se utilizan salvaguardas que propone dicha metodología, sin utilizar los controles establecidos por la ISO 27002:2013, que son necesarios para poder manejar un adecuado SGSI basado en la ISO 27001:2013; realizando un doble trabajo y redundando en la información utilizada para proteger los activos.

Así mismo se notó que utilizan la herramienta PILAR para la implementación de la metodología Magerit, obteniendo valores que puedan ayudar a la alta dirección a la toma de decisiones con el fin de poder mejorar la gestión y el análisis de los riesgos

Siendo PILAR la única herramienta de software que puede soportar dicha metodología, se propuso la elaboración de un nuevo software siendo este muy intuitivo y fácil de usar.

2.2 Marco Teórico

2.2.1 Seguridad de Información

(Areitio, 2008) La seguridad de la información es un proceso en el que se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc; abarcando no solo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc.

Los objetivos principales de la seguridad son los siguientes:

a. **Disponibilidad y Accesibilidad de los Sistemas y Datos**, solo para su uso autorizado. Es un requisito necesario para garantizar que el sistema trabaje puntualmente, con prontitud y que no se deniegue el servicio a ningún usuario autorizado. La disponibilidad protege al sistema contra determinados problemas como los intentos deliberados o accidentales de realizar un borrado no autorizado de datos, de causar cualquier tipo de denegación del servicio o de acceso a los datos y de los intentos de utilizar el sistema o los datos para propósitos no autorizados. La disponibilidad frecuentemente, es uno de los objetivos de seguridad más importante de toda organización (Areitio, 2008).

b. **Integridad.** Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia. Presenta dos facetas (Areitio, 2008):

- Integridad de datos
- Integridad del sistema.

c. Confidencialidad de Datos y de la Información del Sistema. Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmiten y se encuentran en tránsito. Para muchas organizaciones, la confidencialidad se encuentra, frecuentemente, detrás de la disponibilidad y de la integridad, en términos de importancia. Para algunos sistemas y para tipos específicos de datos, como los autenticadores, la confidencialidad es de extrema importación (Areitio, 2008).

d. Responsabilidad a Nivel Individual. Es el requisito que permite que puedan trazarse las acciones de una entidad de forma única. A menudo, es un requisito de la política de la organización y soporta de forma directa el no repudio, la disuasión, el aislamiento de fallos, la detección y la prevención de intrusiones y, después, la acción de recuperación (Areitio, 2008).

e. Confiabilidad. Es la garantía en que los cuatro objetivos anteriores se han cumplido adecuadamente. Es la base de la confianza en que las medidas de seguridad, tanto técnicas, como operacionales, funcionan tal y como se idearon para proteger el sistema y la información que procesa (Areitio, 2008).

2.2.2 Sistemas de Información

Es un conjunto de recursos técnicos, humanos y económicos, interrelacionados dinámicamente, y organizados en torno al objetivo de satisfacer las necesidades de información de una organización empresarial para

la gestión y la correcta adopción de decisiones. (De Pablos, López, Romo, Medina, 2011)

De la definición anterior podemos señalar que los elementos o componentes fundamentales que constituyen un Sistema de Información empresarial actual son:

- La información, es decir todo lo capturado, almacenado, procesado y distribuidos por el sistema
- Las personas, quienes introducen y utilizan la información del sistema.
- Los equipos de tratamiento de la información e interacción con los usuarios, hardware, software y redes de comunicaciones
- Las normas y/o técnicas de trabajo, métodos utilizados por las personas y las tecnologías para desarrollar sus actividades (De Pablos et al., 2011).

2.2.3 Riesgos

(Areitio, 2008) en el nivel más simple, el proceso de gestión de riesgos, identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización. La gestión del riesgo es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado.

La valoración de riesgos es el proceso consistente en identificar los problemas antes de que aparezcan.

2.2.4 Aseguramiento

El proceso de aseguramiento en el libro de (Areitio, 2008), es un elemento muy importante de la ingeniería de seguridad que se define como el grado de confianza que satisfacen los requisitos de seguridad.

El aseguramiento no añade ningún control adicional al cálculo de riesgos relacionados con la seguridad, pero proporciona la confianza en que las salvaguardas implementadas reducirán el riesgo anticipado.

2.2.5 Magerit

Magerit. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Magerit persigue los siguientes objetivos Magerit. (2012):

Directos:

a) concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

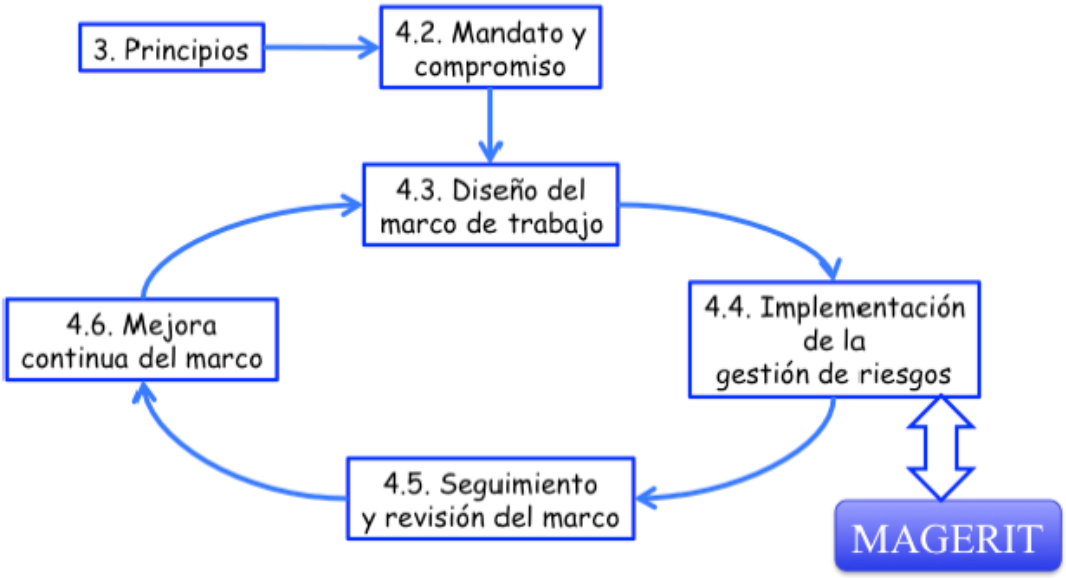
b) ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

c) ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

a) preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Figura 1. ISO 31000 – Marco de Trabajo para la gestión de riesgos



Fuente: Magerit (2012)

2.2.6 Activos

Areitio (2008) Un activo es un componente o una parte de un sistema global al que a la que la organización asigna un valor, por lo tanto, que requiere protección.

Para la identificación de los activos se debe tener en cuenta que un sistema de información consta de más elementos además del hardware y software: Posibles activos a identificar

- Activo de TIC: hardware, software, información
- Personal: empleados, invitados, como el personal externo, auditores externos, subcontratados o usuarios de empresas de externalización
- Entorno: edificios, instalaciones.
- Actividades: operaciones.

2.2.7 Amenazas

(Aguilera, 2010) Se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad, atacarían al sistema produciendo daños aprovechándose de su nivel de vulnerabilidad.

Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos de hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso o el robo, destrucción o modificación de la información.

2.2.8 Riesgos

(Aguilera, 2010) Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad, ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño. La dirección de la empresa es por lo general quien determina los niveles de riesgo que puedes ser asumidos por las diferentes áreas.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (por ejemplo, contratando un seguro).

2.2.9 Vulnerabilidades

(Aguilera, 2010) Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas.

Por ejemplo: Los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

2.2.10 Impacto

(Aguilera, 2010) Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o dicho de otra manera, el daño causado.

Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

2.2.11 Circular G140-2009-SBS

Villena. M (2011). La circular G-140-2009-SBS, elaborada en abril del 2009 por la SBS, obliga a las entidades financieras que son reguladas por este organismo a establecer, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI) tomando como referencia la ISO 17799 e ISO 27001. El objetivo de implementar el SGSI es de brindar seguridad a los activos de información más importantes como resultado del análisis de riesgo y sobre todo cumpliendo con las expectativas de todos los interesados del sistema, clientes, comunidad, estado, proveedores, y la misma entidad financiera entre otros. Los controles con los que cuenta la circular, son los siguientes:

- ✓ Seguridad lógica
- ✓ Seguridad de personal
- ✓ Seguridad física y ambiental
- ✓ Inventario de activos y clasificación de la información
- ✓ Administración de las operaciones y comunicaciones
- ✓ Adquisición, desarrollo y mantenimiento de sistemas informáticos
- ✓ Procedimientos de respaldo
- ✓ Gestión de incidentes de seguridad de información.
- ✓ Cumplimiento normativo
- ✓ Privacidad de Información

2.2.12 Calidad

El diccionario de la Real Academia Española define el concepto de calidad como la propiedad o conjunto de propiedades inherentes a una cosa que permite apreciarla como igual, mejor o peor que las restantes de su misma especie. Esta definición muestra las dos características esenciales del término. De un parte, la subjetividad de su valoración: de otra, su relatividad. No es una cualidad absoluta que se posee o no se posee, sino un atributo relativo: se tiene más o menos calidad.

2.2.13 ISO 31000

IsoTools. (2016) La ISO 31000 es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones.

Esta norma fue publicada en noviembre del 2009 por la Organización Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los riesgos en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de riesgos en cada una de sus actividades.

Como complemento a esta norma se ha desarrollado otro estándar: la ISO 31010 “Gestión del riesgo. Técnicas de evaluación de riesgos”. Esta norma provee de una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.

2.2.14 ISO 27002

Welive Security. (2013). La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799, la cual se basaba en un documento publicado por el gobierno del Reino Unido, que se convirtió en estándar en 1995. Fue en el 2000 cuando se publicó por primera vez como ISO 17799, y en 2005 aparece una nueva versión, junto con la publicación de la norma ISO 27001. No debe olvidarse que estos dos documentos están destinados a ser utilizados de forma complementaria.

Dentro de ISO/IEC 27002 se extiende la información de los renovados anexos de ISO/IEC 27001-2013, donde básicamente se describen los dominios de control y los mecanismos de control, que pueden ser implementados dentro de una organización, siguiendo las directrices de ISO 27001.

En esta nueva versión de la norma se encuentran:

- 14 dominios
- 35 objetivos de control
- 114 controles

Los controles buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales se encuentra expuesta la organización y minimizar el daño que puedan sufrir los activos, que puedan ocasionar la serie de amenazas a las cuales se encuentran expuestos.

Con la actualización de esta norma las organizaciones pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información.

2.2.15 Cuadro comparativo de la Metodología MAGERIT y OCTAVE

Tabla 1. Cuadro comparativo entre la metodología Magerit y la metodología Octave

MAGERIT	OCTAVE
Se enfatiza en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contra medidas para evitar así cualquier inconveniente.	Es una técnica de planificación y Consultoría estratégica en seguridad basada en el riesgo.
Ofrece un método sistemático para analizar tales riesgos.	Maneja tres métodos: auto-dirigido, flexibles y evolucionado.
Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.	Desmitifica la falsa creencia: La Seguridad Informática es un asunto meramente técnico.
Prepara a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.	Presenta los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.
Concientiza a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.	Divide los activos en dos tipos: sistemas, (Hardware. Software y Datos) y personas.
Genera el uso de las tecnologías de la información.	Se especializa en el riesgo organizacional y el foco son los temas relativos a la estrategia y la practica.
Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema	Consolidación de la información y creación de perfiles de amenazas.
Relación de las amenazas a que están expuestos los activos.	Identifica los elementos críticos y las amenazas para los activos.

Fuente: Rios. P (2012)

CAPITULO III

PRESENTACIÓN DEL PROYECTO

3.1 Resumen del Proyecto

DISEÑO DE UN MODELO SISTÉMICO DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN, INTEGRANDO LA METODOLOGÍA MAGERIT Y LA NORMA ISO 27002:2013 EN EMPRESAS FINANCIERAS.

3.1.1 Descripción del Proyecto a Medio y Largo Plazo

El modelo propuesto permitirá que cualquier colaborador que esté ligado al área de Tecnologías de Información, sin necesidad de que este sea especialista en el análisis de riesgos pueda identificar de manera rápida, sencilla y eficaz los riesgos a los que están expuestos los activos de las entidades financieras; así mismo le permitirá implementar las medidas necesarias para hacer frente a estos riesgos siguiendo estándares ligados a la seguridad de la información; y así poder realizar una buena toma de decisiones de cómo hacer frente a estos riesgos.

La implementación del modelo propuesto le permitirá a la entidad financiera desarrollar una ventaja competitiva volviéndola más eficiente, fortaleciendo sus procesos internos y así contar con una base robusta para alcanzar certificaciones en los estándares ISO 31000 e ISO 27001.

3.1.2 Usuarios del Proyecto

El modelo propuesto está enfocado a utilizarse por el personal de Tecnologías de Información, en especial está destinado para los colaboradores que estén vinculados con las áreas de Riesgos y Seguridad de la información de empresas financieras y que sus labores diarias estén ligadas a estas; las cuales se ven expuestas a constantes amenazas y están fuertemente ligadas a procesos de Tecnologías de Información.

3.1.3 Beneficios

- ✓ Asegurar la continuidad operacional del negocio.
- ✓ Implementar medidas prácticas que permitan mitigar los riesgos encontrados.
- ✓ Tomar las mejores decisiones en inversiones para la optimizar la seguridad de la información.
- ✓ Implementar un adecuado modelo de Gestión de Riesgos para la Seguridad de la Información.
- ✓ Desarrollar ventaja competitiva volviendo la empresa más eficiente en el manejo de Gestión de Riesgos.
- ✓ Llevar un adecuado control y seguimiento de las mejoras hechas en base a los controles de la ISO 27002:2013.
- ✓ Fortalecer los procesos internos de la empresa en cuanto a Gestión de Riesgos y así contar con una base robusta para alcanzar certificaciones en los estándares ISO 31000 e ISO 27001.

3.1.4 Localización

La localización de la implementación de este modelo sistémico estará localizada en el área de Entrega de Servicios de T.I. (Infraestructura de Servidores, Redes y Telecomunicaciones, Tecnologías Cliente) de la empresa "Financiera Arequipa"

3.1.5 Impacto y Sostenibilidad del Proyecto

La implementación del modelo permitirá al área de Riesgos no Financieros robustecer el proceso de identificación y análisis de los riesgos, así como también el desarrollo de un modelo de gestión de riesgos altamente eficaz, caracterizado por su simplicidad de implementación, ayudando a mejorar los niveles de madurez asociados a la ISO 27002:2013.

3.1.6 Riesgos que debemos afrontar

Económicos:

- Designar a personal exclusivo a tiempo completo por parte de la empresa para la implementación del modelo.

Competencia:

- Resistencia al cambio, pues la actual área ya cuenta con procesos definidos para el análisis de los riesgos.
- Falta de compromiso del personal para lograr la implementación del modelo sistémico.

Tecnológicos:

- No aplica.

No Tecnológicos:

- Restricción de acceso a la información para realizar el análisis de los riesgos.

3.2 Plan de Implantación del Proyecto

3.2.1 Definición del Proyecto

Puesta en aplicación del modelo de gestión de riesgos, aplicando la metodología MAGERIT y la norma 27002:2013.

3.2.1.1 Técnicos

Los tesistas poseen experiencia laboral en áreas de Tecnologías de la información donde se llevan a cabo labores en torno a la gestión de riesgos y tratamiento de normas ISO.

3.2.1.2 Aspectos Económicos

Para el desarrollo de la herramienta se necesitó contratar un plan de dominio y hosting, con el fin de poder tener la herramienta disponible en un ambiente web, los costos de los planes contratados se detallan a continuación:

- Dominio = S/. 29.25
- Hosting = S/.117.00
- Capacidad = 250 Mb
- Subdominios = 100
- Velocidad Alta

3.2.1.3 Aspectos Comerciales

En cuanto a los aspectos comerciales, el presente proyecto permitirá que las empresas financieras se vean beneficiadas con la implementación de este modelo sistémico, pues proporciona una fácil compresión y aplicación de la gestión de riesgos en todas las empresas de este rubro; la implementación del modelo generará ventaja competitiva pues la adecuada gestión de los riesgos volverá más confiable a la empresa; así como la utilización de la herramienta desarrollada que permitirá tener toda la información disponible cuando se necesario.

3.2.1.4 Recursos del Proyecto

En cuanto a los recursos necesarios para la ejecución del proyecto, se requiere la participación activa de todos los colaboradores del área de Entrega de Servicios de Tecnologías de Información quienes participarán brindando la información necesaria acerca de los activos analizados y 02 personas que se encargarán de implementación del modelo sistémico de gestión de riesgos y el desarrollo de la herramienta de soporte, aplicando a su vez la mejora continua de los procesos.

CAPITULO IV

DESARROLLO DE LA PROPUESTA

4.1 Resumen del Esquema

El siguiente modelo se desarrolló en base a un análisis de interrelación entre la Metodología Magerit y la ISO 27002:2013. Lo que nos permitió identificar la mejor manera de recopilar y tratar la información para una adecuada implementación del modelo de Gestión de Riesgos.

Se realizara un análisis cualitativo de riesgos el cual consiste en priorizar los riesgos, evaluando la probabilidad de ocurrencia y el impacto de los riesgos. El resultado de este análisis sirve para poder definir la respuesta a los riesgos, y a su vez poder definir los plazos de respuesta y la tolerancia al riesgo que la organización pueda asumir. Para el modelo propuesto se tomó en cuenta las exigencias mínimas establecidas por la SBS, para entidades financieras en cuanto a la seguridad de la información.

A su vez en el análisis cualitativo se definen escalas las cuales permiten avanzar con el análisis de una manera más rápida y eficaz, tomando valores en un orden relativo respecto a los demás. Este análisis sienta las condiciones para realizar un análisis cuantitativo de riesgos.

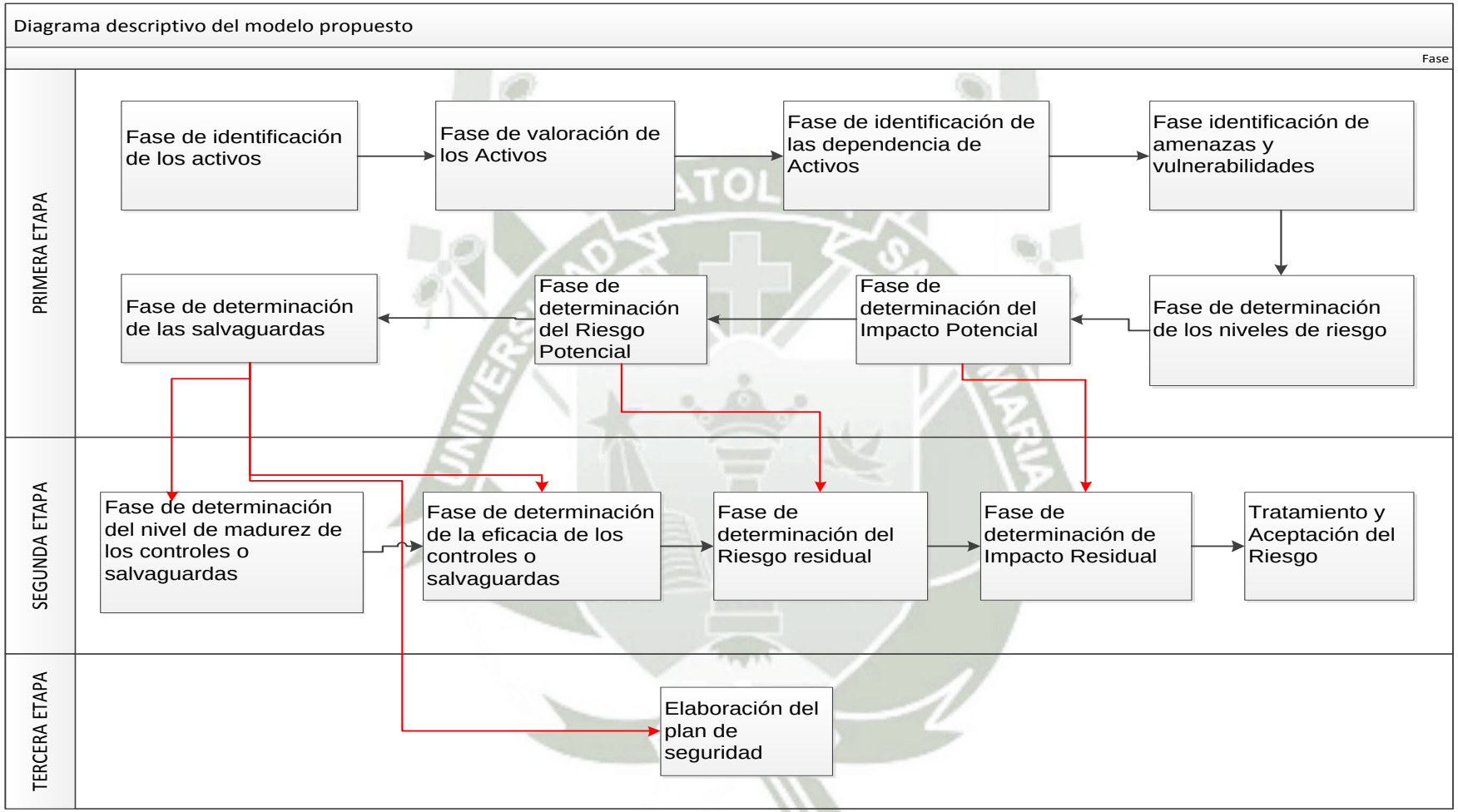
Se tiene que tomar en cuenta que el análisis de riesgos cualitativos requiere que se utilicen métodos para poder evaluar la probabilidad y las consecuencias que traen consigo los riesgos.

A continuación se detallan las etapas propuestas en el modelo:

4.2 Modelo Propuesto para la Gestión de Riesgos

1. **Primera Etapa: Identificación y Análisis del Riesgo**
   - 1.1 Fase de Identificación de los Activos
   - 1.2 Fase de Valoración de los Activos
   - 1.3 Fase de Identificación de las Dependencias de los Activos
   - 1.4 Fase de Identificación de Amenazas y Vulnerabilidades
   - 1.5 Fase de Valorización de Amenazas
   - 1.6 Fase de Determinación de los Niveles de Riesgo
   - 1.7 Fase de Determinación del Impacto Potencial
     - Impacto Acumulado
   - 1.8 Fase de Determinación del Riesgo Potencial
     - Riesgo Acumulado
   - 1.9 Fase de Determinación de las Salvaguardas
2. **Segunda Etapa: Gestión de los Riesgos**
   - 2.1 Fase de Determinación del Nivel de Madurez de los Controles o Salvaguardas
   - 2.2 Fase de Determinación de la eficacia de los Controles o Salvaguardas
   - 2.3 Fase de Determinación del Impacto Residual
   - 2.4 Fase de Determinación de Riesgo Residual
   - 2.5 Tratamiento y Aceptación del Riesgo
3. **Tercera etapa: Elaboración del Plan de Seguridad**
   - 3.1 Implementación del plan seguridad
   - 3.2 Cumplimiento y Mejora continua del Plan de Seguridad

Figura 2.Diagrama descriptivo del modelo



Fuente: Elaboración propia

4.3 Desarrollo de las etapas del Modelo de Gestión de Riesgos

<table>
<tr><td colspan="2">1. Primera Etapa: Análisis del riesgo</td></tr>
<tr><td colspan="2">1.1 Fase de Identificación de los Activos

La identificación de los activos de T.I. permitirá evaluar de manera eficaz todos los componentes críticos e identificar las relaciones que existen entre estos dentro de la Organización, además nos permitirá determinar la criticidad de estos. Es el punto de partida para realizar una adecuada gestión de riesgos, con el fin de poder proteger los activos de cualquier amenaza identificada.</td></tr>
<tr><td colspan="2">DATOS DE ENTRADA</td></tr>
<tr><td colspan="2">• Organigrama del área de T.I.
• Información de inventario activos gestionados por T.I.
• Información recopilada en entrevistas con encargados de los activos.</td></tr>
<tr><td colspan="2">ACTIVIDADES</td></tr>
<tr><td>Verificación de Información existente que pueda ser usada en el proyecto.</td><td>(Van, 2008) Los riesgos para los activos de información se deberían evaluar en función de:
1. su naturaleza (por ejemplo: funcionamiento defectuoso del software, errores de operación, fallos de comunicación)
2. probabilidad
3. impacto potencial para el negocio
4. experiencias pasadas</td></tr>
</table>

DATOS DE SALIDA
• Listado de activos de T.I. identificados. • Listado de los responsables de los activos de T.I. • Función que cumplen los activos en la Organización.

1.2 Fase de Valoración de los Activos

Cuando ya se tienen identificados los activos se procede a valorar los mismos, para lo cual se deben identificar las dimensiones por las cuales se llevará el análisis de valoración y los criterios para los activos, al momento de valorar un activo se determina cuan prescindible es para la organización, en caso de que no tenga valor simplemente no genera ningún bien dentro de la organización, cuanto más valioso es un activo, mayor es el nivel de protección que se le debe de dar.

DATOS DE ENTRADA	
• Listado de activos generados.	
ACTIVIDADES	
Identificación de la criticidad de los activos	• Entreviste a los responsables directos de los servicios brindados por los activos, quienes tienen conocimiento de las funciones de estos y fallas de seguridad a las cuales están expuestos.
Valoración unitaria de los activos	• Utilice las siguientes dimensiones para la valoración: ○ Confidencialidad ○ Integridad

- Disponibilidad
- Autenticidad
- Trazabilidad

- Determine el valor que le corresponde a cada activo identificado utilizando la siguiente matriz de valoración:

Tabla 2. Matriz de valoración de activos

Valor	Rango	Criterio
Extremo	10	Daño extremadamente grave
Muy alto	8-9	Daño muy grave
Alto	6-7	Daño grave
Medio	3-5	Daño importante
Bajo	1-2	Daño menor
Despreciable	0	Irrelevante a efectos prácticos

Fuente: Magerit (2012)

Donde:

0: No representa un activo con valor para la Empresa.

10: Representa un activo con máximo valor para la Empresa.

DATOS DE SALIDA

- Listado de valoración unitaria de activos de T.I.

1.3 Fase de identificación de las Dependencia de Activos

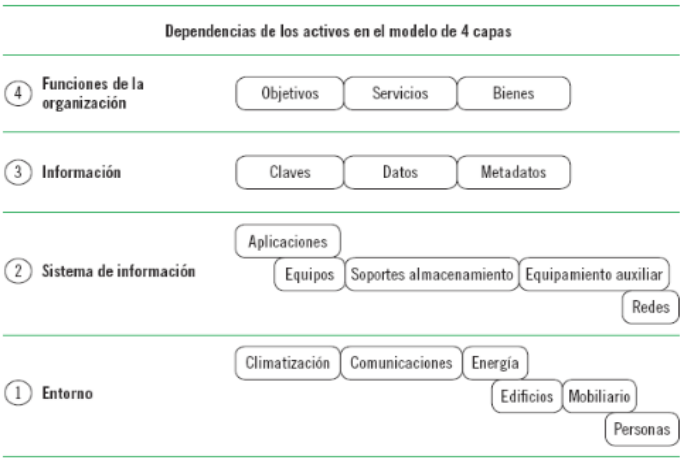
DATOS DE ENTRADA

- Resultados de la identificación de los activos
- Diagramas de flujo
- Topologías de red
- Encuestas a los propietarios de los activos

<table>
<tr><th colspan="2">ACTIVIDADES</th></tr>
<tr><td>Identificar las dependencias entre activos</td><td>

- Verificar la dependencia entre los diferentes activos identificados dentro de la organización, para saber cuál es la dependencia que tienen con otros activos ya sean de nivel superior o inferior
- Se trabajara con un nivel de porcentaje de 0% y 100% con el fin de determinar si existe dependencia alguna para determinar si son activos totalmente independientes (0%) y activos totalmente dependientes (100%)
- Utilice el siguiente diagrama para conseguir una mejor identificación del grado de dependencia entre los activos:

Figura 3. Dependencia de los activos en el modelo de 4 capas



Fuente: Giménez (2014)

- Diagrame grafos los cuales le permita identificar la dependencia entre los activos; teniendo en cuenta que los activos que se encuentran en estas estructuras reflejan de

</td></tr>
</table>

	arriba hacia abajo las dependencias; mientras que de abajo hacia arriba reflejan la propagación del daño.
Obtención del Valor Acumulado del Activo	El valor acumulado de un activo se considera como el mayor valor entre el propio y el de cualquiera que dependen de él. Para determinar el valor acumulado utilice el diagrama de dependencia de activos y aplique la siguiente formula: VA = Valor Acumulado valor_acumulado(B) = max (valor(B), maxi {valor(Ai)}) Se tiene que tener en cuenta lo siguiente: • El nodo padre depende para su funcionamiento del nodo hijo y/o necesita de el para un correcto funcionamiento. • El nodo hijo hereda el valor del nodo padre
DATOS DE SALIDA	
• Diagrama de dependencia entre activos • Valor Acumulado de los Activos	

1.4 Fase Identificación de Amenazas y vulnerabilidades Posterior a la identificación de los activos, se procede a la identificación de las amenazas que puedan afectar a los activos, por cada activo se consideran una serie de amenazas que pueden afectar a dichos activos
DATOS DE ENTRADA
• Listado de activos generados.

• Catálogo de amenazas detallado en el anexo B generado en base a Magerit.	
ACTIVIDADES	
Identificación de Amenazas	• Adicione al catálogo otras amenazas identificadas dentro de la organización.
Identificación de Vulnerabilidades	• Utilice las vulnerabilidades encontradas por los propietarios de los activos, así como los expertos que tienen amplio conocimiento del tema.
DATOS DE SALIDA	
• Listado del catálogo de amenazas y vulnerabilidades detallada por activo.	

1.5 Valorización de amenazas Cuando ya se tienen identificados los activos y las amenazas a las que se encuentran expuestos se tiene que valorar la influencia en el valor del activo.	
DATOS DE ENTRADA	
• Listado de amenazas y vulnerabilidades	
ACTIVIDADES	
Valorización de Amenazas	• Utilice las siguientes matrices para valorar la influencia de la amenaza en el valor del activo. **Degradación**: Mide el daño causado por un incidente respecto a los activos.

Tabla 3. Degradación del valor

Nivel	Degradación	Daño	Verbalizado
MA	99% - 100%	Muy alto	Casi seguro
A	75% - 98%	Alto	Muy alta
M	50% - 74%	Medio	Posible
B	25% - 49%	Bajo	Poco probable
CB	10% - 24%	Casi bajo	Poco probable
MB	1% - 9%	Muy bajo	Raro

Fuente Magerit (2012)

Probabilidad: Cuan probable es que se materialice la amenaza.

Tabla 4. Probabilidad de ocurrencia

Nivel	Verbalizando	Probabilidad	Frecuencia
5	Casi segura, Muy alta	80%-100%	Más de una vez al mes
4	Grande, muy probable	60%-79%	De 6 a 12 veces cada 12 meses
3	Probable	40%-59%	Más de 2 a menos de 6 veces cada 12 meses
2	Pequeña, poco probable	20%-39%	Más de 1 a 2 veces cada 12 meses
1	Remota, Mínima	1%-19%	De 0 a 1 vez cada 12 meses

Fuente: Magerit (2012)

DATOS DE SALIDA

- Listado de valorización de amenazas detallada por activo.

1.6 Fase de Determinación del Impacto Potencial

El impacto se considera como el daño que afecta a un activo derivado de la materialización de una amenaza, teniendo los resultados de la valoración

de activos y la degradación, es necesario medir el impacto que estos pueden causar sobre el sistema.

En el modelo propuesto se considerará el impacto acumulado y el impacto residual.

Tabla 5. Matriz Impacto Potencial

Degradación	Impacto										
	Valor del activo										
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
100%	[-]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
75%	[-]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
50%	[-]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
25%	[-]	[0]	[0]	[0]	[0]	[3]	[4]	[5]	[6]	[7]	[8]
10%	[-]	[0]	[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
1%	[-]	[0]	[0]	[0]	[0]	[0]	[0]	[1]	[2]	[3]	[4]

Fuente: Elaboración propia

- **Impacto Acumulado**

Es el calculado sobre un activo teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto el activo. A su vez sirve para determinar qué ocurriría si es que un activo que se encuentra en un nivel inferior cayese, lo cual nos sirve para poder definir las salvaguardas.

DATOS DE ENTRADA

- Listado de la valorización de los activos
- Valor acumulado del activo
- Degradación que le provocaría la amenaza

ACTIVIDADES

Obtención del Impacto Acumulado	Al realizar un análisis cualitativo se utilizara la tabla definida en el impacto potencial, con el fin de poder identificar el impacto acumulado en base al valor acumulado de los activos

	y la degradación que puede causar la materialización de una amenaza, cabe recalcar que estos valores se calcularan por cada dimensión en las cuales las amenazas fueron valorizadas por medio de la degradación que puedan ocasionar.
DATOS DE SALIDA	
• Impacto acumulado por cada activo.	

1.7 Determinación de los niveles de riesgo

Los niveles de riesgo se calculan a través de la probabilidad por el nivel del impacto y según el valor final se obtiene el nivel del riesgo, los cuales se categorizan de la siguiente manera.

Tabla 6. Matriz Riesgo Potencial

		Riesgo									
		[1]	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**	**[8]**	**[9]**	**[10]**
Probabilidad	**5**	M	M	A	A	A	A	E	E	E	E
	4	M	M	M	A	A	A	A	E	E	E
	3	B	M	M	M	M	A	A	A	A	E
	2	B	B	B	M	M	M	A	A	A	A
	1	B	B	B	B	M	M	M	M	A	A

Fuente: Elaboración Propia

Tabla 7. Definición Niveles de Riesgo

Nivel	Abreviatura	Descripción
Extremo	E	Atención inmediata
Alto	A	Bajo responsabilidad de las Gerencias
Medio	M	Bajo responsabilidad de las Jefaturas
Bajo	B	Evaluados en procesos rutinarios

Fuente: Elaboración Propia

1.8 Determinación del Riesgo Potencial

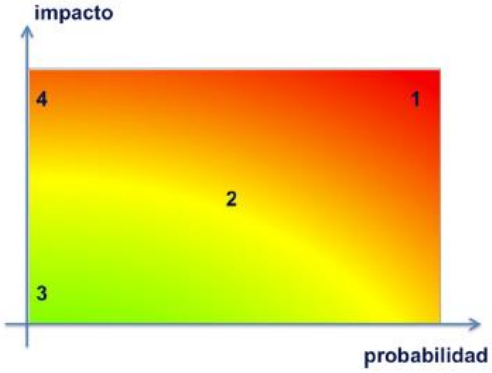
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto
- zona 4 – riesgos improbables, pero de muy alto impacto

Fuente: Magerit (2012)

Figura 4. Riesgo en función del impacto y probabilidad



Fuente: Magerit (2012)

- **Riesgo acumulado**

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza. Además permite determinar las salvaguardas de que hay que dotar a los activos con el fin de reducir el riesgo a los que están sujetos los activos.

