Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA

Eddy Adrián López Rodríguez
Asesorado por el Ing. Rafael Rubén Sanic Maguirre

Guatemala, febrero de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

EDDY ADRIÁN LÓPEZ RODRÍGUEZ
ASESORADO POR EL ING. RAFAEL RUBÉN SANIC MAGUIRRE

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO INDUSTRIAL

GUATEMALA, FEBRERO DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Vladimir Armando Cruz
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Byron Gerardo Chocooj Barrientos
EXAMINADOR	Ing. Selvin Estuardo Joachín Juárez
EXAMINADORA	Inga. María Martha Wolford E. de Hernández
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Industrial con fecha 6 de septiembre de 2019.

Eddy Adrián López Rodríguez

Guatemala 25 de septiembre de 2020

Ingeniero César Ernesto Urquizú Rodas
Director
Escuela de ingeniería Mecánica Industrial
Facultad de ingeniería
Universidad de San Carlos de Guatemala

Por medio de la presente hago constar, que he revisado y aprobado el trabajo de graduación que lleva por nombre **DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA,** del estudiante **EDDY ADRIÁN LÓPEZ RODRÍGUEZ** de la Escuela de Ingeniería Mecánica Industrial.

Sin otro particular, me despido.

Rafael Rubén Sanic Maguirre
Ingeniero Industrial
Col. 11988

Rafael Rubén Sanic Maguirre
Ingeniero industrial
No. De colegiado 11,988

ESCUELA DE
INGENIERÍA MECÁNICA INDUSTRIAL
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF.REV.EMI.113.020

Como Catedrático Revisor del Trabajo de Graduación titulado **DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA,** presentado por el estudiante universitario **Eddy Adrián López Rodríguez,** apruebo el presente trabajo y recomiendo la autorización del mismo.

"ID Y ENSEÑAD A TODOS"

Renaldo Girón Alvarado
Ingeniero Industrial
Colegiado No. 5977

Ing. Renaldo Girón Alvarado
Catedrático Revisor de Trabajos de Graduación
Escuela de Ingeniería Mecánica Industrial

Guatemala, noviembre de 2020.

/mgp

ESCUELA DE
INGENIERÍA MECÁNICA INDUSTRIAL
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF.DIR.EMI.009.021

El Director de la Escuela de Ingeniería Mecánica Industrial de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el Visto Bueno del Revisor y la aprobación del Área de Lingüística del trabajo de graduación titulado **DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA,** presentado por el estudiante universitario **Eddy Adrián López Rodríguez,** aprueba el presente trabajo y solicita la autorización del mismo.

"ID Y ENSEÑAD A TODOS"

Ing. César Ernesto Urquizú Rodas
DIRECTOR
Escuela de Ingeniería Mecánica Industrial

Guatemala, febrero de 2021.

/mgp

Decanato
Facultad de Ingeniería
24189101- 24189102

DTG. 055.2021.

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Industrial, al Trabajo de Graduación titulado: **DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DEDICADA A LA SEGURIDAD ELECTRÓNICA,** presentado por el estudiante universitario: **Eddy Adrián López Rodríguez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Anabela Cordova Estrada
Decana

Guatemala, febrero de 2021.

AACE/asga

ACTO QUE DEDICO A:

Mis padres	Aura Rodríguez y Víctor López, por el esfuerzo y sacrificios realizados para brindarme estudios.
Mis hermanos	Estuardo, Lourdes, Sergio y Amarilis López Rodríguez, por su apoyo y cariño.
Mi novia	Olimpia Marroquín, por la compañía, apoyo y motivación.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por la oportunidad y el privilegio de pertenecer a esta casa de estudios.
Facultad de Ingeniería	Por la formación académica brindada.
Mi asesor	Ing. Rubén Sanic, por el apoyo y la guía en la realización de este trabajo de graduación.
Mis amigos	Brandon Velásquez, Claudia Valiente, Dayreem Núñez, Elvis Ávila, Emerson Villatoro, Erick Quevedo, Jorge Ortiz, Nery Moreno, Omar Aquino, Osbin Miranda, Oscar Barrios, Rafael Meoño, Sergio Salazar, Thelmy Cruz y Walter Villalta, por el apoyo y amistad durante la carrera.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
A	Alto
B	Bajo
C	Confidencialidad
D	Disponibilidad
I	Integridad
M	Medio
MA	Muy alto
MB	Muy bajo
%	Porcentaje
Q	Quetzal, moneda de la República de Guatemala

GLOSARIO

Arquitectura del sistema	Estructura de funcionamiento de los sistemas entre el software, el hardware y el usuario.
CCTV	Siglas del inglés *closed circuit television,* sistema de videovigilancia compuesto por cámaras, equipos de grabación y monitores de video.
CD	Siglas del inglés *compact disc*, disco compacto, es una unidad de almacenamiento de datos digitales, en forma de disco.
Centro de procesamiento de datos	Instalaciones acondicionadas para albergar equipos electrónicos de computación, donde se centraliza la operación de los sistemas de información de una organización.
Disco duro	Dispositivo de almacenamiento de datos digitales, compuesto de un disco rígido dentro de un compartimiento sellado, que es utilizado por equipos de cómputo.
Disuasorio	Propiedad de las medidas de seguridad que hace que un atacante renuncie o abandone la intención de atacar.

DVD	Siglas del inglés *digital versatile disc*, disco digital versátil; es una unidad de almacenamiento de datos digitales, en forma de disco con mayor capacidad que un disco compacto o CD.
DVR	Siglas del inglés *digital video recorder*, grabador de video digital; es un equipo que almacena el video procedente de las cámaras de videovigilancia.
Encriptación	Procedimiento en el que los datos son descompuestos por algoritmos, tomando formas ilegibles para almacenar o enviar información de forma segura; solo el intérprete con la clave del algoritmo puede volver a estructurarlo.
Ignífugo	Característica de un material que lo hace resistente a la combustión.
Lista blanca	Direcciones de equipos o servidores a los que está permitido el acceso desde la red de computación.
Lista negra	Direcciones de equipos o servidores a las que está restringido el acceso desde la red de computación.
Nube	Cualquier servicio informático disponible a través de internet.
Ofimático	Aplicaciones de computadora utilizadas para ejecutar tareas de oficina.

Red	Conjunto de equipos interconectados que comparten información entre sí.
Router	Dispositivo electrónico dedicado a la administración del tráfico de datos de una red de computadoras.
Salvaguarda	Conocidos también como controles, son las medidas de protección para activos de información.
Seguridad electrónica	Uso de tecnologías de la información y comunicación para la seguridad física y protección de activos.
Servicios web	Aplicaciones intérpretes para comunicar e intercambiar información entre aplicaciones de diferentes lenguajes que se ejecutan en diferentes plataformas.
UPS	Siglas del inglés *uninterruptible power supply*, fuente de energía no interrumpible; es un equipo compuesto por un conjunto de baterías recargables, que dan energía eléctrica cuando la fuente primaria de electricidad se interrumpe.

RESUMEN

La investigación se basa en el análisis y gestión de riesgos a la seguridad de la información en la organización dedicada a la seguridad electrónica. Con base en el modelo de proceso de gestión de riesgos y utilizando la metodología de análisis cualitativo por tablas, se desarrolla un análisis de riesgo desde la definición de un modelo de valor a través de la identificación y valoración de los activos, identificación de las amenazas y vulnerabilidades que dan paso a la estimación del estado de riesgo, fase en la que se identifican y proponen los controles adecuados que deben existir para cada una de las amenazas definidas, según las políticas y dirección de la organización, concluyendo con la estimación de los impactos y riesgos potenciales y residuales.

El resultado del análisis y gestión de los riesgos es la presentación de un plan de seguridad en el que se proponen las acciones que se deben llevar a llevar a cabo para implementar o mejorar los controles existentes que lleven el impacto y riesgo hacia los niveles considerados aceptables por la organización. El plan contiene un programa de seguridad compuesto por los controles, la definición de áreas y personas a cargo, las estimaciones de los recursos necesarios, así como una estimación del impacto operativo y económico que el desarrollo y la implementación del plan tendrá para la organización.

OBJETIVOS

General

Diseñar un modelo que contenga la estructura viable para la gestión de riesgos de la seguridad de la información física y electrónica.

Específicos

1. Identificar y caracterizar los activos de información para definir su valor dentro del sistema de información.

2. Establecer las amenazas para conocer la degradación que tendrá sobre el valor del activo y la probabilidad de que se materialicen.

3. Estimar el impacto y riesgo potencial para cuantificar la magnitud de la degradación, causados por las amenazas y su probabilidad de ocurrencia.

4. Definir y caracterizar los controles, procedimientos o mecanismos de seguridad para evaluar su eficacia y eficiencia ante las amenazas.

5. Evaluar el impacto y el riesgo residual para determinar las decisiones de tratamiento de riesgos.

INTRODUCCIÓN

La información es uno de los activos más importantes y es la base fundamental de todas las organizaciones para mantener sus niveles de competitividad, rentabilidad, apego legal e imagen, con los que busca alcanzar sus objetivos y beneficios económicos que sostienen la continuidad de un negocio.

La empresa en estudio es consciente de las deficiencias en la seguridad de sus sistemas de información, y consideran que estos están expuestos a una cantidad de amenazas cada vez mayor, las cuales toman ventaja de cualquier vulnerabilidad que pueda existir para someter a los activos de información, a diversas formas de daño. Estos activos pueden ser víctimas de actos como robo de información, fraudes y sabotajes, y también ser afectados por *software* malintencionado o más conocidos como virus informáticos, ataques de personas y ataques de denegación de servicio.

Es importante para la empresa conocer la existencia de riesgos provocados voluntaria o involuntariamente por las condiciones de la organización, fallos técnicos y de su personal; también los que podrían ocasionar accidentalmente las catástrofes naturales.

La existencia de estos riesgos puede tener como consecuencia un impacto negativo para la empresa tales como pérdidas económicas, pérdida de confianza o imagen de la empresa, reducción de la productividad, así como el daño o perjuicio a sus socios de negocio. Dado el tipo de negocio y mercado, deben cumplir con los compromisos de resguardo, administración y confidencialidad.

1. MARCO TEÓRICO

Conjunto de fundamentos o conceptos que permitirán contextualizar el problema planteado.

1.1. La seguridad de la información

La seguridad es una propiedad que determina un nivel de confianza de los sistemas de información para soportar y defenderse ante eventos accidentales o deliberados que provoquen daños.

1.1.1. Definiciones

- Datos: símbolos que potencialmente representan algo.

- Información: es un conjunto de datos que, procesados, organizados y puestos es una estructura describen algo. Las imágenes, ficheros, documentos, videos, audio o una conversación son ejemplos de información; esta puede presentarse en distintos formatos como el físico, impreso, digital y magnético.

- Seguridad: de manera general, la seguridad es un estado o característica de que algo o alguien están protegidos ante peligros o daños que como consecuencia lo perturben o destruyan.

- Sistema: es un conjunto de elemento dinámicos interrelacionados, que poseen funciones orientadas al cumplimiento de un objetivo común.

- Sistemas de información: “Conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.”[1]

- Seguridad de la información: es el estado de protección que poseen los sistemas de información ante posibles eventos que pueden ocasionarle daños. La protección de los sistemas son todos aquellos mecanismos, políticas o actividades que mitigan o eliminan los posibles eventos dañinos denominados amenazas. Si el sistema cuenta con poca o ninguna protección, esto indica que ese sistema está en riesgo elevado de sufrir daños o que las amenazas se materialicen. La seguridad de la información está conformada por elementos o características denominadas ejes o dimensiones.

“La seguridad se caracteriza como la protección frente a las amenazas de confidencialidad, integridad y disponibilidad y pueden ser amenazas de fuerza mayor, fallos de organización, humanos o técnicos o actos malintencionados. Algunas de las amenazas más frecuentes están relacionadas con el incumplimiento de las medidas de seguridad y con la administración incorrecta de los sistemas y la comisión de errores en su configuración y operación.” [2]

1.1.2. Ejes

Los ejes o dimensiones son los atributos inherentes de la seguridad de la información. Estas dimensiones son: confidencialidad, integridad y disponibilidad.

[1] EcuRed**.** *Sistema de Información*. https://www.ecured.cu/Sistema-de_Informaci%C3%B3n.
[2] LÓPEZ RIVAS, Jose Luis. *Protección de la información*. http://jlrivas.webs.uvigo.es/downloads/publicaciones/protinf.pdf.

Para un mismo elemento de información a analizar, interesa conocer la magnitud, en una valoración cuantitativa; o su nivel o rango en una valoración cualitativa, de cada una de sus dimensiones de seguridad; los resultados son independientes entre cada una de ellas.

1.1.2.1. Confidencialidad

Característica consistente en la restricción al acceso y divulgación de información exclusivamente a usuarios, dispositivos o sistemas autorizados. La confidencialidad conserva la privacidad de la información.

Determina qué y quiénes están permitidos para conocer la información. El valor de la confidencialidad es alto cuando se tiene certeza de que el acceso no autorizado a la información provocará un gran daño a la organización; y bajo o despreciable cuando se conoce que el acceso no provocará ningún perjuicio.

1.1.2.2. Integridad

"La integridad es la propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales." [3]

Indica la preservación de la información en su estructura y contenido inicial u original. La valoración de integridad es alta cuando se tiene certeza que la

[3] Instituto Nacional de Ciberseguridad**.** *Glosario de términos de ciberseguridad*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf.

alteración o destrucción de la información provocará un gran daño a la organización; y bajo o despreciable cuando se conoce que la alteración a esta no provocará ningún perjuicio.

1.1.2.3. Disponibilidad

Es la característica en la cual la información es accesible por los usuarios, dispositivos o sistemas autorizados en el momento que lo demanden. Indica si la información o la herramienta de acceso a esta son utilizables en todo momento. La valoración de la disponibilidad es alta si la falta de acceso a la información provoca un daño a la organización; y es bajo o despreciable, cuando la falta de acceso no tiene consecuencias negativas.

1.2. Análisis y evaluación de riesgos

El análisis de riesgos describe los elementos que componen un sistema de información, las amenazas y vulnerabilidades para determinar y calificar los riesgos que se identifiquen en el proceso. Describe la situación actual del sistema. La evaluación de riesgos es la fase en la que se determinan las acciones que se desarrollarán para mitigar las deficiencias en el sistema detectadas por el análisis, con el fin de reducir el riesgo.

1.2.1. Análisis de riesgo

Es la primera fase del proceso de gestión de riesgos, cuyo objetivo es describir el sistema y estimar el estado de riesgo.

1.2.1.1. Definiciones de análisis de riesgo

El análisis de riesgo es un estudio que identifica las amenazas a las que está expuesto los elementos de un sistema y determina sus vulnerabilidades. Como resultado se obtiene una estimación o evaluación del impacto sobre el sistema de las amenazas encontradas en función de su vulnerabilidad. Para el desarrollo del análisis se requiere la identificación de los elementos del sistema: activos, amenazas, vulnerabilidades, riesgo, impacto y controles o salvaguardas.

"Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo."[4]

1.2.1.2. Activo

"Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones."[5]

Son los elementos tangibles e intangibles que contienen o manejan información de valor y son susceptibles a ser atacados. El daño o violación a los activos tiene consecuencias negativas para la organización. En todo sistema de información hay dos activos esenciales: los datos que contiene y el servicio que brinda.