DATOS DE ENTRADA

- Impacto acumulado de los activos
- Probabilidad de ocurrencia de las amenazas

ACTIVIDADES

Obtención del Riesgo Acumulado	Se calcula sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a la materialización de una amenaza y la probabilidad de ocurrencia de la amenaza. El cálculo se realiza en cada dimensión en las que los activos fueron valorizados.

Para determinar la probabilidad de amenaza utilice:

Probabilidad que el riesgo ocurra dentro de los próximos 12 meses basado en un puntaje de 1 a 5 en base a la experiencia humana de la gestión del riesgo y la intuición del área encargada de la evaluación.

Para determinar el valor del riesgo se utilizara la siguiente tabla:

Tabla 8. Matriz de Riesgos

		Impacto									
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Probabilidad	5	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)	(5,7)	(5,8)	(5,9)	(5,10)
	4	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)	(4,7)	(4,8)	(4,9)	(4,10)
	3	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)	(3,10)
	2	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)	(2,9)	(2,10)
	1	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)	(1,10)

Fuente: Elaboración Propia

DATOS DE SALIDA

- Riesgo Acumulado por Activo

2. Segunda etapa: Gestión de los riesgos

2.1 Fase de determinación de las Salvaguardas

Se deben determinar las salvaguardas o contramedidas que ayudan a reducir el riesgo, se utilizaran como salvaguardas los controles establecidos en la ISO 27002:2013 y los requisitos mínimos que establece la circular N° G-140-2009 para lo cual se realizó una matriz de análisis entre la circular y la ISO 27002:2013.

DATOS DE ENTRADA	
• Listado de controles otorgados por la ISO 27002 • Listado de amenazas y vulnerabilidades encontrados	
ACTIVIDADES	
Determinación de las salvaguardas	Luego que se identificaron las amenazas y las vulnerabilidades a las cuales están sometidos los activos, se procederá a identificar las salvaguardas; se utilizaran los controles de la ISO 27002:2013 seleccionados que se ajusten a las necesidades de las empresas financieras, de acuerdo a los tipos de activos con los que cuenten para contrarrestar el daño que puedan ser generados por las amenazas identificadas.
Determinación de la eficacia de la salvaguarda	Es necesario definir cuan eficaz es una salvaguarda para saber cuál es el nivel de protección que puede brindar a los activos frente al riesgo presentado. Una salvaguarda ideal es la que tiene un 100% de eficacia y se califica con 0% a la que no existe aún. A continuación se presenta el factor de porcentaje para determinar la eficacia de los controles o salvaguardas.

Determinación de la eficacia de las salvaguardas

Tabla 9. Eficacia de las salvaguardas

Factor - Rango	Significado
96% - 100%	Optimizado
91% - 95%	Gestionado y medible
51% - 90%	Proceso definido
11% - 50%	Reproducible pero intuitivo
1% - 10%	Inicial / adoc
0%	Inexistente

Fuente: Magerit (2012)

Se pueden usar una o más salvaguardas por activo, para hallar la eficacia total se realizara una sumatoria de los porcentajes establecidos en cada salvaguarda y se divide entre el número total de salvaguardas detectadas por amenaza.

Eficacia_Real = Σ del % total de salvaguardas / # de salvaguardas

DATOS DE SALIDA

- Controles o salvaguardas elegidos.
- Listado de Salvaguardas por activo.
- Salvaguardas valorizados por activo

2.2. Fase de Determinación del Nivel de Madurez de los Controles o Salvaguardas

En la evaluación se han establecido 5 niveles que servirán para medir cuan desarrollados se encuentran los controles basados en la ISO 27002:2013 en la organización, la evaluación se realizara con las personas encargadas del área de seguridad de la información en el caso de que la empresa contara con un plan de seguridad ya establecido, caso contrario se sugiere empezar a elaborar dicho plan en base a los controles que nos otorga la ISO 27002:2013. La determinación del nivel de madurez puede variar entre 30 minutos y 180 minutos dependiendo del tamaño de la organización.

Se estableció la siguiente tabla para poder determinar el nivel de madurez de cada uno de los procesos.

Tabla 10. Niveles de madurez

Nivel de Madurez	Nivel	Descripción
No existe	1	0%
Procesos Ad-hoc y desorganizados	2	1% - 40%
Procesos están documentados y comunicados	3	41% - 99%
Procesos se monitorizan y se miden	4	100%
Procesos se mejoran y optimizan	5	100% se evalúa y se hace mejoras

Fuente: Elaboración Propia

Se tiene que seleccionar el nivel de madurez más próximo a la realidad de la organización, con el fin de tener un control de cómo va el desarrollo de la misma.

2.3 Fase de Determinación del Impacto Residual

El impacto residual nos indica el impacto luego de implementar las salvaguardas para cada activo, modificado el desde un valor potencial a un valor residual. Las salvaguardas implementadas en el modelo estarán dadas por los controles que nos otorga la ISO 27002:2013 y que están alineadas con los requisitos mínimos establecidos por la SBS en el rubro de las entidades financieras.

DATOS DE ENTRADA
• Listado de la valoración de los activos • Nueva degradación que provocaría la amenaza • Eficacia de la Salvaguarda

ACTIVIDADES	
Obtención del Impacto Residual	El cálculo para el impacto residual se da por el nuevo valor de la degradación de la amenaza, ya que se ve mejorada debido a la eficacia de las salvaguardas o controles que fueron seleccionados para mitigar el daño producido por dichas amenazas, estas salvaguardas o controles están basados en la norma ISO 27002:2013.. Se utilizara la matriz definida para el cálculo del impacto potencial utilizando los valores en relación a la nueva degradación hallada y al valor del activo.

DATOS DE SALIDA
• Impacto residual por cada activo.

2.4 Fase de Determinación del Riesgo Residual

Seguidamente que se desplegaron las salvaguardas el sistema queda en una situación de riesgo que se denomina residual, modificando el riesgo, desde un valor potencial a un valor residual.

DATOS DE ENTRADA	
• Listado de la valoración de los activos • Impacto residual del activo • Probabilidad de ocurrencia de la amenaza	
ACTIVIDADES	
Obtención del Impacto Residual	Ya que solo se ha cambiado la degradación de la amenaza que se consideró para hacer el cálculo del impacto residual mejorando la frecuencia de la amenaza, el riesgo residual se calcula teniendo en cuenta el impacto residual sobre un activo debido a una amenaza y la probabilidad de ocurrencia de la amenaza que se ve mejorado, teniendo en cuenta que las salvaguardas fueron desplegadas mejorando el nivel de protección de los activos. El cálculo se realiza en cada dimensión en las que los activos fueron valorizados, utilizando la matriz definida en la determinación del riesgo potencial.
DATOS DE SALIDA	
• Riesgo residual por cada activo.	

2.5 Tratamiento y Aceptación del Riesgo

La Dirección de la Organización es quien debe determinar el nivel de impacto y riesgo aceptable aceptando las responsabilidades de las insuficiencias.

- Se pueden tener presentes los siguientes criterios de aceptación del riesgo los cuales pueden diferir en diferentes aspectos:
  - Criterios del negocio
  - Operaciones
  - Tecnológica
  - Finanzas
  - Factores sociales y humanos
- Cualquier nivel de impacto y/o riesgo es aceptable si la gerencia o la dirección lo conoce y acepta formalmente; siempre es arriesgada y hay que tomarla con prudencia y justificación.
- Se establece un periodo máximo de 3 meses para que un riesgo permanezca en un nivel extremo, el cual puede ser ampliado en caso de ser solicitado por el directorio de la financiera a un plazo máximo de 6 meses.
- La documentación de la misma debe ser revisada cada 12 meses, a través de un proceso de auditoría.

Las opciones del tratamiento de riesgos son los siguientes:

Tratamiento	**Descripción**
Aceptar	El riesgo es aceptable cuando: • No es posible desarrollar un control adecuado para el tratamiento de los riesgos. • El costo de la implementación del control es mayor al costo de que se concrete el riesgo. • El nivel de riesgo se encuentra dentro del apetito del riesgo.
Mitigar	El riesgo se debe mitigar cuando: • Se busca reducir la probabilidad o el impacto del riesgo para reducir el riesgo a un nivel aceptable o hasta que desaparezca por completo.
Transferir	El riesgo de debe transferir cuando: • No se cuente con los recursos suficientes para poder atacar el riesgo por lo que se trasfiere o comparte a través de un asegurador que sea capaz de tratar el riesgo.

- Los niveles de aceptación del riesgo serán los niveles medio y bajo, en los casos de niveles extremos y altos estos se deben reducir a niveles medio y bajos, en los plazo establecidos.

- Se deben reducir o mitigar los riesgos que se encuentren en un nivel alto y extremo, las excepciones a estos casos deben ser asumidas por la gerencia o la dirección de la empresa bajo toda responsabilidad.
- Se considerara un riesgo crítico a los valores que den como resultado un nivel de riesgo extremo, los cuales deben ser una prioridad al momento de ser tratados.

3. Tercera etapa: Elaboración del Plan de Seguridad

3.1 Implementación del plan seguridad en base a la norma ISO 27002:2013

En esta fase se trata de llevar a cabo los planes de seguridad, de acuerdo a las decisiones acogidas para el tratamiento de los riesgos.

Un programa de seguridad es una agrupación de tareas, la cual se la realiza según la conveniencia de la organización, en este modelo que se propone se adoptan los dominios de seguridad establecidos en la ISO 27002:2013, pues estos engloban todos los activos de información que interesa proteger.

El punto de partida para el desarrollo del plan de seguridad será la implementación de una política de seguridad, que es un documento de alto nivel firmado por la persona con el cargo de mayor nivel en la empresa. Una vez firmado, la política de seguridad tiene que ser publicada, con el fin de que todo el personal de la empresa pueda tener acceso a ella, una de las formas más comunes de difundirla es colocándola en la intranet de la empresa .

Para definir que dominios, objetivos de control y controles se utilizaran, dependerán de las decisiones de la organización basándose en los criterios de

aceptación de riesgos, las opciones de tratamiento y el enfoque general de gestión de riesgos.

Los dominios a desarrollar según el presente modelo se han seleccionado en base a las necesidades del área de tecnologías de información lo cual contribuirá a la mejora de la gestión de riesgos de la SGSI, los cuales se detallan a continuación.

Tabla 11. Tabla de dominios - ISO 27002:2013

Dominios establecidos por la ISO 27002:2013
1. Políticas de Seguridad.
2. Seguridad ligada a los Recursos Humanos.
3. Gestión de Activos.
4. Control de Accesos.
5. Cifrado.
6. Seguridad física y ambiental.
7. Seguridad en la operativa.
8. Seguridad en las telecomunicaciones.
9. Adquisición, desarrollo y mantenimiento de los sistemas de información.
10. Relaciones con los suministradores
11. Gestión de incidentes en la seguridad de la información
12. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
13. Cumplimiento.

Fuente: ISO 27002:2013

3.2. Cumplimiento y Mejora continua del Plan de Seguridad

- **Elaboración de Solicitudes de Acción Correctivas y de Mejora (SAC y SAM)**

Estas Solicitudes no cuestionan las actividades de un proceso ni tampoco a las personas que las desarrollan, sino más bien nos sirven para corregir, prevenir o mejorar los procesos y otros; con el fin de fortalecer la seguridad de la información dentro de la empresa y concientizar a los colaboradores sobre los riesgos existentes dentro de la organización.

Los controles y descripción del plan de seguridad deberán estar publicados y disponibles para todos los colaboradores. Cada fin de mes se realizara la elección de las mejores propuestas formuladas, y se reconocerá a los autores de estas a través de un reconocimiento institucional; así mismo la dirección establecerá el premio a brindar por las propuestas ganadoras.

- **Solicitud de Acción Correctiva (SAC):** Es la solicitud propuesta por el auditor o cualquier integrante de la empresa para que el responsable del área proponga y proceda a establecer acciones correctivas a las no conformidades identificadas que puedan afectar la seguridad de la información.
- **Solicitud de Acción de Mejora (SAM):** Es la solicitud propuesta por cualquier auditor o cualquier integrante de la empresa para implementar acciones que permitan desarrollar mejoras en base a

oportunidades detectadas basadas en mejoras referentes a la seguridad de la información.

Se utilizara el siguiente formato para la recolección de dichas solicitudes:

Tabla 12. Plantilla Solicitudes SAC-SAM

SOLICITUD DE ACCIÓNES CORRECTIVAS O DE MEJORA	
Fecha de detección del evento :	
Activo en riesgo:	
Lugar identificado:	
Control de seguridad afectado:	
Tipo de solicitud: SAC ☐ SAM ☐	
Descripción del evento:	
Nombre del solicitante:	Fecha de la solicitud: ___/___/___

Fuente: Elaboración Propia

- Se debe concientizar a las personas de los riesgos que se puedan presentar tanto como para ellas, como para la organización; con el fin de que comprendan la importancia de dar un tratamiento adecuado a la información, para lo cual se propone lo siguiente:

- Realizar una campaña de concientización para los colaboradores de la organización, en el cual se debe definir un eslogan que impacte en los colaboradores.
- Elaborar materiales didácticos como posters y afiches para ser colocados en las diferentes áreas de la organización.
- Elaborar protectores y fondos de pantalla relacionados a la seguridad de la información.
- Realizar ataques de ingeniería social en vivo, con el fin de poder generar contraseñas seguras a cambio de algún incentivo por parte de la organización.
- Entregar recordatorios como tazas, lapiceros y llaveros con mensajes que generen impacto en base a la utilización de controles establecidos por la ISO 27002.
- Realizar capacitaciones con cláusulas que indiquen que han recibido entrenamiento y sensibilización en temas de seguridad de la información.
- Crear videos en los cuales el usuario final podrá visualizar la importancia de contar con un SGSI y generar conciencia a través de los riegos que puedan existir.
- Elaborar presentaciones en power point con el fin de capacitar al nuevo personal que se esté incorporando a la organización en temas se seguridad de la información.

- **Matriz de análisis entre la Circular N° G-140-2009 y la ISO 27002:2013**

Como punto de partida se tiene un conjunto de dominios y controles que fueron establecidos en función de la Circular N° G-140-2009, la cual establece un mínimo de controles como parte del sistema de gestión de seguridad a ser implementados en instituciones financieras, a estos se agregaron otros que tienen importancia dentro de los objetivos del modelo propuesto para lo cual se va a realizar un cruce entre los dominios de la ISO y de la circular, a fin de ver las similitudes que tienen ambas. Así mismo se puede apreciar que la circular G-140 tiene su base en la ISO27002.

Tabla 13. Circular G-140-2009 VS ISO 27002:2013

Circular G-140-2009	ISO 27002:2013
3. Sistema de gestión de la seguridad de la información	5. Políticas de Seguridad
4. Estructura organizacional	6. Aspectos organizativos de la seguridad de la información.
5.1. Controles de Seguridad de información / Seguridad Logica	9. Control de Accesos
5.2. Controles de Seguridad de información / Seguridad de personal	7. Seguridad Ligada a los RRHH
5.3. Controles de Seguridad de información / Seguridad física y ambiental	11. Seguridad Física y Ambiental
5.4. Controles de Seguridad de información / Inventario de activos y clasificación de la información	8. Gestión de Activos
5.5. Controles de Seguridad de información / Administración de las operaciones y comunicaciones	12. Seguridad en la operativa 13. Seguridad en las telecomunicaciones

5.6. Controles de Seguridad de información / Adquisición, desarrollo y mantenimiento de sistemas informáticos	14. Adquisición, desarrollo y mantenimiento de sistemas informáticos
5.7. Controles de Seguridad de información / Procedimientos de respaldo	12. Seguridad en la operativa
5.8. Controles de Seguridad de información / Gestión de incidentes de seguridad de información	15. Gestión de incidentes de seguridad de información
5.9. Controles de Seguridad de información / Cumplimiento normativo	18. Cumplimiento
5.10. Controles de Seguridad de información / Privacidad de la información	12. Seguridad en la operativa
6. Seguridad de operaciones de transferencia de fondos por canales electrónicos	13. Seguridad en la telecomunicaciones
7. Subcontratación	15. Relaciones con suministradores

Fuente: Elaboración propia

CAPITULO V:

DESARROLLO DEL SOFTWARE DE APOYO PARA LA IMPLEMENTACION DEL MODELO.

5.1 Identificación de Requerimientos

En esta sección se muestran los requerimientos que la herramienta a desarrollar, debe contemplar, tanto funcionales como no funcionales, así como las características de software y hardware que se deben de cumplir.

Se llevaron a cabo reuniones con los expertos de las áreas involucradas con el fin de determinar las necesidades del sistema a desarrollar el cual debe ser capaz de manejar el análisis y gestión de riesgos, basándose en el modelo que se realizó en base a la metodología Magerit y la ISO 27002:2013

5.1.1 Requerimientos Funcionales

A continuación se muestran los requerimientos funcionales que debe cumplir el sistema a desarrollar, estos requerimientos se deben de expresar en diagramas y casos de uso.

Tabla 14. Requerimientos Funcionales

Requerimiento N°	Descripción
RQ-01	El sistema llevara a cabo la gestión de accesos para la seguridad de la información mediante usuarios y contraseñas.
RQ-02	El sistema debe permitir definir los parámetros de probabilidad de ocurrencia y degradación en caso de amenazas.
RQ-03	El sistema debe permitir ingresar la escala de valoración de los activos con los que se trabajará.
RQ-04	El sistema debe permitir definir los valores de valoración del impacto y riesgo.

RQ-05	El sistema debe permitir el registro, modificación y valoración de los activos de TI.
RQ-06	El sistema debe permitir el registro, modificación y valoración de las amenazas.
RQ-07	El sistema debe calcular los valores del impacto y riesgo (acumulado y residual) en base a los valores definidos, por cada una de las dimensiones.
RQ-08	El Sistema debe permitir ingresar el conjunto de dominios, objetivos de control y controles o salvaguardas basados en la ISO 27002:2013 con los cuales se va a trabajar.
RQ-09	El sistema debe permitir generar reportes en base a los activos tratados.

Fuente: Elaboración Propia

5.1.2 Requerimientos no Funcionales

Los requerimientos no funcionales no pueden asociarse a un caso de uso específico, pero son de gran utilidad para el desarrollo del sistema, los requerimientos encontrados son:

Tabla 15. Requerimientos no funcionales

Requerimiento N°	Descripción
RQNF-01	El sistema debe ser desarrollado de forma evolutiva e incremental, de tal forma que puedan ser añadidos nuevos requerimientos a posterior.
RQNF -02	El sistema debe ser de fácil uso y fácil adaptación por parte de los usuarios.
RQNF -03	El sistema debe ser desarrollado en su totalidad en un entorno web utilizando software Open Source.
RQNF -04	Motor de base de datos MySQL 5.6
RQNF -05	Framework CakePHP 2.6, PHP 5.6
RQNF -06	Java Script, Boostrap, HTML, CSS

Fuente: Elaboración Propia

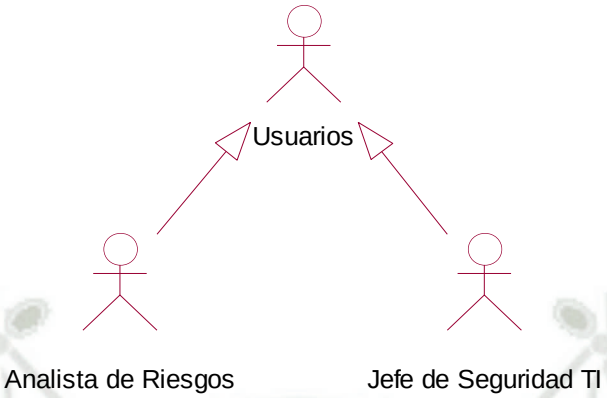
5.2 Modelado del Sistema

5.2.1 Especificación de Actores del Sistema

Rumbaugh, Jacobson, Booch. (2000). Un actor es una idealización de una persona externa, de un proceso, o de una cosa que interactúa con un sistema, un subsistema, o una clase. Un actor caracteriza las interacciones que los exteriores pueden tener con el sistema.

A continuación se listan los actores principales en el sistema.

Figura 5. Actores del Sistema

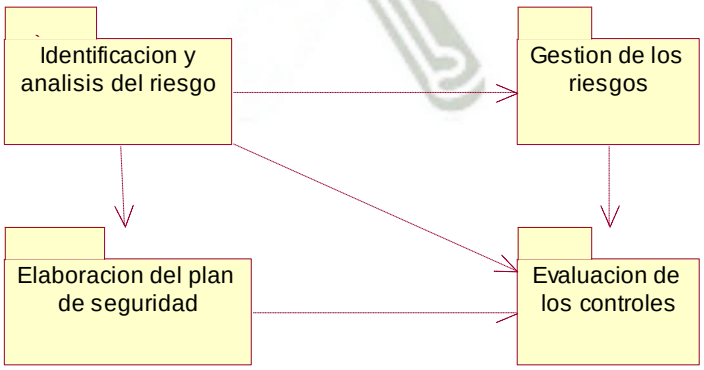


Fuente: Elaboración Propia

5.2.2 Diagrama de Paquetes

(Rumbaugh et al. 2000) Un paquete es una parte de un modelo. Cada parte de un modelo debe pertenecer a un paquete. Los paquetes contienen elementos del modelo al más alto nivel, tales como clases y sus relaciones, máquinas de estado, diagramas de casos de uso, interacciones y colaboraciones y cualquier elemento que no este contenido en otro.

Figura 6. Diagrama por paquetes



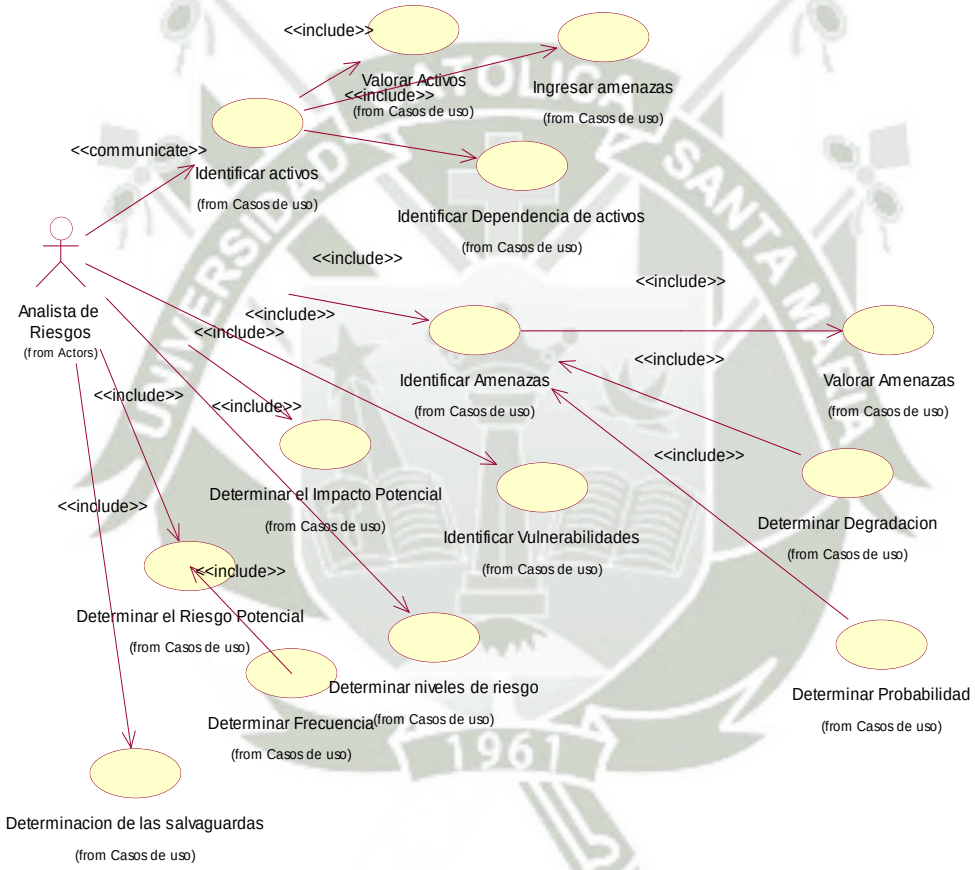
Fuente: Elaboración Propia

5.2.3 Casos de Usos por Paquetes

En esta sección se realizan los casos de uso que fueron identificados a partir de los requisitos de la herramienta, los cuales fueron agrupados en paquetes relacionados al tipo de funcionabilidad.

5.2.3.1 Caso de uso por Paquetes: Identificación y Análisis de riesgos

Figura 7. Caso de uso por paquetes: Identificación y análisis de riesgos



Fuente: Elaboración Propia

5.2.3.2 Especificación de Casos de Usos por Paquetes

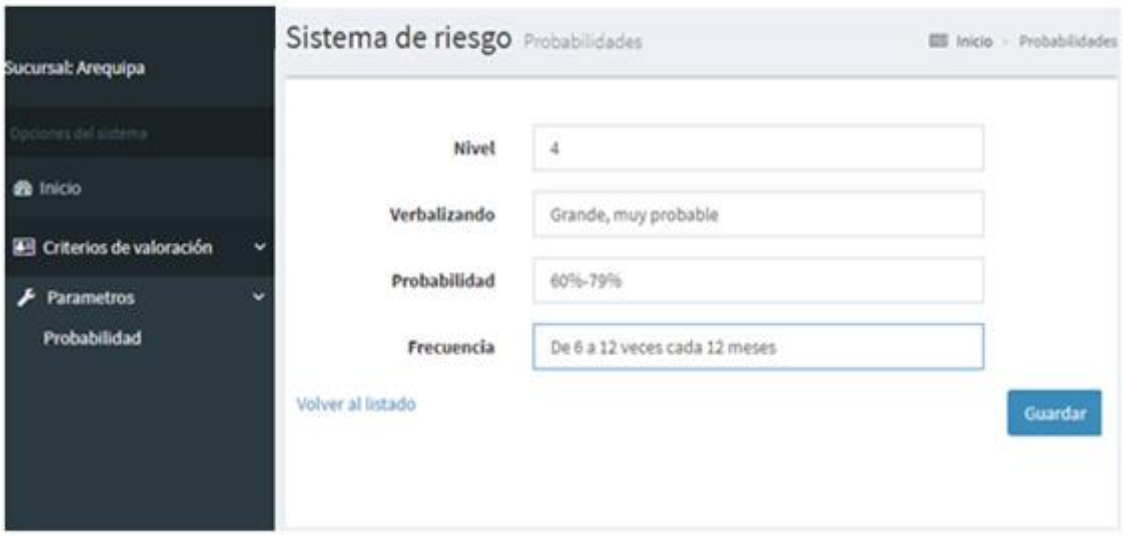
Tabla 16. Determinar probabilidad

ID	CU-001 Determinar probabilidad
Descripción	Determinar la probabilidad para ver cuán probable es que un evento ocurra.
Pre-condición	El usuario debe estar registrado en el sistema
Post-condición	El sistema tendrá registrados los valores con los que se trabajara en relación a la probabilidad.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Criterios de valoración” 2. El Analista de riesgo selecciona la opción “Parámetros” 3. El Analista de riesgo selecciona la opción “Probabilidad” 4. El Analista de riesgo deberá definir los niveles de probabilidad de ocurrencia con los cuales se trabajará. 5. El sistema almacena lo cambios realizados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo principal del caso de uso**

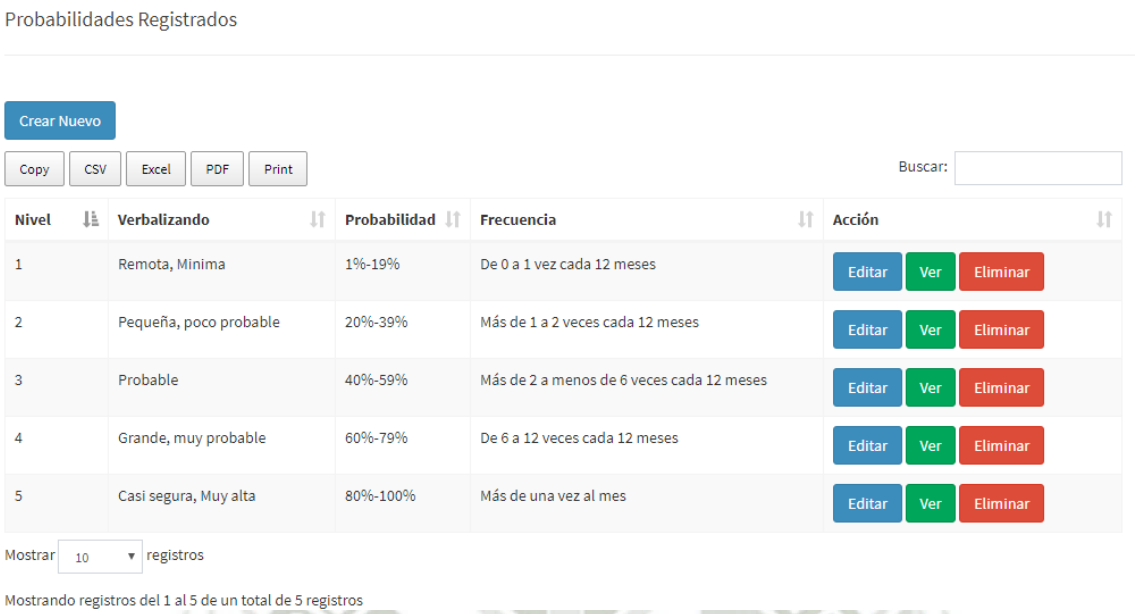
Figura 8. Flujo principal - Determinar Probabilidad



Fuente: Elaboración Propia

- **Post- Condición**

Figura 9. Niveles de probabilidad registrados



Fuente: Elaboración Propia

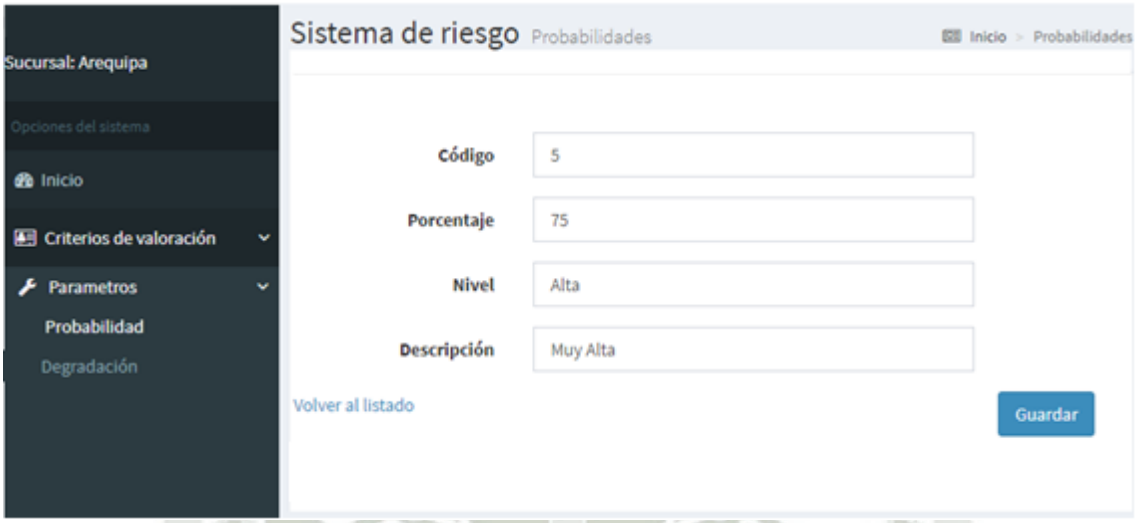
Tabla 17. Determinación de los niveles de degradación

ID	**CU-002 Determinar degradación**
Descripción	Determinar el daño que es causado por un incidente.
Pre-condición	El usuario debe estar registrado en el sistema
Post-condición	El sistema tendrá registrados los valores con los que se trabajara en relación a la degradación ocasionada por una amenaza.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Criterios de valoración” 2. El Analista de riesgo selecciona la opción “Parámetros” 3. El Analista de riesgo selecciona la opción “Degradación” 4. El Analista de riesgo deberá definir los niveles de la escala de degradación con los cuales se trabajará. 5. El sistema almacena lo cambios realizados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo principal del caso de uso**

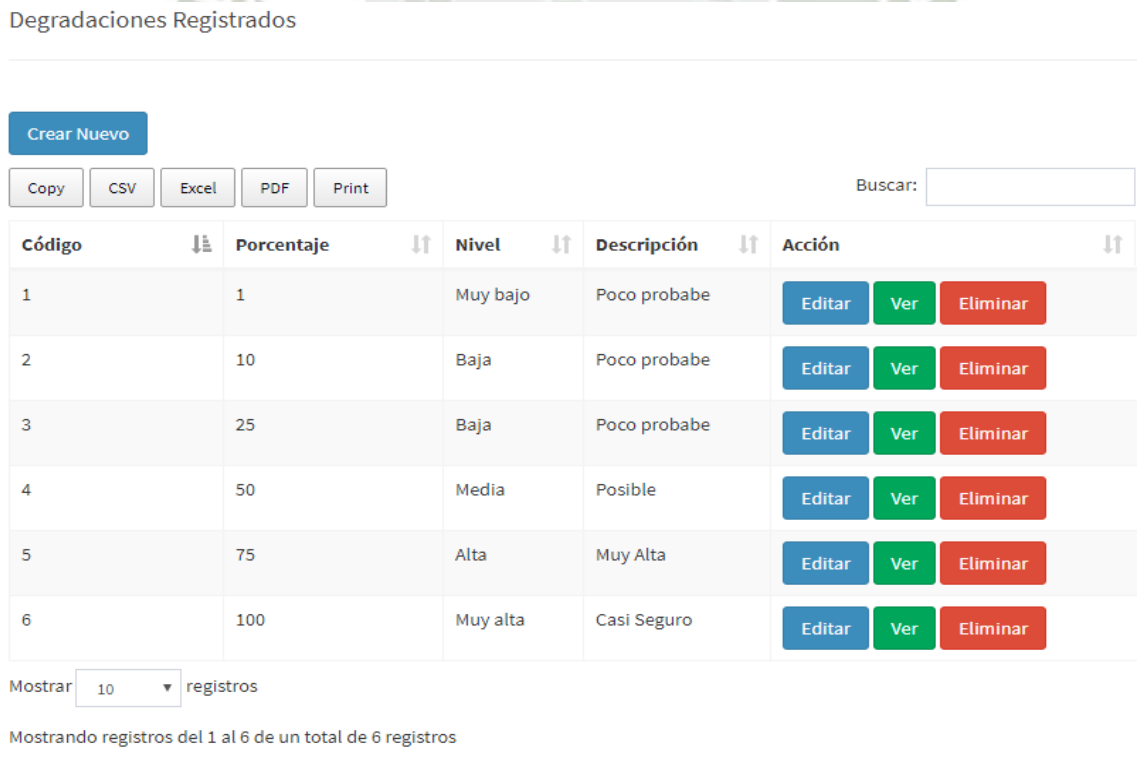
Figura 10. Ingresar los niveles de degradación



Fuente: Elaboración Propia

- **Post Condiciones**

Figura 11. Niveles de degradación registrados



Fuente: Elaboración Propia

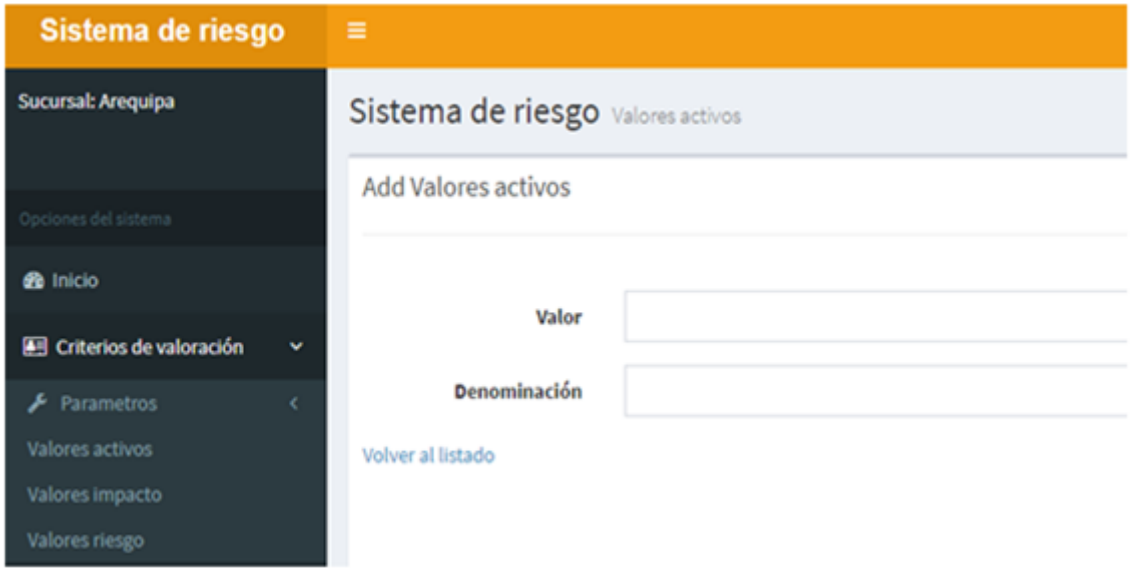
Tabla 18. Determinación de la escala de valoración de activos

ID	**CU-003 Determinar escala de valoración de activos**
Descripción	Determinar la escala de valores que se utilizara para definir los valores de los activos
Pre-condición	El usuario debe estar registrado en el sistema
Post-condición	El sistema tendrá registrados los valores con los que se trabajara en relación a la escala de valoración de activos.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Criterios de valoración” 2. El Analista de riesgo selecciona la opción “Valores activos” 3. El Analista de riesgo deberá definir la escala de valores que se utilizara para dar una valoración cualitativa a los activos que serán identificados. 4. El sistema almacena lo cambios realizados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo principal del caso de uso**

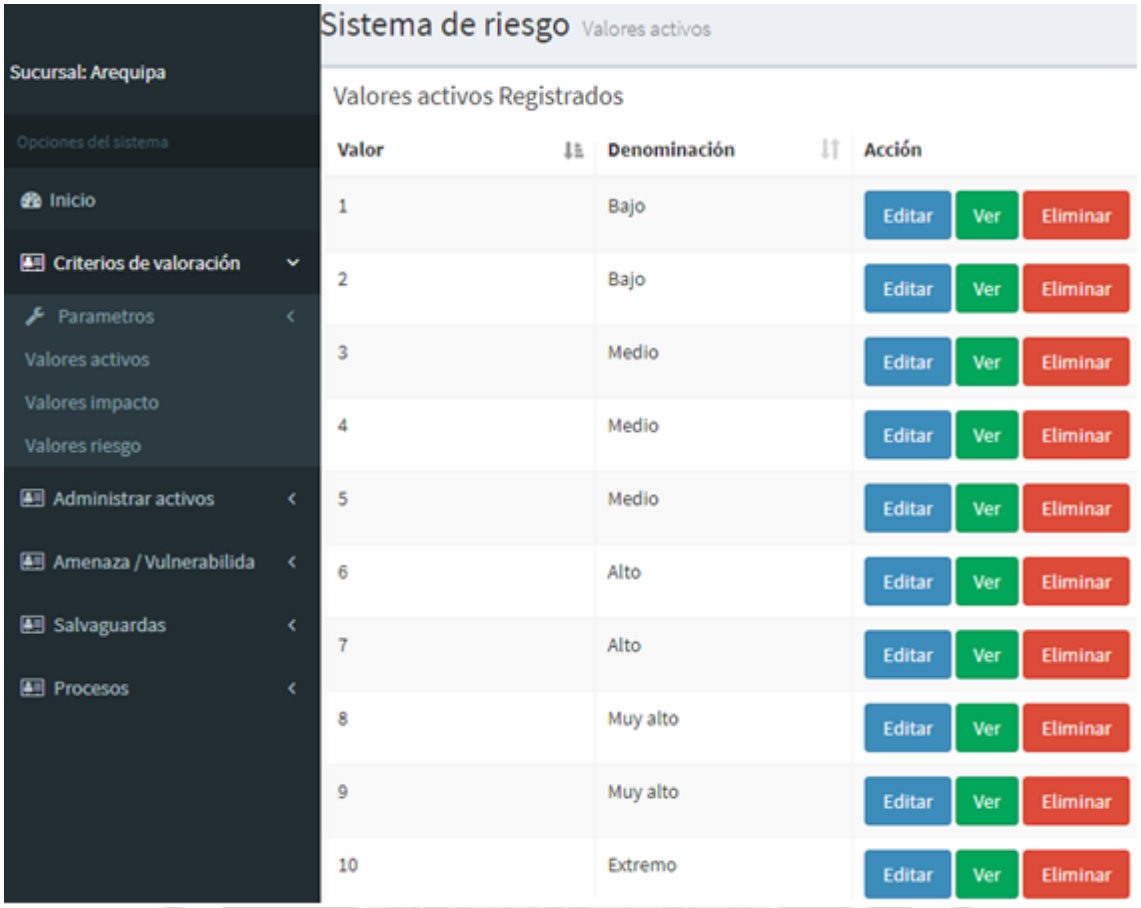
Figura 12. Valoración de Activos



Fuente: Elaboración Propia

- **Post-Condición**

Figura 13. Valores de activos registrados



Fuente: Elaboración Propia

Tabla 19. Determinación de los valores de la matriz de impacto

ID	**CU-004 Determinar valores de impacto**
Descripción	Ingresar los valores de la matriz de impacto que se utilizara para determinar los valores de impacto acumulado e impacto residual.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los valores de la degradación. • Se deben de haber ingresado la escala de valoración de los activos.
Post-condición	El sistema tendrá definida la matriz de impacto para cálculos posteriores.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Criterios de valoración”

	2. El Analista de riesgo selecciona la opción "Valores Impacto" 3. El Analista de riesgo deberá ingresar los valores establecidos en la metodología establecida a la matriz formada por los valores de la degradación y los valores de los activos. 4. El sistema almacena lo cambios realizados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal del caso de uso**

Figura 14. Matriz de Impacto Registrados

Fuente: Elaboración Propia

Tabla 20. Determinación de la matriz de riesgos

ID	**CU-005 Determinar valores de riesgo**
Descripción	Ingresar los valores de la matriz de riesgos que se utilizara para determinar los valores de riesgo acumulado y riesgo residual.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben de tener ingresados los valores de los rangos de las probabilidades. • Se deben tener ingresados los valores del impacto.

Post-condición	El sistema tendrá definida la matriz de riesgos para cálculos posteriores.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Criterios de valoración” 2. El Analista de riesgo selecciona la opción “Valores Riesgo” 3. El analista de riesgos deberá seleccionar un color para el mapa de calor con el fin de indicar el nivel de riesgo. 4. El Analista de riesgo deberá ingresar los valores a la matriz de riesgos, en relación a la probabilidad de ocurrencia y a los valores que se ingresaron en la matriz de impacto. 5. El sistema almacena lo cambios realizados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal del caso de uso**

Figura 15.Matriz de riesgos

Fuente: Elaboración Propia

Tabla 21. Identificación de activos

ID	**CU-006 Identificar activos**
Descripción	Identificar los activos de T.I. para evaluar de manera eficaz todos los componentes críticos y determinar la criticidad de estos.
Pre-condición	• El usuario debe estar registrado en el sistema • Tener las áreas registradas • Tener los tipos de activos registrados. • Tener la ubicación de los activos registrados. • Tener registrados los propietarios.
Post-condición	El sistema tendrá ingresados una serie de activos que podrán ser analizados posteriormente.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Administrar activos” 2. El Analista de riesgo selecciona la opción “Identificar activos” 3. El Analista de riesgo deberá ingresar los datos referentes al activo, tales como: • Código del activo • Nombre del activo • Descripción del activo • Ubicación del activo • Propietario del activo • Área al que pertenece el activo
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal del caso de uso**

Figura 16. Ingreso de activos

Fuente: Elaboración Propia

- **Post- Condición**

Figura 17. Listado de activos Ingresados

Tipo activo	Código	Nombre	Acción
Instalaciones	001	Ambiente Centro de Datos	Editar Ver Eliminar
Equipamiento informático (hardware)	002	NAS de Almacenamiento de información	Editar Ver Eliminar
Equipamiento auxiliar	003	Equipo de proteccion electrica	Editar Ver Eliminar
Equipamiento auxiliar	004	Aire Acondicionado	Editar Ver Eliminar
Equipamiento informático (hardware)	005	Servidores	Editar Ver Eliminar
Datos / Información	006	Base de datos	Editar Ver Eliminar
Servicios	007	Servicio File Server	Editar Ver Eliminar
Personal	008	Proveedor de mantenimiento equipos de cómputo	Editar Ver Eliminar
Equipamiento informático (hardware)	009	Switch Core	Editar Ver Eliminar
Software - Aplicaciones informáticas	010	Servicio de internet	Editar Ver Eliminar

Fuente: Elaboración Propia

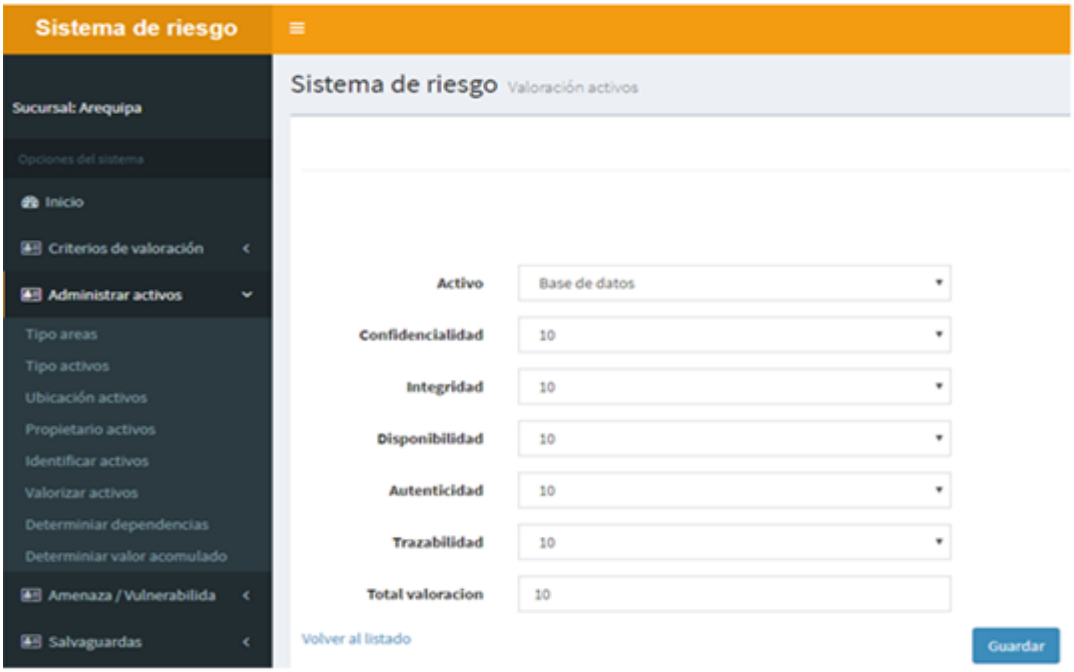
Tabla 22. Valoración de activos

ID	**CU-007 Valorar activos**
Descripción	Ingresar los valores para cada activo que fueron definidos en la escala de valoración de activos.
Pre-condición	• El usuario debe estar registrado en el sistema • Se debe tener definida la escala de valoración de los activos. • Se deben tener ingresados los activos.
Post-condición	El sistema tendrá valorizados todos los activos que fueron sometidos a este proceso.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Administrar activos” 2. El Analista de riesgo selecciona la opción “Valorizar Activos” 3. El Analista de riesgo deberá ingresar los valores para cada dimensión del activo que fueron definidos en la escala de valoración de los activos • Confidencialidad • Integridad • Disponibilidad • Autenticidad • Trazabilidad
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal**

Figura 18. Valoración de activos



Fuente: Elaboración Propia

- **Post-Condición**

Figura 19. Listado de activos valorizados

Activo	C	I	D	A	T	Total valoración	Acción
Aire Acondicionado	0	8	6	0	0	7	Editar Ver Eliminar
Ambiente Centro de Datos	8	8	8	8	8	8	Editar Ver Eliminar
Base de datos	10	10	10	10	10	10	Editar Ver Eliminar
Cableado de datos	6	0	10	0	0	8	Editar Ver Eliminar
Directorio activo	8	8	8	8	8	8	Editar Ver Eliminar
Edificio empresa	7	7	7	7	7	7	Editar Ver Eliminar
Equipo de proteccion electrica	0	8	6	0	0	7	Editar Ver Eliminar
Firewall	10	10	10	10	10	10	Editar Ver Eliminar
Generador Eléctrico	6	0	10	0	0	8	Editar Ver Eliminar
NAS de Almacenamiento de información	10	10	10	0	0	10	Editar Ver Eliminar

Fuente: Elaboración Propia

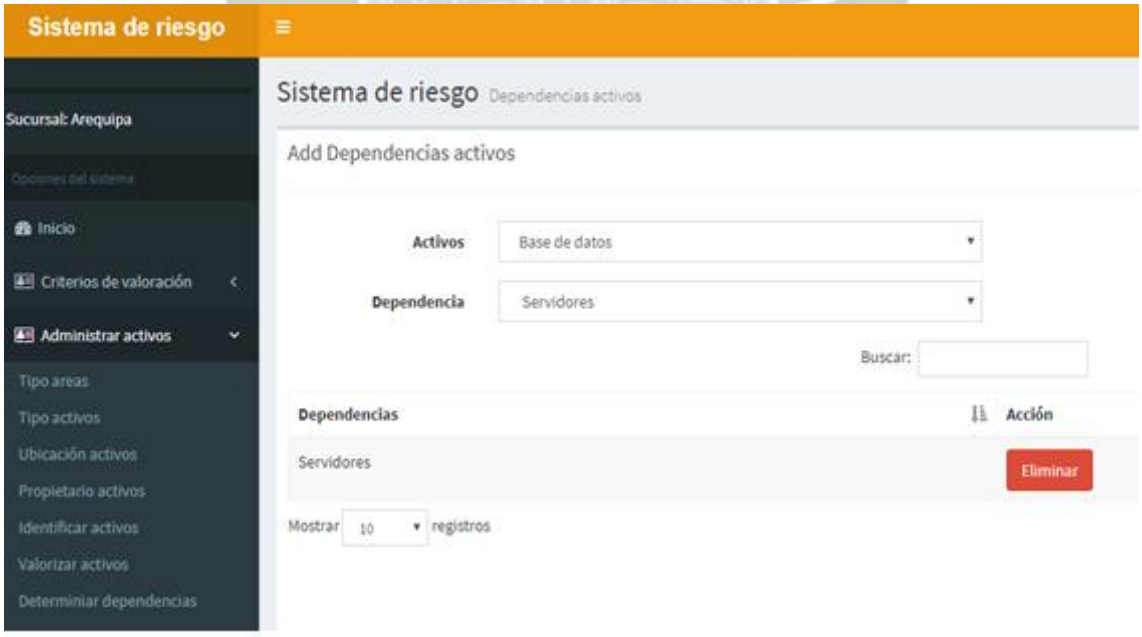
Tabla 23. Identificación de activos

ID	CU-008 Identificar dependencia de activos
Descripción	Identificar la dependencia que existen entre los activos de la organización.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los activos.
Post-condición	• El sistema tendrá la relación de dependencia que existe entre uno o más activos. • Se tendrá el diagrama de dependencia que existen entre los activos.
Flujo principal del caso de uso	1. El Analista de riesgo selecciona la opción “Administrar activos” 2. El Analista de riesgo selecciona la opción “Determinar Dependencias” 3. El analista deberá ingresar la relación de dependencia entre un activo padre y un activo hijo, donde el padre necesita del hijo para poder funcionar correctamente y el hijo hereda el valor del padre, cabe señalar que un activo puede tener muchos activos que dependan de él.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo principal del caso de uso**

Figura 20. Determinación de las dependencias entre activos



Fuente: Elaboración Propia

- **Post-Condición**

Figura 21. Dependencia entre activos

Padre	Hijo
Ambiente Centro de Datos	Edificio empresa
Base de datos	Servidores
Firewall	Ambiente Centro de Datos
NAS de Almacenamiento de información	Ambiente Centro de Datos
PCs	Proveedor de mantenimiento equipos de cómputo
Redes de comunicación	Cableado de datos
Servicio Corre Electronico en la nube	Servicio de internet
Servicio Correo Electronico	Servidores
Servicio de Telefonia IP	Servidores
Servicio File Server	Directorio activo

Fuente: Elaboración Propia

Tabla 24. Determinación del valor acumulado

ID	**CU-009 Determinar valor acumulado**
Descripción	Se determinara el valor acumulado de un activo mediante el mayor valor entre el propio y el de cualquiera que dependa de él.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los activos. • Se debe determinar la relación de dependencia entre los activos.
Post-condición	El sistema tendrá el valor acumulado de los activos.
Flujo principal del caso de uso	1. El Analista de riesgo deberá seleccionar la opción Determinar valor acumulado 2. El sistema mostrara los valores acumulados de los activos, en base a la determinación de la dependencia de activos que se realizó.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Post-Condición**

Figura 22. Valor acumulado de los activo

Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Total valoración
Aire Acondicionado	0	8	6	0	0	7
Ambiente Centro de Datos	10	10	10	10	10	10
Base de datos	10	10	10	10	10	10
Cableado de datos	10	10	10	10	10	10
Directorio activo	8	8	8	8	8	8
Edificio empresa	10	10	10	10	10	10
Equipo de proteccion electrica	0	8	6	0	0	7
Firewall	10	10	10	10	10	10
Generador Eléctrico	6	0	10	0	0	8
NAS de Almacenamiento de información	10	10	10	0	0	10

Fuente: Elaboración Propia

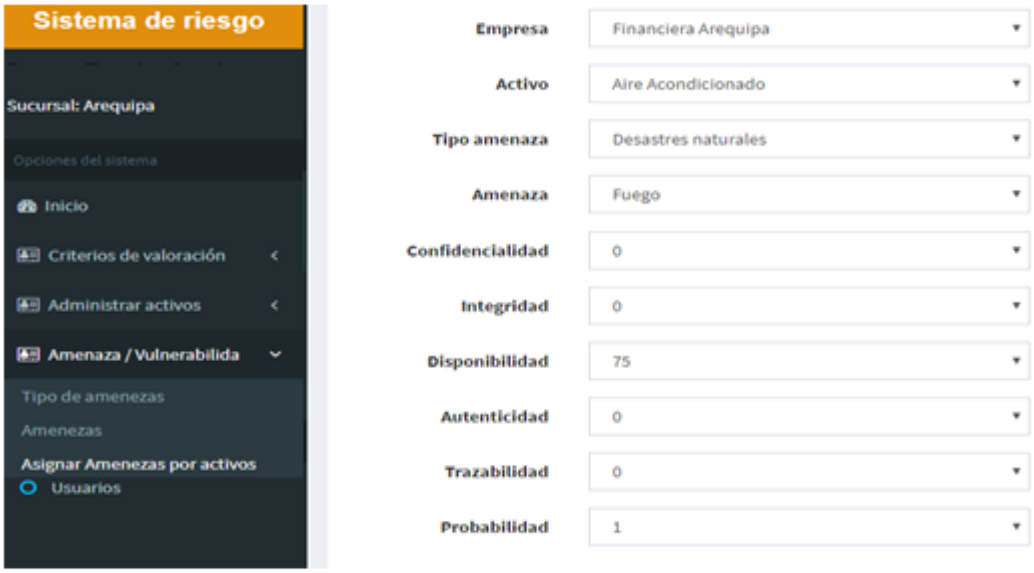
Tabla 25. Identificación y valorización de amenazas

ID	**CU-010 Identificar y valorar amenazas**
Descripción	Se identificaran las amenazas que puedan afectar a los activos, cada activo puede estar sujeta a una o varias amenazas.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los activos. • Se deben tener ingresados los tipos de amenazas • Se debe tener ingresada la escala de degradación. • Se debe tener ingresada la escala de probabilidad de ocurrencia.
Post-condición	El sistema tendrá asignadas las amenazas que puedan afectar a los activos
Flujo principal del caso de uso	El Analista de riesgo deberá seleccionar las amenazas que puedan afectar a los activos, una vez que se tenga seleccionada la amenaza por el activo, se procederá a identificar el daño que pueda producir la amenaza mediante la degradación, en caso de que esta se materialice y la probabilidad de ocurrencia con la que pueda darse este evento.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal**

Figura 23. Valorización de las amenazas



Fuente: Elaboración Propia

- **Post-condición**

Figura 24. Degradación causada por las amenazas

Activo	Amenaza	C	I	D	A	T	P
Aire Acondicionado	Fuego	0 %	0 %	75 %	0 %	0 %	1%-19%
Aire Acondicionado	Avería de origen físico o lógico	0 %	75 %	75 %	0 %	75 %	1%-19%
Aire Acondicionado	Ataque destructivo	0 %	0 %	100 %	0 %	0 %	1%-19%
Aire Acondicionado	Corte del suministro eléctrico	0 %	0 %	100 %	0 %	0 %	20%-39%
Aire Acondicionado	Condiciones inadecuadas de temperatura o humedad	0 %	0 %	75 %	0 %	0 %	20%-39%
Aire Acondicionado	Daños por agua	0 %	0 %	100 %	0 %	0 %	1%-19%
Ambiente Centro de Datos	Fuego	0 %	0 %	100 %	0 %	0 %	1%-19%
Ambiente Centro de Datos	Daños por agua	0 %	0 %	50 %	0 %	0 %	20%-39%
Ambiente Centro de Datos	Fugas de información	50 %	50 %	50 %	0 %	0 %	1%-19%
Ambiente Centro de Datos	Acceso no autorizado	100 %	25 %	75 %	25 %	0 %	1%-19%

Fuente: Elaboración Propia

Tabla 26. Calculo del Impacto Acumulado

ID	CU-011 Determinar el Impacto Acumulado
Descripción	Se calculara el impacto acumulado en base al valor de los activos y a la degradación causada por la materialización de una amenaza.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados y valorizados los activos. • Se deben tener ingresadas las amenazas por activo • Se debe tener ingresada la degradación causada por una amenaza en cada dimensión. • Se debe tener ingresada la matriz de impacto con sus respectivos valores
Post-condición	El sistema podrá calcular el impacto producido en cada activo, por cada amenaza y por cada dimensión
Flujo principal del caso de uso	El Analista de riesgo deberá seleccionar la pestaña de procesos y seleccionar la opción de impacto acumulado, con el fin de realizar el cálculo en cada uno de los valores mencionados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal**

Figura 25. Impacto acumulado

Activo	Amenaza	C	I	D	A	T
Aire Acondicionado	Fuego	-	-	6	-	-
Aire Acondicionado	Avería de origen físico o lógico	-	8	6	-	-
Aire Acondicionado	Ataque destructivo	-	-	6	-	-
Aire Acondicionado	Corte del suministro eléctrico	-	-	6	-	-
Aire Acondicionado	Condiciones inadecuadas de temperatura o humedad	-	-	6	-	-
Aire Acondicionado	Daños por agua	-	-	6	-	-
Ambiente Centro de Datos	Fuego	-	-	10	-	-
Ambiente Centro de Datos	Daños por agua	-	-	9	-	-
Ambiente Centro de Datos	Fugas de información	9	9	9	-	-
Ambiente Centro de Datos	Acceso no autorizado	10	8	10	8	-

Fuente: Elaboración Propia

Tabla 27. Calculo del Riesgo Acumulado

ID	CU-012 Determinar el Riesgo Acumulado
Descripción	Se calculara el riesgo acumulado en base al valor calculado del impacto acumulado y la probabilidad de ocurrencia.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados y valorizados los activos. • Se deben tener ingresadas las amenazas por activo. • Se deben tener los cálculos de los valores del impacto acumulado. • Se debe tener ingresada la matriz de riesgos con sus respectivos valores • Se debe tener ingresada la probabilidad de ocurrencia de la amenaza.
Post-condición	El sistema podrá calcular el riesgo acumulado producido en cada activo, por cada amenaza y por cada dimensión
Flujo principal del caso de uso	El Analista de riesgo deberá seleccionar la pestaña de procesos y seleccionar la opción de riesgo acumulado, con el fin de realizar el cálculo en cada uno de los valores mencionados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración propia

- **Flujo principal**

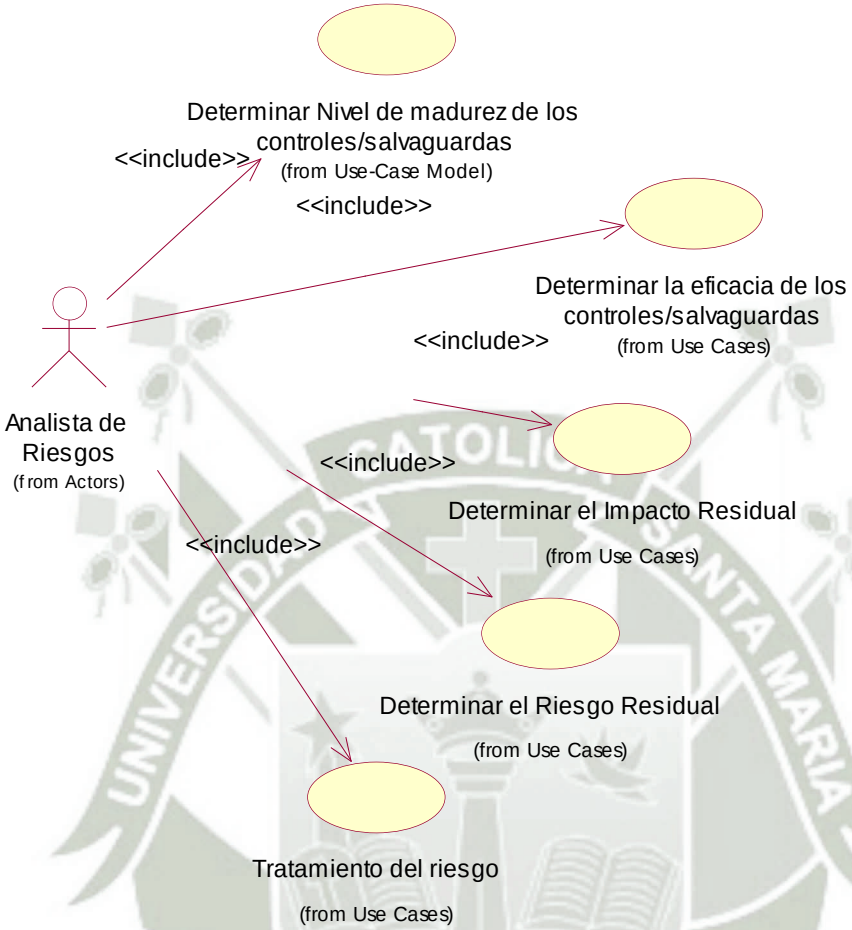
Figura 26. Determinación del riesgo acumulado

Activo	Amenaza	C	I	D	A	T	Probabilidad
Aire Acondicionado	Fuego	-	-	1,6	-	-	1
Aire Acondicionado	Avería de origen físico o lógico	-	1,8	1,6	-	-	1
Aire Acondicionado	Ataque destructivo	-	-	1,6	-	-	1
Aire Acondicionado	Corte del suministro eléctrico	-	-	2,6	-	-	2
Aire Acondicionado	Condiciones inadecuadas de temperatura o humedad	-	-	2,6	-	-	2
Aire Acondicionado	Daños por agua	-	-	1,6	-	-	1
Ambiente Centro de Datos	Fuego	-	-	1,10	-	-	1
Ambiente Centro de Datos	Daños por agua	-	-	2,9	-	-	2
Ambiente Centro de Datos	Fugas de información	1,9	1,9	1,9	-	-	1
Ambiente Centro de Datos	Acceso no autorizado	1,10	1,8	1,10	1,8	-	1

Fuente: Elaboración propia

5.2.3.3. Caso de uso por paquetes: Gestión de riesgos

Figura 27. Caso de uso por paquetes Gestión de Riesgos



Fuente: Elaboración propia

Tabla 28. Determinación del nivel de madurez de los controles o salvaguardas

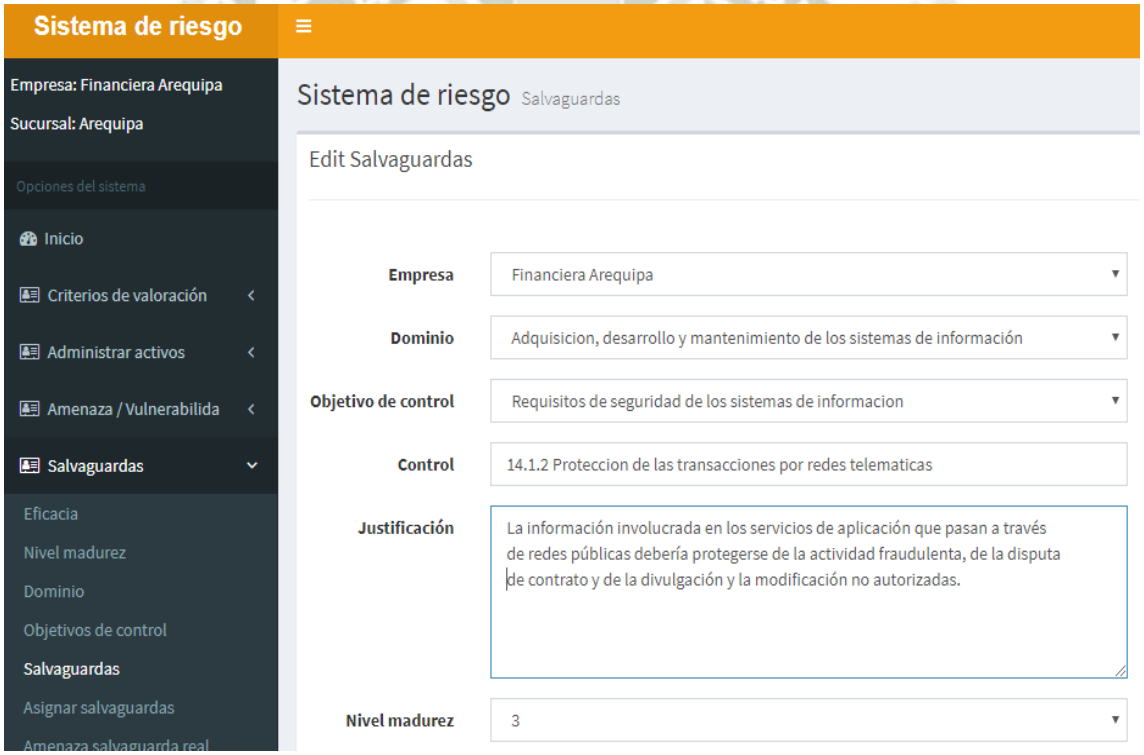
ID	**CU-013 Determinar nivel de madurez de los controles/salvaguardas**
Descripción	Determinar el nivel en el que se encuentran implantados los controles/salvaguardas en la organización.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los activos. • Se deben tener ingresados los dominios • Se deben tener ingresados los objetivos de control. • Se deben tener ingresados los controles y/o salvaguardas.
Post-condición	• El sistema contara con el nivel de madurez en el que se encuentra la organización en base a la ISO 27002

	• El sistema contara con una gráfica donde muestre el nivel de madurez en base a todos los dominios definidos.
Flujo principal del caso de uso	• El Analista de riesgo deberá determinar el nivel de madurez de cada uno de los controles con los que se piensa trabajar, en una escala del 1 al 5, antes y después de aplicar el modelo para poder ver el impacto generado a través de su utilización. • El Analista de riesgo podrá generar un reporte, donde se podrá visualizar el nivel de cumplimiento de los dominios, en base al nivel de madurez otorgado a cada control.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal**