---

[4] Instituto Nacional de Ciberseguridad. *Glosario de términos de ciberseguridad.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf.
[5] Íbíd.

Los activos se clasifican según sus propiedades:

- Datos: activo esencial, es la representación a través de símbolos que potencialmente describen algo. Todos los demás activos son medios o herramientas para su interpretación y uso.

- Servicios: activo esencial, representan el trabajo de procesar datos para obtener información.

- Aplicaciones informáticas o software: son los programas utilizados en los dispositivos de computación que ayudan al acceso, manejo y presentación de la información. Un ejemplo de estos son los programas ofimáticos.

- Dispositivos informáticos o hardware: equipos donde se almacenan los datos y se ejecutan las aplicaciones. Ejemplo de estos son las computadoras o los teléfonos móviles.

- Soportes de información: son los dispositivos diseñados para el almacenamiento de información, por ejemplo, los discos duros externos, o las memorias USB.

- Equipo auxiliar: son equipos que cumplen funciones específicas dentro de un sistema de información, por ejemplo, las fuentes de poder auxiliar o UPS que mantienen encendidos los equipos conectados a este.

- Redes de comunicación: son dispositivos diseñados para comunicar o compartir información entre equipos, como los conmutadores o *router*.

- Instalaciones: son las estructuras físicas que hospedan otros activos de información.

- Personal: las personas involucradas en los sistemas de información. Pueden ser el recurso humano de la organización, los clientes o agentes externos con los que se comparte información.

1.2.1.2.1. Dependencia

Es la relación de existencia o funcionamiento de un activo con otro. Un activo casi siempre dependerá de otro. Un dato o información necesita de algún medio, otro activo, para poder ser accedido. Un ejemplo de dependencia es una computadora y la información que ella almacena, puesto que para acceder a la información se necesita de la computadora.

La dependencia se visualiza como una estructura jerárquica en la que los activos ubicados en la parte superior dependen de los que están en la parte inferior. Analizando de arriba hacia abajo, la estructura indica la dependencia, mientras que de abajo hacia arriba indica la propagación del impacto o daño cuando una amenaza suceda, o en otros términos qué consecuencias tendrá en un activo superior, el daño en un activo inferior.

1.2.1.2.2. Valoración de activos

Es darles un valor a los activos, ignorando su costo monetario o de adquisición. Esto quiere decir, qué tan valioso es un activo para una organización, sus características financieras, legales, fiscales, administrativas, operativas, entre otras, que la organización deba valorar, y para lo cual necesite protegerlos.

La protección estará en función de la valoración; si un activo es muy valioso dadas sus características, entonces mayor debe ser la protección hacia este.

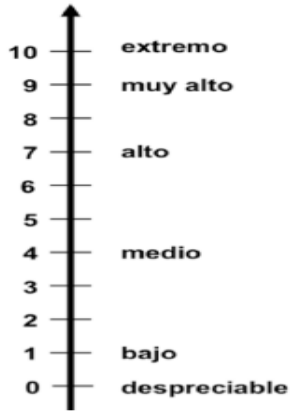
Los activos tienen un valor propio y acumulado. El valor propio es el valor de los activos esenciales que pueden contener, datos o servicios. El valor acumulado es aquel que toma en cuenta sus dependencias.

La valoración debe realizarse para cada una de las dimensiones: confidencialidad, integridad y disponibilidad.

1.2.1.2.3. Criterios de valoración

Para la valoración de activos es permitida cualquier escala de valores, siempre que esta se utilice en todas las dimensiones, y se base en una escala logarítmica con diferencias relativas.

Figura 1. **Escalas de valor**



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. *MAGERIT versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información*, p. 19.

1.2.1.3. Amenaza

Las amenazas son los eventos o acciones perjudiciales que pueden materializarse sobre un activo. Se clasifican de la siguiente forma:

- De origen natural: las que no son provocadas por un factor humano como las inundaciones, terremotos, incendios y tormentas eléctricas.

- Del entorno: son provocados por los elementos o condición que rodea a un activo como contaminación mecánica o cortes eléctricos, entre otros.

- Fallos o defectos inherentes del activo: problemas en el diseño o implementación de los activos, tales como problemas de fabricación.

- Error humano no deliberado: errores accidentales de las personas que interactúan con la información.

- Error humano deliberado: errores ocasionados intencionalmente por las personas que interactúan con la información, con el objetivo de causar daño.

1.2.1.3.1. Valoración de amenazas

Es la magnitud de la influencia de la amenaza en el valor del activo en dos direcciones: degradación y probabilidad.

- Degradación: indica la pérdida del valor del activo. Comúnmente se indica en una fracción del valor del activo, de manera cualitativa o cuantitativa.

- Probabilidad: nivel de certeza de que una amenaza se materialice.

1.2.1.4. Vulnerabilidad

Es el conjunto de debilidades o defectos que posee un activo o sistema; pueden ser propias o de su entorno. Las vulnerabilidades aumentan la probabilidad de que una amenaza se materialice.

1.2.1.5. Impacto

Es la magnitud del daño ocasionado a un activo, cuando se materializa una amenaza. El valor del impacto se obtiene aplicando el valor de degradación ocasionada por la amenaza al valor del activo en todos sus ejes o dimensiones. A este cálculo primario que no toma en cuenta factores de protección implementados o propuestos se le denomina impacto potencial, debido a que es el mayor valor de impacto.

Se distinguen dos valoraciones para el impacto: el acumulado y el repercutido. El impacto acumulado se estima sobre el valor cumulado del activo, mientras que el impacto repercutido se estima sobre el valor propio del activo.

1.2.1.6. Riesgo

Es la probabilidad de que una amenaza se materialice, tomando en cuenta las vulnerabilidades que se identifiquen. El valor del riesgo se obtiene aplicando el valor de probabilidad de ocurrencia de la amenaza al valor del activo. A este cálculo primario que no toma en cuenta factores de protección implementados o propuestos se le denomina riesgo potencial, debido a que es el mayor valor del riesgo.

Se distinguen dos valoraciones para el riesgo: el acumulado y el repercutido. El riesgo acumulado se estima sobre el valor acumulado del activo, mientras que el riesgo repercutido se estima sobre el valor propio del activo.

1.2.2. Evaluación de riesgos

Es la fase del proceso de gestión de riesgos en la que se interpretan las valoraciones de riesgo e impacto residuales.

1.2.2.1. Definiciones

La evaluación de riesgos muestra los valores de impacto y riesgos, luego de introducir en el sistema las medidas de seguridad que disminuyen o eliminan los riesgos e impactos potenciales.

“Una vez se han valorado las consecuencias o impactos y la probabilidad de los incidentes para los activos del ámbito elegido, se ha de realizar el producto de ambos para calcular los riesgos. Los resultados obtenidos se compararán con los criterios de aceptación de riesgo.” [6]

1.2.2.2. Controles

Lo conforman las acciones o procedimientos para la mitigación o eliminación de los riesgos e impacto. Según su naturaleza se pueden establecer las siguientes clases de control:

[6] Instituto Nacional de Ciberseguridad. *Gestion de riesgos.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf.

- Técnica: medidas de carácter tecnológico dentro del ámbito de la seguridad. Son medidas técnicas los antivirus, cortafuegos o sistemas de copias de seguridad.

- Organizativa: medidas que se centran en la mejora de la seguridad teniendo en cuenta a las personas, por ejemplo: formación en seguridad, identificación de responsables o implantación de procedimientos, gestión de usuarios, entre otros.

- Física: incluye las medidas físicas para proteger la organización; por ejemplo, acondicionar la sala de servidores frente a riesgos de incendio, inundaciones o accesos no autorizados, establecer un sistema de control de acceso para entrar en las oficinas, poner cerraduras en los despachos y armarios o guardar las copias de seguridad en una caja ignífuga.

1.2.2.2.1. Selección de los controles

Es el proceso de elección de las medidas de protección o seguridad. Ante un conjunto inicial de todos los posibles controles, se debe hacer un análisis con el objetivo de seleccionar los controles convenientes; para este proceso se deben tomar en cuenta las siguientes consideraciones:

- Los controles existentes y su efectividad
- El tipo de activo y sus características
- Los ejes o dimensiones de la seguridad que requieren mayor atención
- Las amenazas
- Investigar y analizar controles alternativos

Seleccionado el grupo de controles, es conveniente analizar su aplicabilidad y su justificación para cada uno de estos. La aplicabilidad indica si el control es factible y la justificación, si el control es viable.

1.2.2.2.2. Efecto de los controles

Los controles tienen dos objetivos: reducir la probabilidad de ocurrencia y limitar el daño que puede provocar una amenaza.

1.2.2.2.3. Tipos de protección

Los controles tienen diferentes funciones de protección, cumplen una tarea o acción específica según su naturaleza:

- Prevenir: disminuye la probabilidad de ocurrencia de una amenaza.
- Disuadir: alerta a la fuente del ataque para que desista de intentarlo.
- Eliminar: acción previa que impide la realización de una amenaza.
- Minimizar el impacto: limita las consecuencias.
- Corregir: acción de reparación del daño posterior al incidente.
- Recuperar: capacidad de volver a un estado normal previo.
- Monitorear: estado de revisión permanente para detectar amenazas.
- Administrar: organiza los elementos del sistema para prevenir amenazas.
- Es un proceso de mejora continua para conocer todo aquello que vulnera los activos y al sistema de información.

1.2.2.2.4. Eficacia de los controles

Es un indicador de cumplimiento de la protección del control. Un control ideal será un 100 % eficaz; esto quiere decir que cumple con todos los objetivos

de seguridad para el activo o sistema. La eficacia dependerá del cumplimiento de las expectativas técnicas y operativas. En su factor técnico se analiza si es la correcta para el tipo de amenazas de las que debe proteger y si puede ser empleada en todo momento.

Operativamente, un control tendrá cierto nivel de eficacia cuando esté implementado correctamente, exista un conocimiento de cómo operarlos adecuadamente, se haya instruido o capacitado a los usuarios y si el control mismo es capaz de alertar acerca de sus fallos. El factor de la madurez de la organización respecto de sus capacidades de gestión también influye en la eficacia de los controles.

1.2.2.3. Impacto residual

“Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Entonces se dice que se ha modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.” [7]

Es la estimación del impacto que persiste luego de identificar y aplicar el conjunto de controles.

1.2.2.4. Riesgo residual

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la probabilidad residual, tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

“El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.”[8]

Es la estimación del riesgo que persiste luego de identificar y aplicar el conjunto de controles. Este riesgo es el que la organización asume, puesto que en la mayoría de las ocasiones un riesgo no se puede eliminar, pero su reducción o mitigación hasta ciertos niveles es aceptable.

---

[7] Ministerio de Hacienda y Administraciones Públicas*. MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. libro i - Método*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XIBt1YgzbIV.

[8] Ibíd.

1.2.2.5. Deficiencias o vulnerabilidades

Cuando se compara el conjunto de controles adecuados propuestos con los existentes en el sistema, se puede encontrar que hay ausencias e ineficiencia de los controles actuales. Este análisis contrasta las acciones tomadas con las pendientes relativas a la protección de los activos y el sistema. Esto da origen a un informe que debe ser revisado por la organización, y sirve de base para el tratamiento del impacto y riesgo residuales.

1.2.3. Metodologías

Para el análisis y evaluación de riesgos se pueden tomar como base algunas de las siguientes metodologías para el proceso de gestión de riesgos más utilizadas a nivel mundial:

- CRAMM: método para el análisis de riesgos, desarrollado por la agencia gubernamental británica CCTA (*Central Communication and Telecommunication Agency*). Este método utiliza una herramienta que lleva el mismo nombre. Es ampliamente utilizado por el gobierno del Reino Unido, pero también se utiliza en otros países. Es método el apropiado para grandes industrias y organismos de gobierno.

- ISO/IEC 27001: estándar certificable para la administración de la seguridad de la información basado en un conjunto de controles de seguridad. Puede ser utilizado para cualquier tipo de organización.

- MAGERIT: modelo de implementación de un proceso de gestión de riesgos, desarrollado por el Ministerio de Administraciones Públicas de

España, con un enfoque de administración pública, pero que puede ser utilizado por cualquier organización.

- MEHARI: brinda un conjunto de herramientas y elementos necesarios para la implementación de la ISO/IEC 27005:2008. [9]

- OCTAVE: desarrollado por la Carnegie Mellon University, SEI (*Software Engineering Institute*) de Estados Unidos, *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM* (OCTAVE®), es una metodología para la evaluación de riesgos con un entorno autodirigido y de baja inversión de recursos en cualquier tipo de organización.

1.2.4. Modelos de análisis

Para las valoraciones de los elementos en un proceso de análisis de riesgos es posible utilizar el modelo cualitativo o cuantitativo.

1.2.4.1. Modelo cualitativo

Es un modelo basado en características de un objeto de análisis, que no poseen una magnitud absoluta. Tienen un valor relativo que describe sus calidades y puede ser comparado con otro objeto similar. En el análisis y evaluación de riesgos a los elementos que se van a valorar, se utiliza un modelo cualitativo; se les asigna un atributo que describe la característica de análisis. Los enunciados: nulo, bajo, medio, alto y muy alto, son cualidades para valorar un elemento.

[9] CLUSIF. *MEHARI 2010.* http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf.

1.2.4.2. Modelo cuantitativo

Es un modelo basado en una escala discreta o continua, que le otorga un valor absoluto a las características de un objeto analizado. En el análisis y evaluación de riesgos a los elementos que van a valorarse, se utiliza un modelo cuantitativo, se les asigna un valor numérico a las características analizadas. Por ejemplo, si se hiciera una valoración respecto del costo de un activo, se podría utilizar una escala discreta: Q 1 000, Q 10 000, Q 100 000.

1.3. Gestión de riesgos

Etapa posterior al análisis y evaluación de riesgos en la que la organización toma las decisiones de cómo gestionar o tratar los riesgos, basados en los resultados de los análisis antes mencionados.

Los riesgos son calificados en una escala de criticidad, donde se enfoca mayor interés en lo más grave, y menos en lo asumible o despreciable.

"La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones." [10]

Todas las decisiones tomadas en la fase de gestión de riesgos se enmarcan en las estrategias políticas, objetivos y recursos de la organización.

[10] Ministerio de Hacienda y Administraciones Públicas. *MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I - Método*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XIBt1YgzbIV.

1.3.1. Aceptación del riesgo

Es el nivel de impacto y riesgo residual aceptado por la organización. Los resultados de la evaluación de riesgos son analizados dentro de los contextos de interés para la organización:

- Objetivos empresariales
- Obligaciones legales
- Reglamentos y políticas
- Convenios y contratos
- Seguros y fianzas
- Imagen publica
- Relaciones con los socios de negocio
- Certificaciones y acreditaciones

1.3.2. Tratamiento del riesgo

Proceso cuyo objetivo es modificar los valores de riesgo, basados en su aceptación, a través de medidas como la eliminación de la fuente de riesgo, mitigación, compartición y financiación.

1.3.2.1. Eliminación

Eliminación de la fuente de riesgo es prescindir de aquellos elementos del sistema o activos no esenciales. Comprende el cambio de tecnologías y medios de tratamiento de la información o la reestructuración de la arquitectura del sistema. Esta medida requiere un análisis profundo y detallado por parte de la organización.