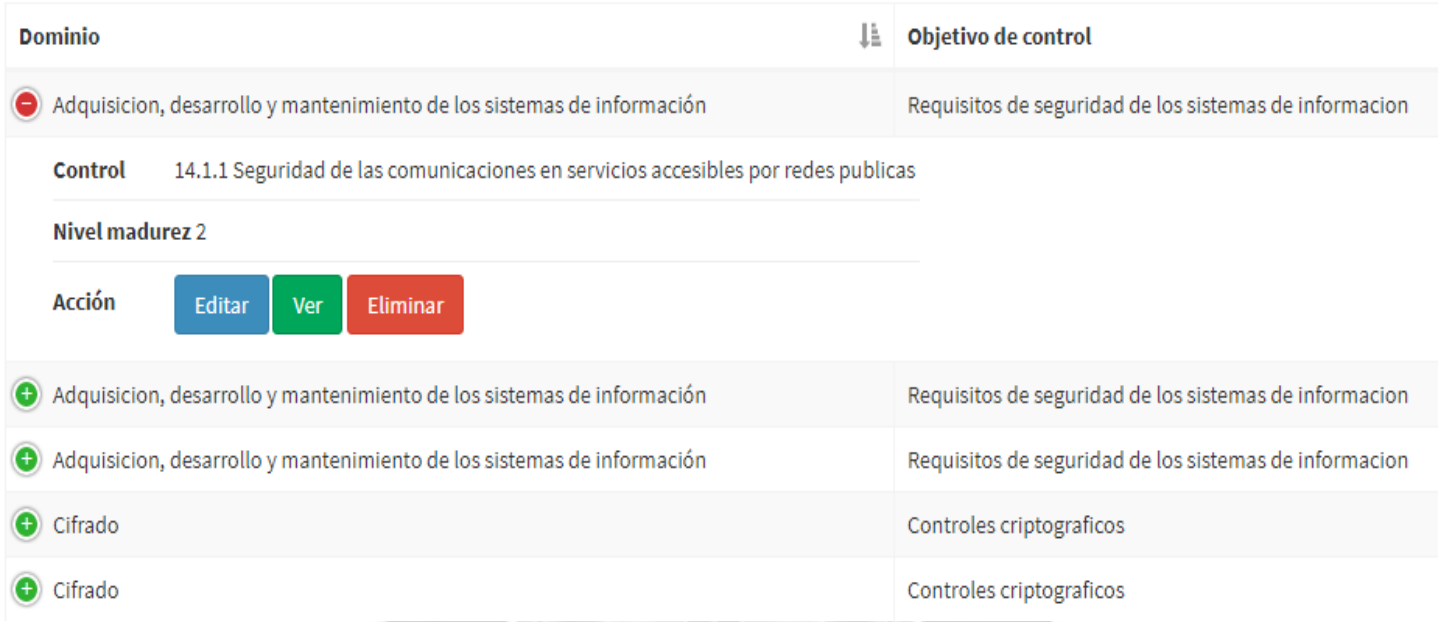
Figura 28. Determinar nivel de madurez de los controles/salvaguardas



Fuente: Elaboración Propia

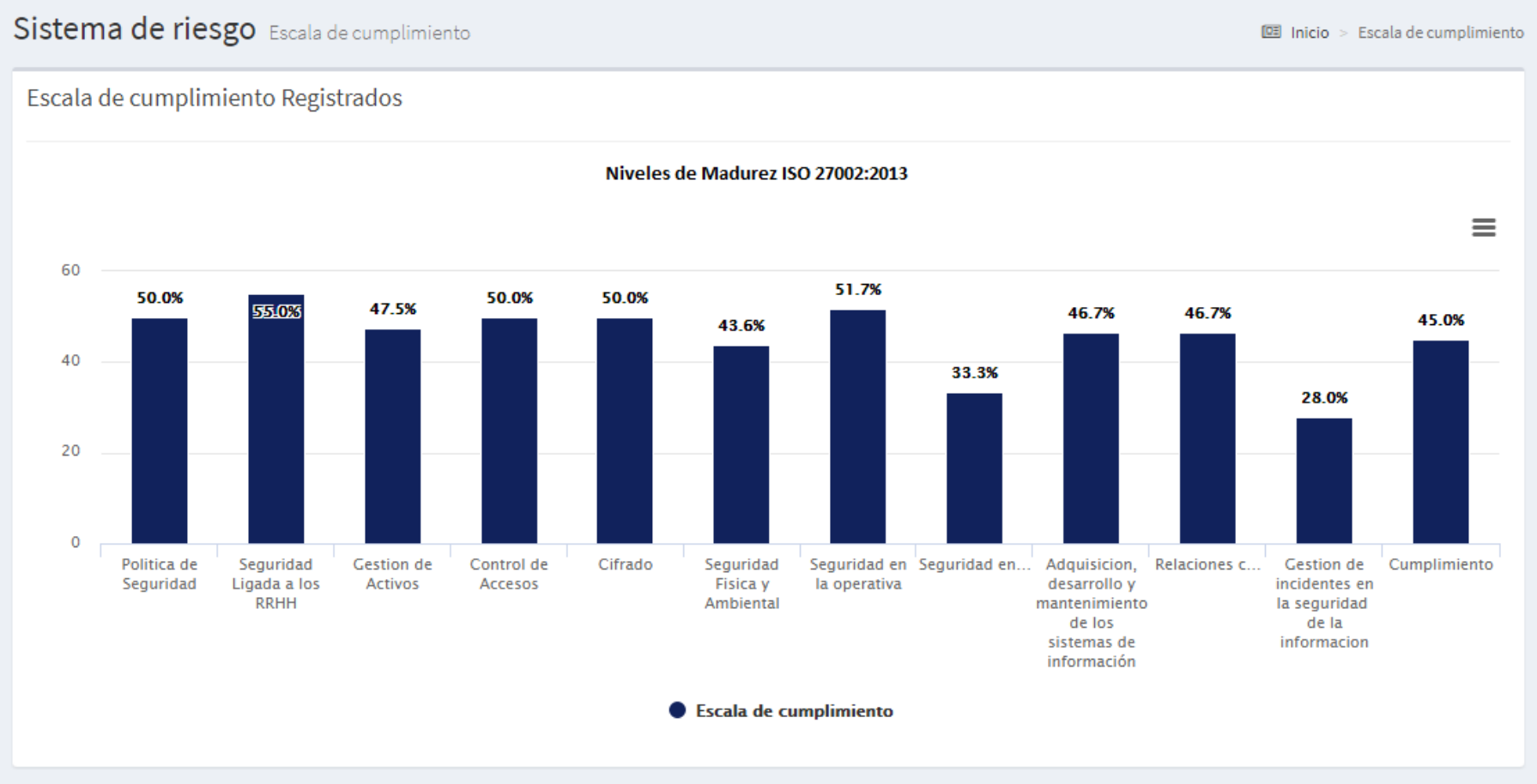
- **Post- Condición**

Figura 29. Nivel de madurez por cada control definido



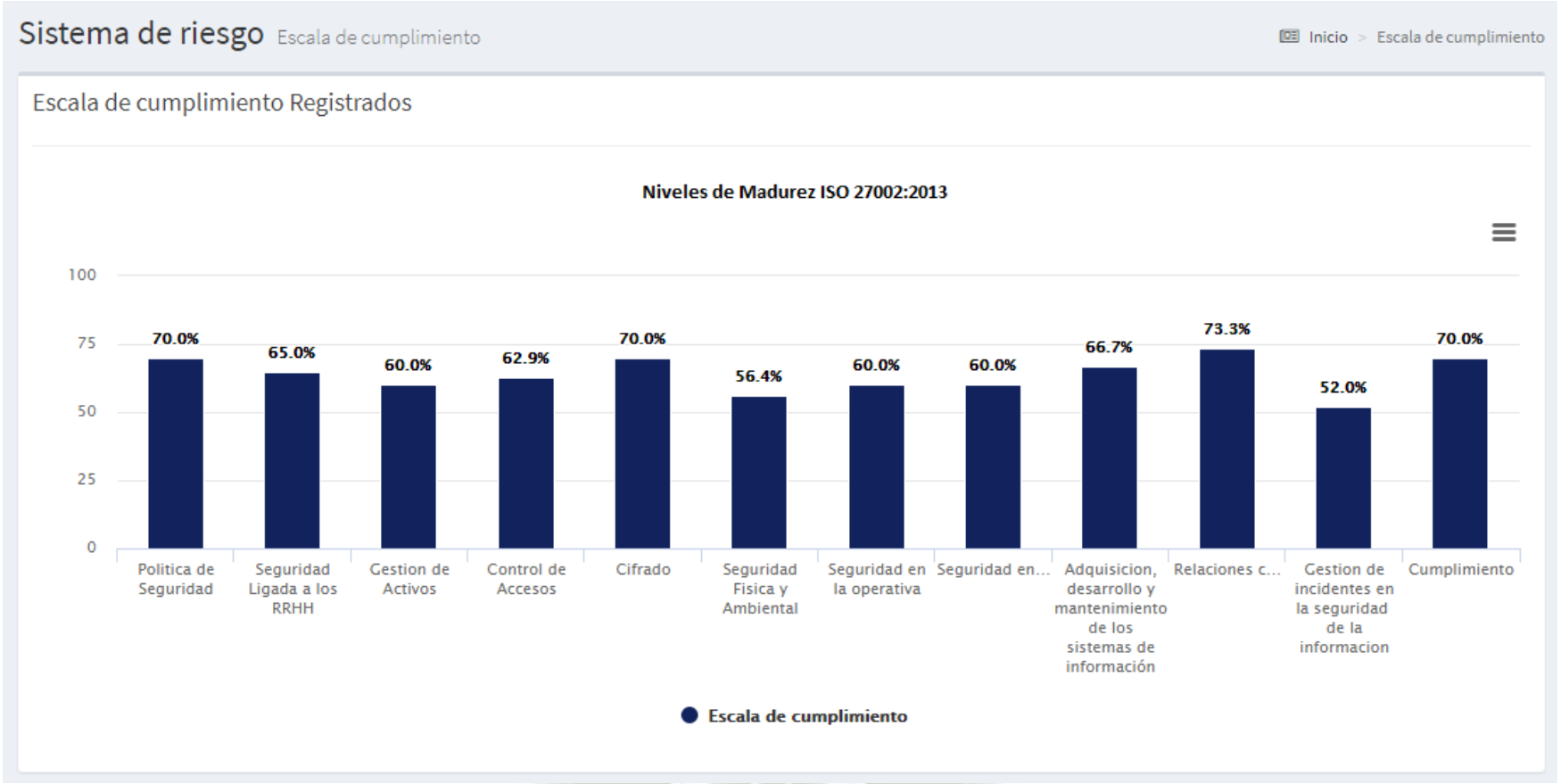
Fuente: Elaboración Propia

Figura 30. Nivel de Madurez ISO 27002, antes de la implementación



Fuente: Elaboración Propia

Figura 31. Nivel de Madurez ISO 27002, después de la implementación



Fuente: Elaboración Propia

Tabla 29. Eficacia de los controles/salvaguardas.

ID	**CU-014 Determinar la eficacia de los controles/salvaguardas**
Descripción	Determinar la eficacia de los controles/salvaguardas frente al daño que puede producir una amenaza en cuestión de que esta se materialice.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los activos. • Se deben tener ingresadas las amenazas a las que esta sujetos los activos. • Se deben tener ingresados los controles/salvaguardas-
Post-condición	El sistema contara con el porcentaje de eficacia de las salvaguardas frente al daño que puedan generar las amenazas.
Flujo principal del caso de uso	El Analista de riesgo deberá determinar el porcentaje que otorgaran los controles/salvaguardas.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración propia

- **Flujo Principal**

Tabla 30. Determinación de la eficacia de los controles/salvaguardas

Fuente: Elaboración Propia

- **Post-Condición**

Figura 32. Eficacia de las salvaguardas por amenaza

Fuente: Elaboración Propia

Tabla 31. Determinación del Impacto Residual

ID	**CU-014 Determinar el impacto residual**
Descripción	Determinar el impacto residual luego de implementar los controles/salvaguardas para cada uno de los activos que fueron identificados.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados y valorizados los activos. • Se deben tener ingresadas las amenazas a las que esta sujetos los activos. • Se deben tener calculadas las nuevas degradaciones producidas por las amenazas en cada una de las dimensiones. • Se deben tener ingresados los controles/salvaguardas. • Se debe tener ingresados la matriz de parámetros para el cálculo del impacto.
Post-condición	El sistema contara con el impacto residual que refleja el daño que pueda causar las amenazas en caso de que estas se materialicen, después de aplicar un conjunto de salvaguardas.
Flujo principal del caso de uso	El Analista de riesgo deberá seleccionar la pestaña de procesos y seleccionar la opción de impacto residual, con el fin de realizar el cálculo en cada uno de los valores mencionados.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

- **Flujo Principal**

Figura 33. Impacto Residual

Activo	Amenaza	C	I	D	A	T
Aire Acondicionado	Fuego	-	-	4	-	-
Aire Acondicionado	Avería de origen físico o lógico	-	6	4	-	-
Aire Acondicionado	Ataque destructivo	-	-	4	-	-
Aire Acondicionado	Corte del suministro eléctrico	-	-	5	-	-
Aire Acondicionado	Condiciones inadecuadas de temperatura o humedad	-	-	4	-	-
Aire Acondicionado	Daños por agua	-	-	4	-	-
Ambiente Centro de Datos	Fuego	-	-	8	-	-
Ambiente Centro de Datos	Daños por agua	-	-	7	-	-
Ambiente Centro de Datos	Fugas de información	7	7	7	-	-
Ambiente Centro de Datos	Acceso no autorizado	9	7	8	7	-

Fuente: Elaboración propia

Tabla 32. Determinación del Riesgo Residual

ID	**CU-015 Determinar el Riesgo residual**
Descripción	Determinar el riesgo residual luego de implementar los controles/salvaguardas para cada uno de los activos que fueron identificados, verificando la madurez que adquirió el sistema de gestión.
Pre-condición	• El usuario debe estar registrado en el sistema • Se deben tener ingresados los activos. • Se deben tener ingresadas las amenazas a las que esta sujetos los activos. • Se deben tener calculadas las degradaciones producidas por las amenazas en cada una de las dimensiones. • Se deben tener ingresados los controles/salvaguardas. • Se debe tener calculado el valor del impacto residual por cada activo. • Se debe tener ingresados la matriz de parámetros para el cálculo del riesgo.
Post-condición	El sistema contara con el riesgo residual que refleja el daño probable que pueda causar las amenazas en caso de que estas se materialicen luego de haber implementado un conjunto de salvaguardas.

Flujo principal del caso de uso	El Analista de riesgo deberá seleccionar la pestaña de procesos y seleccionar la opción de impacto residual, con el fin de que el sistema calcule los valores del impacto residual en base a la degradación calculada después de la implementación de las salvaguardas y al impacto residual de los activos.
Excepciones	No dejar campos en blanco ya que no se podrán validar los datos ingresados.

Fuente: Elaboración Propia

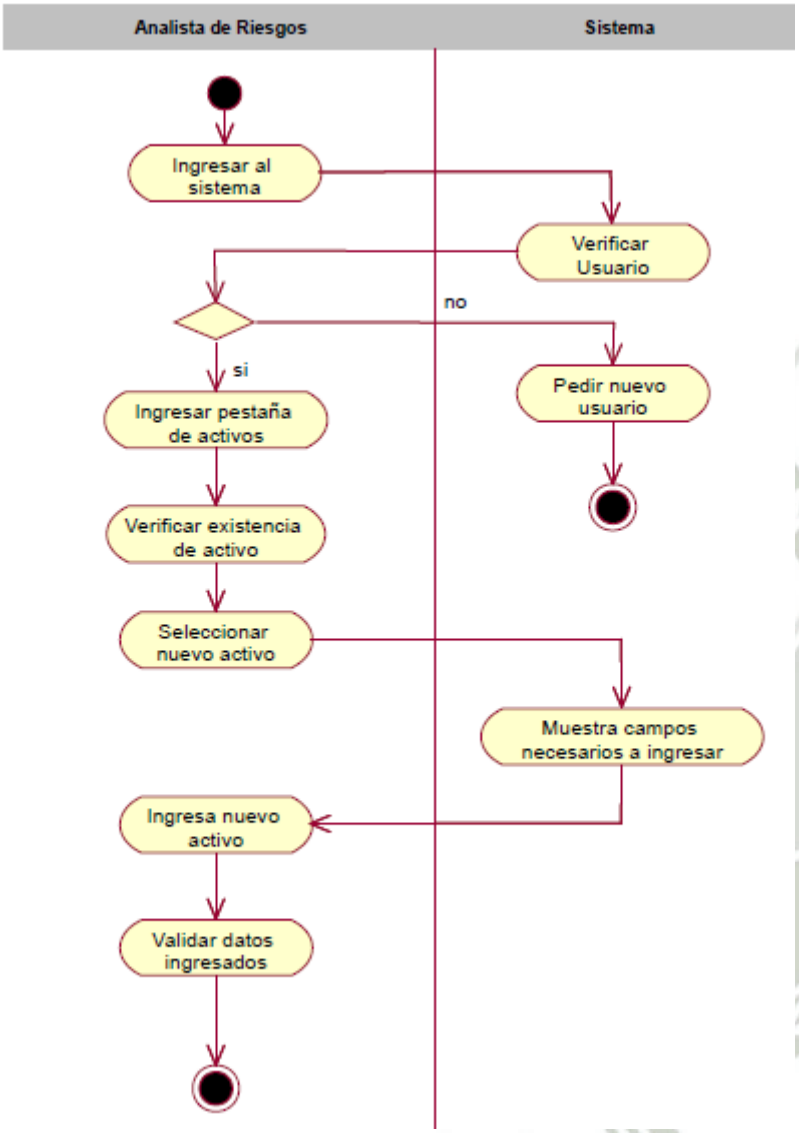
Figura 34. Riesgo Residual

Activo	Amenaza	C	I	D	A	T	Probabilidad
Aire Acondicionado	Fuego	-	-	1,4	-	-	1
Aire Acondicionado	Avería de origen físico o lógico	-	1,6	1,4	-	-	1
Aire Acondicionado	Ataque destructivo	-	-	1,4	-	-	1
Aire Acondicionado	Corte del suministro eléctrico	-	-	2,5	-	-	2
Aire Acondicionado	Condiciones inadecuadas de temperatura o humedad	-	-	2,4	-	-	2
Aire Acondicionado	Daños por agua	-	-	1,4	-	-	1
Ambiente Centro de Datos	Fuego	-	-	1,8	-	-	1
Ambiente Centro de Datos	Daños por agua	-	-	2,7	-	-	2
Ambiente Centro de Datos	Fugas de información	1,7	1,7	1,7	-	-	1
Ambiente Centro de Datos	Acceso no autorizado	1,9	1,7	1,8	1,7	-	1

Fuente: Elaboración Propia

5.2.3.4 Diagrama de Actividades: Caso de uso Identificación de Activos

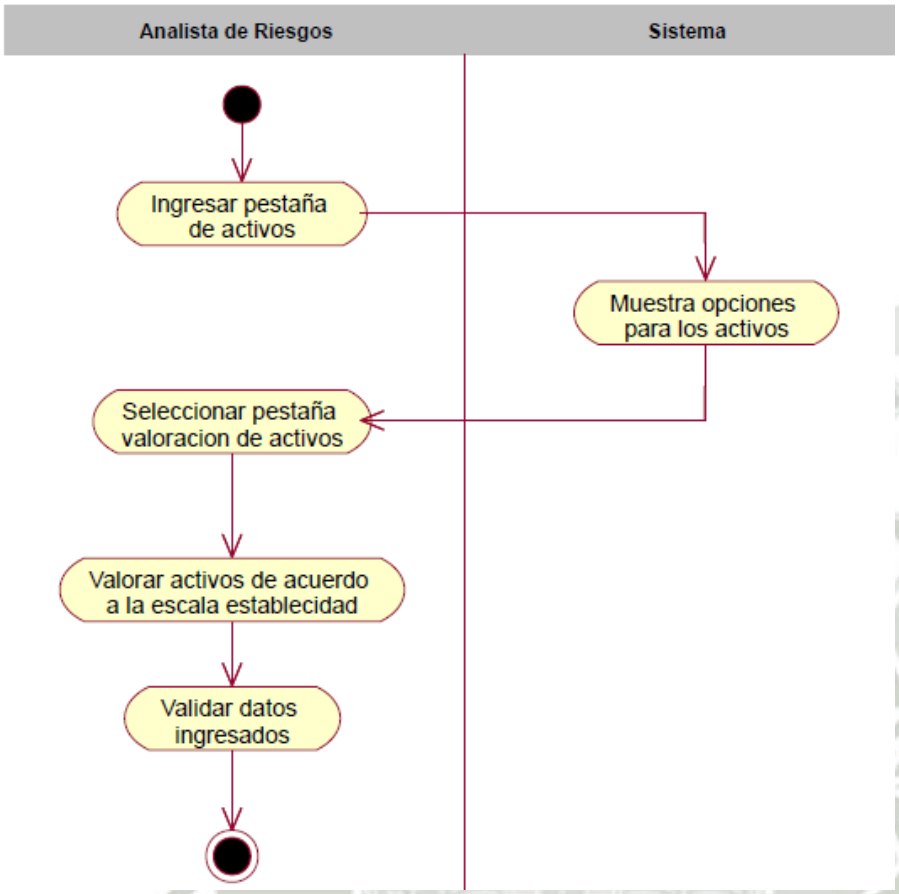
Figura 35.Diagrama actividades - Identificación de activos



Fuente: Elaboración Propia

5.2.3.5 Diagrama de Actividad: Valoración de Activos

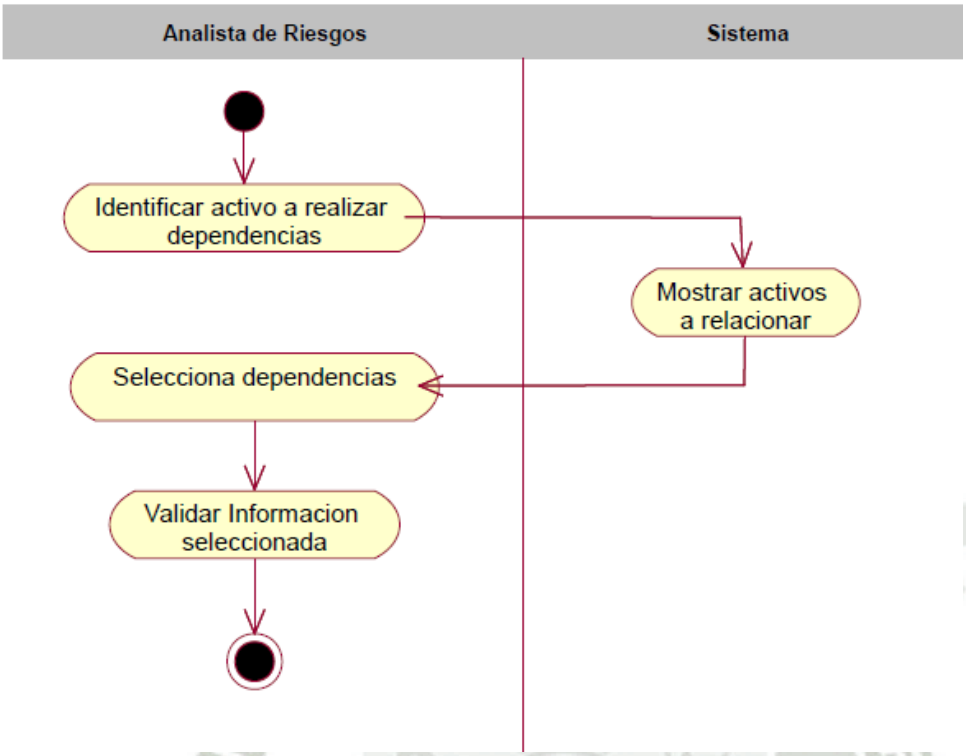
Figura 36.Diagrama de actividades - Valoración de activos



Fuente: Elaboración Propia

5.2.3.6 Diagrama de Actividades: Dependencia de Activos

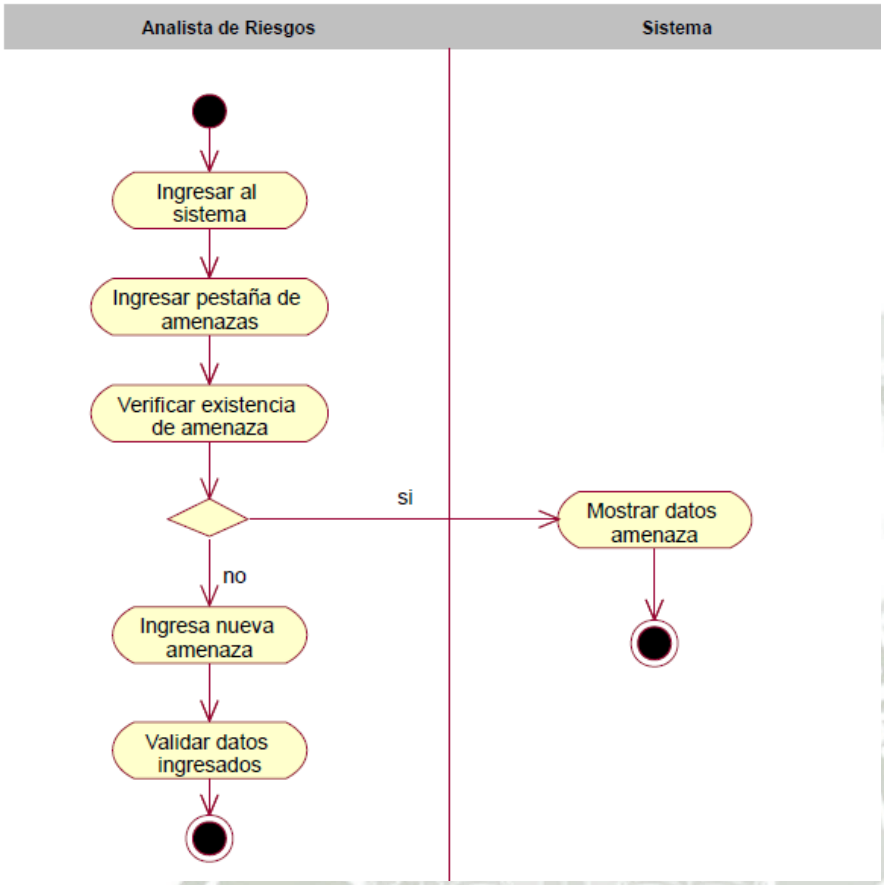
Figura 37. Diagrama de actividades - Dependencia de activos



Fuente: Elaboración Propia

5.2.3.7 Diagrama de Actividades: Identificar Amenazas

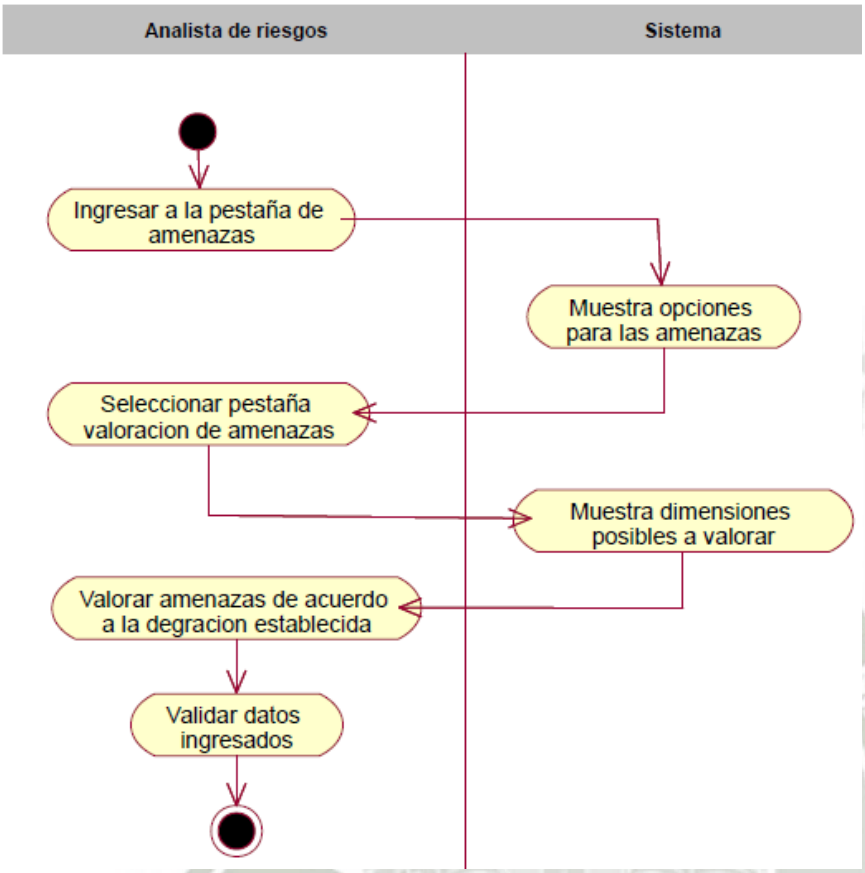
Figura 38. Diagrama de actividades -Identificar amenazas



Fuente: Elaboración Propia

5.2.3.8 Diagrama de Actividades: Valorar Amenazas

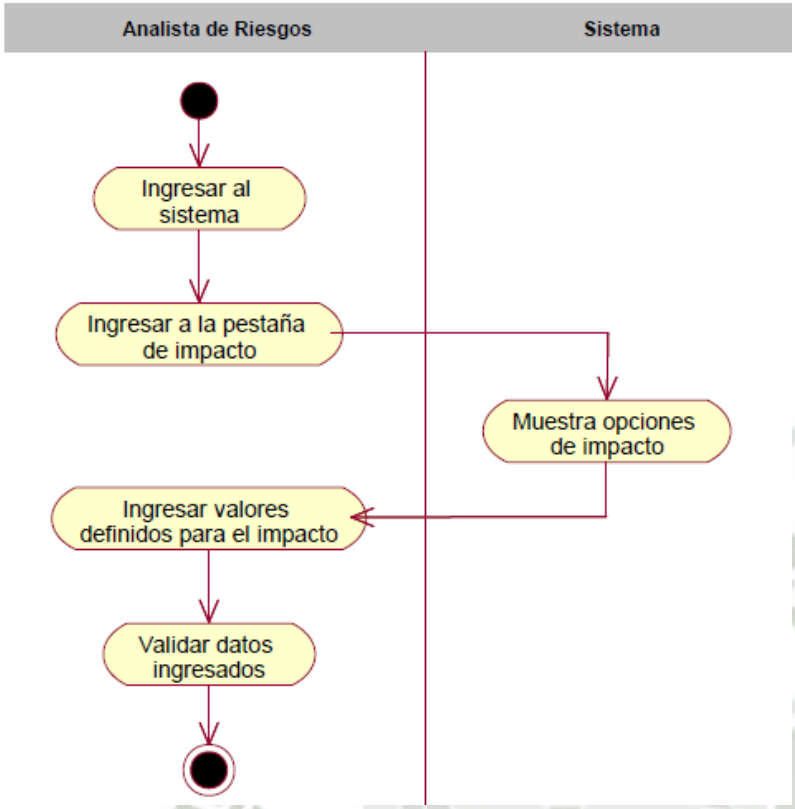
Figura 39. Diagrama de actividades - Valorar amenazas



Fuente: Elaboración propia

5.2.3.9 Diagrama de Actividades: Determinación del Impacto

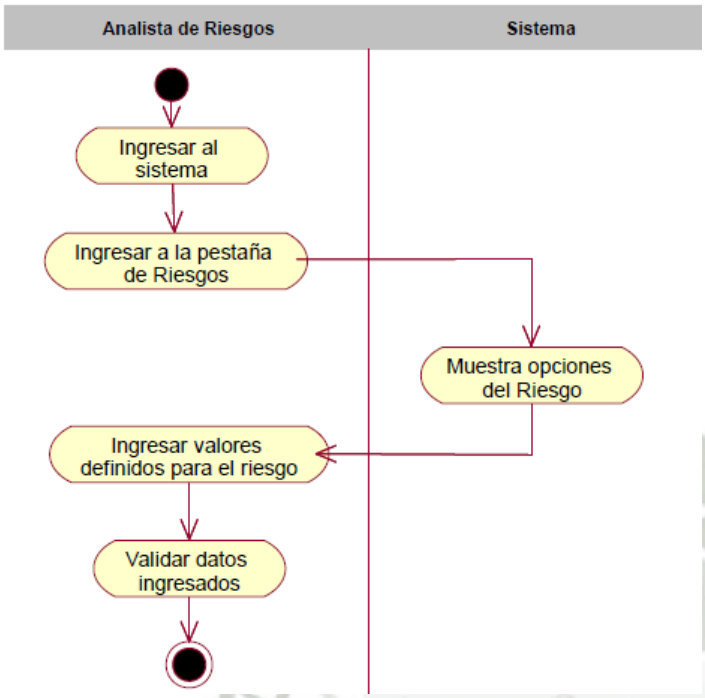
Figura 40. Diagrama de actividades - Determinación del impacto



Fuente: Elaboración Propia

5.2.3.10 Diagrama de Actividades: Determinar Riesgo

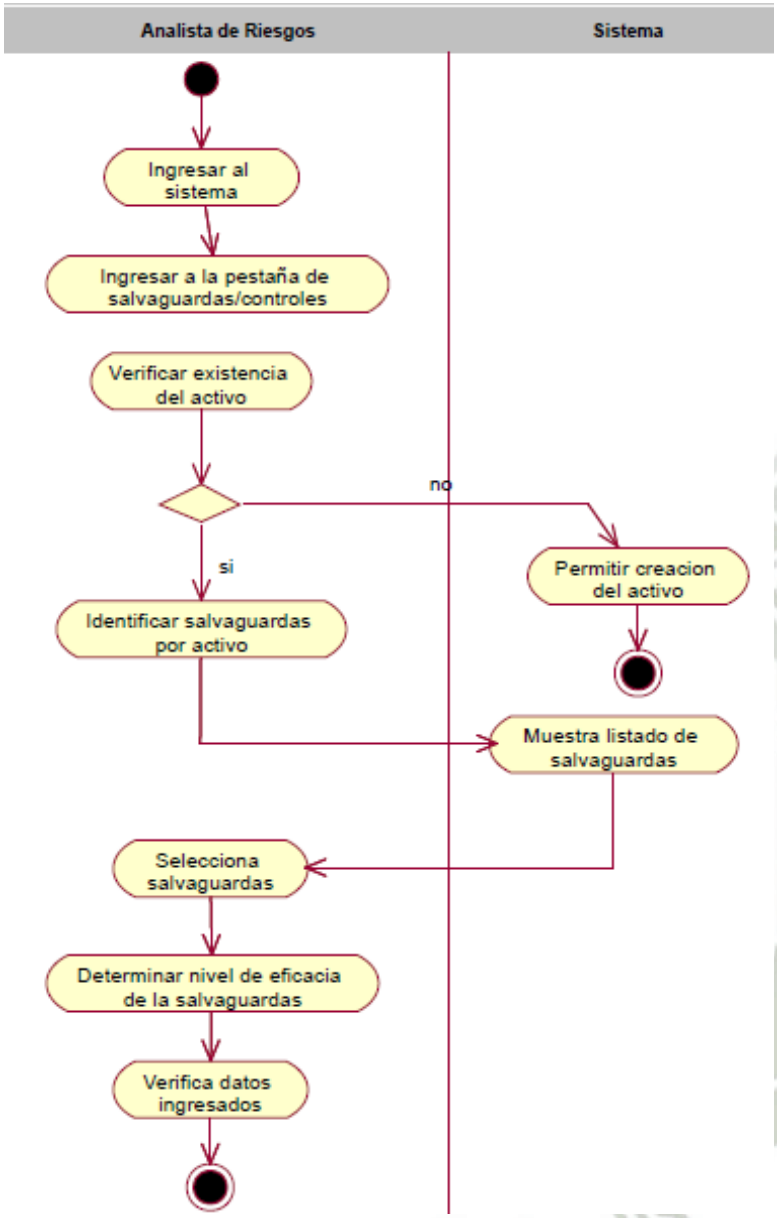
Figura 41. Diagrama de actividades - Determinar Riesgo



Fuente: Elaboración Propia

5.2.3.11 Diagrama de Actividades: Determinación de las Salvaguardas

Figura 42. Diagrama de actividades - Determinación de las salvaguardas



Fuente: Elaboración Propia

CAPITULO VI:

VALIDACIÓN DE LA METODOLOGÍA

6.1 Primera Etapa: Análisis de Riesgo

6.1.1 Fase de Identificación de los Activos

Se proceden a utilizar los datos de entrada nombrados en la metodología, teniendo como dato de salida el listado de los activos identificados.

Tabla 33. Identificación de los activos

Información del Activo				
N°	**Area**	**Nombre de Activo**	**Descripción corta**	**Propietario**
1	T.I	Ambiente Centro de Datos	Accesos a equipos	Administrador de Infraestructura
2	T.I	NAS de Almacenamiento de información	Almacenamiento de Datos	Administrador de Infraestructura
3	T.I	Equipo de proteccion electrica	Energia con Baterias	Administrador de Infraestructura
4	T.I	Aire Acondicionado Centro de Datos Principal	Enfriamiento de Equipos	Administrador de Infraestructura
5	T.I	Servidores	Servidores físicos o virtuales	Administrador de Infraestructura
6	T.I	Base de Datos	Base de datos	Administrador de Infraestructura
7	T.I	Servicio File Server	Servicio File Server	Administrador de Infraestructura
8	T.I	Proveedor de mantenimiento equipos de cómputo	Servicio de mantenimiento equipos de cómputo	Administrador de Tecnologias Cliente
9	T.I	Switch Core	Comunicación con Servidores	Adm. De Telecomunicaciones
10	T.I	Servicio de internet	Servicio que permite acceso a la nube	Adm. De Telecomunicaciones
11	T.I	Firewall	Gestiona la seguridad de las comunicaciones	Adm. De Telecomunicaciones
12	T.I	Software de monitoreo	Software que permite monitorear las redes	Adm. De Telecomunicaciones
13	T.I	Redes de comunicación	Permite las conexiones con agencias	Adm. De Telecomunicaciones
14	T.I	Servicio Sistema Core	Software para el manejo de todas las actividades de la empresa	Adm. De Telecomunicaciones
15	T.I	Servicio Correo Electronico	Servicio para el manejo de correo electronico	Adm. De Telecomunicaciones

Fuente: Elaboración Propia

6.1.2 Fase de Valoración de los Activos

Se procede a valorizar los activos en las 5 dimensiones identificadas con las que se va a trabajar, dando un valor entre 0 y 10 de acuerdo al nivel de importancia que tienen los activos dentro de la organización.

Tabla 34. Valoración de Activos

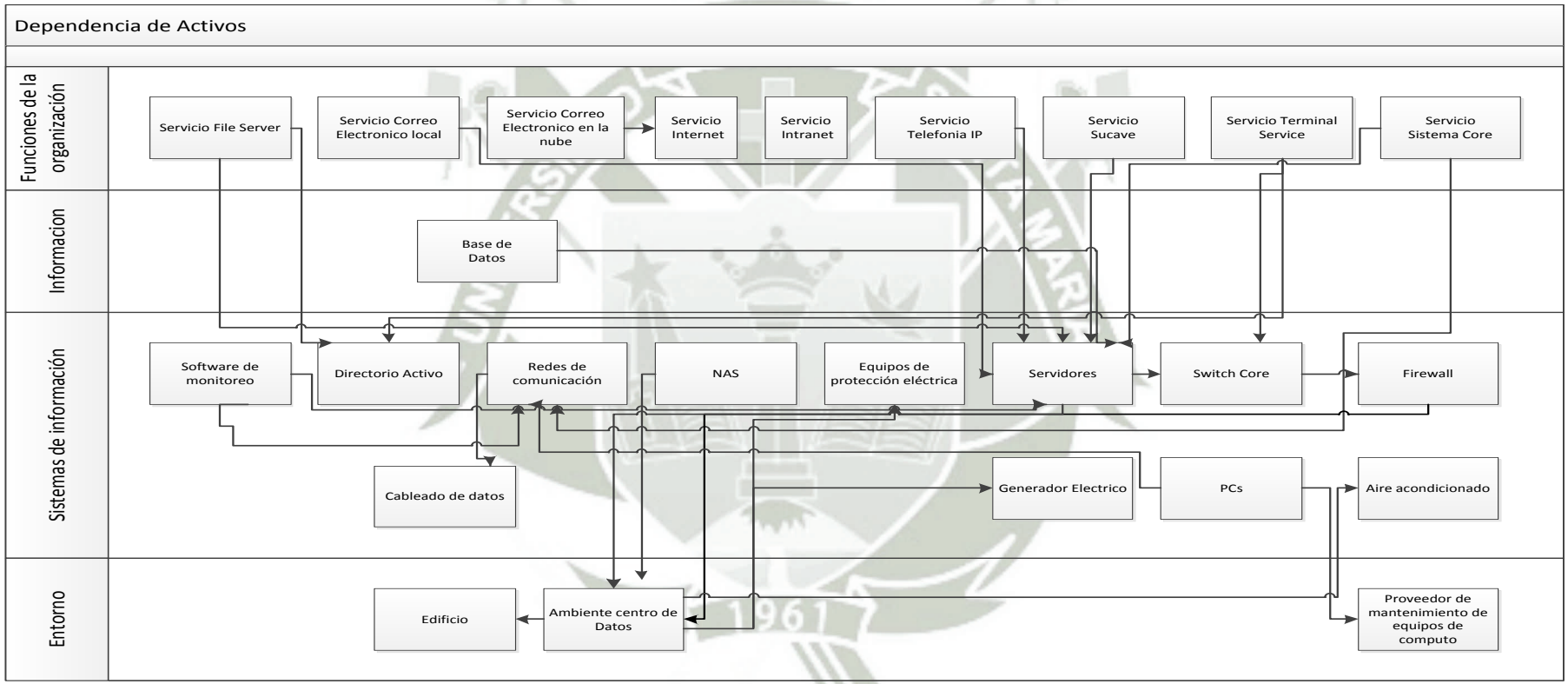
ACTIVOS DE INFORMACIÓN											
Información del Activo					Valorización						
N°	Area	Nombre de Activo	Tipo de activo	Ubicación	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Total Valoración	Valor
1	T.I	Ambiente Centro de Datos	[L] Instalaciones	Centro Principal	8	8	8	8	8	8	MUY ALTO
2	T.I	NAS de Almacenamiento de información	[HW] Equipamiento informático (hardware)	Centro Principal	10	10	10	0	0	10	EXTREMO
3	T.I	Equipo de proteccion electrica	[AUX] Equipamiento auxiliar	Centro Principal	0	8	6	0	0	7	ALTO
4	T.I	Aire Acondicionado Centro de Datos Principal	[AUX] Equipamiento auxiliar	Centro Principal	0	8	6	0	0	7	ALTO
5	T.I	Servidores	[HW] Equipamiento informático (hardware)	Caja de Servidores	8	8	10	0	0	9	MUY ALTO
6	T.I	Base de Datos	[D] Datos / Información	Of. Entrega de Servicios	10	10	10	10	10	10	EXTREMO
7	T.I	Servicio File Server	[S] Servicios	Of. Entrega de Servicios	8	8	6	0	0	7	ALTO
8	T.I	Proveedor de mantenimiento equipos de cómputo	[P] Personal	Of. Entrega de Servicios	4	4	4	4	0	4	MEDIO
9	T.I	Switch Core	[HW] Equipamiento informático (hardware)	CD	10	10	10	0	0	10	EXTREMO
10	T.I	Servicio de internet	[SW] Software - Aplicaciones informáticas	CD	0	0	10	6	0	8	MUY ALTO
11	T.I	Firewall	[HW] Equipamiento informático (hardware)	CD	10	10	10	10	10	10	EXTREMO
12	T.I	Software de monitoreo	[SW] Software - Aplicaciones informáticas	Centro Principal	0	0	10	0	0	10	EXTREMO
13	T.I	Redes de comunicación	[COM] Redes de comunicaciones	Centro Principal	10	10	10	0	0	10	EXTREMO
14	T.I	Servicio Sistema Core	[S] Servicios	Centro Principal	10	10	10	10	10	10	EXTREMO
15	T.I	Servicio Correo Electronico	[S] Servicios	Centro Principal	8	8	8	8	8	8	MUY ALTO

Fuente: Elaboración propia

6.1.3 Fase de Identificación de los las Dependencias de los Activos

Se procede a identificar las dependencias que existe entre los activos con el fin de determinar el valor acumulado de los activos.

Figura 43. Dependencia de activos



Fuente: Elaboración propia

6.1.4 Valor Acumulado de los Activos

Se obtuvo el valor acumulado de los activos, determinado por las dependencias que existen entre los activos, se utilizó el diagrama de dependencias para un mejor análisis y comprensión en la obtención de dicho valor.

Tabla 35. Valor acumulado de los activos

ACTIVOS DE INFORMACIÓN										
		Información del Activo		Valor Acumulado						
N°	Area	Nombre de Activo	Tipo de activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Total Valoración	Valor
1	T.I	Ambiente Centro de Datos	[L] Instalaciones	10	10	10	10	10	10	EXTREMO
2	T.I	NAS de Almacenamiento de información	[HW] Equipamiento informático (hardware)	10	10	10	0	0	10	EXTREMO
3	T.I	Equipo de proteccion electrica	[AUX] Equipamiento auxiliar	0	8	6	0	0	7	ALTO
4	T.I	Aire Acondicionado Centro de Datos Principal	[AUX] Equipamiento auxiliar	0	8	6	0	0	7	ALTO
5	T.I	Servidores	[HW] Equipamiento informático (hardware)	10	10	10	10	10	10	EXTREMO
6	T.I	Base de Datos	[D] Datos / Información	10	10	10	10	10	10	EXTREMO
7	T.I	Servicio File Server	[S] Servicios	8	8	6	0	0	7	ALTO
8	T.I	Proveedor de mantenimiento equipos de cómputo	[P] Personal	7	5	7	5	0	6	ALTO
9	T.I	Switch Core	[HW] Equipamiento informático (hardware)	10	10	10	10	10	10	EXTREMO
10	T.I	Servicio de internet	[SW] Software - Aplicaciones informáticas	0	8	10	6	0	8	MUY ALTO
11	T.I	Firewall	[HW] Equipamiento informático (hardware)	10	10	10	10	10	10	EXTREMO
12	T.I	Software de monitoreo	[SW] Software - Aplicaciones informáticas	0	0	10	0	0	10	EXTREMO
13	T.I	Redes de comunicación	[COM] Redes de comunicaciones	10	10	10	10	10	10	EXTREMO
14	T.I	Servicio Sistema Core	[SW] Software - Aplicaciones informáticas	10	10	10	10	10	10	EXTREMO
15	T.I	Servicio Correo Electronico	[S] Servicios	8	8	8	8	8	8	MUY ALTO

Fuente: Elaboración propia

6.1.5 Fase Identificación de Amenazas y Vulnerabilidades

Se procedió a la identificación de las amenazas a las cuales están sujetos los activos, utilizando el catalogo brindado por Magerit y otras amenazas que fueron identificadas en el transcurso de la investigación. En el caso de las vulnerabilidades se procedió a nombrarlas en base a la experiencia del experto.

Tabla 36. Identificación de amenazas y vulnerabilidades

AMENAZAS - VULNERABILIDADES						
		Información del Activo		Amenazas		
N°	Departamento	Nombre de Activo	Descripción corta	Tipo de amenaza	Amenazas	Vulnerabilidades
1	T.I.	Ambiente Centro de Datos	Accesos a equipos	Desastres Naturales	Fuego	Acceso de Personal no autorizado Monitoreo insuficiente se seguridad para infraestructura y medio ambiente
				Desastres Naturales	Daños por agua	Falta de controles para reducir el riesgo de amenazas
				Errores y fallos no intencionados	Fugas de Informacion	No se mantiene un control o registro de acceso a las áreas restringidas
				Ataques intencionados	Acceso no autorizado	Falta de un registro de acceso a la sala.
				Ataques intencionados	Ataque destructivo	No se tienen procedimientos para el personal que realiza mantenimiento en la institución.
				De origen industrial	Condiciones inadecuadas de temperatura o humedad	No se tiene un control de la temperatura diaria en el area
2	T.I.	NAS de Almacenamiento de información	Almacenamiento de Datos	Desastres Naturales	Fuego	Acceso de Personal no autorizado. Monitoreo insuficiente se seguridad para infraestructura y medio ambiente
				De origen industrial	Avería de origen físico o lógico	Falla de hadware y componentes.
				Ataques intencionados	Ataque destructivo	No se tienen procedimientos para el personal que realiza mantenimiento en la institución. Procedimientos inadecuados de contratacion

Fuente: Elaboración propia

AMENAZAS - VULNERABILIDADES						
		Información del Activo		Amenazas		
N°	Departamento	Nombre de Activo	Descripción corta	Tipo de amenaza	Amenazas	Vulnerabilidades
				De origen industrial	Condiciones inadecuadas de temperatura o humedad	No se tiene un control de la temperatura diaria en el area
				De origen industrial	Daños por agua	Falta de controles para reducir el riesgo de amenazas
				De origen industrial	Corte del suministro Electrico	Falta de mantenimientos en la infraestructura
				Errores y fallos no intencionados	Condiciones inadecuadas de temperatura o humedad	No se tiene un control de la temperatura diaria en el area
				Errores y fallos no intencionados	Errores del administrador	Falta de capacitacion al personal
				Ataques intencionados	Errores de mantenimiento / actualización de equipos Hardware)	Degradacion del hadware Falta plan de mantenimiento para los equipos
				Ataques intencionados	Uso no Previsto	Falta de controles para la supervision y el uso adecuado de los activos.
				Ataques intencionados	Acceso no autorizado	Falta de procedimiento formal para el registro y retiro del registro de usuario Falta del proceso formal para la revision de los derechos de acceso Personal de vigilancia no lleva un control de los ingresos de las personas a areas no autorizadas.
				Ataques intencionados	Manipulación de los equipos	Falta de procedimientos para el uso correcto de los equipos
				Ataques intencionados	Robo	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la informacion Falta de control de los activos que se encuentran fuera de las instalaciones
3	T.I.	UPS Centro de Datos	Energia con Baterias	Desastres Naturales	Fuego	Acceso de Personal no autorizado. Monitoreo insuficiente se seguridad para infraestructura y medio ambiente
				De origen industrial	Avería de origen físico o lógico	Falla de hadware y componentes.

Fuente: Elaboración propia

AMENAZAS - VULNERABILIDADES						
		Información del Activo		Amenazas		
N°	Departamento	Nombre de Activo	Descripción corta	Tipo de amenaza	Amenazas	Vulnerabilidades
				Ataques intencionados	Ataque destructivo	No se tienen procedimientos para el personal que realiza mantenimiento en la institución. Procedimientos inadecuados de contratacion
				De origen industrial	Corte de Suministro Electrico	Falta de mantenimientos en la infraestructura
				Errores y fallos no intencionados	Condiciones inadecuadas de temperatura o humedad	No se tiene un control de la temperatura diaria en el area
4	T.I.	Aire Acondicionado Centro de Datos Principal	Enfriamiento de Equipos	Desastres Naturales	Fuego	Acceso de Personal no autorizado. Monitoreo insuficiente se seguridad para infraestructura y medio ambiente
				De origen industrial	Avería de origen físico	Falla de hadware y componentes.
				Ataques intencionados	Ataque destructivo	No se tienen procedimientos para el personal que realiza mantenimiento en la institución. Procedimientos inadecuados de contratacion
				De origen industrial	Corte de Suministro Electrico	Falta de mantenimientos en la infraestructura
				Errores y fallos no intencionados	Condiciones inadecuadas de temperatura o humedad	No se tiene un control de la temperatura diaria en el area
				De origen industrial	Daños por agua	Falta de controles para reducir el riesgo de amenazas

Fuente: Elaboración propia

AMENAZAS - VULNERABILIDADES						
		Información del Activo		Amenazas		
N°	Departamento	Nombre de Activo	Descripción corta	Tipo de amenaza	Amenazas	Vulnerabilidades
5	T.I.	Servidores	Servidores físicos o virtuales	Desastres Naturales	Fuego	Acceso de Personal no autorizado. Monitoreo insuficiente se seguridad para infraestructura y medio ambiente
				De origen industrial	Avería de origen físico o lógico	Falla de hadware y componentes.
				De origen industrial	Daños por agua	Falta de controles para reducir el riesgo de amenazas
				De origen industrial	Corte del suministro Electrico	Falta de mantenimientos en la infraestructura
				Errores y fallos no intencionados	Condiciones inadecuadas de temperatura o humedad	No se tiene un control de la temperatura diaria en el area
				Errores y fallos no intencionados	Errores del administrador	Falta de capacitacion al personal
				Errores y fallos no intencionados	Errores de mantenimiento / actualización de equipos Hardware)	Degradacion del hadware Falta plan de mantenimiento para los equipos
				Ataques intencionados	Uso no Previsto	Falta de controles para la supervision y el uso adecuado de los activos.
				Ataques intencionados	Acceso no autorizado	Falta de procedimiento formal para el registro y retiro del registro de usuario Falta del proceso formal para la revision de los derechos de acceso
				Ataques intencionados	Manipulación de los equipos	Falta de procedimientos para el uso correcto de los equipos
				Ataques intencionados	Robo	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la informacion Falta de control de los activos que se encuentran fuera de las instalaciones
				Ataques intencionados	Ataque destructivo	No se tienen procedimientos para el personal que realiza mantenimiento en la institución. Procedimientos inadecuados de contratacion

Fuente: Elaboración propia

AMENAZAS - VULNERABILIDADES						
		Información del Activo		Amenazas		
N°	Departamento	Nombre de Activo	Descripción corta	Tipo de amenaza	Amenazas	Vulnerabilidades
6	T.I.	Base de Datos	Base de datos	De origen industrial	Avería de origen físico o lógico	Falla de hadware y componentes.
				De origen industrial	Cortes del suministro eléctrico	Falta de mantenimientos en la infraestructura
				Errores y fallos no intencionados	Errores del administrador	Falta de capacitacion al personal Falta de personal especializado
				Errores y fallos no intencionados	Errores de monitorización	Falta de personal especializado
				Errores y fallos no intencionados	Errores de configuración	Falta de personal especializado
				Ataques intencionados	Difusión de software dañino	Falta de controles para la proteccoin de virus
				Errores y fallos no intencionados	Escape de información	Realización de copias no autorizadas de la Base de Datos. Exceso de privilegios al administrador de Base de Datos. Falta de controles para el manejo de informacion
				Errores y fallos no intencionados	Alteración accidental de la información	Falta de personal especializado
				Errores y fallos no intencionados	Destrucción de información	Falta de personal especializado
				Errores y fallos no intencionados	Fugas de información	Falta de controles para el manejo de informacion
				Ataques intencionados	Acceso no autorizado	Falta de procedimiento formal para el registro y retiro del registro de usuario Falta del proceso formal para la revision de los derechos de acceso
				Ataques intencionados	Modificación deliberada de la información	Privilegios para los usuarios de acceso a las aplicaciones no son revisados periódicamente
				Ataques intencionados	Denegación de servicio	Acceso a la BD desde otras aplicaciones

Fuente: Elaboración propia

6.1.6 Valorización de Amenazas

Ya identificadas las amenazas a las que están expuestos los activos, se procede a determinar la degradación que puedan causar las amenazas y la probabilidad de ocurrencia que puedan tener.

Tabla 37. Valoración de amenazas

VALORACION AMENAZAS									
		Información del Activo		Valorización					
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probalidad
1	T.I.	Ambiente Centro de Datos	Fuego	-	-	100%	-	-	MPF
			Daños por agua	-	-	50%	-	-	PF
			Fugas de Informacion	50%	50%	50%	-	-	MPF
			Acceso no autorizado	100%	25%	75%	25%	-	PF
			Ataque destructivo	100%	100%	100%	100%	100%	MPF
			Condiciones inadecuadas de temperatura o humedad	-	-	75%	-	-	PF
2	T.I.	NAS de Almacenamiento de información	Fuego	-	100%	100%	-	100%	MPF
			Avería de origen físico o lógico	-	100%	100%	-	100%	MPF
			Ataque destructivo	-	100%	100%	100%	100%	MPF

Fuente: Elaboración propia

VALORACION AMENAZAS									
		Información del Activo		Valorización					
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probalidad
			Condiciones inadecuadas de temperatura o humedad	-	100%	100%	-	100%	PF
			Daños por agua	-	-	100%	-	-	PF
			Corte del suministro Electrico	-	-	100%	-	-	PF
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF
			Errores del administrador	100%	100%	100%	-	-	PF
			Errores de mantenimiento / actualización de equipos Hardware)	-	100%	100%	-	-	PF
			Uso no Previsto	100%	100%	100%	-	-	MPF
			Acceso no autorizado	75%	75%	-	-	-	MPF
			Manipulación de los equipos	25%	-	25%	-	-	MPF
			Robo	25%	-	25%	-	-	MPF
3	T.I.	UPS Centro de Datos	Fuego	-	-	100%	-	-	MPF
			Avería de origen físico o lógico	-	100%	100%	-	100%	MPF

Fuente: Elaboración propia

VALORACION AMENAZAS									
		Información del Activo		Valorización					
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probalilidad
			Ataque destructivo	-	-	25%	-	-	MPF
			Corte de Suministro Electrico	-	-	100%	-	-	PF
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF
4	T.I.	Aire Acondicionado Centro de Datos Principal	Fuego	-	-	100%	-	-	MPF
			Avería de origen físico	-	100%	100%	-	100%	MPF
			Ataque destructivo	-	-	25%	-	-	MPF
			Corte de Suministro Electrico	-	-	100%	-	-	PF
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF
			Daños por agua	-	-	100%	-	-	PF

Fuente: Elaboración propia

VALORACION AMENAZAS									
		Información del Activo		Valorización					
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probalidad
5	T.I.	Servidores	Fuego	-	-	100%	-	-	MPF
			Avería de origen físico o lógico	-	-	100%	-	-	MPF
			Daños por agua	-	-	100%	-	-	PF
			Corte del suministro Electrico	-	-	100%	-	-	PF
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF
			Errores del administrador	100%	100%	100%	-	-	PF
			Errores de mantenimiento / actualización de equipos Hardware)	-	100%	100%	-	-	PF
			Uso no Previsto	100%	100%	100%	-	-	MPF
			Acceso no autorizado	75%	75%	-	-	-	MPF
			Manipulación de los equipos	25%	-	25%	-	-	MPF
			Robo	25%	-	25%	-	-	MPF
			Ataque destructivo	-	-	100%	-	-	MPF

Fuente: Elaboración propia

VALORACION AMENAZAS									
		Información del Activo		Valorización					
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probailidad
6	T.I.	Base de Datos	Avería de origen físico o lógico	-	-	100%	-	-	MPF
			Cortes del suministro eléctrico	-	-	100%	-	-	MPF
			Errores del administrador	100%	100%	100%	-	-	MPF
			Errores de monitorización	-	100%	-	-	100%	MPF
			Errores de configuración	-	100%	-	-	-	MPF
			Difusión de software dañino	100%	100%	100%	-	-	MPF
			Escape de información	100%	-	-	-	-	MPF
			Alteración accidental de la información	-	100%	-	-	-	MPF
			Destrucción de información	-	-	100%	-	-	MPF
			Fugas de información	100%	-	-	-	-	MPF
			Acceso no autorizado	100%	100%	-	-	-	MPF
			Modificación deliberada de la información	-	100%	-	-	-	MPF
			Denegación de servicio	-	-	100%	-	-	PF

Fuente: Elaboración propia

6.1.7 Fase de Determinación del Impacto Potencial

- **Impacto Acumulado**

Ya identificados y valorizados los activos, las amenazas a las que están expuestos los mismos y valorizadas por medio de la degradación que puedan causar, se procede al cálculo del impacto acumulado, en base a la matriz definida en el modelo.

Tabla 38. Impacto acumulado

IMPACTO ACUMULADO								
		Información del Activo		Impacto Acumulado				
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
1	T.I.	Ambiente Centro de Datos	Fuego	[-]	[-]	[10]	[-]	[-]
			Daños por agua	[-]	[-]	[9]	[-]	[-]
			Fugas de Informacion	[9]	[9]	[9]	[-]	[-]
			Acceso no autorizado	[10]	[8]	[10]	[8]	[-]
			Ataque destructivo	[10]	[10]	[10]	[10]	[10]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[10]	[-]	[-]
2	T.I.	NAS de Almacenamiento de información	Fuego	[-]	[10]	[10]	[-]	[10]
			Avería de origen físico o lógico	[-]	[10]	[10]	[-]	[10]
			Ataque destructivo	[-]	[10]	[10]	[10]	[10]

Fuente: Elaboración propia

N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
			Condiciones inadecuadas de temperatura o humedad	[-]	[9]	[9]	[-]	[9]
			Daños por agua	[-]	[-]	[10]	[-]	[-]
			Corte del suministro Electrico	[-]	[-]	[9]	[-]	[-]
			Errores del administrador	[10]	[10]	[10]	[-]	[-]
			Errores de mantenimiento / actualización de equipos Hardware)	[-]	[10]	[10]	[-]	[-]
			Uso no Previsto	[9]	[9]	[9]	[-]	[-]
			Acceso no autorizado	[10]	[10]	[-]	[-]	[-]
			Manipulación de los equipos	[8]	[-]	[8]	[-]	[-]
			Robo	[10]	[-]	[10]	[-]	[-]
3	T.I.	UPS Centro de Datos	Fuego	[-]	[-]	[10]	[-]	[-]
			Avería de origen físico o lógico	[-]	[10]	[10]	[-]	[10]

Fuente: Elaboración propia

IMPACTO ACUMULADO								
		Información del Activo		Impacto Acumulado				
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
			Ataque destructivo	[-]	[-]	[8]	[-]	[-]
			Corte de Suministro Electrico	[-]	[-]	[10]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[10]	[-]	[-]
4	T.I.	Aire Acondicionado Centro de Datos Principal	Fuego	[-]	[-]	[10]	[-]	[-]
			Avería de origen físico	[-]	[10]	[10]	[-]	[10]
			Ataque destructivo	[-]	[-]	[8]	[-]	[-]
			Corte de Suministro Electrico	[-]	[-]	[10]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[10]	[-]	[-]
			Daños por agua	[-]	[-]	[10]	[-]	[-]

Fuente: Elaboración propia

IMPACTO ACUMULADO								
		Información del Activo		Impacto Acumulado				
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
5	T.I.	Servidores	Fuego	[-]	[-]	[10]	[-]	[-]
			Daños por agua	[-]	[-]	[10]	[-]	[-]
			Avería de origen físico o lógico	[-]	[-]	[10]	[-]	[-]
			Corte del suministro Electrico	[-]	[-]	[10]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[10]	[-]	[-]
			Errores del administrador	[10]	[10]	[10]	[-]	[-]
			Errores de mantenimiento / actualización de equipos Hardware)	[-]	[10]	[10]	[-]	[-]
			Uso no Previsto	[10]	[10]	[10]	[-]	[-]
			Acceso no autorizado	[10]	[10]	[-]	[-]	[-]
			Manipulación de los equipos	[8]	[-]	[8]	[-]	[-]
			Robo	[8]	[-]	[8]	[-]	[-]
			Ataque destructivo	[-]	[-]	[10]	[-]	[-]

Fuente: Elaboración propia

IMPACTO ACUMULADO								
		Información del Activo		Impacto Acumulado				
N°	Departamento	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
6	T.I.	Base de Datos	Avería de origen físico o lógico	[-]	[-]	[10]	[-]	[-]
			Cortes del suministro eléctrico	[-]	[-]	[10]	[-]	[-]
			Errores del administrador	[10]	[10]	[10]	[-]	[-]
			Errores de monitorización	[-]	[10]	[-]	[-]	[10]
			Errores de configuración	[-]	[10]	[-]	[-]	[-]
			Difusión de software dañino	[10]	[10]	[10]	[-]	[-]
			Escape de información	[10]	[-]	[-]	[-]	[-]
			Alteración accidental de la información	[-]	[10]	[-]	[-]	[-]
			Destrucción de información	[-]	[-]	[10]	[-]	[-]
			Fugas de información	[10]	[-]	[-]	[-]	[-]
			Acceso no autorizado	[10]	[10]	[-]	[-]	[-]
			Modificación deliberada de la información	[-]	[10]	[-]	[-]	[-]
			Denegación de servicio	[-]	[-]	[10]	[-]	[-]

Fuente: Elaboración propia

6.1.8 Determinación de los Niveles de Riesgo

Se es necesario definir los valores con los que se trabajara para el cálculo del riesgo, en la metodología propuesta se definió la matriz con los siguientes valores, hay que tener en cuenta que esos valores pueden ser variables, dependiendo de la organización donde se implemente dicha metodología.

Tabla 39. Riesgo Potencial

		Riesgo									
		Impacto									
		[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Probabilidad	5	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)	(5,7)	(5,8)	(5,9)	(5,10)
	4	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)	(4,7)	(4,8)	(4,9)	(4,10)
	3	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)	(3,10)
	2	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)	(2,9)	(2,10)
	1	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)	(1,10)

Fuente: Elaboración propia

6.1.9 Determinación del Riesgo Potencial

Luego de haber determinado el impacto acumulado de los activos en base a la degradación causada por la amenaza y al valor de los activos. Se procedió a realizar el cálculo del riesgo acumulado en base al impacto acumulado y a la probabilidad.

- **Riesgo Acumulado**

Tabla 40. Riesgo Acumulado

RIESGO ACUMULADO										
		Información del Activo		Riesgo Acumulado						
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probabilidad
1	T.I.	Ambiente Centro de Datos	Fuego	(-)	(-)	(5,10)	(-)	(-)	5
			Daños por agua	(-)	(-)	(1,9)	(-)	(-)	1
			Fugas de Informacion	(2,9)	(2,9)	(2,9)	(-)	(-)	2
			Acceso no autorizado	(1,10)	(1,8)	(1,10)	(1,8)	(-)	1
			Ataque destructivo	(1,10)	(1,10)	(1,10)	(1,10)	(1,10)	1
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(3,10)	(-)	(-)	3
2	T.I.	NAS de Almacenamiento de información	Fuego	(-)	(1,10)	(1,10)	(-)	(1,10)	1
			Avería de origen físico o lógico	(-)	(2,10)	(2,10)	(-)	(2,10)	2
			Ataque destructivo	(-)	(1,10)	(1,10)	(1,10)	(1,10)	1

Fuente: Elaboración propia

			Condiciones inadecuadas de temperatura o humedad	(-)	(2,10)	(2,10)	(-)	(2,10)	2
			Daños por agua	(-)	(-)	(1,10)	(-)	(-)	1
			Corte del suministro Electrico	(-)	(-)	(3,10)	(-)	(-)	3
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,10)	(-)	(-)	2
			Errores del administrador	(1,10)	(1,10)	(1,10)	(-)	(-)	1
			Errores de mantenimiento / actualización de equipos Hardware)	(-)	(1,10)	(1,10)	(-)	(-)	1
			Uso no Previsto	(2,10)	(2,10)	(2,10)	(-)	(-)	2
			Acceso no autorizado	(1,10)	(1,10)	(-)	(-)	(-)	1
			Manipulación de los equipos	(1,8)	(-)	(1,8)	(-)	(-)	1
			Robo	(1,8)	(-)	(1,8)	(-)	(-)	1
3	T.I.	UPS Centro de Datos	Fuego	(-)	(-)	(1,10)	(-)	(-)	1
			Avería de origen físico o lógico	(-)	(1,10)	(1,10)	(-)	(1,10)	1

Fuente: Elaboración propia

			Ataque destructivo	(-)	(-)	(1,8)	(-)	(-)	1
			Corte de Suministro Electrico	(-)	(-)	(3,10)	(-)	(-)	3
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,10)	(-)	(-)	2
4	T.I.	Aire Acondicionado Centro de Datos Principal	Fuego	(-)	(-)	(1,10)	(-)	(-)	1
			Avería de origen físico	(-)	(1,10)	(1,10)	(-)	(1,10)	1
			Ataque destructivo	(-)	(-)	(1,8)	(-)	(-)	1
			Corte de Suministro Electrico	(-)	(-)	(3,10)	(-)	(-)	3
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,10)	(-)	(-)	2
			Daños por agua	(-)	(-)	(1,10)	(-)	(-)	1

Fuente: Elaboración propia

5	T.I.	Servidores	Fuego	(-)	(-)	(1,10)	(-)	(-)	1
			Daños por agua	(-)	(-)	(1,10)	(-)	(-)	1
			Avería de origen físico o lógico	(-)	(-)	(1,10)	(-)	(-)	1
			Corte del suministro Electrico	(-)	(-)	(3,10)	(-)	(-)	3
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,10)	(-)	(-)	2
			Errores del administrador	(1,10)	(1,10)	(1,10)	(-)	(-)	1
			Errores de mantenimiento / actualización de equipos Hardware)	(-)	(1,10)	(1,10)	(-)	(-)	1
			Uso no Previsto	(1,10)	(1,10)	(1,10)	(-)	(-)	1
			Acceso no autorizado	(1,10)	(1,10)	(-)	(-)	(-)	1
			Manipulación de los equipos	(2,8)	(-)	(2,8)	(-)	(-)	2
			Robo	(1,8)	(-)	(1,8)	(-)	(-)	1
			Ataque destructivo	(-)	(-)	(1,10)	(-)	(-)	1

Fuente: Elaboración propia

6	T.I.	Base de Datos	Avería de origen físico o lógico	(-)	(-)	(1,10)	(-)	(-)	1
			Cortes del suministro eléctrico	(-)	(-)	(3,10)	(-)	(-)	3
			Errores del administrador	(1,10)	(1,10)	(1,10)	(-)	(-)	1
			Errores de monitorización	(-)	(1,10)	(-)	(-)	(1,10)	1
			Errores de configuración	(-)	(1,10)	(-)	(-)	(-)	1
			Difusión de software dañino	(2,10)	(2,10)	(2,10)	(-)	(-)	2
			Escape de información	(2,10)	(-)	(-)	(-)	(-)	2
			Alteración accidental de la información	(-)	(1,10)	(-)	(-)	(-)	1
			Destrucción de información	(-)	(-)	(1,10)	(-)	(-)	1
			Fugas de información	(2,10)	(-)	(-)	(-)	(-)	2
			Acceso no autorizado	(1,10)	(1,10)	(-)	(-)	(-)	1
			Modificación deliberada de la información	(-)	(1,10)	(-)	(-)	(-)	1
			Denegación de servicio	(-)	(-)	(1,10)	(-)	(-)	1

Fuente: Elaboración propia

6.2 Segunda Etapa: Gestión de los Riesgos

6.2.1 Fase de Determinación de la Eficacia de las Salvaguardas

Ya identificados los riesgos a los cuales se encuentran sometidos los activos, se tienen que seleccionar un conjunto de salvaguardas que ayuden a mitigar el riesgo, la metodología propone la utilización de los controles establecidos por la ISO 27002:2013. Por cada salvaguarda seleccionada se debe definir un nivel de eficacia.