1.3.2.2. Mitigación

Uso o implementación de controles para la reducción de la degradación y la probabilidad de ocurrencia. Se evalúa si es necesario agregar controles o modificar los existentes en busca de una mejora en los índices de impacto y riesgo.

1.3.2.3. Compartición

Es trasladar parte o todo el riesgo hacia agentes externos al sistema. Su objetivo es compartir la responsabilidad del riesgo. Es posible realizarlo a través de la tercerización de elementos del sistema como, por ejemplo, contratación de servicios de resguardo, soporte técnico, servicios web entre otros. También es posible contratando seguros sobre los activos de información.

1.3.2.4. Financiación

Es reservar y destinar fondos para responder a las consecuencias ocasionadas por la materialización de un riesgo.

1.3.3. Análisis costo-beneficio

En un concepto general, el análisis costo/beneficio es una herramienta utilizada para la evaluación de proyectos donde se miden los beneficios obtenidos y los costos que supone la realización un proyecto para conocer la viabilidad o rentabilidad de este. Los costos son todos los recursos invertidos para la implementación del proyecto, mientras que los beneficios pueden ser tangibles, cuando representan un ingreso dinerario, o intangibles cuando no se percibe un ingreso dinerario.

En la gestión de riesgos este análisis evalúa la inversión o costo de los controles y el valor del riesgo (el costo de la inseguridad) con los beneficios esperados tras la implementación de los controles. Debido a que los costos y beneficios relativos a la seguridad de la información no siempre pueden ser cuantificables en dinero, existe el análisis cuantitativo, cualitativo y mixto.

- Análisis cuantitativo: es posible cuantificar el riesgo o costo de inseguridad, costo de los controles y los beneficios esperados, ingresos o ahorros.

- Análisis cualitativo: utiliza elementos intangibles no es posible desarrollar cálculos numéricos, dado que toma en cuenta aspectos como imagen, competitividad, asuntos legales, normas, productividad, entre otros.

- Análisis mixto: se puede desarrollar un cálculo de los costos de inseguridad y de los controles, y se compara con beneficios intangibles. Se realiza primero un análisis económico de los costos y luego un análisis cualitativo de los beneficios.

1.4. Plan de seguridad

Son documentos que contienen las actividades que la organización debe realizar para el tratamiento de los riesgos determinados durante el proceso de gestión de riesgos. Su objetivo es poner en marcha las acciones de tratamiento de riesgo. Este informe contiene, como mínimo, los siguientes elementos:

- Controles elegidos a implementar
- Personas responsables de la ejecución
- Estimación de los recursos necesarios
- Estimación de costos

- Cronograma de trabajo

2. MODELO DE VALOR

El modelo de valor es la base para el análisis y gestión de riesgos, determina los elementos del sistema que tienen un valor para la organización y que están expuestos a amenazas. A estos elementos se les denomina activos y son el objetivo de la protección del sistema.

2.1. Descripción del sistema

Información básica y esencial del sistema en estudio, importante entender el contexto de su análisis, elementos y valoraciones.

2.1.1. Información general de la organización

La organización inició sus operaciones en el año 2011 y se dedica a la venta de soluciones de seguridad electrónica incluyendo desarrollo de software a la medida. Su principal mercado son las entidades bancarias y empresas de seguridad. Cuentan con cerca de 35 colaboradores y sus instalaciones están ubicadas en la ciudad capital de Guatemala.

2.1.2. Estructura del sistema

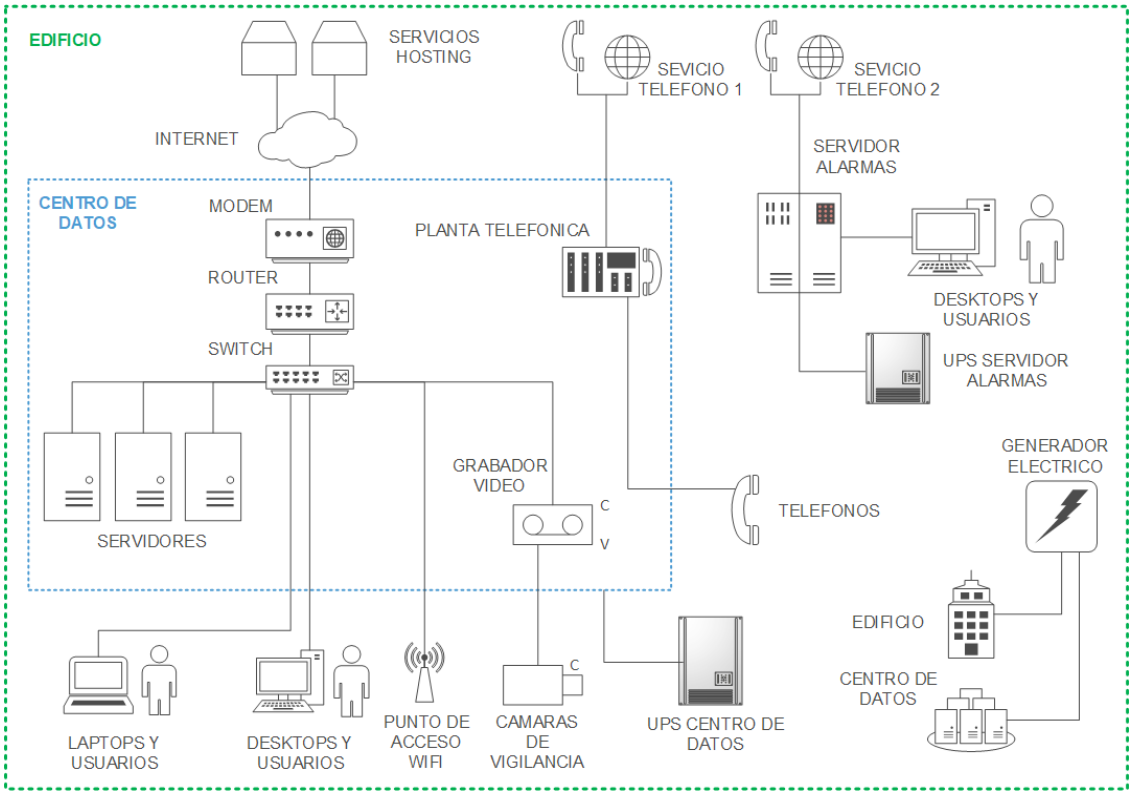
El sistema está conformado por todos los elementos que intervienen en el proceso de la información:

- Generación
- Almacenamiento

- Manejo
- Distribución
- Acceso
- Administración
- Transporte
- Resguardo

La figura muestra el diagrama del sistema, en ella se representa la relación de los elementos.

Figura 2. **Diagrama del sistema**



Fuente: elaboración propia, utilizando Microsoft Visio 2013.

2.2. Caracterización de los activos

Descripción e identificación de los elementos que conforman el sistema de análisis por sus propiedades o atributos. Estos elementos se denominan activos, ya que tienen un valor para la organización, relativo a la importancia de cada uno de ellos en el sistema.

2.2.1. Clasificación

Determinados los elementos que componen al sistema y tomando como base la clasificación para activos del capítulo anterior (datos, servicios, software, hardware, soportes, equipos auxiliares, redes de comunicación, instalaciones y personal), se detallan las subclasificaciones o tipos de los activos identificados.

2.2.1.1. Datos/información

Son objetos abstractos o codificados. Esta codificación puede ser alfanumérica (letras y números) o símbolos que se materializa de forma digital (que puede ser leída por programadas de computadora) o física como los documentos de papel. Para el sistema analizado se determinaron los siguientes tipos de información:

- Ficheros digitales: son contenedores de datos o información que tienen una estructura específica. Estos se encuentran en forma digital (interpretados por computadora).
    - Ficheros de base de datos: archivos digitales que contienen los datos colectados de diversos sistemas y sobre los cuales operan. Es uno de los elementos más importantes pues almacenen la

información de los sistemas utilizados por la organización como por los clientes de esta.

- Ficheros de código fuente: archivos digitales que contienen las instrucciones en leguajes de computadora de los sistemas o aplicaciones desarrollados por la empresa.

- Ficheros de configuración de programas: archivos digitales con las configuraciones o parámetros de funcionamiento de los programas desarrollados.

- Fichero de correo electrónico: archivos digitales con correos, contactos y calendario de los correos electrónicos.

- Ficheros de programas ofimáticos: archivos digitales de documento, hojas de cálculo, presentaciones y diagramas; estos contienen información legal, contable, financiera, comercial, operativa y administrativa.

- Ficheros de sistema: archivos digitales propios de los sistemas operativos y que son utilizados para su funcionamiento. Están presentes en cada equipo de cómputo físico o virtual.

- Ficheros de imágenes: archivos digitales de imágenes, fotografías, dibujos, gráficos, diagramas, planos, entre otros.

- Ficheros de imágenes de discos: archivos digitales que contienen una imagen o copia de un disco CD o DVD, que comúnmente sirven para la instalación de programas adquiridos.

- Ficheros de video: archivos digitales multimedia con fotogramas tales como presentaciones institucionales, presentaciones de proyectos, grabaciones de seguridad, evidencia de trabajos realizados, entre otros.

- Ficheros de texto plano: archivos digitales de texto que pueden contener instrucciones, apuntes, claves o cualquier otra información no clasificada.

- Ficheros físicos: son contenedores de datos o información que tienen una estructura específica. Estos se encuentran en forma física, transcrita o impresa:

  - Documentos en papel: archivos físicos principalmente de índole legal, contable y financiera, comercial, operativa y administrativa.

2.2.1.2. Servicios

Son las prestaciones que brindan los activos de información a la organización. Las prestaciones responden a los objetivos y naturaleza de la información a proveer.

2.2.1.3. Software

Conjunto de programas de computación que permiten a usuarios a través de dispositivos realizar determinadas tareas. En el sistema se encuentra el tipo de software estándar.

- Estándar: es el software que es adquirido por la organización a un proveedor y que funciona bajo licencia. La organización cuenta con varios tipos de software estándar, entre ellos software ofimático, de sistemas operativos, de desarrollo de aplicaciones, software para bases de datos, entre otros.

2.2.1.4. Hardware

Son elementos físicos o dispositivos que constituyen un sistema de información. Por medio de estos dispositivos es posible el manejo de la información (creación, manejo, visualización, entre otros). En el sistema se identificaron los siguientes tipos de hardware:

- Servidor: en una estructura de red se les denomina así a los equipos cuyas características permite atender peticiones de equipos clientes. En el sistema existen servidores para aplicaciones o bases de datos, a los que se conectan tanto clientes internos como externos.

Figura 3. **Servidor**

Fuente: PIXABAY. *Server rack*. https://pixabay.com/es/vectors/equipo-archivo-montado-158930/. Consulta: 21 de octubre de 2020.

- Computadoras de escritorio: son los equipos utilizados por los usuarios para la realización de sus tareas. Estos equipos están dentro de las instalaciones y son accedidos únicamente por personal autorizado de la organización.

Figura 4. **Computadora de escritorio**

Fuente: KLIPARTS*. Torre de computadora negra*. https://www.klipartz.com/es/sticker-png-tryhb. Consulta: 22 de octubre de 2020.

- Computadoras portátiles: dispositivos utilizados por los usuarios para la realización de sus tareas, también llamadas *laptops.* Estos equipos son usados dentro y fuera de las instalaciones por personal de la organización.

Figura 5. **Computadora portátil**

Fuente: PIKIST. *Notebook*. https://www.pikist.com/free-photo-ijdvd. Consulta: 22 de octubre de 2020.

- Equipo de videovigilancia: equipos de seguridad electrónica, conocido también como equipo CCTV. En el sistema existen cámaras y grabadores de video en diversas áreas dentro de las instalaciones y en su perímetro.

Figura 6. **Equipo de videovigilancia**

Fuente: INDIAMART. *CCTV Camera System*. https://www.indiamart.com/proddetail/cctv-camera-system-4-channel-17059297797.html. Consulta: 22 de octubre de 2020.

- Equipo de red de comunicación: equipos que gestionan la trasmisión de datos entre los dispositivos del sistema. El sistema cuenta en su centro de datos donde se ubican los principales equipos de red tanto privada como pública.

Figura 7. **Equipos de red de comunicación**

Fuente: PICKPIK. *Ethernet hub*. https://www.pickpik.com/ethernet-hub-network-connection-pc-web-address-internet-41862. Consulta: 22 de octubre de 2020.

- Telefonía: dispositivos que gestionan la red de teléfonos del sistema. Permiten la comunicación de los usuarios (externos e internos) a través de teléfonos fijos. El sistema cuenta con una planta telefónica o PBX.

Figura 8. **Equipos de red telefónica**

Fuente: FLICKR. *Network closet*. https://www.flickr.com/photos/helixblue/367353370/. Consulta: 22 de octubre de 2020.

2.2.1.5. Soportes

Dispositivos que almacenan información digital. Son utilizados para transportar y resguardar archivos. Los soportes presenten en el sistema se clasifican de la siguiente forma:

- Unidades de disco: son dispositivos que almacenan datos. Son utilizados en otros medios, como las computadoras, para la escritura y lectura de la información. En el sistema hay discos internos, que fueron extraídos de computadoras, y discos externos, que son utilizados para el resguardo y transporte de datos.

Figura 9. **Disco duro interno**

Fuente: PXHERE. *Disco Duro*. https://pxhere.com/es/photo/1136693. Consulta: 22 de octubre de 2020.

- Memorias USB: dispositivos de almacenamiento de datos portátiles y de pequeñas dimensiones, se conectan a los equipos a través de su entrada USB. La organización provee a sus colaboradores con estos dispositivos cuando se requiere, y en ellas se almacena información sin clasificar.

Figura 10. **Memoria USB**

Fuente: PXHERE. *USB*. https://pxhere.com/es/photo/819719. Consulta: 22 de octubre de 2020.

- Discos compactos: dispositivos de almacenamiento de datos. En ella se encuentra almacenada mayormente datos de programas como archivos de instalación de software, sistemas operativos, archivos de configuración, entre otros.

Figura 11. **Disco compacto**

Fuente: PXHERE. *Disco compacto*. https://pxhere.com/es/photo/1588951. Consulta: 22 de octubre de 2020.

2.2.1.6. Equipo auxiliar

Son los equipos que no forman parte de los elementos que contienen o prestan un servicio de información, pero sirven a esos elementos para su funcionamiento. Se identificaron los siguientes equipos auxiliaren en el sistema:

- Sistema de alimentación ininterrumpida: equipo que almacena energía y puede suministrarla por un periodo a los dispositivos que estén conectados a él. Son conocidos como UPS y además de dar energía protegen a los equipos de alteraciones en el voltaje. En el sistema se identificaron

equipos para los servidores y para los equipos menores como computadoras de escritorio, portátiles y DVR, entre otros.

Figura 12. **Equipos de alimentación ininterrumpida o UPS**

Fuente: TRIPPLITE. *Battery backup*. https://www.tripplite.com/products/ups-buying-guide. Consulta: 22 de octubre de 2020.

- Generador eléctrico: equipo que transforma energía mecánica en energía eléctrica. También conocida como planta eléctrica, esta es accionada durante los cortes de energía de la red eléctrica pública o privada, y funciona a base de combustibles. En las instalaciones del sistema evaluado se encuentra un generador eléctrico que es accionado manualmente cuando es requerido.

Figura 13. **Generador eléctrico a gasolina**

Fuente: PIXABAY. *Generator*. https://pixabay.com/es/photos/generator-alternator-equipment-5476642/. Consulta: 22 de octubre de 2020.

- Equipo de climatización: son equipos que mantienen espacios o ambientes a una determinada temperatura. Comúnmente llamados aires acondicionados, su uso en el sistema está en el centro de datos, donde ayudan a mantener una temperatura adecuada en el ambiente para que los equipos funcionen en condiciones adecuadas.

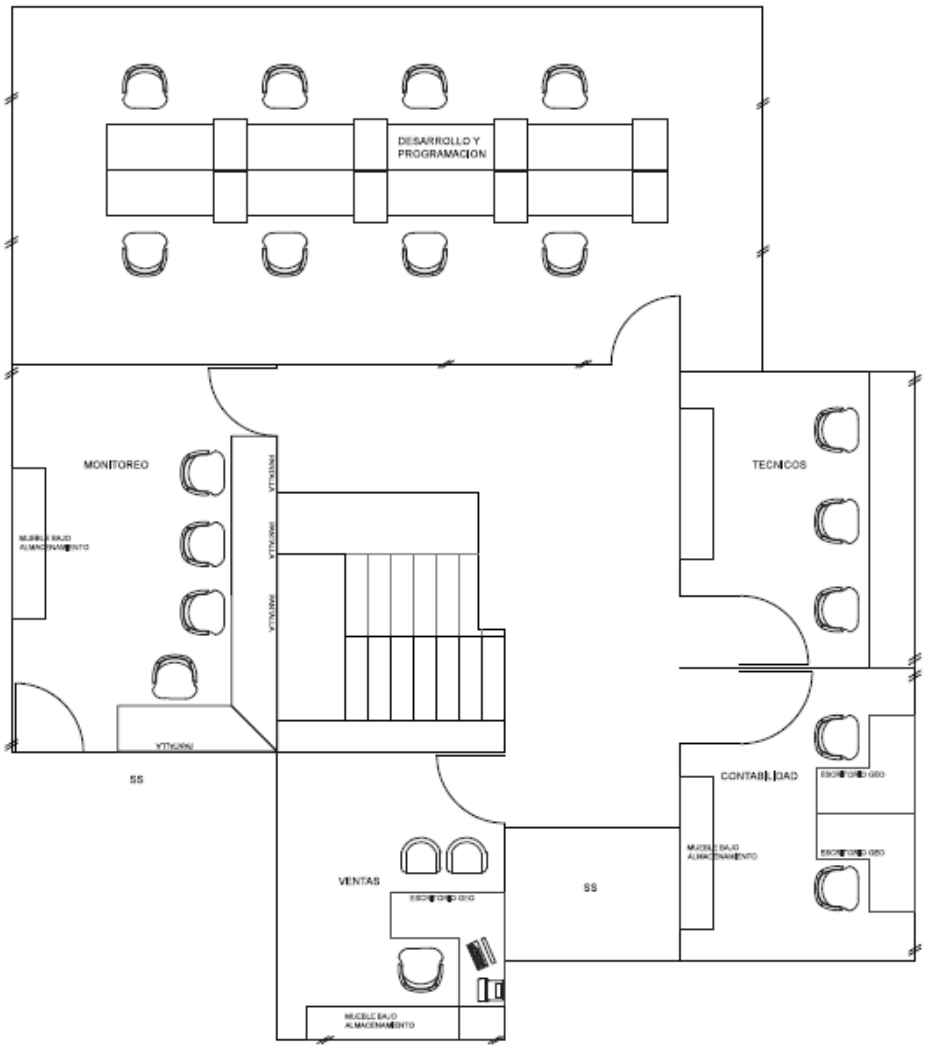
Figura 14. **Equipo de aire acondicionado**

Fuente: PIXABAY. *Acondicionador de aire*. https://pixabay.com/es/illustrations/acondicionador-de-aire-ac-fresco-4204637/. Consulta: 22 de octubre de 2020.

2.2.1.7. Instalaciones

Son las ubicaciones físicas donde se encuentra los elementos del sistema a evaluar. En el análisis se identifican dos tipos de instalaciones: el edificio y el centro de procesamiento de datos.

Figura 15. **Plano de las instalaciones**



Fuente: ROBLES, Rocío. *Planta alta distribución*. p 1.

- Edificio: se estudia un solo edificio, debido a que este concentra todos los elementos del sistema de información a analizar. Son sus oficinas centrales y es un edificio con las siguientes características: construcción de concreto, acabados, de dos niveles, y sus ambientes divididos por departamentos, según la naturaleza del trabajo realizado.

- Centro de procesamiento de datos: área dentro del edificio acondicionado específicamente para alojar los equipos de información y telecomunicaciones. Denominado también como Data Center, en él se encuentran servidores, equipos de red y comunicaciones.

- Oficinas: son divisiones o áreas delimitadas dentro del edificio según sus funciones. También se les denomina departamentos, y estos agrupan a los empleados y sus estaciones de trabajo, según el área de la organización a la que pertenecen.

2.2.1.8. Servicios subcontratados

Es el conjunto de recursos externos contratados por la organización.

- Telefonía: es el servicio de línea telefónica de la empresa.

- Internet: servicio de conexión a internet.

- *Hosting*: son espacios de servidor que se alquilan para alojar una aplicación o un sitio web. La empresa cuenta con dos servicios *hosting*.

2.2.1.9. Personal

Son las personas que interactúan con los medios de información y con la información o servicios que estos contienen. Se clasifican dos tipos de personas que actúan en el sistema de información: usuarios internos y usuarios externos.

- Usuario interno: son las personas que trabajan directamente para la organización y tienen contacto o acceso a alguno de los elementos del sistema. En el análisis se hace una clasificación de estos usuarios, por su área o departamento al que pertenecen.

- Usuario externo: son personas o entidades que no trabajan para la organización, pero tienen acceso a algún elemento del sistema de información. Pueden ser clientes, proveedores, auditores, entidades fiscales, entidades bancarias, entre otros.

2.2.2. Identificación

Se identifican los activos del sistema, asignándoles un código y un nombre, que en algunos casos contendrá una descripción genérica por privacidad de la empresa.

Para la asignación de los códigos se utilizó la siguiente nomenclatura:

- El prefijo del código está compuesto por letras que representan las iniciales del tipo de activo. Luego del prefijo se asigna una numeración correlativa dependiendo del tipo de activo.

La siguiente tabla muestra la identificación de todos los activos del sistema:

Tabla I. **Identificación de activos**

Tipo	**Clasificación**	**Código**	**Nombre**
Información	Fichero digital	INF-1	Operativa interna
Información	Fichero digital	INF-2	Operativa externa 1
Información	Fichero digital	INF-3	Financiera
Información	Fichero digital	INF-4	Comercial
Información	Fichero digital	INF-5	Códigos fuente y tecnologías
Información	Fichero digital	INF-6	Administrativa
Información	Fichero digital	INF-7	Recursos humanos y salarios
Información	Fichero digital	INF-8	Directiva/estratégica
Información	Fichero digital	INF-9	Operativa externa 2
Información	Fichero físico	INF-10	Documentos legales
Información	Fichero físico	INF-11	Documentos varios
Servicio	Servicio interno	SEI-1	Servicios ERP
Servicio	Servicio interno	SEI-2	Conexión a red interna y externa
Servicio	Servicio interno	SEI-3	Servicios 2 clientes externos
Servicio	Servicio interno	SEI-4	Servicios de comunicación interna y externa
Servicio	Servicio interno	SEI-5	Desarrollo de software
Servicio	Servicio interno	SEI-6	Gestión de operaciones
Servicio	Servicio interno	SEI-7	Servicios administrativos
Servicio	Servicio interno	SEI-8	Administración de personal
Servicio	Servicio interno	SEI-9	Servicios gerenciales
Servicio	Servicio interno	SEI-10	Servicios comerciales
Servicio	Servicio interno	SEI-11	Servicios de vigilancia interna
Servicio	Servicio interno	SEI-12	Servicios 1 clientes externos
Software	Estándar	SW-1	Sistema operativo
Software	Estándar	SW-2	Software ofimático
Software	Estándar	SW-3	Software de videovigilancia
Software	Estándar	SW-4	Software ERP
Software	Estándar	SW-5	Software base de datos
Software	Estándar	SW-6	Software de alarmas
Software	Estándar	SW-7	Software de contabilidad
Software	Estándar	SW-8	Software de desarrollo

Continuación de la tabla I.

Hardware	Servidor	HW-1	Servidor ERP
Hardware	Servidor	HW-2	Servidor contabilidad
Hardware	Servidor	HW-3	Servidor videovigilancia
Hardware	Servidor	HW-4	Servidor de alarmas
Hardware	Computadora de escritorio	HW-5	Desktop 1 operaciones
Hardware	Computadora de escritorio	HW-6	Desktop 2 operaciones
Hardware	Computadora de escritorio	HW-7	Desktop 1 desarrollo
Hardware	Computadora de escritorio	HW-8	Desktop 2 desarrollo
Hardware	Computadora de escritorio	HW-9	Desktop 3 desarrollo
Hardware	Computadora de escritorio	HW-10	Desktop 4 desarrollo
Hardware	Computadora de escritorio	HW-11	Desktop 1 monitoreo
Hardware	Computadora de escritorio	HW-12	Desktop 2 monitoreo
Hardware	Computadora de escritorio	HW-13	Desktop 3 monitoreo
Hardware	Computadora portátil	HW-14	Laptop 1 contabilidad
Hardware	Computadora portátil	HW-15	Laptop 1 administración
Hardware	Computadora portátil	HW-16	Laptop 2 administración
Hardware	Computadora portátil	HW-17	Laptop 1 operaciones
Hardware	Computadora portátil	HW-18	Laptop 2 operaciones
Hardware	Computadora portátil	HW-19	Laptop 1 desarrollo
Hardware	Computadora portátil	HW-20	Laptop 2 desarrollo
Hardware	Computadora portátil	HW-21	Laptop 3 desarrollo
Hardware	Computadora portátil	HW-22	Laptop 4 desarrollo
Hardware	Computadora portátil	HW-23	Laptop 5 desarrollo
Hardware	Computadora portátil	HW-24	Laptop 1 comercial
Hardware	Computadora portátil	HW-25	Laptop 1 gerencia
Hardware	Equipo de videovigilancia	HW-26	Grabador de video digital
Hardware	Equipo de videovigilancia	HW-27	Cámaras de videovigilancia
Hardware	Equipos de red de comunicación	HW-28	*Router*
Hardware	Equipos de red de comunicación	HW-29	*Switch*
Hardware	Equipos de red de comunicación	HW-30	Módem

Continuación de la tabla I.

Hardware	Equipos de red de comunicación	HW-31	Punto de acceso inalámbrico
Hardware	Telefonía	HW-32	Planta telefónica
Hardware	Telefonía	HW-33	Teléfonos fijos
Soportes	Unidad de disco	SOP-1	Discos duros internos
Soportes	Unidad de disco	SOP-2	Discos duros externos
Soportes	Memorias USB	SOP-3	Memorias USB
Soportes	Discos compactos	SOP-4	Discos compactos
Equipo auxiliar	Sistema de alimentación ininterrumpida	AUX-1	Ups data center
Equipo auxiliar	Generador eléctrico	AUX-2	Planta eléctrica
Equipo auxiliar	Equipo de climatización	AUX-3	Aire acondicionado
Equipo auxiliar	Sistema de alimentación ininterrumpida	AUX-4	Ups servidor alarmas
Instalaciones	Edificio	INS-1	Oficinas centrales
Instalaciones	Centro de procesamiento de datos	INS-2	Data center
Instalaciones	Oficina	INS-3	Oficina monitoreo
Instalaciones	Oficina	INS-4	Oficina informática
Instalaciones	Oficina	INS-5	Oficina administración
Instalaciones	Oficina	INS-6	Oficina contabilidad
Instalaciones	Oficina	INS-7	Oficina gerencia
Instalaciones	Oficina	INS-8	Oficina comercial
Instalaciones	Oficina	INS-9	Oficina operaciones
Servicio subcontratado	Telefonía	SES-1	Servicio telefónico 1
Servicio subcontratado	Telefonía	SES-2	Servicio telefónico 2
Servicio subcontratado	Internet	SES-3	Internet
Servicio subcontratado	*Hosting*	SES-4	Página web empresarial

Continuación de la tabla I.

Servicio subcontratado	*Hosting*	SES-5	Correo electrónico
Servicio subcontratado	Computación en la nube	SES-6	Planificación de desarrollo
Personal	Usuarios externos	PER-1	Usuarios externos
Personal	Usuario interno	PER-2	Usuario monitoreo 1
Personal	Usuario interno	PER-3	Usuario monitoreo 2
Personal	Usuario interno	PER-4	Usuario monitoreo 3
Personal	Usuario interno	PER-5	Usuario contabilidad 1
Personal	Usuario interno	PER-6	Usuario administración 1
Personal	Usuario interno	PER-7	Usuario administración 2
Personal	Usuario interno	PER-8	Usuario operaciones 1
Personal	Usuario interno	PER-9	Usuario operaciones 2
Personal	Usuario interno	PER-10	Usuario operaciones 3
Personal	Usuario interno	PER-11	Usuario operaciones 4
Personal	Usuario interno	PER-12	Usuario desarrollo 1
Personal	Usuario interno	PER-13	Usuario desarrollo 2
Personal	Usuario interno	PER-14	Usuario desarrollo 3
Personal	Usuario interno	PER-15	Usuario desarrollo 4
Personal	Usuario interno	PER-16	Usuario desarrollo 5
Personal	Usuario interno	PER-17	Usuario comercial 1
Personal	Usuario interno	PER-18	Usuario gerencia 1

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

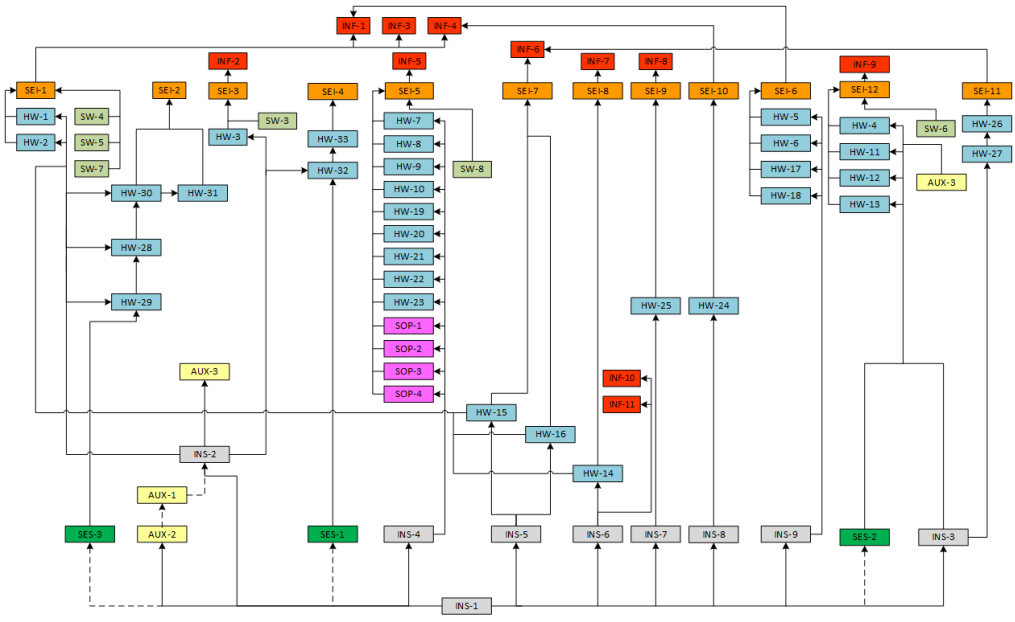
2.2.3. Dependencias

Es la relación de seguridad entre los activos. No es la dependencia funcional dentro del sistema, sino sobre si la seguridad de un activo está vinculada a la seguridad de otro activo. Para su análisis se determinan las rutas de desencadenamiento y los efectos repercutidos de un activo sobre otro, cuando se materializa una amenaza.