Tabla 41. Determinación de las salvaguardas

VALORACION AMENAZAS											
		Información del Activo		Valorización							
N°	Area	Nombre de Activo	Amenazas	C	I	D	A	T	P	Salvaguardas	Eficacia
1	T.I.	Ambiente Centro de Datos	Fuego	-	-	100%	-	-	MPF	Seguras (70%) 11.2.1 Emplazamiento y proteccion de equipos (60%)	65%
			Daños por agua	-	-	50%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	40%
			Fugas de Informacion	50%	50%	50%	-	-	MPF	11.2.1 Emplazamiento y proteccion de equipos	30%
			Acceso no autorizado	100%	25%	75%	25%	-	PF	11.2.1 Emplazamiento y proteccion de equipos	40%
			Ataque destructivo	100%	100%	100%	100%	100%	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	65%
			Condiciones inadecuadas de temperatura o humedad	-	-	75%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	70%
2	T.I.	NAS de Almacenamiento de información	Fuego	-	100%	100%	-	100%	MPF	11.1.1 Perimetros de Segruidad Fisica Seguras (70%) 11.2.1 Emplazamiento y proteccion de equipos (60%)	65%
			Avería de origen físico o lógico	-	100%	100%	-	100%	MPF	11.2.4 Mantenimiento de los equipos.	40%
			Ataque destructivo	-	100%	100%	100%	100%	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	60%

Fuente: Elaboración propia

VALORACION AMENAZAS											
		Información del Activo		Valorización							
N°	Area	Nombre de Activo	Amenazas	C	I	D	A	T	P	Salvaguardas	Eficacia
			Condiciones inadecuadas de temperatura o humedad	-	100%	100%	-	100%	PF	11.2.1 Emplazamiento y proteccion de equipos	70%
			Daños por agua	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	60%
			Corte del suministro Electrico	-	-	100%	-	-	PF	11.2.2 Instalaciones de suministro	60%
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	70%
			Errores del administrador	100%	100%	100%	-	-	PF	12.3.1 Copias de seguridad de la informacion	80%
			Errores de mantenimiento / actualización de equipos Hardware)	-	100%	100%	-	-	PF	11.2.4 Mantenimiento de los equipos.	60%
			Uso no Previsto	100%	100%	100%	-	-	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	50%
			Acceso no autorizado	75%	75%	-	-	-	MPF	9.1.1 Politica de Control de Accesos (50%) 9.1.2 Control de acceso a las redes y servicios asociados (60%) 9.2.2 Gestion de los derechos de acceso asigandos a usuarios(70%)	60%
			Manipulación de los equipos	25%	-	25%	-	-	MPF	8.2.3 Manipulacion de activos	50%
			Robo	25%	-	25%	-	-	MPF	11.2.1 Emplazamiento y proteccion de equipos	40%
3	T.I.	UPS Centro de Datos	Fuego	-	-	100%	-	-	MPF	11.1.1 Perimetros de Segruidad Fisica Seguras (70%) 11.2.1 Emplazamiento y proteccion de equipos (60%)	65%
			Avería de origen físico o lógico	-	100%	100%	-	100%	MPF	11.2.4 Mantenimiento de los equipos.	40%

Fuente: Elaboración propia

VALORACION AMENAZAS											
		Información del Activo		Valorización							
N°	Area	Nombre de Activo	Amenazas	C	I	D	A	T	P	Salvaguardas	Eficacia
			Ataque destructivo	-	-	25%	-	-	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	60%
			Corte de Suministro Electrico	-	-	100%	-	-	PF	11.2.2 Instalaciones de suministro	50%
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	70%
4	T.I.	Aire Acondicionado Centro de Datos Principal	Fuego	-	-	100%	-	-	MPF	11.1.1 Perimetros de Segruidad Fisica Seguras (70%) 11.2.1 Emplazamiento y proteccion de equipos (60%)	65%
			Avería de origen físico	-	100%	100%	-	100%	MPF	11.2.4 Mantenimiento de los equipos.	50%
			Ataque destructivo	-	-	25%	-	-	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	70%
			Corte de Suministro Electrico	-	-	100%	-	-	PF	11.2.2 Instalaciones de suministro	80%
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	60%
			Daños por agua	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	67%

Fuente: Elaboración propia

VALORACION AMENAZAS											
		Información del Activo		Valorización							
N°	Area	Nombre de Activo	Amenazas	C	I	D	A	T	P	Salvaguardas	Eficacia
5	T.I.	Servidores	Fuego	-	-	100%	-	-	MPF	11.1.1 Perimetros de Segruidad Fisica Seguras (70%) 11.2.1 Emplazamiento y proteccion de equipos (60%)	65%
			Avería de origen físico o lógico	-	-	100%	-	-	MPF	11.2.4 Mantenimiento de los equipos.	50%
			Daños por agua	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	40%
			Corte del suministro Electrico	-	-	100%	-	-	PF	11.2.2 Instalaciones de suministro	60%
			Condiciones inadecuadas de temperatura o humedad	-	-	100%	-	-	PF	11.2.1 Emplazamiento y proteccion de equipos	40%
			Errores del administrador	100%	100%	100%	-	-	PF	12.3.1 Copias de seguridad de la informacion 12.4.3 Registros de actividad del administrador y operador del sistema	50%
			Errores de mantenimiento / actualización de equipos Hardware)	-	100%	100%	-	-	PF	11.2.4 Mantenimiento de los equipos.	60%
			Uso no Previsto	100%	100%	100%	-	-	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	54%
			Acceso no autorizado	75%	75%	-	-	-	MPF	9.1.1 Politica de Control de Accesos 9.1.2 Control de acceso a las redes y servicios asociados 9.2.2 Gestion de los derechos de acceso asigandos a usuarios	45%
			Manipulación de los equipos	25%	-	25%	-	-	MPF	8.2.3 Manipulacion de activos	65%
			Robo	25%	-	25%	-	-	MPF	11.2.1 Emplazamiento y proteccion de equipos	60%
			Ataque destructivo	-	-	100%	-	-	MPF	11.1.4 Proteccion contra amenazas externas y del ambiente	76%

Fuente: Elaboración propia

VALORACION AMENAZAS											
		Información del Activo		Valorización							
N°	Area	Nombre de Activo	Amenazas	C	I	D	A	T	P	Salvaguardas	Eficacia
6	T.I.	Base de Datos	Avería de origen físico o lógico	-	-	100%	-	-	MPF	11.2.4 Mantenimiento de los equipos.	87%
			Cortes del suministro eléctrico	-	-	100%	-	-	MPF	11.2.2 Instalaciones de suministro	54%
			Errores del administrador	100%	100%	100%	-	-	MPF	12.3.1 Copias de seguridad de la informacion 12.4.3 Registros de actividad del	60%
			Errores de monitorización	-	100%	-	-	100%	MPF	12.1.3 Gestión de capacidades.	65%
			Errores de configuración	-	100%	-	-	-	MPF	12.4.1 Registro y gestion de eventos de actividad	30%
			Difusión de software dañino	100%	100%	100%	-	-	MPF	12.6.2 Restricciones en la instalación de software.	50%
			Escape de información	100%	-	-	-	-	MPF	11.2.1 Emplazamiento y proteccion de equipos 12.6.2 Restricciones en la instalación de software.	40%
			Alteración accidental de la información	-	100%	-	-	-	MPF	12.1.4 Separación de entornos de desarrollo, prueba y producción.	50%
			Destrucción de información	-	-	100%	-	-	MPF	18.1.3 Proteccion de los registros de la organización	20%
			Fugas de información	100%	-	-	-	-	MPF	11.2.1 Emplazamiento y proteccion de equipos	80%
			Acceso no autorizado	100%	100%	-	-	-	MPF	9.1.1 Politica de Control de Accesos 9.2.2 Gestion de los derechos de acceso asigandos a usuarios	60%
			Modificación deliberada de la información	-	100%	-	-	-	MPF	8.2.1 Directrices de clasificacion	70%
			Denegación de servicio	-	-	100%	-	-	PF		60%

Fuente: Elaboración propia

6.2.2 Fase de Determinación del Nivel de Madurez de los Controles o Salvaguardas

Ya identificadas las salvaguardas o controles de la ISO 27002:2013, se procedió a determinar el niveles de madurez en el que se encuentran los controles con el fin de tener un panorama más claro de cómo es que se encuentra la empresa.

Tabla 42. Nivel de madurez

DETERMINACION DEL NIVEL DE MADUIREZ DE LA ISO 27002:2012			
DOMINIO	**OBJETIVO DE CONTROL**	**CONTROL**	**Valoracion del Nivel de Madurez**
Politica de Seguridad			3.5
	Directrices de la direccion en seguridad de la informacion	5.1.1 Conjunto de politicas para la seguridad de información	4
		5.1.2 Revision de las politicas para la seguridad de información	3
Seguridad Ligada a los RRHH			2.75
	Antes de la Contratacion	7.1.1 Terminos y condiciones de la contratacion	2
	Durante la contratación	7.2.1 Responsabilidades de Gestion	3
		7.2.2 Concienciacion, educacion y capacitacion en seg. De la Inf.	3
	Cese o cambio de puesto de trabajo	7.3.1 Ceso o cambio de puesto de trabajo	3
Gestion de Activos			3.125
	Responsabilidad sobre los activos	8.1.1 Inventario de activos	3
		8.1.2 Propiedad de los activos	4
		8.1.3 Uso Aceptable de los activos	3
	Clasificacion de la Informacion	8.2.1 Directrices de clasificacion	2
		8.2.3 Manipulacion de activos	3
	Manejo de los soportes de almacenamiento	8.3.1 Gestion de soportes extraibles	3
		8.3.2 Eliminacion de soportes	3
		8.3.3 Soportes Fisicos en transito	4

Fuente: Elaboración propia

Control de Accesos			2.50
	Requisitos de negocio para el control de accesos	9.1.1 Politica de Control de Accesos	4
		9.1.2 Control de acceso a las redes y servicios asociados	1
	Gestion de acceso de usuario	9.2.1 Gestion de altas/bajasen el registro de usuarios	2
		9.2.2 Gestion de los derechos de acceso asigandos a usuarios	0
		9.2.3 Gestion de los derechos de acceso con privilegios especiales	3
		9.2.4 Gestion de informacion confidencial de autenticacion de usuarios	2
		9.2.5 Revisión de los derechos de acceso de los usuarios	2
		9.2.6 Retirada o adaptacion de los derechos de acceso	1
	Responsabilidades del usuario	9.3.1 Uso de informacion confidencial para la autenticacion	3
	Control de acceso a sistemas y aplicaciones	9.4.1 Restriccion del acceso a la informacion	5
		9.4.2 Procedimientos seguros de inicio de sesion	2
		9.4.3 Gestion de contraseñas de usuario	3
		9.4.4 Uso de la herramienta de administracion de sistemas	2
		9.4.5 Control de acceso al codigo fuente de los programas	5
Cifrado			3.50
	Controles criptograficos	10.1.1 Politica de uso de los controles criptograficos	5
		10.1.2 Gestión de claves	2

Fuente: Elaboración propia

Seguridad Fisica y Ambiental			2.18
	Areas Seguras	11.1.1 Perimetros de Segruidad Fisica Seguras	3
		11.1.4 Proteccion contra amenazas externas y del ambiente	3
	Seguridad de los equipos	11.2.1 Emplazamiento y proteccion de equipos	2
		11.2.2 Instalaciones de suministro	3
		11.2.3 Seguridad del cableado.	2
		11.2.4 Mantenimiento de los equipos.	3
		11.2.5 Salida de activos fuera de las dependencias de la empresa.	2
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	2
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	2
		11.2.8 Equipo informático de usuario desatendido.	1
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	1
Seguridad en la operativa			2.58
	Responsabilidades y procedimientos de operación	12.1.1 Documentacion de procedimientos de operación	2
		12.1.2 Gestion de cambios	4
		12.1.3 Gestión de capacidades.	2
		12.1.4 Separación de entornos de desarrollo, prueba y producción.	3
	Proteccion contra codigo malicioso	12.2.1 Controles contra el codigo malicioso	3
	Copias de seguridad	12.3.1 Copias de seguridad de la informacion	3
	Registro de actividad y supervision	12.4.1 Registro y gestion de eventos de actividad	3
		12.4.2 Proteccion de la informacion de registros (logs)	3
		12.4.3 Registros de actividad del administrador y operador del sistema	2
	Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.	1
		12.6.2 Restricciones en la instalación de software.	2
	Consideraciones de las auditorías de los sistemas de información.	12.7.1 Controles de auditoría de los sistemas de información.	3

Fuente: Elaboración propia

Seguridad en las telecomunicaciones			1.67
	Gestion de la seguridad en las redes	13.1.1 Controles de red	2
		13.1.2 Mecanismos de seguridad asociados a servicios en red.	1
		13.1.3 Segregación de redes.	2
Adquisicion, desarrollo y mantenimiento de los sistemas de informacion			2.50
	Requisitos de seguridad de los sistemas de informacion	14.1.1 Seguridad de las comunicaciones en servicios accesibles por redes publicas	2
		14.1.2 Proteccion de las transacciones por redes telematicas	3
Relaciones con Suministradores			2.33
	Seguridad de la informacion en las relaciones con suministradores	15.1.1 Politica de Seguridad de la informacion para suministradores.	2
	Gestion de la prestacion del servicio por suministradores	15.2.1 Supervicion y revision de los servicios prestados por terceros	2
		15.2.2 Gestion de cambios en los servicios prestados por terceros	3
Gestion de incidentes en la seguridad de la informacion			1.00
	Gestion de incidentes de seguridad de la informacion y mejoras	16.1.1 Responsabilidades y procedimientos	2
		16.1.2 Notificacion de los eventos de seguridad de la informacion	1
		16.1.3 Notificacion de puntos debiles de seguridad	1
		16.1.5 Respuesta a los incidentes de seguridad	0
		16.1.6 Recopilacion de evidencias	1
Cumplimiento			2.25
	Cumplimiento de los reuisitos legales y contractuales	18.1.3 Proteccion de los registros de la organización	1
	Revisiones de la seguridad de la informacion	18.2.1 Revisión independiente de la seguridad de la información.	3
		18.2.2 Cumplimiento de las políticas y normas de seguridad.	2
		18.2.3 Comprobación del cumplimiento.	3

Fuente: Elaboración propia

6.2.3 Fase de Determinación del Impacto Residual

Ya implementadas las salvaguardas o controles de la ISO 27002:2013, el nivel de degradación que causan las amenazas es menor, debido a la eficacia que tienen dichas salvaguardas frente al daño que puedan ocasionar las amenazas, reduciendo el impacto de un valor potencial a un valor residual.

Tabla 43. Impacto Residual

IMPACTO RESIDUAL								
		Información del Activo		Impacto Residual				
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
1	T.I.	Ambiente Centro de Datos	Fuego	[-]	[-]	[8]	[-]	[-]
			Daños por agua	[-]	[-]	[7]	[-]	[-]
			Fugas de Informacion	[7]	[7]	[7]	[-]	[-]
			Acceso no autorizado	[9]	[7]	[8]	[7]	[-]
			Ataque destructivo	[8]	[8]	[8]	[8]	[8]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[9]	[-]	[-]
2	T.I.	NAS de Almacenamiento de información	Fuego	[-]	[8]	[8]	[-]	[8]
			Avería de origen físico o lógico	[-]	[9]	[9]	[-]	[9]
			Ataque destructivo	[-]	[8]	[8]	[8]	[8]

Fuente: Elaboración propia

IMPACTO RESIDUAL								
		Información del Activo		Impacto Residual				
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
			Condiciones inadecuadas de temperatura o humedad	[-]	[9]	[9]	[-]	[9]
			Daños por agua	[-]	[-]	[8]	[-]	[-]
			Corte del suministro Electrico	[-]	[-]	[8]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[8]	[-]	[-]
			Errores del administrador	[7]	[7]	[7]	[-]	[-]
			Errores de mantenimiento / actualización de equipos Hardware)	[-]	[8]	[8]	[-]	[-]
			Uso no Previsto	[9]	[9]	[9]	[-]	[-]
			Acceso no autorizado	[8]	[8]	[-]	[-]	[-]
			Manipulación de los equipos	[7]	[-]	[7]	[-]	[-]
			Robo	[7]	[-]	[7]	[-]	[-]
3	T.I.	UPS Centro de Datos	Fuego	[-]	[-]	[8]	[-]	[-]
			Avería de origen físico o lógico	[-]	[10]	[10]	[-]	[10]

Fuente: Elaboración propia

IMPACTO RESIDUAL								
		Información del Activo		Impacto Residual				
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
			Ataque destructivo	[-]	[-]	[7]	[-]	[-]
			Corte de Suministro Electrico	[-]	[-]	[9]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[8]	[-]	[-]
4	T.I.	Aire Acondicionado Centro de Datos Principal	Fuego	[-]	[-]	[8]	[-]	[-]
			Avería de origen físico	[-]	[10]	[10]	[-]	[10]
			Ataque destructivo	[-]	[-]	[7]	[-]	[-]
			Corte de Suministro Electrico	[-]	[-]	[10]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[8]	[-]	[-]
			Daños por agua	[-]	[-]	[8]	[-]	[-]

Fuente: Elaboración propia

IMPACTO RESIDUAL								
		Información del Activo		Impacto Residual				
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
5	T.I.	Servidores	Fuego	[-]	[-]	[8]	[-]	[-]
			Daños por agua	[-]	[-]	[9]	[-]	[-]
			Avería de origen físico o lógico	[-]	[-]	[9]	[-]	[-]
			Corte del suministro Electrico	[-]	[-]	[8]	[-]	[-]
			Condiciones inadecuadas de temperatura o humedad	[-]	[-]	[9]	[-]	[-]
			Errores del administrador	[9]	[9]	[9]	[-]	[-]
			Errores de mantenimiento / actualización de equipos Hardware)	[-]	[8]	[8]	[-]	[-]
			Uso no Previsto	[8]	[8]	[8]	[-]	[-]
			Acceso no autorizado	[8]	[8]	[-]	[-]	[-]
			Manipulación de los equipos	[7]	[-]	[7]	[-]	[-]
			Robo	[7]	[-]	[7]	[-]	[-]
			Ataque destructivo	[-]	[-]	[7]	[-]	[-]

Fuente: Elaboración propia

IMPACTO RESIDUAL								
		Información del Activo		Impacto Residual				
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
6	T.I.	Base de Datos	Avería de origen físico o lógico	[-]	[-]	[7]	[-]	[-]
			Cortes del suministro eléctrico	[-]	[-]	[8]	[-]	[-]
			Errores del administrador	[8]	[8]	[8]	[-]	[-]
			Errores de monitorización	[-]	[8]	[-]	[-]	[9]
			Errores de configuración	[-]	[9]	[-]	[-]	[-]
			Difusión de software dañino	[9]	[9]	[9]	[-]	[-]
			Escape de información	[9]	[-]	[-]	[-]	[-]
			Alteración accidental de la información	[-]	[9]	[-]	[-]	[-]
			Destrucción de información	[-]	[-]	[10]	[-]	[-]
			Fugas de información	[7]	[-]	[-]	[-]	[-]
			Acceso no autorizado	[8]	[8]	[-]	[-]	[-]
			Modificación deliberada de la información	[-]	[8]	[-]	[-]	[-]
			Denegación de servicio	[-]	[-]	[8]	[-]	[-]

Fuente: Elaboración propia

6.2.4 Fase de Determinación del Riesgo Residual

Ya calculados los nuevos valores del Impacto Residual al aplicar las salvaguardas o controles, se tiene un nuevo nivel de riesgo, debido a que los mecanismos de seguridad implementados ayudaran a reducir el daño generado por las amenazas.

Tabla 44. Riesgo Residual

RIESGO RESIDUAL											
		Información del Activo		Riesgo Residual							
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probabilidad		
1	T.I.	Ambiente Centro de Datos	Fuego	(-)	(-)	(1,8)	(-)	(-)	1		
			Daños por agua	(-)	(-)	(1,7)	(-)	(-)	1		
			Fugas de Informacion	(2,7)	(2,7)	(2,7)	(-)	(-)	2		
			Acceso no autorizado	(1,9)	(1,7)	(1,8)	(1,7)	(-)	1		
			Ataque destructivo	(1,8)	(1,8)	(1,8)	(1,8)	(1,8)	1		
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(3,9)	(-)	(-)	3		
2	T.I.	NAS de Almacenamiento de información	Fuego	(-)	(1,8)	(1,8)	(-)	(1,8)	1		
			Avería de origen físico o lógico	(-)	(2,9)	(2,9)	(-)	(2,9)	2		
			Ataque destructivo	(-)	(1,8)	(1,8)	(1,8)	(1,8)	1		

Fuente: Elaboración propia

RIESGO RESIDUAL											
		Información del Activo		Riesgo Residual							
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probabilidad		
			Condiciones inadecuadas de temperatura o humedad	(-)	(2,9)	(2,9)	(-)	(2,9)	2		
			Daños por agua	(-)	(-)	(1,8)	(-)	(-)	1		
			Corte del suministro Electrico	(-)	(-)	(3,8)	(-)	(-)	3		
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,8)	(-)	(-)	2		
			Errores del administrador	(1,7)	(1,7)	(1,7)	(-)	(-)	1		
			Errores de mantenimiento / actualización de equipos Hardware)	(-)	(1,8)	(1,8)	(-)	(-)	1		
			Uso no Previsto	(2,9)	(2,9)	(2,9)	(-)	(-)	2		
			Acceso no autorizado	(1,8)	(1,8)	(-)	(-)	(-)	1		
			Manipulación de los equipos	(1,7)	(-)	(1,7)	(-)	(-)	1		
			Robo	(1,7)	(-)	(1,7)	(-)	(-)	1		
3	T.I.	UPS Centro de Datos	Fuego	(-)	(-)	(1,8)	(-)	(-)	1		
			Avería de origen físico o lógico	(-)	(1,10)	(1,10)	(-)	(1,10)	1		

Fuente: Elaboración propia

RIESGO RESIDUAL											
		Información del Activo		Riesgo Residual							
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probabilidad		
			Ataque destructivo	(-)	(-)	(1,7)	(-)	(-)	1		
			Corte de Suministro Electrico	(-)	(-)	(3,9)	(-)	(-)	3		
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,8)	(-)	(-)	2		
4	T.I.	Aire Acondicionado Centro de Datos Principal	Fuego	(-)	(-)	(1,8)	(-)	(-)	1		
			Avería de origen físico	(-)	(1,10)	(1,10)	(-)	(1,10)	1		
			Ataque destructivo	(-)	(-)	(1,7)	(-)	(-)	1		
			Corte de Suministro Electrico	(-)	(-)	(3,10)	(-)	(-)	3		
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,8)	(-)	(-)	2		
			Daños por agua	(-)	(-)	(1,8)	(-)	(-)	1		

Fuente: Elaboración propia

RIESGO RESIDUAL											
		Información del Activo		Riesgo Residual							
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probabilidad		
5	T.I.	Servidores	Fuego	(-)	(-)	(1,8)	(-)	(-)	1		
			Daños por agua	(-)	(-)	(1,9)	(-)	(-)	1		
			Avería de origen físico o lógico	(-)	(-)	(1,9)	(-)	(-)	1		
			Corte del suministro Electrico	(-)	(-)	(3,8)	(-)	(-)	3		
			Condiciones inadecuadas de temperatura o humedad	(-)	(-)	(2,9)	(-)	(-)	2		
			Errores del administrador	(1,9)	(1,9)	(1,9)	(-)	(-)	1		
			Errores de mantenimiento / actualización de equipos Hardware)	(-)	(1,8)	(1,8)	(-)	(-)	1		
			Uso no Previsto	(1,8)	(1,8)	(1,8)	(-)	(-)	1		
			Acceso no autorizado	(1,8)	(1,8)	(-)	(-)	(-)	1		
			Manipulación de los equipos	(2,7)	(-)	(2,7)	(-)	(-)	2		
			Robo	(1,7)	(-)	(1,7)	(-)	(-)	1		
			Ataque destructivo	(-)	(-)	(1,7)	(-)	(-)	1		

Fuente: Elaboración propia

RIESGO RESIDUAL											
		Información del Activo		Riesgo Residual							
N°	Area	Nombre de Activo	Amenazas	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Probabilidad		
6	T.I.	Base de Datos	Avería de origen físico o lógico	(-)	(-)	(1,7)	(-)	(-)	1		
			Cortes del suministro eléctrico	(-)	(-)	(3,8)	(-)	(-)	3		
			Errores del administrador	(1,8)	(1,8)	(1,8)	(-)	(-)	1		
			Errores de monitorización	(-)	(1,8)	(-)	(-)	(1,9)	1		
			Errores de configuración	(-)	(1,9)	(-)	(-)	(-)	1		
			Difusión de software dañino	(2,9)	(2,9)	(2,9)	(-)	(-)	2		
			Escape de información	(2,9)	(-)	(-)	(-)	(-)	2		
			Alteración accidental de la información	(-)	(1,9)	(-)	(-)	(-)	1		
			Destrucción de información	(-)	(-)	(1,10)	(-)	(-)	1		
			Fugas de información	(2,7)	(-)	(-)	(-)	(-)	2		
			Acceso no autorizado	(1,8)	(1,8)	(-)	(-)	(-)	1		
			Modificación deliberada de la información	(-)	(1,8)	(-)	(-)	(-)	1		
			Denegación de servicio	(-)	(-)	(1,8)	(-)	(-)	1		

Fuente: Elaboración propia

6.3 Tercera etapa: Elaboración del Plan de Seguridad

6.3.1 Implementación del Plan de Seguridad en base a la Norma ISO 27002:2013

- **Desarrollo de los dominios, objetivos de control y controles a tratar.**

SEGURIDAD LIGADA A LOS RRHH	
Versión: 1.0	

7.1. Antes de la contratación

7.1.2 Términos y condiciones del empleo

Control

Se deben indicar las responsabilidades de los trabajadores y las de la organización para la seguridad de la información, definidos en acuerdos contractuales los cuales deben ser aceptados y firmados por los colaboradores de la empresa.

Implementación

- El personal contratado deberá dejar constancia de conocimiento y aceptación de la política de Seguridad y Confidencialidad de la Información o no divulgación, en el momento de la contratación. El contratado debe firmar:
  - Acuerdo de Confidencialidad o no divulgación
  - Acuerdo de Protección de Datos Personales.
- Toda obligación del trabajo para el cual se es contratado deberá estar especificado en los contratos de locación de servicios.

- Todo personal externo que tenga acceso a algún activo comprometido a la seguridad de la información está en la responsabilidad de velar por la integridad de los mismos.
- Todo el personal de la empresa está en la obligación de comunicar cualquier tipo de incidente que pueda afectar la seguridad de los activos.
- El acceso por contratación de servicios, a áreas protegidas de la institución en especial áreas de acceso restringido, requerirá la emisión de un documento de autorización de ingreso, en el que se precise los datos de identificación del personal asignado a la atención del servicio.
- Los términos y condiciones del empleo reflejarán los lineamientos de la política de seguridad y confidencialidad de la información.
- El acceso de terceros se llevara a cabo recién cuando se tengan implementadas salvaguardas de protección.
- La empresa puede sancionar a cualquier empleado que desatienda los requisitos de seguridad de la información.
- Todo el personal de la empresa deberá tener conocimiento sobre la clasificación general de los activos que puedan afectar la seguridad de la información.

7.2 Durante la contratación

7.2.1 Responsabilidades de Gestión

Control

La dirección requerirá a los empleados y contratistas que apliquen la seguridad de la información de acuerdo a las políticas establecidas.

Implementación

- La dirección se compromete a entregar la política de seguridad de la información en la cual se resume las responsabilidades y roles que deben ser de conocimiento del personal que accede a información sensible así como sistemas de información.
- La dirección debe motivar a los empleados y contratistas a cumplir con las políticas de seguridad de la información.
- La dirección debe de informar a todo el personal de la realización de auditorías para verificar el cumplimiento de las políticas establecidas dentro del área de TI.
- El área encargada del control de la seguridad de la información debe supervisar el cumplimiento de los controles establecidos dentro de la organización.

7.3 Cese o cambio de puestos de trabajo

7.3.1 Cese o cambio de puestos de trabajo

Control

Deberían definirse, comunicarse y cumplirse las responsabilidades que siguen vigentes después de la finalización del contrato de los empleados

Implementación

- La desvinculación laboral debería incluir requisitos de seguridad de la información y responsabilidades en curso, dentro de cualquier acuerdo de confidenciabilidad.
- Los términos y condiciones del empleo deberían continuar por un periodo luego de la desvinculación de los empleados.

- Se debe comunicar al área respectiva el cese de los empleados para la desactivación y/o eliminación de accesos que tenían asignados a su cargo.
- En caso de ser algún puesto crítico, se deberá dejar constancia de comunicación respectiva a los interesados según corresponda.

GESTION DE ACTIVOS	
Versión: 1.0	

8.1 Responsabilidad sobre los activos

8.1.1 Inventario de activos

Control

Realizar un listado de activos de información en la organización debidamente identificados, con el fin de monitorearlos y hacer el respectivo seguimiento.

Implementación

- Contar con un inventario de activos de TI, teniendo en cuenta los siguientes datos mínimos.

➢ Tipo

➢ Nombre

➢ Descripción Corta

➢ Propietario

➢ Ubicación

➢ Valorización de criticidad

- El responsable de la seguridad de la información será la única persona en poder crear nuevos tipos de activos para la clasificación de estos.
- El inventario de activos debe mantenerse actualizado cada 12 meses.

8.1.2 Propiedad de los activos

Control

Todos los activos mantenidos en el inventario deberán tener un propietario, el cual debe ser asignado cuando los activos son creados o transferidos a la organización. Así mismo el propietario de los activos debería ser responsable de la gestión de los mismos durante su ciclo de vida.

Implementación

- Cada uno de los activos debe ser asignado a una persona que es la encargada de velar por la seguridad e integridad del mismo.
- El propietario deberá aceptar la responsabilidad del activo ya sea por cualquiera de los siguientes motivos:

➢ Incorporación a la empresa

➢ Cambio de puesto

➢ Incorporación de un nuevo activo a la empresa

- El propietario de cada activo deberá revisar las restricciones de acceso y clasificación del mismo.
- Las tareas o acciones a tomar sobre los activos pueden ser derogadas a otras personas, teniendo en cuenta que la responsabilidad ante cualquier evento imprevisto seguirá siendo del responsable.
- El propietario de los activos deberá garantizar el manejo de los activos durante su uso y en caso de ser eliminado o destruido.

8.1.3 Uso aceptable de los activos

Control

Se deberán identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de la información.

Implementación

- Los trabajadores de la empresa deberán seguir las reglas de uso aceptable de los activos que son definidos por la financiera.
- Los trabajadores de la empresa serán responsables del uso que le dan a los activos que se les fueron asignados.

8.2 Clasificación de la información

8.2.1 Directrices y clasificación

Control

En relación con el inventario de activos de información, se debe clasificar en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.

Implementación

- Clasificar los activos por los niveles de criticidad determinados por confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, para determinar el nivel de protección que se les dará.
- La información será clasificada en función de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

- Los propietarios de cada activo son responsables de la clasificación de los mismos.
- Los resultados de la clasificación deben indicar el nivel de criticidad de cada activo.

8.2.3 Manipulación de los activos

Control

Se deberán adoptar, desarrollar e implantar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información dentro de la organización.

Implementación

- Se debe tener en cuenta las restricciones que soportan los requisitos para cada nivel clasificación.
- Almacenar en un lugar adecuado los activos de información para evitar su deterioro en un determinado tiempo.
- Reservar en un área diferente las copias temporales con la protección de la información original
- Borrar el marcado de todas las copias para atender al destinatario.

8.3 Manejo de los soportes de almacenamiento

8.3.1 Gestión de soportes extraíbles

Control

Implantar procedimientos para la gestión de medios a fin de mantener un registro de auditoria.

Implementación

- Los contenidos de los medios que ya no sean requeridos en un futuro deben ser retirarse y ser irrecuperables para evitar fugas de información.
- Se debe tener autorización para retirar medios fuera de la organización y llevar un registro de las salidas de los mismos con el fin de poder ser auditables.
- Almacenar los medios en un ambiente adecuado de acuerdo a las especificaciones del proveedor.
- Utilizar técnicas criptográficas en caso de que los niveles de criticidad e integridad sean elevados.
- Almacenar varias copias de los datos valiosos en diferentes medios independientes para reducir el riesgo y pérdida de información.
- En caso de que los medios se encuentren muy deteriorados, se deben transferir los datos a nuevos medios con el fin de mitigar el riesgo de pérdida de información.
- Solo se deben tener habilitadas las unidades de medios extraíbles cuando se tenga autorización de la alta gerencia por ser motivo principal de fuga de información.
- Documentar los niveles de autorización para cada uno de los usuarios que los requieran.

8.3.2 Eliminación de soportes

Control

Eliminar los medios que contienen información confidencial de manera segura cuando ya no sea necesarios, utilizando procedimientos formales.

Implementación

- Los medios que contengan información confidencial deben ser eliminados definitivamente, estos pueden ser mediante:
  - Incineración
  - Trituración
  - Borrado de datos permanente
- Establecer que elementos requieran eliminación segura.
- Los dispositivos dañados deben ser analizados para ver si deben ser eliminados definitivamente o puedan ser reparados teniendo en cuenta el lugar donde serían reparados.
- La eliminación de medios que contengan información crítica deben de registrarse para mantener un registro de auditoria.

8.3.3 Soportes físicos en transito

Control

Es necesario proteger los medios que contienen información durante el transporte, contra el acceso no autorizado, mal uso o corrupción.

Implementación

- Utilizar transportes de los medios confiables.
- Acordar con la dirección una lista de proveedores que brinden el servicio y ver el nivel de confidencialidad que puedan brindar a la organización.
- Determinar el tipo de embalaje de acuerdo a los activos en tránsito para evitar cualquier deterioro en el mismo.

CONTROL DE ACCESOS	
Versión: 1.0	

9.1 Requisitos de negocio para el control de accesos

9.11Politica de control de accesos

Control

Se deberá establecer, documentar y revisar una política de controles de acceso basada en la seguridad de la información.

Implementación

- Las reglas de control de acceso tanto físicos y lógicos son definidas por los propietarios de los activos.
- La política de control de accesos debe tener en cuenta lo siguiente:
  - Requisitos de seguridad
  - Consistencia entre la clasificación de la información y los derechos de acceso
  - Limitaciones de accesos ya sean datos o servicios
  - Revisiones periódicas de controles de acceso.
  - Roles con acceso privilegiado
  - Registro de eventos
- Debe existir un requerimiento formal del pedido de acceso, el cual debe ser elaborado por el responsable del servicio.
- No se deberá otorgar accesos hasta que estos hayan sido autorizados por la persona correspondiente.

9.1.2 Acceso a las redes y a los servicios de red

Control

Solo deberán tener acceso a las redes y servicios de red los usuarios que estén plenamente identificados y autorizados.

Implementación

- Debe formularse una política para el uso de redes y servicios de red, la cual debe cubrir los siguientes aspectos:

➢ Las redes y servicios de red a los cuales los usuarios están permitidos de acceder.

➢ Procedimientos de autorización.

➢ Requisitos de autenticación

➢ Supervisión de los servicios de red

- La política para el uso de redes y servicios de red, debe estar relacionado con la política de control de accesos

9.2 Gestión de acceso de usuario

9.2.1 Gestión de altas/bajas en el registro de usuarios

Control

Se deberá implantarse un proceso formal para el registro y cancelación de usuarios así como la asignación de los derechos de acceso.

Implementación

- La asignación de IDs de usuario a los empleados es único, excepto para equipos donde los accesos son de uso grupal.

- Los propietarios de los activos deberán realizar la verificación de acceso a los activos que estén autorizados y su uso sea necesario para desarrollar labores pertinentes dentro de la organización.
- Se debe identificar y eliminar los usuarios redundantes, o en caso de necesitarlo a futuro se procederá a la desactivación por un periodo de tiempo.
- Se deben eliminar o desactivar los IDs de los usuarios que han sido removidos de su puesto de trabajo.

9.2.2 Gestión de los derechos de accesos asignados a usuarios

Control

Se deberá implantar un proceso formal de gestión de acceso del usuario para asignar o revocar derechos de acceso a los usuarios.

Implementación

- Los niveles de accesos deben ser contrarrestados con las políticas de seguridad y confidenciabilidad.
- Se deberá revisar que los derechos de accesos no se encuentren activos, antes que estos sean autorizados.
- Se deberá verificar los derechos de accesos en caso de que los usuarios hayan cambiado de puesto de trabajo o de los roles que desempeñan.
- Revisar periódicamente los derechos de acceso a sistemas y servicios de información.
- Se podrán crear usuarios genéricos siempre y cuando exista algún área encargada de aceptar el riesgo que pueda presentar realizar esta operación.

9.2.3 Gestión de los derechos de acceso con privilegios especiales

Control

Controlar y restringir la asignación y uso de los derechos privilegiados a usuarios.

Implementación

- Deberán identificarse los derechos de acceso privilegiados de cada sistema o servicio como:
  - Sistema operativo
  - Sistema de Gestor de base de Datos
  - Servicios y recursos de red
  - Servicios de Correo
  - Servicios de Telefonía IP
  - Accesos a internet
- Deberán identificarse las categorías y grupos de trabajo de los usuarios.
- Deberán establecerse un registro de todos los procesos de autorización y todos los privilegios asignados.
- Definir requisitos para la expiración de derechos de accesos privilegiados
- Actividades que son operadas regularmente no deben de ser utilizadas por cuentas privilegiadas.
- Revisar periódicamente los usuarios con derechos de acceso privilegiados.
- Deberán de establecerse procedimientos con el fin de evitar el uso de IDs genéricos para accesos a sistemas de uso común.

9.3 Responsabilidades del usuario

9.3.1 Uso de información confidencial para la autenticación

Control

Se deberán seguir prácticas responsables respecto al uso información de autenticación secreta.

Implementación

- Mantener la información de autenticación confidencial en secreto, asegurando que no sean divulgadas.
- Mantener registro de la información de autenticación secreta en forma segura, sin que este expuesto a ataques.
- Cambiar la información de autenticación secreta periódicamente, y en caso de tener sospechas de que estas puedan ser vulnerables.
- No utilizar la información de autenticación secreta para diferentes usos que se le puedan dar.

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción de acceso a la información

Control

Se deberá restringir el acceso a la información y a los sistemas de acuerdo con la política de accesos

Implementación

- Se deberá autorizar el acceso a módulos dentro de los sistemas que maneje la organización de acuerdo a los cargos que los usuarios ocupen para el desarrollo de sus funciones.

- Solo usuarios autorizados tendrán accesos a los sistemas institucionales controlados por el área correspondiente.
- Controlar los accesos de escritura, lectura y ejecución.
- Limitar la información que pueda ser proporcionada.
- Se deberá verificar la instalación de programas licenciados.
- Todo software que no esté autorizado ni licenciado deberá ser retirado de los equipos en los que se encuentren.
- Brindar controles de acceso físico y/o lógico para el aislamiento de aplicaciones críticas.

9.4.2 Procedimientos seguros de inicio de sesión

Control

- Se deberá controlar el acceso a los sistemas mediante procedimientos de conexión segura (log-on)

Implementación

- Elegir técnicas de autenticación adecuadas para verificar la identidad del usuario.
- Se deberán de proteger los sistemas y aplicaciones contra intentos de inicio de sesión por fuerza bruta.
- Se deberán registrar los intentos fallidos y exitosos de conexión
- Está prohibido transmitir contraseñas en texto limpio por una red.
- No mostrar las contraseñas al momento de ser ingresadas.
- Es necesario terminar sesiones inactivas después de un periodo de tiempo que se encuentren sin uso.

9.4.3 Gestión de contraseñas de usuario

Control

Se deberá definir un proceso formal con el fin de controlar la asignación de contraseñas.

Implementación

- Al momento de ingresar un nuevo empleado a la organización, este deberá firmar el acuerdo de confidenciabilidad que indica guardar en secreto todas las contraseñas que sean dadas para poder desarrollar sus actividades para la cual fue contratado.
- Permitir a los usuarios el cambio de sus contraseñas, validando las mismas mediante un proceso de confirmación.
- Se deberá mantener un registro de las contraseñas antiguas y prohibir que estas sean reutilizadas.
- Se deberán de transmitir las contraseñas en formatos protegidos
- Las contraseñas nunca deben ser almacenadas de forma desprotegida, estas deben ser almacenadas mediante métodos de encriptación.

CIFRADO	
Versión: 1.0	

10.1 Controles criptográficos

10.1.1 Política de uso de los controles criptográficos

Control

Se deberá desarrollar e una política sobre el empleo de controles criptográficos.

Implementación

- Se deberá evaluar el nivel requerido de protección evaluando la calidad del algoritmo de protección.
- Se deberá emplear el cifrado para la protección de información que pueda ser transportada a través de líneas de comunicación o medios extraíbles.
- La política debe establecer responsabilidades y funciones del encargado de la misma.

10.1.2 Gestión de Claves

Control

Se deberá implementar procedimientos sobre el uso, protección y duración de las claves criptográficas.

Implementación

- Se deberán seleccionar algoritmos criptográficos y longitudes para la gestión de las claves.
- La gestión de claves requiero procesos seguros para:

➢ Generación

➢ Archivo

➢ Almacenamiento

➢ Recuperación

➢ Distribución

➢ Retiro

➢ Destrucción de claves

- Se debe poder generar claves criptográficas para los diferentes sistemas y aplicaciones.

SEGURIDAD FISICA Y AMBIENTAL	
Versión: 1.0	

11.1 Áreas Seguras

11.1.1 Perímetro de seguridad Física

Control

Utilizar un perímetro de seguridad física protegido por rejas, barreras, paredes, cámaras de vigilancia, los cuales ayuden a proteger las áreas que contenga sistemas de información y/o activos que sean esenciales para el correcto funcionamiento de la organización.

Implementación

- Los perímetros estarán perfectamente definidos de acuerdo a la ubicación de los activos que se requieran proteger.
- Los perímetros del edificio en el cual se encuentran ubicados todos los activos, deberán de ser de material concreto, no permitiendo el ingreso de personas no autorizadas contando con puertas protegidas por claves y letreros de señalización.
- Las puertas y ventanas que queden desatendidas deben ser aseguradas y/o bloqueadas considerando agregar protección externa a las ventanas teniendo en cuenta más aún si estas se encuentran en el primer piso o a ras del suelo.
- Se debería contar con un área de recepción donde se pueda controlar el acceso de personas ajenas a la organización, restringiendo el acceso a la misma solo a personas autorizadas.

- Se debería construir barreras en las áreas de acceso para proteger el área y contrarrestar de la misma forma la contaminación ambiental.
- El centro de datos debe estar delimitado por paredes y puertas con clave o cerradura.
- El acceso al centro de datos será por medio de huella biométrica.
- Deberían separarse las instalaciones de procesamiento de información que sean controladas por la organización de aquellas gestionadas por terceros.
- Se debería contar con luces de emergencia que permitan evacuar al personal y personas ajenas a la organización en caso de cualquier imprevisto, ubicando estas en pasillos, escaleras, puertas y otro cambio de nivel.
- Se debería implementar el uso de sistemas de seguridad, sistemas de alarma y protección para la detección de intrusos según lo normado por la SBS, los tipos mínimos que deberán cubrir los sistemas de alarma serán de: Intrusión, robo, asalto, incendio e inundación, principalmente para el centro de datos primario.
- Las instalaciones del centro de datos principal deben contar con sensores de control de temperatura, humedad y que puedan ser monitoreados por el personal autorizado.

11.1.4 Protección contra amenazas externas y del ambiente

Control

Diseñar e implementar la protección física contra desastres naturales, ataques maliciosos o daños causados por el hombre.

Implementación

- Capacitar al personal de la empresa en el tratamiento de siniestros con el fin de conocer todos los medios posibles para el tratamiento de los mismos.
- Se deben de llevar al menos una vez al año capacitaciones a todo el personal con el fin de tenerlos alertas en cualquier caso fortuito que ocurra dentro de la empresa, en el caso de ingreso de nuevo personal se deberá de dar una charla con los puntos mínimos de seguridad establecidos.
- Tener un control estricto de la localización y estado de todos los extintores que se encuentren ubicados en zonas que requieran salvaguarda en casa de fuego.
- Todo material peligroso, inflamable o combustible debe ser almacenado y utilizado en lugares seguros, lejos del centro de datos y de aquellos lugares donde se procese información o se encuentren equipos que sean de vital importancia para el correcto funcionamiento de la empresa.
- El centro de datos alterno se debe de ubicar en otra ciudad en caso de que ocurra cualquier desastre natural que dañe por completo el centro de datos principal.

11.2 Seguridad en los equipos

11.2.1 Emplazamiento y protección de equipos

Control

Debería de ubicarse y protegerse todos los equipos para reducir los riesgos ocasionados por amenazas y peligros ambientales ; así como todas las oportunidades de acceso no autorizado que puedan presentarse y puedan ser usadas por personas ajenas a la organización.

Implementación

- Los equipos deben ser colocados de tal manera que se encuentren libres de cualquier accidente que pueda ser ocasionado por personal de la empresa.
- Las instalaciones de procesamiento de información donde se manejen datos sensibles debe ser ubicada en lugares donde no pueda ser visible durante su uso y evitar el riesgo de fuga de información.
- Asegurar las instalaciones de almacenamiento para evitar el acceso no autorizado.
- Deben usarse protectores de energía eléctrica y en servidores y equipos críticos estos deben estar conectados a un UPS.
- Mantener los equipos en condiciones ambientales optimas y a su vez supervisarlas para el correcto funcionamiento de los equipos:

➢ Humedad: debe estar entre 20 y 50% no condensada

➢ Temperatura: debe estar entre 15° C y 30° C, pero lo óptimo es entre 21° C y 23° C.

- El centro de datos debe estar ubicado en un suelo firme, donde no ocurran vibraciones ni tránsito de maquinaria pesada, ya que estos pueden ocasionar daños en los equipos.
- Deberían de colocarse pararrayos en los techos de las instalaciones de la empresa y aplicar filtros de protección contra rayos en las líneas entrantes de energía.
- Tener un responsable de la protección de los equipos en aquellas areas de la financiera donde los equipos sean de uso común.

- Inventariar y rotular todos los activos para su control e identificación.
- Prohibir el ingreso a personas no autorizadas donde se encuentren equipos críticos para la empresa.

11.2.2 Instalaciones de Suministro

Control

Debería protegerse el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.

Implementación

- Definir un procedimiento para llevar acabo la revisión y mantenimientos de equipos que den soporte a equipos informáticos tales como UPS, estabilizadores y grupo electrógeno.
- Llevar un control de los mantenimientos preventivos que se realizan sobre los equipos de soporte.
- Contar con grupos electrógenos de respaldo que tengan la capacidad de cubrir las necesidades de la financiera.

11.2.3 Seguridad del cableado

Control

Debería protegerse contra la interferencia o daños el cableado de energía, la interceptación, y de telecomunicaciones que trasporta datos o brinda soporte a servicios de información.

Implementación

- Verificar la implementación de cableado de acuerdo a los estándares de cableado estructurado.
- El cableado de las instalaciones deben de pasar por canaletas las cuales deben pasar por los bordes de las paredes.
- Esta terminantemente prohibido que personas no autorizadas pueden abrir las canaletas, solo el personal de la entrega de servicio podrá tener la autorización para poder realizar cualquier cambio que sea pertinente.

Cableado de Red

- Separar los cables de energía de los cables de red para evitar interferencias y pérdidas de información.
- Las canalizaciones no deben superar los 20 metros.
- En caso de existir cielo raso suspendido se recomienda la utilización de canaletas para transportar los cables horizontales

Cableado eléctrico

- Conservar en buen estado el cableado eléctrico
- Reemplazar los cables deteriorados.
- Queda prohibido introducir cables pelados en los enchufes.
- No tocar los cables o equipos electrónicos con las manos mojadas.
- Evitar colocar una sola clavija en una sola toma de corriente, ya que puede producir calentamiento y este originar un incendio de origen eléctrico.

11.2.4 Mantenimiento de los equipos

Control

Mantener adecuadamente los equipos para asegurar su continua disponibilidad e integridad.

Implementación

- Mantener el equipamiento de acuerdo a las especificaciones de servicio del proveedor.
- Los mantenimientos preventivos deben planificarse periódicamente en un cronograma de trabajo, de acuerdo a las necesidades de los equipos.
- Solo el personal autorizado y debidamente acreditado, deberá realizar los mantenimientos y reparaciones de los equipos.
- Mantener registros de todos los fallos, así como dejar constancia de todos los mantenimientos correctivos y preventivos.
- Programar los mantenimientos en horarios donde los usuarios no necesiten de los equipos y en lugares donde no molesten a los demás usuarios.
- Antes de entregar los equipos, se debe realizar una prueba en presencia del responsable del equipo para corroborar el perfecto funcionamiento del mismo.

11.2.5 Salida de activos fuera de las dependencias de la empresa

Control

No deberían retirarse los equipos, software o información de la empresa sin previa autorización del área encargada.

Implementación

- Identificar a los empleados y personal externo que sean contratados por la empresa, que tengan autorización para permitir el retiro de activos fuera de las instalaciones de la misma.
- Verificar los tiempos de entrega establecidos en los permisos de salidas de los activos.

- Debe de mantenerse un registro de las salidas y entradas de todos los activos que necesiten ser llevados fueras de las instalaciones de la empresa.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

Control

Debería tenerse en cuenta la seguridad de los equipos fuera de las instalaciones, debido a los riesgos que presentan al estar fuera de la empresa.

Implementación

- El uso de cualquier activo fuera de la empresa debe ser autorizado por la dirección.
- No deben dejarse desatendidos los equipos el lugares publicados.
- Si los activos son transferidos a diferentes personas en el trascurso que estuvieron fuera, debería llevarse un control de quienes fueron las personas que manipularlos estos activos.

SEGURIDAD EN LA OPERATIVA	
Versión: 1.0	

12.1 Responsabilidades y procedimientos de operación

12.1.2 Gestión de cambios

Control

Controlar los cambios en la organización, los sistemas e instalaciones de procesamiento de información que afecten a la seguridad de la información.

Implementación

- Todos los cambios deben ser autorizados y solo los autorizados son aceptados.

➢ Ningún cambio esta permito sobre los activos que se encuentren en producción fuera de los tiempos establecidos

➢ Todos los cambios deben ser mapeados a una correspondiente autorización.

- Controlar las etapas de la gestión del cambio tales como:

➢ Solicitud del cambio

➢ Registro y filtrado

➢ Clasificación y análisis

➢ Evaluar aprobar y planificar

➢ Construir y probar

➢ Implementación

➢ Monitorización

- Comunicar los detalles de los cambios a todas las personas pertinentes

12.1.3 Gestión de Capacidades

Control

Supervisar y adaptar el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño del sistema.

Implementación

- Los procesos que comprenden la gestión de la capacidad son:

➢ Monitoreo del performance y rendimiento de los servicios que ofrece TI y los componentes de infraestructura que los soporta.

- ➢ Realizar actividades de ajustes para hacer el uso más eficiente de los recursos existentes.
- ➢ Influenciar en la demanda de los recursos
- En necesario que la empresa se comprometa en garantizar la capacidad necesaria para ofrecer servicios de TI de calidad
- Informar acerca de los planes de negocios y los acuerdos de nivel de servicio con el fin de pronosticar la capacidad necesaria.
- La revisión de la capacidad para los sistemas críticos se deben realizar cada 3 meses.
- La revisión de la capacidad de equipos no críticos se deben realizar cada 6 meses.

12.2 Protección contra código malicioso

12.2.1 Controles contra el código malicioso

Control

Implantar controles de detección, prevención y recuperación para proteger al sistema ante ataques de software malicioso.

Implementación

- Los usuarios están prohibidos de instalar cualquier tipo de software en los equipos que tengan a su cargo
- Restringir los derechos de administrador en los equipos locales, a excepción de los siguientes usuarios:
- ➢ Personal de desarrollo de sistemas.
- ➢ Administradores de base de datos.

- Usuarios que requieran administración de software de aplicaciones.
- Usuarios asignados a equipos portátiles de uso gerencial.

- Llevar un registro de todos los usuarios que tengan permisos de cambiar los privilegios de administrador y en que equipos, estos equipos necesariamente deben contar con un antivirus.
- El administrador de tecnología cliente y personal de soporte son las únicas personas encargadas de instalar software antivirus.
- Implementar software antivirus, anti spams y anti pishings y ubicarlo delante del servidor del correo institucional.
- Contar con filtros URL con el fin de reforzar la seguridad.
- Utilizar los filtros URL con el fin de controlar la navegación y las descargas de los usuarios.
- Aplicar y administrar actualizaciones de virus a través de la consola de administración de antivirus.
- Administrar y monitorear las actualizaciones de los sistemas operativos y todo software que requiera actualización.
- Se debe realizar la actualización de los antivirus cada 3 meses.
- En caso de que un equipo haya sido detectado con software maliciosos se debe solicitar al área responsable para que ejecute su plan de recuperación en caso que este allá ocasionado daño sobre los equipos.
- Contar con un firewall para evitar y denegar las transmisiones de información.

12.3 Copias de Seguridad

12.3.1 Copias de seguridad de la información

Control

Realizar copias de respaldo periódicamente tanto para la seguridad de la información como para software utilizado.

Implementación

- Deberían de realizarse copias de seguridad exactas y completas para poder ser restauradas en caso sea necesario.

Es necesario tomar en cuenta el siguiente cuadro para poder realizar los backups.

Tabla 45. Periocidad de los Backups

Generación de copias de seguridad	**Periodicidad**
Base de datos OLTP	Diaria
Base de datos OLAP	Diaria
Código Fuente	Semanal (Sujeta a cambios)
Archivos y documentos generados por las diferentes unidades de negocio	Trimestral
Sistemas de información CORE	Mensual (Sujeta a cambios)
Archivos de configuración Lógica	Trimestral
Servidores de producción	Diario
File Server	Diario
Correo electrónico	Semanal

Fuente: Elaboración Propia

- Comprimir con claves las copias de seguridad de bases de datos.
- Etiquetar y/o rotular medios como CD donde sean almacenados los backups.
- Almacenar los backups en condiciones ambientales adecuadas, teniendo en cuenta el medio donde se almaceno.
- Reemplazar los backups en forma periódica antes que se deteriore.
- Almacenar los backups en diferentes locales en caso de ocurrir cualquier desastre.
- Se deben realizar revisiones periódicas para comprobar que los backups se hicieron correctamente, estos dependerán de la criticidad y frecuencia de extracción.
- Se deberá controlar que los servidores replicados mantengan una sincronización adecuada con el servidor principal.

12.4 Registros de actividad y supervisión

12.4.1 Registro y gestión de eventos de actividad

Control

Se deberían producir, mantener y revisarse registros de las actividades realizadas y eventos de la seguridad de la información.

Implementación

Registro de auditoria en Bases de Datos

- Generar registros de auditoria de las bases de datos para trazar y registrar la actividad en cada instancia de SQL SERVER.
- Las herramientas de auditoria y SQL SERVER deben generar registros automáticos de:

- Actividades del usuario final
- Cierres e inicios de sesión
- Comandos de copias de seguridad
- Restauración
- Inserción

- Los registros automáticos deben incluir:

- ID de usuario
- Fecha, hora y detalles de los eventos ocurridos
- Registros de intentos de acceso al sistema exitoso o rechazado
- Identidad del dispositivo
- Texto de la instrucción SQL
- Nombre del objeto al que se tuvo acceso y tipo de acceso
- Direcciones y protocolos de red

Registros de auditoria en los sistemas de información

- Llevar un registro de auditoria que contenga los eventos relacionados a la seguridad, así mismo mantenerlo durante todo el tiempo necesario en el cual pueda ser utilizado.
- Se deben incluir registros automáticos que hagan seguimiento a las transacciones y a los procedimientos, deben incluir:

- ID de usuario.
- Actividades del sistema
- Fecha y hora de la última modificación de datos
- Cambios en la configuración del sistema
- Uso de privilegios y aplicaciones del sistema

- Direcciones y protocolos de red
- Registro de las transacciones realizadas por los usuarios en las aplicaciones
- Registros de hora y fecha de inicio de sesión y fin de sesión de los sistemas institucionales.
- Registro de donde se produjeron los accesos

Registro de auditoria de Servidores

- Llevar un registro de todas las operaciones realizadas en los servidores que puedan servir de registro de las operaciones realizadas.
- Deben capturar:
  - Eventos de autorización
  - Autenticación
  - Gestión de los servidores
  - Revisión de visor de sucesos o archivos de registros
  - Servicio de DNS
  - Servicios de Active directory
  - Configuraciones de servicios básicos

12.4.2 Protección de los registros de información

Control

Se deberá proteger la información del registro y su medio para evitar su alteración y modificaciones no autorizadas.

Implementación

- El administrador de base de datos debe controlar que no sean alterados los logs que son almacenados por los sistemas de información.

- Monitorear los registros de los servidores, con el fin de que no sean eliminados o editados.
- Verificar periódicamente los registros de los logs.

12.4.3 Registros de actividad del administrador y operador del sistema

Control

Las actividades del administrador de operaciones y de los usuarios del sistema de información deberían registrarse, protegerse y revisarse regularmente.

Implementación

- Registrar los incidentes de las fallas en el Sistema de Información Institucional.
- Registrar a todos los usuarios que reportaron algún incidente y quien fue la persona que dio solución a dicho incidente.
- Es necesario registrar la fecha y hora del incidente.
- Revisar periódicamente las cuentas de usuarios privilegiados con el fin de proteger y mantener los registros.

12.6 Gestión de la vulnerabilidad técnica

12.6.1 Gestión de las vulnerabilidades técnicas

Control

Se debería tener información sobre las vulnerabilidades técnicas de los sistemas de información que se usan en la empresa, evaluarlas y tomar medidas para controlar el riesgo.

Implementación

- Definir, establecer roles y responsabilidades y supervisar la gestión de las vulnerabilidades, la evaluación de los riesgos y el seguimiento de los activos
- Identificar las vulnerabilidades técnicas, los riesgos y las acciones que pueden ser tomadas.
- Mantener un registro de auditoria para los procedimientos a implantar.
- Supervisar y evaluar con regularidad el proceso de gestión de vulnerabilidades técnicas.
- Verificar periódicamente los controles y salvaguardas que se tienen implementados con el fin de poder salvaguardar los activos

12.6.2 Restricciones en la instalación del software

Control

Establecer e implantar reglas para la instalación de software por parte de los usuarios.

Implementación

- Definir qué tipo de software puede ser instalado por los usuarios
- Aplicar el principio de privilegios mínimos.
- Tener un control estricto sobre la instalación de parches

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoría de los sistemas de información.

Control

Deberían coordinarse los requisitos y actividades de auditoria que impliquen llevar a cabo correcciones en sistemas en producción con el fin de evitar interrupciones en los servicios.

Implementación

- Llevar un cronograma de los planes de auditoria que se tienen identificados.
- Limitar las verificaciones a solo lectura tanto para el software como para los datos.
- Supervisar y registrar todo accesos con el fin de mantener un registro histórico.

SEGURIDAD EN LAS TELECOMUNICACIONES	
Versión: 1.0	

13.1 Gestión de la seguridad en las redes

13.1.1 Controles de red

Control

Las redes deberían ser manejadas adecuadamente para protegerlas de amenazas y así mantener la seguridad en los sistemas que necesiten el uso de redes.

Implementación

Controles de Redes WAN

- Se debe contar con un documento donde se encuentren las especificaciones de configuración y diseños de red implementados.
- Realizar pruebas de disponibilidad de acuerdo a lo especificado en el cronograma de pruebas de continuidad.

- Se debe Verificar el ancho de banda aplicando muestreos y la revisión de los servicios externos.
- Se debe verificar las líneas de contingencia que se encuentran preparadas para el centro de datos principal y externo.
- Se debe implementar herramientas para fragmentar el ancho de banda de la red WAN con el fin de disponer de un ancho de banda dedicado a transacciones críticas.
- Se tendrá que monitorear el servicio haciendo uso de herramientas de monitoreo de tráfico y verificar que equipos están haciendo uso de mayor ancho de banda.
- Se deben contar con alertas en caso de superar límites establecidos.

Controles de redes LAN

- Se deben manejar controles de calidad que aseguren el cumplimiento de las normativas vigentes tales como:

➢ Norma ANSI EIA/TIA 568-B cableado en edificios comerciales.

➢ Norma EIA/TIA 569 para espacios, ductos y canaletas

➢ Norma EIA/TIA 606-A para infraestructura de rotulados y etiquetados

➢ Norma EIA/TIA 607-A para aterramientos

➢ Norma IEEE 802.3 para lo referido a tecnología de redes

➢ Norma IEEE 802.11 para redes inalámbricas.

- Contar con el documento de configuración de red para detallar los equipos de comunicación y estaciones de trabajo con que se cuenta.

Control para el cableado

- Se deberá contar con la certificación de instalación de puntos de datos que acrediten ser una categoría 5 o 6.
- Se deberá de rotular tomas de datos y gabinetes.
- Se deberá contar con los planos de ubicación de puntos de datos.
- Se deberá establecer un cronograma de revisión de cableado dependiendo de la antigüedad de los mismos.

13.1.2 Mecanismos de seguridad asociados a servicios en red

Control

Se deben establecer lineamientos que definan la seguridad, niveles de servicio y requerimientos de gestión en los servicios de redes.

Implementación

Seguridad de redes WAN

- Con el fin de asegurar que las VPNs transmitan la información de manera confiable se debe verificar que se trabaje con los servicios de seguridad para VPNs adecuados, en caso de ser un servicio terciarizado esta información deberá ser solicitada al personal correspondiente.

Seguridad Perimetral

- Se debe contar con un firewall, para filtrar todas las conexiones provenientes del exterior ya sean entradas o salidas.
- Se deben documentar todas las reglas que se establezcan para los firewalls.
- Realizar copias de seguridad de las reglas de configuración de los firewalls.

Seguridad en redes LAN/ Seguridad en Redes inalámbricas

- Se deben de establecer nombres para las redes inalámbricas que no sean fáciles de identificar con el fin de dar mayor seguridad a las mismas
- Todas las redes inalámbricas deben contar con una contraseña

ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	
Version: 1.0	

14.1 Requisitos de seguridad de los sistemas de información

14.1.1 Seguridad de las comunicaciones en servicios accesibles por redes publicas

Control

Debería de protegerse de la actividad fraudulenta y modificaciones no autorizadas, la información de servicios de aplicación que navegan a través de redes públicas.

Implementación

- Cumplir con los siguientes requisitos:
  - ➢ Confidencialidad
  - ➢ Integridad
  - ➢ Prueba de envío
  - ➢ Recepción de documentos clave
- Se deben documentar los acuerdos de servicios entre socios incluyendo detalles de autorización.

- Deben considerarse requisitos para la protección de los servidores de aplicación y asegurar la disponibilidad de las interconexiones de red.

14.1.3 Protección de las transacciones por redes telemáticas

Control

Se debe de proteger la información de las transacciones en línea para evitar que estas transmisiones sean incompletas

Implementación

- Proteger la información utilizando criptografía publica y firmas digitales.
- Se debe emplear firmas electrónicas por cada una de las partes implicadas en la transacción.

RELACIONES CON LOS SUMINISTRADORES	
Versión: 1.0	

15.1 Seguridad de la información en las relaciones con suministradores

15.1.2. Tratamiento del riesgo dentro de acuerdos de suministradores

Control

Debería documentarse los acuerdos con los proveedores con el fin de asegurar cualquier percance que ocurra entre los proveedores y la organización respecto a las obligaciones de ambas partes referente a la seguridad de la información.

Implementación

Se debe tener en cuenta lo siguiente:

- Determinar qué tipo de información será utilizada por los proveedores.

- Proporcionar los requisitos legales, protección de datos, derechos de propiedad intelectual y derechos de autor.
- Las obligaciones de cada parte al momento de realizar un contrato incluyendo que políticas de seguridad de la información deben ser adecuadas.
- Auditar los procesos que apliquen los proveedores, con el fin de ver la calidad de servicio o producto
- Se debe tener en cuenta los casos en que los proveedores queden incapaces de seguir continuando con sus labores, para evitar la demora en la disposición de servicios o productos

15.2 Gestión de la prestación del servicio por suministradores

15.2.1 Supervisión y revisión de los servicios prestados por terceros

Control

Se debería supervisar, revisar y auditar periódicamente la entrega de servicios de los proveedores

Implementación

- Se debe asegurar el cumplimiento de los términos y condiciones de seguridad de la información de los acuerdos.
- Se deben manejar correctamente los incidentes que ocurran referentes a la seguridad de la información.
- Se deben revisar los informes de servicios que son producidos por los proveedores
- Realizar auditorías al menos una vez al año con los proveedores, revisando los acuerdos de servicios establecidos.

- Medir la capacidad de servicio que ofrece el proveedor para asegurar los niveles de servicios acordados.
- Se debe tener asignado un responsable para el trato con los proveedores dentro del área de TI.

15.2.2 Gestión de cambios en los servicios prestados por terceros

Control

Se deberían gestionar los cambios en la prestación de servicios por parte de los proveedores tomando en cuenta la importación de los sistemas e información de la organización que implique una nueva valoración de riesgos.

Implementación

- Considerar los siguientes aspectos

➢ Cambios en los acuerdos con los proveedores

➢ Mejoras de servicios

➢ Implementación de nuevos sistemas

➢ Cambios y/o mejoras en las redes

➢ Cambios de proveedores

➢ Sub-contratación de proveedores

➢ Cambios de herramientas de desarrollo.

➢ Incorporación de nuevas tecnologías

GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	
Versión:	

16.1 Gestión de incidentes de seguridad de la información y mejoras

16.1.1 Responsabilidades y procedimientos

Control

Establecer los procedimientos de gestión con el fin de asegurar respuestas rápidas referentes a los incidentes de Seguridad de la información.

Implementación

- Identificar que colaboradores de la organización son los responsables de reportar y comunicar cualquier incidente de la seguridad de la información.
- Poner en marcha la identificación e informar sobre los incidentes de seguridad.
- Identificar que procedimientos deben ser tomados en cuenta:
  - Procedimientos de respuestas a incidentes
  - Procedimientos para la detección y análisis de incidentes de la seguridad de la información.
- Se deberá tener información referente a la norma ISO 27035 sobre la gestión de incidentes.

16.1.2 Notificación de los eventos de seguridad de la información

Control

Se deberían reportar lo eventos de seguridad de la información a través de canales de gestión.

Implementación

- Se deben de utilizar canales formales para la notificación de eventos de seguridad de la información tales como correo electrónico u otra herramienta con la que la empresa cuente.
- Empleados y terceros que brinden servicios a la empresa deben ser notificados de reportar cualquier evento que pueda perjudicar la seguridad de la información.

16.1.3 Notificación de puntos débiles de seguridad

Control

Se debería exigir a todo el personal reportar cualquier debilidad que pueda ser observada en temas de seguridad de la información.

Implementación

- Prohibir al personal probar cualquier debilidad que haya podido ser observada con el fin de evitar daños en cualquier parte de los sistemas o infraestructura de la empresa.
- Se deben de realizar análisis de vulnerabilidades por lo menos una vez al año, por el personal del área especializada.

16.1.4 Valoración de eventos de seguridad de información y toma de decisiones

Control

Deberían de evaluarse y valorarse los eventos de seguridad de información

Implementación

- Definir una escala para la valoración de eventos de seguridad de información y definir si este debería ser clasificado como incidente de seguridad de la información.
- Se deben priorizar eventos que puedan afectar activos críticos.
- Establecer acuerdos de nivel de servicio para la atención de dichos eventos
- Se deben registrar los resultados de la evaluación con el fin de tener datos históricos para posteriores sucesos.

CUMPLIMIENTO	
Versión:	

18.1 Cumplimiento de los requisitos legales y contractuales

18.1.3 Protección de los registros de la organización

Control

Se debería proteger los registros importantes frente a pérdidas, destrucción, falsificación, acceso no autorizados de acuerdo a requisitos establecidos.

Implementación

- Se deben categorizar los registros por tipos, se propone la siguiente tabla para la protección de los registros
  - Registros de bases de datos: 10 años
  - Registros de auditoria: 5 años

- Registro de log: 3 años

- Las copias de información que son consideradas como reservadas deben ser almacenadas nuevamente en el caso de que ocurra algún cambio de tecnología de almacenamiento dentro de la empresa.
- En caso de deterioro de medios de almacenamiento, deberían adoptarse medidas para el salvaguardo de estos.
- Establecer lineamientos generales para proceder a la eliminación de activos.

6.4 Resultados y Evaluación del Modelo y la Herramienta para su utilización

Se analizaron un total de 25 activos dentro de la empresa, con el fin de realizar las pruebas y ver la aceptabilidad del modelo propuesto; del 100% de los activos identificados el 28% de los activos fueron calificados con un nivel extremo de importancia dentro de la organización, se hallaron un total de 213 amenazas a las cuales están sujetos los activos identificados.