La herramienta para su análisis e interpretación se le denomina árbol de ataque, es una gráfica donde se colocan todos los activos del sistema unidos con líneas que representan la relación de seguridad. En los segmentos inferiores se encuentran las instalaciones (el primer nivel de seguridad al que se debe acceder para intentar cometer una amenaza), luego los medios de acceso (hardware, software, equipos de comunicación y auxiliares) y en la parte superior los servicios internos y la información, que son los elementos primordiales que deben protegerse.

La siguiente gráfica muestra el análisis de dependencia de los activos del sistema; estos se identifican con su código y cada clasificación de activo con un color; las flechas indican hacia dónde podría propagarse los efectos de una amenaza:

Figura 16. **Diagrama de dependencias**



Fuente: elaboración propia, utilizando Microsoft Visio 2013.

2.2.4. Valoración

Cada activo tiene un valor propio y acumulado (según sus otros activos dependientes). Un activo puede no ser tan valioso por sí solo, sino por los sus activos dependientes.

2.2.4.1. Valor propio

Esta valoración es intrínseca de cada activo, determinado en conjunto con los encargados de las áreas. Para la valoración se tomaron en cuenta las tres dimensiones de la seguridad de la información: integridad, confidencialidad y disponibilidad; se utilizó la siguiente escala para cada dimensión:

Tabla II. **Escala de valoración de activos**

Valor	Simbología	Interpretación
9 - 10	MA	Muy alto
7 - 8	A	Alto
5 – 6	M	Medio
3 – 4	B	Bajo
1 - 2	MB	Muy bajo

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla III. **Simbología dimensiones seguridad**

Simbología	Descripción
I	Integridad
C	Confidencialidad
D	Disponibilidad

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla IV. **Valoración de los activos**

Código	Nombre	I	Valor I	C	Valor C	D	Valor D
INF-1	Operativa interna	8	A	9	MA	7	A
INF-2	Operativa externa 1	10	MA	10	MA	10	MA
INF-3	Financiera	10	MA	10	MA	10	MA
INF-4	Comercial	9	MA	9	MA	6	M
INF-5	Códigos fuente y tecnologías	8	A	9	MA	5	M
INF-6	Administrativa	7	A	8	A	5	M
INF-7	Recursos humanos y salarios	8	A	8	A	6	M
INF-8	Directiva/estratégica	8	A	10	MA	7	A
INF-9	Operativa externa 2	10	MA	10	MA	10	MA
INF-10	Documentos legales	10	MA	10	MA	10	MA
INF-11	Documentos varios	10	MA	8	A	6	M
SEI-1	Servicios ERP	10	MA	10	MA	10	MA
SEI-2	Conexión a red interna y externa	10	MA	8	A	10	MA
SEI-3	Servicios 2 clientes externos	10	MA	10	MA	10	MA
SEI-4	Servicios de comunicación interna y externa	8	A	9	MA	8	A
SEI-5	Desarrollo de software	8	A	8	A	7	A
SEI-6	Gestión de operaciones	6	M	7	A	7	A
SEI-7	Servicios administrativos	6	M	8	A	6	M
SEI-8	Administración de personal	8	A	9	MA	6	M
SEI-9	Servicios gerenciales	9	MA	10	MA	8	A
SEI-10	Servicios comerciales	6	M	7	A	6	M
SEI-11	Servicios de vigilancia interna	9	MA	9	MA	9	MA
SEI-12	Servicios 1 clientes externos	10	MA	10	MA	10	MA
SW-1	Sistema operativo	6	M	2	MB	7	A
SW-2	Software ofimático	5	M	2	MB	6	M
SW-3	Software de videovigilancia	10	MA	9	MA	10	MA
SW-4	Software ERP	8	A	6	M	8	A
SW-5	Software base de datos	10	MA	6	M	10	MA

Continuación de tabla IV.

SW-6	Software de alarmas	10	MA	6	M	10	MA
SW-7	Software de contabilidad	10	MA	5	M	9	MA
SW-8	Software de desarrollo	7	A	4	B	7	A
HW-1	Servidor ERP	10	MA	10	MA	10	MA
HW-2	Servidor contabilidad	7	A	8	A	6	M
HW-3	Servidor videovigilancia	10	MA	10	MA	10	MA
HW-4	Servidor de alarmas	10	MA	10	MA	10	MA
HW-5	Desktop 1 operaciones	7	A	7	A	7	A
HW-6	Desktop 2 operaciones	7	A	7	A	7	A
HW-7	Desktop 1 desarrollo	8	A	8	A	8	A
HW-8	Desktop 2 desarrollo	8	A	8	A	8	A
HW-9	Desktop 3 desarrollo	8	A	8	A	8	A
HW-10	Desktop 4 desarrollo	8	A	8	A	8	A
HW-11	Desktop 1 monitoreo	7	A	9	MA	8	A
HW-12	Desktop 2 monitoreo	7	A	9	MA	8	A
HW-13	Desktop 3 monitoreo	7	A	9	MA	8	A
HW-14	Laptop 1 contabilidad	8	A	9	MA	8	A
HW-15	Laptop 1 administración	6	M	6	M	7	A
HW-16	Laptop 2 administración	6	M	6	M	7	A
HW-17	Laptop 1 operaciones	6	M	6	M	5	M
HW-18	Laptop 2 operaciones	6	M	6	M	5	M
HW-19	Laptop 1 desarrollo	7	A	8	A	6	M
HW-20	Laptop 2 desarrollo	7	A	8	A	6	M
HW-21	Laptop 3 desarrollo	7	A	8	A	6	M
HW-22	Laptop 4 desarrollo	7	A	8	A	6	M
HW-23	Laptop 5 desarrollo	7	A	8	A	6	M
HW-24	Laptop 1 comercial	7	A	8	A	7	A
HW-25	Laptop 1 gerencia	7	A	8	A	7	A
HW-26	Grabador de video digital	9	MA	7	A	8	A
HW-27	Cámaras de videovigilancia	8	A	7	A	7	A
HW-28	Router	7	A	8	A	9	MA
HW-29	Switch	5	M	6	M	9	MA
HW-30	Módem	7	A	5	M	9	MA
HW-31	Punto de acceso inalámbrico	6	M	7	A	8	A

Continuación de la tabla IV.

HW-32	Planta telefónica	4	B	8	A	6	M
HW-33	Teléfonos fijos	2	MB	5	M	5	M
SOP-1	Discos duros internos	8	A	9	MA	5	M
SOP-2	Discos duros externos	8	A	9	MA	7	A
SOP-3	Memorias USB	8	A	9	MA	2	MB
SOP-4	Discos compactos	6	M	6	M	2	MB
AUX-1	Ups data center	6	M	1	MB	9	MA
AUX-2	Planta eléctrica	5	M	1	MB	7	A
AUX-3	Aire acondicionado	6	M	1	MB	9	MA
AUX-4	Ups servidor alarmas	6	M	1	MB	8	A
INS-1	Oficinas centrales	9	MA	7	A	9	MA
INS-2	Data center	8	A	8	A	10	MA
INS-3	Oficina monitoreo	6	M	8	A	9	MA
INS-4	Oficina informática	7	A	9	MA	7	A
INS-5	Oficina administración	6	M	5	M	5	M
INS-6	Oficina contabilidad	8	A	8	A	7	A
INS-7	Oficina gerencia	8	A	9	MA	7	A
INS-8	Oficina comercial	5	M	3	B	5	M
INS-9	Oficina operaciones	5	M	3	B	4	B
SES-1	Servicio telefónico 1	8	A	7	A	5	M
SES-2	Servicio telefónico 2	8	A	7	A	9	MA
SES-3	Internet	9	MA	9	MA	9	MA
SES-4	Página web empresarial	7	A	2	MB	3	B
SES-5	Correo electrónico	6	M	7	A	9	MA
SES-6	Planificación de desarrollo	6	M	5	M	7	A
PER-1	Usuarios externos	5	M	3	B	2	MB
PER-2	Usuario monitoreo 1	7	A	7	A	8	A
PER-3	Usuario monitoreo 2	7	A	7	A	8	A
PER-4	Usuario monitoreo 3	7	A	7	A	8	A
PER-5	Usuario contabilidad 1	9	MA	9	MA	8	A
PER-6	Usuario administración 1	8	A	8	A	7	A
PER-7	Usuario administración 2	8	A	8	A	7	A
PER-8	Usuario operaciones 1	4	B	5	M	7	A
PER-9	Usuario operaciones 2	4	B	5	M	7	A

Continuación de la tabla IV.

PER-10	Usuario operaciones 3	4	B	5	M	7	A
PER-11	Usuario operaciones 4	4	B	5	M	7	A
PER-12	Usuario desarrollo 1	5	M	6	M	6	M
PER-13	Usuario desarrollo 2	5	M	6	M	6	M
PER-14	Usuario desarrollo 3	5	M	6	M	6	M
PER-15	Usuario desarrollo 4	5	M	6	M	6	M
PER-16	Usuario desarrollo 5	5	M	6	M	6	M
PER-17	Usuario comercial 1	4	B	5	M	6	M
PER-18	Usuario gerencia 1	9	MA	9	MA	8	A

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

2.2.4.2. Valor acumulado

El valor acumulado es el valor máximo soportado por un activo. Si es mayor a su valor propio, esta toma el valor de su activo dependiente de mayor valor, de lo contrario conserva su valor propio. Se toman como referencias las tablas II y III utilizadas para el cálculo del valor propio de los activos.

Tabla V. **Valor acumulado**

Código	Nombre	I	Valor I	C	Valor C	D	Valor D
INF-1	Operativa interna	8	A	9	MA	7	A
INF-2	Operativa externa 1	10	MA	10	MA	10	MA
INF-3	Financiera	10	MA	10	MA	10	MA
INF-4	Comercial	9	MA	9	MA	6	M
INF-5	Códigos fuente y tecnologías	8	A	9	MA	5	M
INF-6	Administrativa	7	A	8	A	5	M
INF-7	Recursos humanos y salarios	8	A	8	A	6	M
INF-8	Directiva/estratégica	8	A	10	MA	7	A

Continuación de la tabla V.

INF-9	Operativa externa 2	10	MA	10	MA	10	MA
INF-10	Documentos legales	10	MA	10	MA	10	MA
INF-11	Documentos varios	10	MA	8	A	6	M
SEI-1	Servicios ERP	10	MA	10	MA	10	MA
SEI-2	Conexión a red interna y externa	10	MA	8	A	10	MA
SEI-3	Servicios 2 clientes externos	10	MA	10	MA	10	MA
SEI-4	Servicios de comunicación interna y externa	8	A	9	MA	8	A
SEI-5	Desarrollo de software	8	A	9	MA	7	A
SEI-6	Gestión de operaciones	8	A	9	MA	7	A
SEI-7	Servicios administrativos	7	A	8	A	6	M
SEI-8	Administración de personal	8	A	9	MA	6	M
SEI-9	Servicios gerenciales	9	MA	10	MA	8	A
SEI-10	Servicios comerciales	9	MA	9	MA	6	M
SEI-11	Servicios de vigilancia interna	9	MA	9	MA	9	MA
SEI-12	Servicios 1 clientes externos	10	MA	10	MA	10	MA
SW-1	Sistema operativo	6	M	2	MB	7	A
SW-2	Software ofimático	5	M	2	MB	6	M
SW-3	Software de videovigilancia	10	MA	10	MA	10	MA
SW-4	Software ERP	10	MA	10	MA	10	MA
SW-5	Software base de datos	10	MA	10	MA	10	MA
SW-6	Software de alarmas	10	MA	10	MA	10	MA
SW-7	Software de contabilidad	10	MA	10	MA	10	MA
SW-8	Software de desarrollo	8	A	9	MA	7	A
HW-1	Servidor ERP	10	MA	10	MA	10	MA
HW-2	Servidor contabilidad	10	MA	10	MA	10	MA
HW-3	Servidor videovigilancia	10	MA	10	MA	10	MA
HW-4	Servidor de alarmas	10	MA	10	MA	10	MA
HW-5	Desktop 1 operaciones	8	A	9	MA	7	A
HW-6	Desktop 2 operaciones	8	A	9	MA	7	A
HW-7	Desktop 1 desarrollo	8	A	9	MA	8	A
HW-8	Desktop 2 desarrollo	8	A	9	MA	8	A
HW-9	Desktop 3 desarrollo	8	A	9	MA	8	A

Continuación de tabla V.

HW-10	Desktop 4 desarrollo	8	A	9	MA	8	A
HW-11	Desktop 1 monitoreo	10	MA	10	MA	10	MA
HW-12	Desktop 2 monitoreo	10	MA	10	MA	10	MA
HW-13	Desktop 3 monitoreo	10	MA	10	MA	10	MA
HW-14	Laptop 1 contabilidad	10	MA	10	MA	10	MA
HW-15	Laptop 1 administración	7	A	8	A	7	A
HW-16	Laptop 2 administración	7	A	8	A	7	A
HW-17	Laptop 1 operaciones	8	A	9	MA	7	A
HW-18	Laptop 2 operaciones	8	A	9	MA	7	A
HW-19	Laptop 1 desarrollo	8	A	9	MA	7	A
HW-20	Laptop 2 desarrollo	8	A	9	MA	7	A
HW-21	Laptop 3 desarrollo	8	A	9	MA	7	A
HW-22	Laptop 4 desarrollo	8	A	9	MA	7	A
HW-23	Laptop 5 desarrollo	8	A	9	MA	7	A
HW-24	Laptop 1 comercial	9	MA	9	MA	7	A
HW-25	Laptop 1 gerencia	9	MA	10	MA	8	A
HW-26	Grabador de video digital	9	MA	9	MA	9	MA
HW-27	Cámaras de videovigilancia	9	MA	9	MA	9	MA
HW-28	*Router*	10	MA	8	A	10	MA
HW-29	*Switch*	10	MA	8	A	10	MA
HW-30	Módem	10	MA	8	A	10	MA
HW-31	Punto de acceso inalámbrico	10	MA	8	A	10	MA
HW-32	Planta telefónica	8	A	9	MA	8	A
HW-33	Teléfonos fijos	8	A	9	MA	8	A
SOP-1	Discos duros internos	8	A	9	MA	7	A
SOP-2	Discos duros externos	8	A	9	MA	7	A
SOP-3	Memorias USB	8	A	9	MA	7	A
SOP-4	Discos compactos	8	A	9	MA	7	A
AUX-1	Ups data center	6	M	1	MB	9	MA
AUX-2	Planta eléctrica	5	M	1	MB	7	A
AUX-3	Aire acondicionado	6	M	1	MB	9	MA
AUX-4	Ups servidor alarmas	6	M	1	MB	8	A
INS-1	Oficinas centrales	10	MA	10	MA	10	MA
INS-2	Data center	10	MA	10	MA	10	MA

Continuación de la tabla V.