Con la implementación del modelo propuesto se redujo a un 84.61% el riesgo con calificación extrema a niveles con calificación inferior para que puedan ser aceptados por parte de la organización.

Los riesgos con calificación baja serán aceptados y los que tengan calificación extrema, alta o media no serán aceptados por la organización por lo consecuente se procederá a mitigar estos riesgos mejorando las estrategias de protección utilizando controles normados por la ISO 27002:2013.

Se utilizaron 12 dominios, que contienen 70 controles ya definidos dentro de la norma ISO 27002:2013, los cuales están alineados con los requisitos mínimos que propone la circular G-140-2009 establecida por la Superintendencia de Banca y Seguros, todos estos controles fueron seleccionados con el fin de establecer estrategias de protección para los activos en caso de estar sujetos a amenazas.

Para la evaluación del modelo propuesto y la herramienta desarrollada se ha utilizado la técnica de cuestionario, evaluando a expertos que cumplan con los requisitos establecidos.

6.4.1 Perfil de los expertos evaluados

El perfil de los expertos evaluados está sujetos a profesionales relaciones con la gestión de riesgos, con un promedio de 3 años de experiencia con el fin de evaluar la aplicabilidad de la metodología.

6.4.2 Resultados del cuestionario

La muestra tomada fue de 10 profesionales que cumplían con el perfil descrito líneas arriba

6.4.2.1 ¿Cree Ud. Que la metodología ayude a la mejora de la gestión de riesgos relacionados a la seguridad de la información?

( ) Totalmente de acuerdo

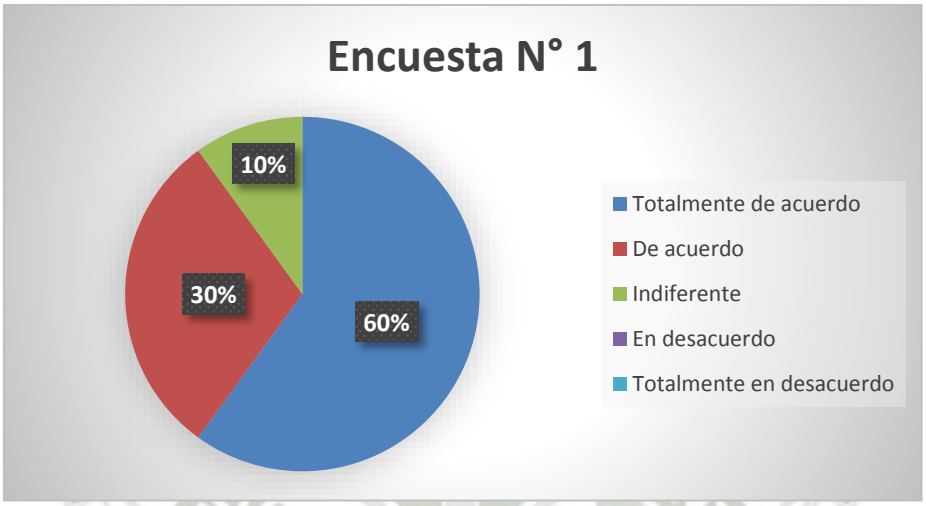
( ) De acuerdo

( ) Indiferente

( ) En desacuerdo

( ) Totalmente en desacuerdo

Figura 44. Encuesta N°1



Fuente: Elaboración propia

El porcentaje de aceptación por parte de los profesionales encuestados es alta, con un 60% de profesionales que están totalmente de acuerdo, un 30% que están de acuerdo y un 10% indiferente.

6.4.2.2. ¿Cree Ud. Que la metodología ayude a la toma de decisiones a empresas financieras para mejorar su gestión ligada a la seguridad de la información?

( ) Totalmente de acuerdo

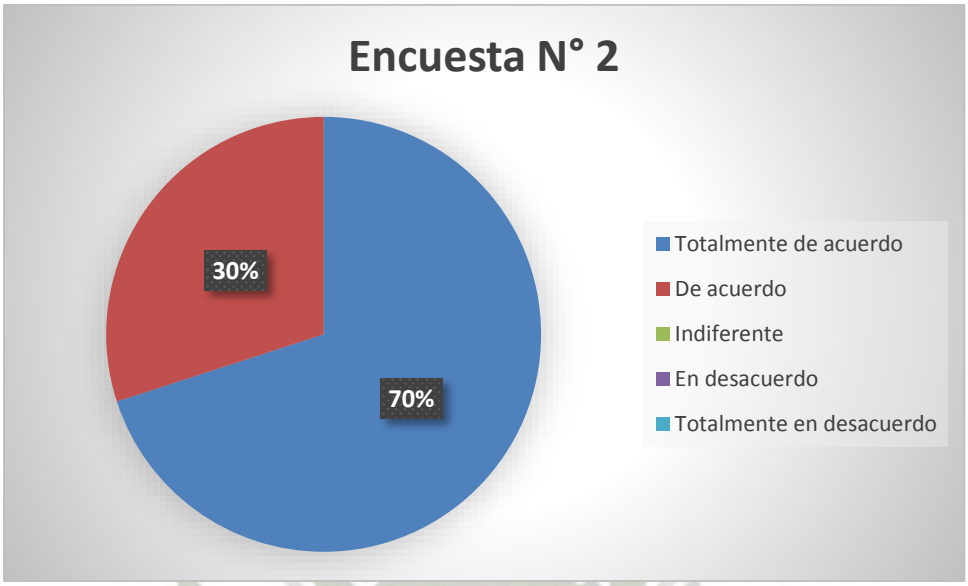
( ) De acuerdo

( ) Indiferente

( ) En desacuerdo

( ) Totalmente en desacuerdo

Figura 45. Encuesta N°2



Fuente: Elaboración propia

Un 70% de los encuestados está totalmente de acuerdo que la metodología propuesta ayude a la toma de decisiones por parte de la dirección y jefaturas, con el fin de brindar mayor seguridad a sus recursos ligados a las áreas de T.I, el otro 30% está de acuerdo que dicha metodología servirá para la toma de decisiones.

6.4.2.3 El modelo propuesto en cuanto a su aplicación resulta:

( ) Muy sencilla

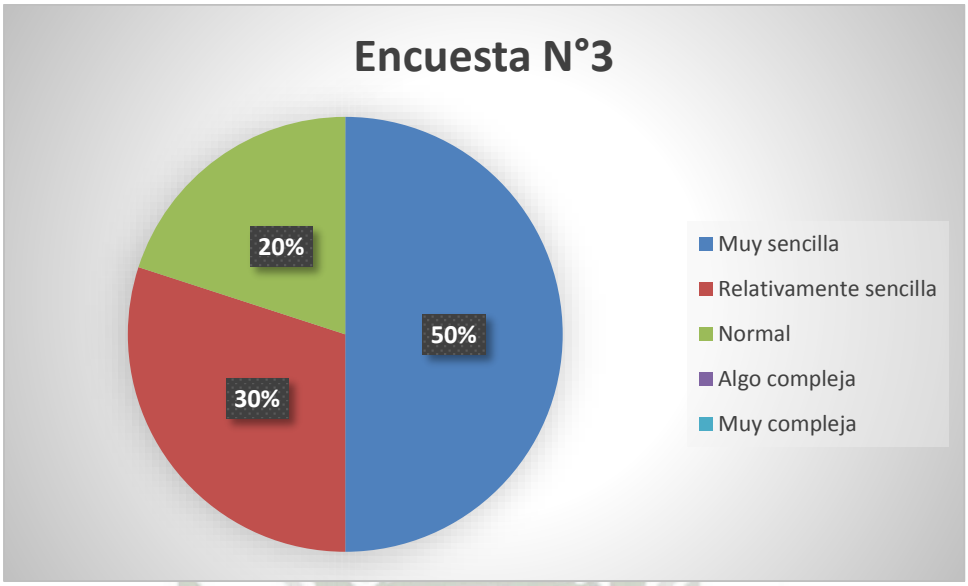
( ) Relativamente sencilla

( ) Normal

( ) Algo compleja

( ) Muy compleja

Figura 46. Encuesta N°3



Fuente: Elaboración propia

El 50% de los encuestados creen que la aplicación de la metodología es muy sencilla en comparación con otras, un 30% creen que es relativamente sencilla y el otro 20% opinaron que les parece una metodología normal en cuanto a su aplicación.

6.4.2.4 Los resultados ofrecidos por la metodología son:

( ) Totalmente entendible

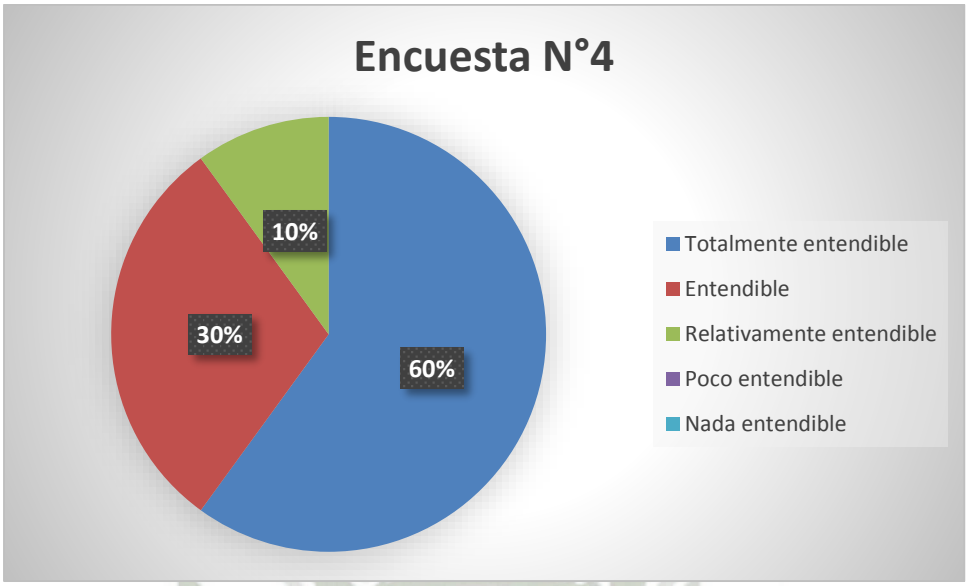
( ) Entendible

( ) Relativamente entendible

( ) Poco entendible

( ) Nada entendible

Figura 47. Encuesta N°4



Fuente: Elaboración propia

El 60% cree que la metodología de gestión de riesgos es totalmente entendible, por ser una metodología sencilla y eficaz para los usuarios, el 30% la considera que es entendible y un 10% cree que es relativamente entendible.

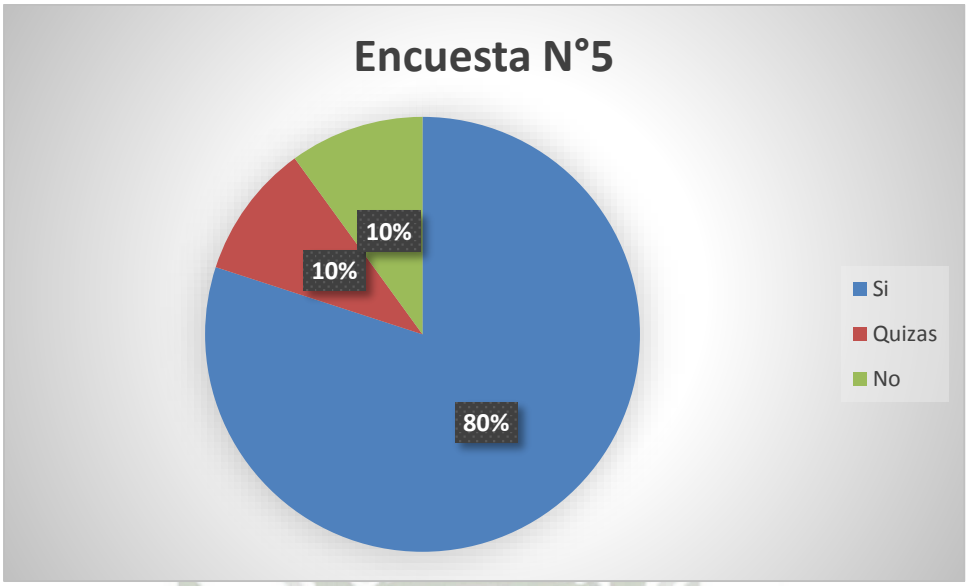
6.4.2.5 ¿Recomendaría el uso de la metodología propuesta a empresas de rubro?

( ) Si

( ) Quizás

( ) No

Figura 48. Encuesta N°5



Fuente: Elaboración propia

El 80% de los encuestados recomendaría el uso de la metodología propuesta y solo un 10% no la recomendaría o quizás la recomendaría, dando como resultado un alto nivel de aceptación por parte de los expertos en el tema.

6.4.2.6 ¿La herramienta de apoyo para la metodología propuesta es?

( ) Muy Buena

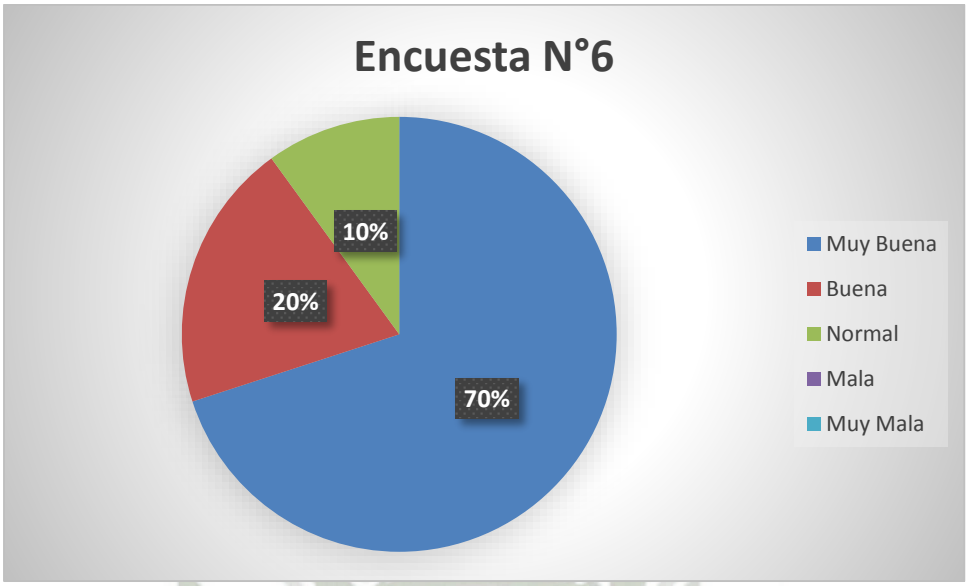
( ) Buena

( ) Normal

( ) Mala

( ) Muy Mala

Figura 49. Encuesta N°6



Fuente: Elaboración propia

El 70% de los encuestados creen que la herramienta de apoyo es muy buena, debido a la sencillez y manejo de datos precisos para la toma de decisiones, un 20% creen que es buena y el otro 10% creen que es normal.

6.4.2.7 ¿Cómo calificaría la usabilidad del sistema?

( ) Muy Buena

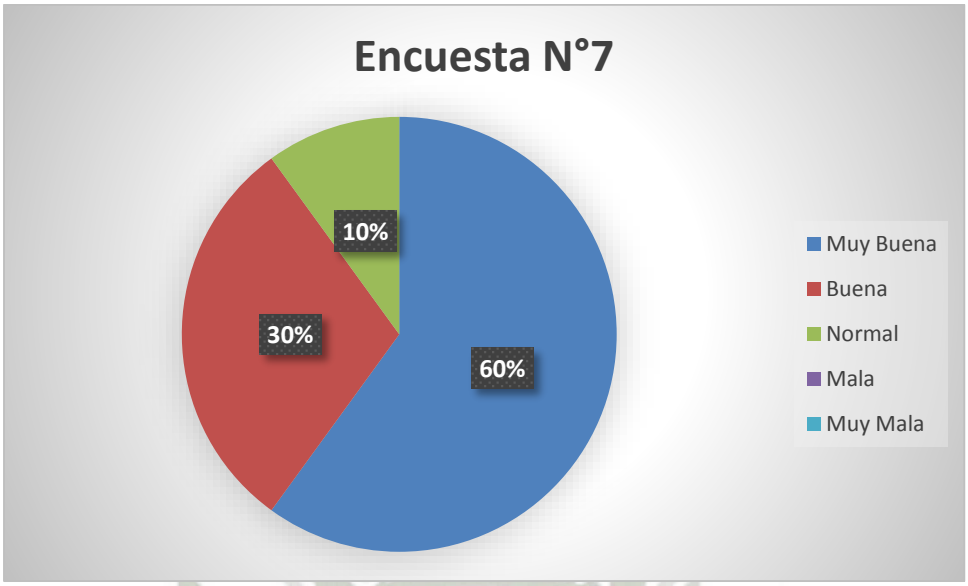
( ) Buena

( ) Normal

( ) Mala

( ) Muy Mala

Figura 50. Encuesta N°7



Fuente: Elaboración propia

El 60% de los encuestados creen que la herramienta de apoyo es muy buena en cuanto a la usabilidad del sistema, un 30% creen que es buena y el otro 10% creen que es normal.

CONCLUSIONES

1. Se diseñó un modelo de gestión de riesgos integrando la metodología MAGERIT y la ISO 27002:2013, utilizando los controles definidos dentro de la norma como salvaguardas.
2. Se identificó una seria de amenazas que afectan directamente a los activos de la empresa, con el fin de mitigar el riesgo que puedan producir a través de controles/salvaguardas definidos en la norma ISO 27002:2013.
3. Se identificó y mitigó los riesgos de una manera oportuna, evitando que generen perjuicios que afecten la continuidad de los servicios que son primordiales para que la empresa cumpla con sus actividades.
4. Se implementaron controles de seguridad que salvaguarden la información crítica de la entidad cumpliendo con lo requerido por la SBS.
5. Se otorgó a la empresa el perfil de uso de buenas prácticas que le permitirá optar por la certificación internacional ISO 27001.
6. Se optimizó el método de identificación y evaluación de activos, proponiendo la utilización de estándares volviéndola más sencilla y eficaz.
7. Se elaboró el plan de seguridad basado en la ISO 27002:2013, con el fin de mitigar los riesgos que se puedan presentar.
8. Se proporcionó un modelo que permite que no solamente una especialista pueda gestionar riesgos, optimizando los tiempos de aprendizaje e implementación del mismo.
9. Se desarrolló un software para facilitar la aplicabilidad del modelo propuesto, mejorando el análisis y gestión de riesgos.

10. Se elaboró un modelo que es aplicable en cualquier entidad del ámbito financiero, pues se realizó en base a estándares requeridos por la SBS.
11. Se llevó a cabo un análisis del nivel de madurez de la organización en cuanto a la ISO 27002, antes y después de aplicar el modelo observando mejoras en la gestión de los controles.

RECOMENDACIONES

1. Se recomienda desarrollar el análisis cuantitativo en base al modelo propuesto, pues allí se especificará claramente las pérdidas económicas a las cuales puede estar sujeta la entidad en caso de no mitigar los riesgos.
2. Se debe dar a conocer a todo el personal de T.I. el plan de seguridad para que tengan claramente identificados los factores y tengan conocimiento de cómo actuar frente a posibles apariciones de amenazas.
3. Se deben realizar capacitaciones periódicas que fomenten las buenas prácticas para tener un adecuado control de riesgos.
4. Fomentar el uso del software por parte de los colaboradores de la organización.

REFERENCIAS BIBLIOGRAFICAS

- Aguilera López Purificación (2010). Seguridad Informática. Madrid, España: Editorial Editex.
- Areitio Bertolin Javier (2008). Seguridad de la Información, redes, informática y sistemas de la información. Madrid, España: Editorial Parainfo.
- De Pablos Heredero Carmen - López Hermoso Agius José Joaquín - Romo Romero Santiago Martin - Medina Salgado Sonia (2011) Organización y transformación de los sistemas de información en la empresa. España: Editorial ESIC
- Florentino Galindo Elizabeth - Morales Jaime Gabriel - Peña Velázquez, Juan. (2011). Aplicación de la metodología Magerit en el análisis de riesgo del flujo de información en el área de gestión de una empresa dedica a la aplicación de exámenes de control de confianza. Ciudad de México, México.
- Giménez Albacete José Francisco (2014). Seguridad en equipos informativos. España: Editorial IC
- Lucero Gómez Antonio José - Valverde Padilla John Oswaldo (2011). Análisis y gestión de riesgos de los sistemas de la cooperativa de ahorro y crédito jardín azuayo, utilizando la metodología Magerit. Cuenca, Ecuador.
- Molina Miranda María Fernanda (2015). Propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del Litoral. Guayaquil, Ecuador.

- Rumbaugh James, Jacobson Ivar, Booch Grady. (2000). El lenguaje Unificado de modelado Manual de Referencia. Madrid, España: Editorial Addison Wesley
- Santos Llanos Daniel Elías (2016). Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Lima, Perú.
- Van Selm Leo (2008). ISO/IEC 20000 – Una introducción. Amersfoort Holanda: Editorial Van Haren
- Villena Aguilar Moisés Antonio (2011). Sistema de gestión de la seguridad de la información para una institución financiera. Lima, Perú.
- Advisera. (2016). 20000 academy. Recuperado de: http://advisera.com/20000academy/es/
- Welive Security. (2013). ISO/IEC 27002:2013 y los cambios en los dominios de control. Recuperado de: http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/
- Magerit. (2012). MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/
- Rios. P. (2012). Recuperado de: http://redes-pao.blogspot.pe/2012/04/tabla-comparativa-metodologias-magerit.html
- IsoTools. (2016). ISO 31000 Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000

- Audea (2009). Análisis y gestión de riesgos. Recuperado de: https://www.audea.com/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias/
- ISO 27000 (2012). Portal de ISO 27001 en español. Recuperado de: http://www.iso27000.es/download/doc_iso27000_all.pdf
- El método Magerit (2015). Blog especializado en Gestión de la Seguridad de la Información. Recuperado de: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/
- Vanegas, G & Pardo. C. (2014). Hacia un modelo de gestión de riesgos de TI en MiPyMes: MOGRIT Recuperado de: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/viewFile/1860/2398

ANEXOS

ANEXO A - TIPOS DE ACTIVOS

Magerit (2012)

- Activos esenciales
- Datos de carácter personal
- Arquitectura del sistema
- [D] Datos / Información
- [K] Claves criptográficas
- [S] Servicios
- [SW] Software - Aplicaciones informáticas
- [HW] Equipamiento informático (hardware)
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

ANEXO B - TIPOS DE AMENAZAS

Magerit (2012)

[N] Desastres naturales

[N.1] Fuego

[N.2] Daños por agua

[N.3] Terremotos

[N.4] Tsunamis

[N.*] Desastres Naturales Varios

[I] De origen industrial

[I.1] Fuego

[I.2] Daños por agua

[I.*] Desastres industriales – siniestros mayores

[I.3] Contaminación mecánica

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios y suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios

[E.2] Errores del administrador

[E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia

[E.14] Escapes de información

[E.15] Alteración accidental de la información

[E.18] Destrucción de información

[E.19] Fugas de información

[E.20] Vulnerabilidades de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Pérdida de equipos

[E.28] Indisponibilidad del personal

[A] Ataques intencionados

[A.3] Manipulación de los registros de actividad (log)

[A.4] Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] [Re-]encaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de tráfico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación deliberada de la información

[A.18] Destrucción de información

[A.19] Divulgación de información

[A.22] Manipulación de programas

[A.23] Manipulación de los equipos

[A.24] Denegación de servicio

[A.25] Robo

[A.26] Ataque destructivo

[A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal

[A.29] Extorsión

[A.30] Ingeniería social (picaresca)

ANEXO C - EVALUACIÓN POLÍTICAS DE SEGURIDAD ISO 27002:2013

- ¿Se tiene definidas políticas de seguridad de la información?

  SI ( ) NO ( )

- ¿Se vienen aplicando dichas políticas dentro de la empresa?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Dichas políticas de seguridad de la información están basadas en algún estándar o norma?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuentan con controles implementados basados en la ISO 27002, para el cumplimiento de las políticas de seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿El personal de la empresa tiene conocimiento de la existencia de las políticas de seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Son actualizadas periódicamente las políticas de seguridad de la información, en caso de ser necesario?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO D - EVALUACIÓN DE LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

- ¿Existe algún área responsable y/o encargado de la elaboración, seguimiento y mantenimiento de las políticas de la seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿El área de Tecnologías de la información es independiente para poder tomar decisiones?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Existen clausulas al momento de contratar a terceros en temas respecto a la seguridad de la información?

  SI ( ) NO ( )

- ¿Se tienen identificados los procesos de seguridad de la información?

  ( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tienen definidos los niveles de autorización dentro del área de Tecnologías e la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO E - EVALUACIÓN DE LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

- ¿Se realizan investigaciones de antecedentes a los nuevos postulantes a las áreas de TI?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuentan definidas los roles y responsabilidades de la seguridad de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se incluyen temas de confidencialidad y responsabilidades en los contratos firmados por los colaboradores de la empresa?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tienen implementadas charlas para el personal en temas de seguridad de la información?

SI ( ) NO ( )

- ¿Se realizan procesos de selección para contratistas?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tiene establecido un programa de concientización de seguridad de la información de acuerdo con las políticas de seguridad de la información?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Existen procesos disciplinarios para los empleados que hayan violado alguna regla de la seguridad de la información?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Los empleados informan sobre vulnerabilidades que puedan ser observadas en su área de trabajo?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO F - EVALUACIÓN DE LA GESTIÓN DE ACTIVOS

- ¿Se cuenta con un inventario de activos informáticos en la empresa?

  SI ( ) NO ( )

- ¿El inventario se encuentra automatizado, actualizado y consistente?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se mantiene actualizado el inventario periódicamente?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Los activos son asignados a un responsable, ya sea un individuo o una entidad?

  SI ( ) NO ( )

- ¿Se tienen implementadas reglas para el uso aceptable de la información y de activos que estén asociados con la información y las instalaciones de procesamiento de la información?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Existen formatos establecidos para la devolución de activos dentro de la organización?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿El inventario se encuentra clasificado de acuerdo a los tipos de activos que existen dentro de la organización?

  SI ( ) NO ( )

- ¿Se encuentran rotulados todos los activos de la organización?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Existen procedimientos establecidos para la extracción de medios?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

ANEXO G - EVALUACIÓN DEL CONTROL DE ACCESOS

- ¿Se tiene definidas políticas para el control de accesos?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen definidos los niveles de accesos por usuario de acuerdo al cargo que desempeñen?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen procesos definidos para el registro y cancelación de usuarios, así como la asignación de derechos de acceso?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se llevan controles periódicos para la revisión de los derechos de accesos de los usuarios?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tiene implementado un sistema de gestión de contraseñas?

SI ( ) NO ( )

- ¿Se tiene controlado el acceso al código fuente de programas fuente?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se cuentan con restricciones horarias para el logeo a las diversas aplicaciones de la empresa?

SI ( ) NO ( )

ANEXO H - EVALUACIÓN DEL CIFRADO

- ¿Se tiene definidas políticas para el cifrado?

  SI ( ) NO ( )

- ¿Existe algún control para la gestión de claves durante todo su ciclo de vida?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Existe implementada la norma ISO 11770 para el tratamiento de la gestión de claves?

  SI ( ) NO ( )

ANEXO I - EVALUACIÓN DE LA SEGURIDAD FÍSICA Y AMBIENTAL

- ¿La organización cuenta con un perímetro de seguridad física establecido?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Existen establecidos controles de acceso físico que aseguren solo el acceso a personal autorizado?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen procedimientos para el control de la seguridad de oficinas e instalaciones del área de TI?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tienen implementadas controles o salvaguardas contra amenazas externas y del medio ambiente?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuentan con procedimientos para los trabajos en áreas seguras?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Permanecen encendidos los servidores las 24 horas del día; es necesario que estén prendidos durante todo ese tiempo?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tienen protegidos los activos importantes frente a amenazas y peligros ambientales?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuentan con equipos alternos que permitan el funcionamiento de equipos que necesiten suministro eléctrico en casos de emergencia?

  SI ( ) NO ( )

- ¿Se cuentan con planes de mantenimientos preventivos y correctivos?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Existen extintores colocados en áreas plenamente identificados como prevención en caso cualquier accidente?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuentan con procedimientos para evitar la interceptación, interferencia o daños en el cableado de energía y telecomunicaciones?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO J - EVALUACIÓN DE LA SEGURIDAD EN LA OPERATIVA

- ¿Se cuenta con procedimientos de operación correcta y segura de las instalaciones de procesamiento de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se lleva un control referente a los cambios que ocurren en la organización que afecten a la seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen establecidas responsabilidades y procedimientos formales con el fin de asegurar el control de todos los cambios?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se supervisa el uso de recursos así como las proyecciones futuras de capacidad?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tiene implementado un plan de gestión de capacidades para sistemas críticos?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuentan con diferentes ambientes para desarrollo, prueba y producción?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tienen controles y procedimientos frente al ataque de código malicioso?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se realizan copias de seguridad de la información y software periódicamente?

  SI ( ) NO ( )

- ¿Son revisadas adecuadamente acorde con políticas de respaldo?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se revisan regularmente los registros de eventos de las actividades de los usuarios, excepciones y eventos de la seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen protegidos la información de los registros (logs), así como los registros del administrador y operador?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se mantiene un registro y control del software que es instalado en producción y sistemas operativos?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se tiene información sobre las vulnerabilidades técnicas de los sistemas de información en uso y activos de la organización?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se llevan a cabo planes de auditoria referentes a los sistemas en producción?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO K - EVALUACIÓN DE LA SEGURIDAD EN LAS TELECOMUNICACIONES

- ¿Se controlan y gestionan adecuadamente las redes con el fin de proteger los sistemas y las aplicaciones?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se viene trabajando con la ISO 27003 en la organización?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen identificados los mecanismos de seguridad de los servicios de red y están incluidos en un acuerdo de servicio?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se encuentran divididas las redes para controlar la seguridad?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tiene definidas políticas para proteger el intercambio de información?

  SI ( ) NO ( )

- ¿Se usan técnicas de encriptación para proteger la autenticidad, confidenciabilidad e integridad de la información?

  SI ( ) NO ( )

- ¿Se tienen acuerdos para el intercambio de información seguro entre la organización y terceros?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen identificaos acuerdos de confidenciabilidad o no divulgación para la protección de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO L - EVALUACIÓN DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

- ¿Se incluyen requisitos relacionados con la seguridad de la información para mejoras o nuevos sistemas de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se cuenta con licencias para los productos que lo requieren?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se protegen las transacciones en línea para prevenir la transmisión incompleta con el fin de evitar perdida de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Los usuarios tienen restricciones para la instalación de software independiente del uso de la organización?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se encuentra garantizada la seguridad de la información en el ciclo de vida de desarrollo de los sistemas de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se controlan mediante procedimientos los cambios de los sistemas durante el desarrollo de los mismos?

  ( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Existe un plan anual de desarrollo de sistemas durante el ciclo de vida del software?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se realizan manuales de usuario y son actualizados periódicamente en caso de ser necesarios?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tienen establecidos ambientes de desarrollo seguro para el desarrollo de sistemas que cubran todo el ciclo de vida del desarrollo?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se realizan pruebas seguras antes de llevar cualquier modificación o nueva implementación a producción?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

ANEXO M - RELACIONES CON SUMINISTRADORES

- ¿Se tiene definidas políticas de seguridad de la información para las relaciones con los proveedores?

  SI ( ) NO ( )

- ¿Se tienen acuerdos establecidos para asegurar las obligaciones por ambas partes entre la organización y los proveedores?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se maneja una cadena de suministro de tecnologías de la información y comunicaciones?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se realiza el seguimiento y control de los servicios prestados por terceros, validando los acuerdos establecidos?

( ) Muy de acuerdo

( ) Algo de acuerdo

( ) Ni de acuerdo ni en desacuerdo

( ) Algo en desacuerdo

( ) Muy en desacuerdo

- ¿Se realizan auditorías a los proveedores para analizar el nivel de cumplimiento de los mismos?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se tiene un responsable de gestionar las relaciones con los proveedores?

  SI ( ) NO ( )

ANEXO N - EVALUACIÓN GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

- ¿Se tienen definidos procedimientos y responsabilidades con el fin de gestionar los incidentes de seguridad de una forma eficiente y eficaz?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se llevan a cabo controles de los reportes de eventos de seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se utiliza la norma ISO 27035 sobre la gestión de incidentes de la seguridad de la información?

  SI ( ) NO ( )

- ¿Existen mecanismos para permitir que los tipos y costos de los incidentes de seguridad de la información sean controlados y cuantificados?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Los empleados son conscientes de no realizar pruebas en las debilidades de seguridad que puedan ser encontrados y notificar inmediatamente al área pertinente?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO O - EVALUACIÓN DE LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

- ¿Existen implementados planes de continuidad del negocio?

  SI ( ) NO ( )

- ¿Se tienen establecidos y documentados procedimientos y procesos para garantizar el nivel requerido de continuidad de seguridad de la información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se verifican y evalúan periódicamente los controles de continuidad del negocio?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se utilizan las normas ISO 27031, ISO 22313 e ISO 22301 en la organización sobre la gestión de la continuidad del negocio?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

- ¿Se garantiza la disponibilidad de las instalaciones de procesamiento de información?

  ( ) Muy de acuerdo

  ( ) Algo de acuerdo

  ( ) Ni de acuerdo ni en desacuerdo

  ( ) Algo en desacuerdo

  ( ) Muy en desacuerdo

ANEXO P - EVALUACIÓN DEL CUMPLIMIENTO

- ¿Se tienen definidos controles y responsabilidades para evitar incumplimientos de las obligaciones legales relacionados con la S.I.

SI [ ] NO [ ]

- ¿Se tienen procedimientos para asegurar el cumplimiento sobre los derechos de propiedad intelectual y sobre el uso de productos de software propietario?

SI [ ] NO [ ]

- ¿Se lleva un listado de todos los activos con requisitos protegidos por el derecho de propiedad intelectual?

SI [ ] NO [ ]

- ¿Se tiene documentado las propiedades de las licencias?

SI [ ] NO [ ]

- ¿Se tienen protegidos los datos y privacidad de la información personal?

SI [ ] NO [ ]

- ¿Se utilizan las norma ISO 29100 con el fin de tener protección sobre los datos personas?

SI [ ] NO [ ]

- ¿Se revisa periódicamente que la seguridad de la información es implementada y operada de acuerdo a las políticas ya establecidas?

SI [ ] NO [ ]

- ¿Los directores de la organización revisan periódicamente el cumplimiento de procesamiento de la información?

SI [ ] NO [ ]