INS-3	Oficina monitoreo	9	MA	9	MA	9	MA
INS-4	Oficina informática	8	A	9	MA	7	A
INS-5	Oficina administración	7	A	8	A	6	M
INS-6	Oficina contabilidad	10	MA	10	MA	10	MA
INS-7	Oficina gerencia	9	MA	10	MA	8	A
INS-8	Oficina comercial	9	MA	9	MA	6	M
INS-9	Oficina operaciones	8	A	9	MA	7	A
SES-1	Servicio telefónico 1	8	A	9	MA	8	A
SES-2	Servicio telefónico 2	10	MA	10	MA	10	MA
SES-3	Internet	10	MA	9	MA	10	MA
SES-4	Página web empresarial	7	A	2	MB	3	B
SES-5	Correo electrónico	6	M	7	A	9	MA
SES-6	Planificación de desarrollo	6	M	5	M	7	A
PER-1	Usuarios externos	5	M	3	B	2	MB
PER-2	Usuario monitoreo 1	10	MA	10	MA	10	MA
PER-3	Usuario monitoreo 2	10	MA	10	MA	10	MA
PER-4	Usuario monitoreo 3	10	MA	10	MA	10	MA
PER-5	Usuario contabilidad 1	10	MA	10	MA	10	MA
PER-6	Usuario administración 1	8	A	8	A	7	A
PER-7	Usuario administración 2	8	A	8	A	7	A
PER-8	Usuario operaciones 1	8	A	9	MA	7	A
PER-9	Usuario operaciones 2	8	A	9	MA	7	A
PER-10	Usuario operaciones 3	8	A	9	MA	7	A
PER-11	Usuario operaciones 4	8	A	9	MA	7	A
PER-12	Usuario desarrollo 1	8	A	9	MA	7	A
PER-13	Usuario desarrollo 2	8	A	9	MA	7	A
PER-14	Usuario desarrollo 3	8	A	9	MA	7	A
PER-15	Usuario desarrollo 4	8	A	9	MA	7	A
PER-16	Usuario desarrollo 5	8	A	9	MA	7	A
PER-17	Usuario comercial 1	9	MA	9	MA	6	M
PER-18	Usuario gerencia 1	9	MA	10	MA	8	A

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

2.3. Caracterización de la amenaza

Luego de la identificación, determinación de las dependencias y la valoración de los activos, se procede a determinar las amenazas a las que está expuesto el sistema.

2.3.1. Clasificación de las amenazas

La clasificación agrupa las amenazas según su naturaleza u origen. La siguiente clasificación es tomada del catálogo de amenazas del capítulo 5 del libro 2 “Catálogo de elementos” de la metodología MAGERIT versión 3.0.

- De origen natural: son los eventos o fenómenos naturales que pueden ocurrir y que afectan al sistema tales como incendios, terremotos, huracanes, entre otros.

- De origen industrial: son los originados por el entorno, condiciones de las instalaciones y las actividades de la empresa como fallos eléctricos, vibración, residuos, entre otros.

- Errores y fallos no intencionados: provocados por la intervención de las personas en los elementos del sistema, por ejemplo, desinformación, mala capacitación, desconocimiento entre otros.

- Ataques intencionados: provocados de forma deliberada por parte de las personas con el propósito de hacer daño tales como destrucción de información, daño a equipos, robos de datos o dispositivos, entro otros.

2.3.2. Identificación

Tomando como base el catálogo de amenazas del capítulo 5, del libro 2, “Catálogo de elementos” de la metodología MAGERIT versión 3.0, se determinan cuáles amenazas pueden afectar a los activos identificados, y en qué dimensión de seguridad es afectada (disponibilidad, integridad, confidencialidad).

2.3.2.1. De origen natural

Las amenazas de origen natural detectadas son las siguientes:

- Fuego
    - Descripción: incendio natural o accidental, por ejemplo, un incendio forestal.
    - Tipos de activos afectados: hardware, soportes, equipos auxiliares e instalaciones.
    - Dimensiones que afecta: disponibilidad.
- Daños por agua
    - Descripción: inundaciones, filtraciones, humedad por fenómenos meteorológicos como tormentas, huracanes y lluvias.
    - Tipos de activos afectados: hardware, soportes, equipos auxiliares e instalaciones.
    - Dimensiones que afecta: disponibilidad.

- Desastres naturales

    - Descripción: terremotos, erupciones volcánicas, fenómenos climáticos, hundimientos, corrimientos de tierras, derrumbes, entre otros, derivados de acontecimientos de la naturaleza.
    - Tipos de activos afectados: hardware, soportes, equipos auxiliares e instalaciones.
    - Dimensiones que afecta: disponibilidad.

2.3.2.2. De origen industrial

Las amenazas de origen industrial detectadas son las siguientes:

- Fuego

    - Descripción: incendios provocados accidentalmente como cortocircuitos o mal manejo de equipos eléctricos o inflamables; o deliberados, por personas con intención de provocar daños.
    - Tipos de activos afectados: hardware, soportes, equipos auxiliares e instalaciones.
    - Dimensiones que afecta: disponibilidad.

- Daños por agua

    - Descripción: inundaciones o cualquier daño ocasionado por problemas en los sistemas de trasporte, distribución, y almacenamiento de agua como fugas, rotura de tubería, desbordamiento de tanques, entre otros.

- Tipos de activos afectados: hardware, soportes, equipos auxiliares e instalaciones.
- Dimensiones que afecta: disponibilidad.

- Desastres industriales

  - Descripción: provocados por las actividades y entorno tales como cortocircuitos, sobrecargas y fluctuaciones irregulares de electricidad, explosiones.
  - Tipos de activos afectados: hardware, soportes, equipos auxiliares e instalaciones.
  - Dimensiones afectadas: disponibilidad.

- Contaminación mecánica

  - Descripción: presencia de acumulación de polvo, suciedad o cualquier otro material presente en el ambiente; vibraciones.
  - Tipos de activos afectados: hardware, soportes y equipos auxiliares.
  - Dimensiones afectadas: disponibilidad.

- Avería de origen físico o lógico

  - Descripción: problemas de hardware o software de equipos, ya sea por defecto de origen, por funcionamiento o degradación.
  - Tipos de activos afectados: software, hardware, soportes, equipos auxiliares.
  - Dimensiones afectadas: disponibilidad.

- Corte del suministro eléctrico

    - Descripción: problemas de la energía pública o de los sistemas de alimentación auxiliares (generador eléctrico, UPS).
    - Tipos de activos afectados: hardware, equipos auxiliares.
    - Dimensiones afectadas: disponibilidad.

- Condiciones inadecuadas de temperatura o humedad

    - Descripción: temperaturas altas o bajas para la operación adecuada de equipos. Presencia de humedad debida condiciones en el ambiente de las áreas.
    - Tipos de activos afectados: hardware, soportes, equipos auxiliares.
    - Dimensiones afectadas: disponibilidad.

- Fallo de servicios de comunicaciones

    - Descripción: inconvenientes con servicios de internet y telefonía.
    - Tipos de activos afectados: hardware (equipos de red de comunicación y telefonía).
    - Dimensiones afectadas: disponibilidad.

- Interrupción de otros servicios y suministros

    - Descripción: interrupción en los servicios auxiliares
    - Tipos de activos afectados: equipos auxiliares
    - Dimensiones afectadas: disponibilidad

- Degradación de los soportes de almacenamiento

    - Descripción: debido al tiempo y desuso los equipos de soporte podrían no funcionar.
    - Tipos de activos afectados: hardware, soportes, equipos auxiliares.
    - Dimensiones afectadas: disponibilidad.

2.3.2.3. Errores y fallos no intencionados

Amenazas por errores y fallos no intencionados detectadas son las siguientes:

- Errores de los usuarios

    - Descripción: errores operativos de las personas que manejan los activos.
    - Tipos de activos afectados: información, servicios, software, soportes.
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Errores del administrador

    - Descripción: errores operativos del personal responsable de la administración de los activos.
    - Tipos de activos afectados: información, servicios, software, hardware, soportes.
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Errores de monitorización

    - Inadecuada administración de la información de los logs (bitácora de actividades) de los activos del sistema.
    - Tipos de activos afectados: información.
    - Dimensiones afectadas: integridad.

- Errores de configuración

    - Descripción: incorrecta configuración de los activos, que provocan un mal funcionamiento de los activos del sistema.
    - Tipos de activos afectados: información (fichero digital).
    - Dimensiones afectadas: integridad.

- Deficiencias en la organización

    - Descripción: desconocimiento de la jerarquía para la toma de decisiones sobre los activos por parte del personal.
    - Tipos de activos afectados: personal.
    - Dimensiones afectadas: disponibilidad.

- Difusión de software dañino

    - Descripción: acciones inconscientes que provocan infecciones de virus informáticos, tales como descargas o instalación de dispositivos sin revisión o protección.
    - Tipos de activos afectados: software.
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Errores de reencaminamiento

    - Descripción: difusión de información a receptores incorrectos, como el envío de correos electrónicos a correos equivocados.
    - Tipos de activos afectados: servicios, software, hardware (equipos de red de comunicación y telefonía).
    - Dimensiones afectadas: confidencialidad.

- Alteración accidental de la información

    - Descripción: modificaciones a la información sin tener la intención de hacerlo.
    - Tipos de activos afectados: información, servicios, software, soportes.
    - Dimensiones afectadas: integridad.

- Destrucción de información

    - Descripción: eliminación de información sin tener la intención de hacerlo.
    - Tipos de activos afectados: información, servicios, software, soportes.
    - Dimensiones afectadas: disponibilidad.

- Fugas de información

    - Descripción: fallos de confidencialidad.
    - Tipos de activos afectados: información, servicios, software, soportes, personal.

- Dimensiones afectadas: confidencialidad.

- Vulnerabilidades de los programas

  - Descripción: defectos en el software que generan inconsistencia de información y funcionamiento.
  - Tipos de activos afectados: software.
  - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Errores de mantenimiento / actualización de programas

  - Descripción: aplicación de mantenimientos o actualizaciones al software, que no fueron correctamente aplicados y generan inconvenientes en el funcionamiento.
  - Tipos de activos afectados: software.
  - Dimensiones afectadas: disponibilidad, integridad.

- Errores de mantenimiento / actualización de equipos

  - Descripción: derivados de una mala aplicación en el mantenimiento y/o actualización de dispositivos.
  - Tipos de activos afectados: hardware, equipo auxiliar, soportes.
  - Dimensiones afectadas: disponibilidad.

- Caída del sistema por agotamiento de recursos

  - Descripción: ocurre cuando el volumen de procesamiento del software supera a los recursos de su hardware o servicio, ej. disco duro, memoria, ancho de banda.

- Tipos de activos afectados: servicios, hardware.
- Dimensiones afectadas: disponibilidad.

- Pérdida de equipos

  - Descripción: provocado por descuido, robo o destrucción del activo.
  - Tipos de activos afectados: hardware, soportes, equipos auxiliares.
  - Dimensiones afectadas: disponibilidad, confidencialidad.

- Indisponibilidad del personal

  - Descripción: ausencia al puesto de trabajo o funciones del personal, que puede originar suplantación de actividades o falta de directrices.
  - Tipos de activos afectados: personal (usuario interno).
  - Dimensiones afectadas: disponibilidad.

2.3.2.4. Ataques intencionados

Las amenazas derivadas de ataques intencionados identificadas son las siguientes.

- Manipulación de los registros de actividad

  - Descripción: ocurre cuando se cambia información de los logs (bitácora de actividades) de los sistemas de información.
  - Tipos de activos afectados: servicios.
  - Dimensiones afectadas: integridad.

- Manipulación de la configuración

    - Descripción: las configuraciones son los parámetros con los que un activo funciona. Si estos son manipulados ocasionan un mal funcionamiento.
    - Tipos de activos afectados: servicios.
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Suplantación de la identidad del usuario

    - Descripción: acceso de un usuario a un activo utilizando las autorizaciones otorgadas a otro usuario. Puede generarse interna o externamente, por ejemplo, al compartir información de usuarios.
    - Tipos de activos afectados: información, servicios, software, hardware (equipos de red de comunicación).
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Abuso de privilegios de acceso

    - Descripción: ocurre cuando el usuario que tiene acceso a un activo utiliza los privilegios otorgados para usos que no le competen.
    - Tipos de activos afectados: información, servicios, software, hardware.
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Uso no previsto

    - Descripción: utilización o manejo de los activos para fines ajenos a las funciones del puesto o a los objetivos de la empresa.

- Tipos de activos afectados: servicios, software, hardware, soportes, equipo auxiliar, instalaciones.
- Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Difusión de software dañino

  - Descripción: utilización de software malintencionado o más conocido como virus, con el fin de provocar daños a los activos.
  - Tipos de activos afectados: software.
  - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Reencaminamiento de mensajes

  - Descripción: realizar acciones para redirigir o desviar información a receptores no autorizados o desconocidos.
  - Tipos de activos afectados: servicios, software, hardware (equipos de red de comunicación y telefonía).
  - Dimensiones afectadas: confidencialidad.

- Acceso no autorizado

  - Descripción: ingresar a los activos sin autorización o permisos.
  - Tipos de activos afectados: información, servicios, software, hardware, soportes, equipo auxiliar, instalaciones.
  - Dimensiones afectadas: integridad, confidencialidad.

- Análisis de tráfico

- Descripción: es una actividad que tiene un origen externo del sistema, cuyo objetivo es analizar el tráfico de la red y encontrar información de utilidad para el atacante.
- Tipos de activos afectados: hardware (equipos de red de comunicaciones y telefonía).
- Dimensiones afectadas: confidencialidad.

- Interceptación de información

  - Descripción: cuando la información es accedida pero no es modificada o alterada.
  - Tipos de activos afectados: hardware (equipo de red de comunicación y telefonía).
  - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Modificación deliberada de la información

  - Descripción: manipular Información de acuerdo con una intención.
  - Tipos de activos afectados: información, servicios, software, soportes.
  - Dimensiones afectadas: integridad.

- Destrucción de información

  - Descripción: eliminar información.
  - Tipos de activos afectados: información, servicios, software, soportes.
  - Dimensiones afectadas: disponibilidad.

- Divulgación de información

    - Descripción: revelar información sin conocimiento del propietario de esta.
    - Tipos de activos afectados: información, servicios, software, soportes.
    - Dimensiones afectadas: confidencialidad.

- Manipulación de programas

    - Descripción: alteración del funcionamiento de los programas para que realicen acciones indebidas.
    - Tipos de activos afectados: software.
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Manipulación de los equipos

    - Descripción: alteración del funcionamiento de equipos.
    - Tipos de activos afectados: hardware, soportes, equipo auxiliar.
    - Dimensiones afectadas: disponibilidad, confidencialidad.

- Denegación de servicio

    - Descripción: enviar un gran volumen de solicitudes a uno o varios servicios para consumir sus recursos y que este deje de funcionar.
    - Tipos de activos afectados: hardware.
    - Dimensiones afectadas: disponibilidad.

- Robo

    - Descripción: extracción no autorizada de información.
    - Tipos de activos afectados: hardware, soportes, equipo auxiliar.
    - Dimensiones afectadas: disponibilidad, confidencialidad.

- Ataque destructivo

    - Descripción: su objetivo es destruir o eliminar información.
    - Tipos de activos afectados: hardware, soportes, equipo auxiliar, instalaciones.
    - Dimensiones afectadas: disponibilidad.

- Indisponibilidad del personal

    - Descripción: cuando ocurren huelgas, paros, ausencias no controladas por parte del personal del sistema.
    - Tipos de activos afectados: personal (usuarios internos).
    - Dimensiones afectadas: disponibilidad.

- Extorsión

    - Descripción: busca obtener información o causar daños por medio de amenazas.
    - Tipos de activos afectados: personal (usuarios internos).
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

- Ingeniería social

    - Descripción: manipulación de usuarios para acceder a información.
    - Tipos de activos afectados: personal (usuarios internos).
    - Dimensiones afectadas: disponibilidad, integridad, confidencialidad.

Al obtener las amenazas del sistema se realiza la identificación de estas dentro del mismo. Para la asignación de los códigos se utiliza la siguiente nomenclatura: el prefijo del código está compuesto por letras, que representan las iniciales del tipo de amenaza, luego del prefijo se asigna una numeración correlativa dependiendo del tipo de amenaza.

La siguiente tabla muestra la identificación de todas las amenazas del sistema:

Tabla VI. **Identificación de las amenazas**

Naturaleza de la amenaza	Código	Nombre
De origen natural	NAT-1	Fuego
De origen natural	NAT-2	Daños por agua
De origen natural	NAT-3	Desastres naturales
De origen Industrial	IND-1	Fuego
De origen Industrial	IND-2	Daños por agua
De origen Industrial	IND-3	Desastres industriales
De origen Industrial	IND-4	Contaminación mecánica
De origen Industrial	IND-5	Avería de origen físico o lógico
De origen Industrial	IND-6	Corte del suministro eléctrico
De origen Industrial	IND-7	Condiciones inadecuadas de temperatura o humedad
De origen Industrial	IND-8	Fallo de servicios de comunicaciones
De origen Industrial	IND-9	Interrupción de otros servicios
De origen Industrial	IND-10	Degradación de los soportes de almacenamiento

Continuación de la tabla VI.

Errores y fallos no intencionados	ERR-1	Errores de los usuarios
Errores y fallos no intencionados	ERR-2	Errores del administrador
Errores y fallos no intencionados	ERR-3	Errores de monitorización
Errores y fallos no intencionados	ERR-4	Errores de configuración
Errores y fallos no intencionados	ERR-5	Deficiencias en la organización
Errores y fallos no intencionados	ERR-6	Difusión de software dañino
Errores y fallos no intencionados	ERR-7	Errores de reencaminamiento
Errores y fallos no intencionados	ERR-8	Alteración accidental de la información
Errores y fallos no intencionados	ERR-9	Destrucción de información
Errores y fallos no intencionados	ERR-10	Fugas de información
Errores y fallos no intencionados	ERR-11	Vulnerabilidades de los programas
Errores y fallos no intencionados	ERR-12	Errores de mantenimiento / actualización de programas
Errores y fallos no intencionados	ERR-13	Errores de mantenimiento / actualización de equipos
Errores y fallos no intencionados	ERR-14	Caída del sistema por agotamiento de recursos
Errores y fallos no intencionados	ERR-15	Pérdida de equipos
Errores y fallos no intencionados	ERR-16	Indisponibilidad del personal
Ataques intencionados	ATA-1	Manipulación de registros de actividad
Ataques intencionados	ATA-2	Manipulación de la configuración
Ataques intencionados	ATA-3	Suplantación de identidad del usuario
Ataques intencionados	ATA-4	Abuso de privilegios de acceso
Ataques intencionados	ATA-5	Uso no previsto
Ataques intencionados	ATA-6	Difusión de software dañino
Ataques intencionados	ATA-7	Reencaminamiento de mensajes
Ataques intencionados	ATA-8	Acceso no autorizado
Ataques intencionados	ATA-9	Análisis de tráfico
Ataques intencionados	ATA-10	Interceptación de información
Ataques intencionados	ATA-11	Modificación deliberada de información
Ataques intencionados	ATA-12	Destrucción de información

Continuación de la tabla VI.

Ataques intencionados	ATA-13	Divulgación de información
Ataques intencionados	ATA-14	Manipulación de programas
Ataques intencionados	ATA-15	Manipulación de los equipos
Ataques intencionados	ATA-16	Denegación de servicio
Ataques intencionados	ATA-17	Robo
Ataques intencionados	ATA-18	Ataque destructivo
Ataques intencionados	ATA-19	Indisponibilidad del personal
Ataques intencionados	ATA-20	Extorsión
Ataques intencionados	ATA-21	Ingeniería social

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

2.3.3. Valoración

La valoración tiene dos métricas: la degradación y la probabilidad. La degradación mide el daño que puede provocar la materialización de la amenaza y la probabilidad indica la posibilidad de que ocurra. Para la valoración de las amenazas se toma como base la siguiente tabla cualitativa:

Tabla VII. **Valores para degradación y probabilidad**

Valoración	**Degradación**	**Probabilidad**
Muy alta	Daños severos e irreparables	Se sabe que pasará debido a las condiciones
Alta	Daño grave	Es frecuente
Media	Daño considerable	Poco frecuente
Baja	Daño menor	Ocurrirá bajo diversos factores
Muy baja	No es relevante	No existen condiciones para que se materialice

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

De acuerdo con los significados descritos anteriormente, se valorizan las siguientes amenazas de acuerdo con su degradación y probabilidad:

Tabla VIII. **Valoración de amenaza**

Código	Nombre amenaza	Degradación	Probabilidad
NAT-1	Fuego	Muy alta	Baja
NAT-2	Daños por agua	Muy alta	Media
NAT-3	Desastres naturales	Muy alta	Media
IND-1	Fuego	Muy alta	Media
IND-2	Daños por agua	Muy alta	Baja
IND-3	Desastres industriales	Muy alta	Media
IND-4	Contaminación mecánica	Media	Media
IND-5	Avería de origen físico o lógico	Alta	Alta
IND-6	Corte del suministro eléctrico	Alta	Media
IND-7	Condiciones inadecuadas de temperatura o humedad	Alta	Baja
IND-8	Fallo de servicios de comunicaciones	Muy baja	Baja
IND-9	Interrupción de otros servicios	Muy baja	Muy baja
IND-10	Degradación de los soportes de almacenamiento	Alta	Alta
ERR-1	Errores de los usuarios	Media	Alta
ERR-2	Errores del administrador	Alta	Media
ERR-3	Errores de monitorización (log)	Media	Baja
ERR-4	Errores de configuración	Alta	Baja
ERR-5	Deficiencias en la organización	Media	Baja
ERR-6	Difusión de software dañino	Muy alta	Alta
ERR-7	Errores de reencaminamiento	Media	Muy baja
ERR-8	Alteración accidental de la información	Alta	Media
ERR-9	Destrucción de información	Muy alta	Baja
ERR-10	Fugas de información	Media	Baja
ERR-11	Vulnerabilidades de los programas (software)	Alta	Media
ERR-12	Errores de mantenimiento / actualización de programas (software)	Alta	Baja

Continuación de tabla VIII.

ERR-13	Errores de mantenimiento/ actualización de equipos (hardware)	Media	Baja
ERR-14	Caída del sistema por agotamiento de recursos	Media	Muy baja
ERR-15	Pérdida de equipos	Alta	Media
ERR-16	Indisponibilidad del personal	Media	Baja
ATA-1	Manipulación de los registros de actividad (log)	Alta	Media
ATA-2	Manipulación de la configuración	Alta	Media
ATA-3	Suplantación de la identidad del usuario	Alta	Baja
ATA-4	Abuso de privilegios de acceso	Alta	Media
ATA-5	Uso no previsto	Media	Media
ATA-6	Difusión de software dañino	Muy alta	Alta
ATA-7	Reencaminamiento de mensajes	Media	Baja
ATA-8	Acceso no autorizado	Alta	Media
ATA-9	Análisis de tráfico	Media	Muy baja
ATA-10	Interceptación de información (escucha)	Muy baja	Muy baja
ATA-11	Modificación deliberada de la información	Muy alta	Baja
ATA-12	Destrucción de información	Muy alta	Baja
ATA-13	Divulgación de información	Alta	Baja
ATA-14	Manipulación de programas	Alta	Media
ATA-12	Manipulación de los equipos	Alta	Media
ATA-16	Denegación de servicio	Media	Baja
ATA-17	Robo	Alta	Baja
ATA-18	Ataque destructivo	Alta	Muy baja
ATA-15	Indisponibilidad del personal	Media	Baja
ATA-16	Extorsión	Media	Muy baja
ATA-17	Ingeniería social	Media	Baja

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

3. ESTIMACIÓN DEL ESTADO DE RIESGO

Teniendo el análisis de los activos a proteger y sus amenazas (modelo de valor), se determina el estado de riesgo de sistema. El estado de riesgo genera indicadores de protección del sistema de información, puntualmente el impacto, que cuantifica el daño absoluto hecho por la amenaza, y el riesgo que cuantifica la probabilidad de ocurrencia de la amenaza. Estos valores alertan a la organización sobre su estado de seguridad y son la base para las acciones que tomen.

3.1. Estimación del impacto y riesgo potencial

El impacto y riesgo potencial indican el estado riesgo del sistema, sin considerar las salvaguardas, controles o protección que puedan tener los activos.

3.1.1. Estimación del impacto potencial

Para estimar el impacto potencial, se toman los valores del activo en cada dimensión de seguridad, y los valores de degradación de la amenaza en cada dimensión de seguridad; utilizando el análisis de tablas, se determina el valor del impacto. La escala de valor del impacto tiene las siguientes interpretaciones:

- Muy alto: el daño causado al activo es severo o irreparable con consecuencias en el sistema.
- Alto: el activo es dañado gravemente.
- Medio: los daños pueden ocasionar inestabilidad del activo.
- Bajo: daños menores.

- Muy bajo: daños imperceptibles o sin consecuencias.

Tabla IX. **Tabla para valoración de impacto**

Valor del activo	Degradación				
	Muy baja	Baja	Media	Alta	Muy alta
Muy alto	M	M	A	A	MA
Alto	B	M	M	A	A
Medio	B	B	M	M	A
Bajo	MB	B	B	M	M
Muy bajo	MB	MB	B	B	M

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Por ejemplo, para la amenaza ERR-1 (errores de los usuarios), esta amenaza afecta a los activos de tipo información, servicios, software y soportes en sus tres dimensiones (integridad, confidencialidad y disponibilidad).

El valor de degradación de esta amenaza se determinó como “alta”. Tomando como referencia el activo INF-2 (información operativa externa 1), su valor en las tres dimensiones es “muy alto”; basándonos en la tabla IX, ubicamos la intersección del valor del activo y el valor de degradación, en este caso “muy alto” y “alto” respectivamente, y la tabla nos indica un valor “alto” para el impacto.

La interpretación de este ejemplo indica que el activo INF-2 tienen una degradación “alta”, si la amenaza ERR-1 llega a materializarse sobre dicho activo. La forma de cálculo anterior fue utilizada para generar las tablas de impacto por cada dimensión:

Tabla X. **Impacto en la dimensión de integridad de los activos**

Amenaza	Impacto	Activos afectados en su dimensión de Integridad
ERR-1	Alto	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Medio	INF-1, INF-5, INF-6, INF-7, INF-8, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
ERR-2	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	SW-1, SW-2
ERR-3	Alto	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11
	Medio	INF-1, INF-5, INF-6, INF-7, INF-8
ERR-4	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9
ERR-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ERR-8	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	SW-1, SW-2
ERR-11	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ERR-12	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ATA-1	Alto	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-2	Alto	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-3	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31
	Medio	SW-1, SW-2

Continuación de la tabla X.

ATA-4	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
	Medio	SW-1, SW-2
ATA-5	Alto	SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, INS-1, INS-2, INS-3, INS-6, INS-7, INS-8
	Medio	SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SW-1, SW-2, SW-8, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-4, INS-5, INS-9
ATA-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ATA-8	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9
	Medio	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-10	Medio	HW-28, HW-29, HW-30, HW-31
	Bajo	HW-32, HW-33
ATA-11	Muy alto	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	INF-1, INF-5, INF-6, INF-7, INF-8, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
ATA-14	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ATA-20	Alto	PER-2, PER-3, PER-4, PER-5, PER-17, PER-18
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16

Continuación de la tabla X.

ATA-21	Alto	PER-2, PER-3, PER-4, PER-5, PER-17, PER-18
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XI. **Impacto en la dimensión de confidencialidad de los activos**

Amenaza	Impacto	Activos afectados en su dimensión de confidencialidad
ERR-1	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	INF-6, INF-7, INF-11, SEI-2, SEI-7
	Bajo	SW-1, SW-2
ERR-2	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	SW-1, SW-2
ERR-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ERR-7	Alto	SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-32, HW-33
	Medio	SEI-2, SEI-7, HW-28, HW-29, HW-30, HW-31
	Bajo	SW-1, SW-2
ERR-10	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4, PER-2, PER-3, PER-4, PER-5, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Medio	INF-6, INF-7, INF-11, SEI-2, SEI-7, PER-6, PER-7
	Bajo	SW-1, SW-2, PER-1
ERR-11	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-1, SW-2

Continuación de la tabla XI.

ERR-15	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-2	Alto	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-3	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31
	Bajo	SW-1, SW-2
ATA-4	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
	Bajo	SW-1, SW-2
ATA-5	Alto	SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-8, INS-9
	Medio	SEI-2, SEI-7, HW-15, HW-16, HW-28, HW-29, HW-30, HW-31, INS-5
	Bajo	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ATA-7	Alto	SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-32, HW-33
	Medio	SEI-2, SEI-7, HW-28, HW-29, HW-30, HW-31
	Bajo	SW-1, SW-2

Continuación de la tabla XI.

ATA-8	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9
	Bajo	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-9	Alto	HW-32, HW-33
	Medio	HW-28, HW-29, HW-30, HW-31
ATA-10	Medio	HW-32, HW-33
	Bajo	HW-28, HW-29, HW-30, HW-31
ATA-13	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	SW-1, SW-2
ATA-14	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-1, SW-2
ATA-15	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-17	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-20	Alto	PER-2, PER-3, PER-4, PER-5, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Medio	PER-6, PER-7
ATA-21	Alto	PER-2, PER-3, PER-4, PER-5, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Medio	PER-6, PER-7

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XII. **Impacto en la dimensión de disponibilidad de los activos**

Amenaza	Impacto	Activos afectados en su dimensión de disponibilidad
NAT-1	Muy alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Alto	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
NAT-2	Muy alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Alto	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
NAT-3	Muy alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Alto	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
IND-1	Muy alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Alto	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
IND-2	Muy alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Alto	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9

Continuación de la tabla XII.

IND-3	Muy alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Alto	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
IND-4	Alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
IND-5	Alto	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
	Medio	SW-2
IND-6	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-1, AUX-2, AUX-3, AUX-4
IND-7	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
IND-8	Medio	HW-28, HW-29, HW-30, HW-31
	Bajo	HW-32, HW-33
IND-9	Medio	AUX-1, AUX-3
	Bajo	AUX-2, AUX-4
IND-10	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4

Continuación de la tabla XII.

ERR-1	Alto	INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Medio	INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
ERR-2	Alto	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ERR-5	Alto	PER-2, PER-3, PER-4, PER-5
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ERR-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ERR-9	Muy alto	INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
ERR-11	Alto	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-2
ERR-12	Alto	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-2
ERR-13	Alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
ERR-14	Alto	SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31
	Medio	SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33

Continuación de la tabla XII.

ERR-15	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ERR-16	Alto	PER-2, PER-3, PER-4, PER-5
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-2	Alto	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12
	Medio	SEI-7, SEI-8, SEI-10
ATA-3	Alto	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31
	Medio	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ATA-4	Alto	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
	Medio	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ATA-5	Alto	SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Medio	SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
ATA-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ATA-10	Medio	HW-28, HW-29, HW-30, HW-31
	Bajo	HW-32, HW-33
ATA-12	Muy alto	INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
ATA-14	Alto	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-2

Continuación de la tabla XII.

ATA-15	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ATA-16	Alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33
ATA-17	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ATA-18	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-9
	Medio	INS-5, INS-8
ATA-19	Alto	PER-2, PER-3, PER-4, PER-5
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-20	Alto	PER-2, PER-3, PER-4, PER-5
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Alto	PER-2, PER-3, PER-4, PER-5
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

3.1.2. Estimación del riesgo potencial

Para estimar el riesgo potencial, se toman los valores del impacto potencial y los valores de probabilidad de la amenaza en cada dimensión de seguridad; utilizando el análisis de tablas, se determina el valor del riesgo. La escala de valores del riesgo son los mismos utilizados en la valoración del impacto, con las siguientes interpretaciones:

- Muy alto: hay certeza en que ocurrirá.
- Alto: es muy probable que ocurra.
- Medio: es posible que ocurra bajo ciertos factores.
- Bajo: es improbable que ocurra.
- Muy bajo: las condiciones y factores no son propicios para la ocurrencia de la amenaza.

Tabla XIII. **Tabla para valoración de riesgo**

Impacto potencial	**Probabilidad**				
	Muy baja	**Baja**	**Media**	**Alta**	**Muy alta**
Muy alto	B	M	A	MA	MA
Alto	B	B	M	A	MA
Medio	MB	B	B	M	A
Bajo	MB	MB	B	B	M
Muy bajo	MB	MB	MB	B	B

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

La metodología para la estimación del valor de riesgo es la misma que para la estimación del impacto, considerando el valor de probabilidad de la amenaza y el impacto potencial.

Tabla XIV. **Riesgo en la dimensión de integridad de los activos**

Amenaza	Riesgo	Activos afectados
ERR-1	Alto	SW-6, SW-7, INF-2, INF-3, INF-4, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Medio	SW-8, SOP-1, INF-1, INF-5, INF-6, INF-7, INF-8, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-2, SOP-3, SOP-4, SW-1, SW-2
ERR-2	Medio	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-2, SOP-3, SOP-4, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Bajo	SW-1, SW-2
ERR-3	Bajo	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11
ERR-4	Bajo	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9
ERR-6	Muy alto	SW-5, SW-6, SW-7, SW-3, SW-4
	Alto	SW-8, SW-1, SW-2
ERR-8	Medio	SW-5, SW-6, SW-7, SW-8, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SOP-2, SOP-3, SOP-4, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	SW-1, SW-2
ERR-11	Medio	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Bajo	SW-1, SW-2
ERR-12	Bajo	SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3, SW-4
ATA-1	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-2	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-3	Bajo	SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, SW-5

Continuación de la tabla XIV.

ATA-4	Medio	SW-5, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	SW-1, SW-2
ATA-5	Medio	SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, INS-1, INS-2, INS-3, INS-6, INS-7, INS-8, HW-11, HW-12, HW-13, HW-14, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-8, INS-4, INS-5, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-32, HW-33, SOP-1, SOP-2, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, SW-1, SW-2
ATA-6	Muy alto	SW-5, SW-6, SW-7, SW-3, SW-4
	Alto	SW-8, SW-1, SW-2
ATA-8	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SOP-3, SOP-4, INS-1, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4, SW-1, SW-2
ATA-10	Muy Bajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-11	Medio	SW-6, SW-7, INF-2, INF-3, INF-4, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Bajo	SW-8, SOP-1, SOP-2, INF-1, INF-5, INF-6, INF-7, INF-8, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-3, SOP-4, SW-1, SW-2
ATA-14	Medio	SW-6, SW-7, SW-8, SW-1, SW-2, SW-3, SW-4, SW-5
ATA-20	Bajo	PER-2, PER-3, PER-4, PER-5, PER-17, PER-18
	Muy bajo	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16
ATA-21	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XV. **Riesgo en la dimensión de confidencialidad de los activos**

Amenaza	Riesgo	Activos afectados
ERR-1	Alto	SW-6, SW-7, SW-8, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SOP-2, SOP-3, SOP-4, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Medio	INF-6, INF-7, INF-11, SEI-2, SEI-7
	Bajo	SW-1, SW-2
ERR-2	Medio	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-2, SOP-3, SOP-4, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Bajo	SW-1, SW-2
ERR-6	Muy Alto	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Medio	SW-1, SW-2
ERR-7	Bajo	SW-5, SW-6, SW-7, SW-8, HW-32, HW-33, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Muy Bajo	HW-28, HW-29, HW-30, HW-31, SEI-2, SEI-7, SW-1, SW-2
ERR-10	Bajo	SW-5, SW-6, SW-7, SW-8, PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-2, SOP-3, SOP-4, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Muy Bajo	PER-1, SW-1, SW-2
ERR-11	Medio	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Bajo	SW-1, SW-2
ERR-15	Medio	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-2	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-3	Bajo	SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Muy Bajo	SW-1, SW-2

Continuación de la tabla XV.

ATA-4	Medio	SW-5, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	SW-1, SW-2
ATA-5	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-8, INS-9, HW-11, HW-12, HW-13, HW-14, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-32, HW-33, SOP-1, SOP-2, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SOP-3, SOP-4, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	INS-5, HW-15, HW-16, HW-28, HW-29, HW-30, HW-31, SEI-2, SEI-7, AUX-1, AUX-2, AUX-3, AUX-4, SW-1, SW-2
ATA-6	Muy alto	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Medio	SW-1, SW-2
ATA-7	Bajo	SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Muy bajo	SW-1, SW-2
ATA-8	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SOP-3, SOP-4, INS-1, SEI-10, SEI-11, SEI-12, SW-3, SW-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4, SW-1, SW-2
ATA-9	Bajo	HW-32, HW-33
	Muy bajo	HW-28, HW-29, HW-30, HW-31
ATA-10	Muy ajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-13	Bajo	SEI-1, SW-6, SW-7, SW-8, SOP-1, SOP-2, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SOP-3, SOP-4, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Muy bajo	SW-1, SW-2

Continuación de la tabla XV.

ATA-14	Medio	SW-6, SW-7, SW-8, SW-3, SW-4, SW-5
	Bajo	SW-1, SW-2
ATA-15	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-17	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-20	Bajo	PER-2, PER-3, PER-4, PER-5, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Muy bajo	PER-6, PER-7
ATA-21	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XVI. **Riesgo en la dimensión de disponibilidad de los activos**

Amenaza	Riesgo	Activos afectados
NAT-1	Medio	HW-4, HW-1, HW-2, HW-3, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
NAT-2	Alto	HW-4, HW-1, HW-2, HW-3, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4

Continuación de la tabla XVI.

NAT-3	Alto	HW-4, HW-1, HW-2, HW-3, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
IND-1	Alto	HW-4, HW-1, HW-2, HW-3, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
IND-2	Medio	HW-4, HW-1, HW-2, HW-3, INS-1, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
IND-3	Alto	HW-4, HW-1, HW-2, HW-3, INS-1, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
IND-4	Medio	HW-4, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
IND-5	Alto	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, SW-1, SW-3, SW-4
	Medio	SW-2

Continuación de tabla XVI.

IND-6	Medio	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-1, AUX-2, AUX-3, AUX-4
IND-7	Bajo	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-1, HW-2, HW-3, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
IND-8	Bajo	HW-28, HW-29, HW-30, HW-31
	Muy Bajo	HW-32, HW-33
IND-9	Muy Bajo	AUX-1, AUX-2, AUX-3, AUX-4
IND-10	Alto	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ERR-1	Alto	SW-6, SW-7, INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Medio	SW-8, SOP-1, INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-2, SOP-3, SOP-4, SEI-9, SEI-10, SW-1, SW-2
ERR-2	Medio	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SOP-2, SOP-3, SOP-4, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5
	Bajo	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ERR-5	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ERR-6	Muy Alto	SW-5, SW-6, SW-7, SW-3, SW-4
	Alto	SW-8, SW-1, SW-2
ERR-9	Medio	SW-5, SW-6, SW-7, INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4
	Bajo	SEI-9, SW-8, SOP-1, INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SOP-2, SOP-3, SOP-4, SEI-10, SW-1, SW-2
ERR-11	Medio	SW-5, SW-6, SW-7, SW-8, SW-1, SW-3, SW-4
	Bajo	SW-2

Continuación de la tabla XVI.

ERR-12	Bajo	SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3, SW-4
ERR-13	Bajo	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ERR-14	Bajo	HW-4, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12
	Muy Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10
ERR-15	Medio	HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ERR-16	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-2	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12
	Bajo	SEI-7, SEI-8, SEI-10
ATA-3	Bajo	SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, SW-5
ATA-4	Medio	SW-5, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4
	Bajo	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ATA-5	Medio	SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, INS-1, INS-2, INS-3, INS-6, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, SEI-1, SEI-2, SEI-3, AUX-1, AUX-3, SEI-11, SEI-12, SW-3, SW-4
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, SW-8, INS-4, INS-5, INS-7, INS-8, INS-9, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SOP-3, SOP-4, AUX-2, AUX-4, SEI-10, SW-1, SW-2

Continuación de la tabla XVI.

ATA-6	Muy Alto	SW-5, SW-6, SW-7, SW-3, SW-4
	Alto	SW-8, SW-1, SW-2
ATA-10	Muy Bajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-12	Medio	SW-6, SW-7, INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5
	Bajo	SW-8, SOP-1, SOP-2, INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SOP-3, SOP-4, SEI-10, SW-1, SW-2
ATA-14	Medio	SW-6, SW-7, SW-8, SW-1, SW-3, SW-4, SW-5
	Bajo	SW-2
ATA-15	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ATA-16	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-17	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ATA-18	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-1, HW-2, HW-3, HW-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-9, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
	Muy Bajo	INS-5, INS-8
ATA-19	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-20	Bajo	PER-2, PER-3, PER-4, PER-5
	Muy Bajo	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

3.2. Caracterización de los controles

Los controles, también conocidos como salvaguardas, son todos los elementos que protegen a los activos ante sus amenazas. Estos pueden ser técnicos o procedimientos y su objetivo es la reducción del impacto o del riesgo.

3.2.1. Identificación de los controles pertinentes

Los controles propuestos provienen de una investigación y análisis de los elementos y técnicas más utilizados y los que mejor se adaptan a las condiciones, necesidades, limitaciones y objetivos de la organización. Los controles se describen en orden alfabético, y su identificación se hace con un código de prefijo CON y una numeración.

- Acciones disciplinarias (CON-1)
    - Consecuencias que tiene el personal interno de la organización cuando violan las condiciones o acuerdos pactados, como llamadas de atención, descuentos o terminación de contrato.
    - Dirigidas a las amenazas: ERR-1, ERR-2, ERR-5.
    - Efecto: reducen la probabilidad de la amenaza.
    - Tipo de protección: disuasoria.
- Acciones legales (CON-2): consecuencias que tiene el personal interno y externo de la organización cuando violan las condiciones o acuerdos pactados, pudiendo llegar a demandas judiciales.
    - Dirigidas a las amenazas: ATA-20.
    - Efecto: reducen la probabilidad de la amenaza.

- Tipo de protección: disuasoria.

- Acondicionamiento de instalaciones (CON-3): son las mejoras a las instalaciones donde albergan activos de información, los cuales pueden estar expuestos a degradación por condiciones como el ambiente o la actividad de la empresa. Su objetivo es dar condiciones adecuadas para el funcionamiento y conservación de los activos y contempla la mejora de techos, paredes, piso, ventilación, climatización, ordenamiento, entre otros.

  - Dirigidas a las amenazas: IND-7.
  - Efecto: reducen la probabilidad de la amenaza.
  - Tipo de protección: preventiva.

- Actualización de software (CON-4): es la tarea de buscar e instalar en los dispositivos las actualizaciones de software con los que trabajan. Los proveedores del software comúnmente ponen a disposición de los clientes y usuarios, actualizaciones que contienen mejoras de funcionamiento y seguridad.

  - Dirigidas a las amenazas: ATA-16, ERR-11
  - Efecto: reducen la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Aislamiento de material inflamable (CON-5): aislar todos los elementos que puedan servir de combustible durante un incendio de las áreas donde se encuentren activos de información.

  - Dirigido a las amenazas: IND-1

- Efecto: reduce la probabilidad de la amenaza
- Tipo de protección: preventiva

- Alertas de accesos (CON-6): avisos de acceso de usuarios, especialmente en sistemas y equipos críticos. Estas alertas deben ser monitoreadas para establecer una reacción.

  - Dirigidas a las amenazas: ATA-3, ATA-8
  - Efecto: limitan el daño causado
  - Tipo de protección: preventiva

- Alertas de cambios de los servicios (CON-7): avisos de cambios en las configuraciones de los servicios, especialmente en sistemas y equipos críticos. Estas alertas deben ser monitoreadas para establecer una reacción.

  - Dirigidas a las amenazas: ATA-1, ATA-2
  - Efecto: limitan el daño causado
  - Tipo de protección: minimizadora

- Ampliación de los recursos del equipo (CON-8): consiste en evaluar y determinar si los recursos de los equipos, tales como disco de almacenamiento, memorias y baterías, deben ser de mayor capacidad debido a su uso.

  - Dirigida a las amenazas: ERR-14
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Auditar los registros de actividad (CON-9): revisión de las operaciones (creación, modificación, eliminación) realizadas por los usuarios y sistemas.

    - Dirigida a las amenazas: ATA-4
    - Efecto: reduce la probabilidad y limita el daño de la amenaza
    - Tipo de protección: preventiva y correctiva

- Auditar los servicios (CON-10): revisión de los accesos y solicitudes realizadas a los servicios.

    - Dirigida a las amenazas: ATA-7, ATA-8
    - Efecto: reduce la probabilidad y limita el daño de la amenaza
    - Tipo de protección: preventiva y correctiva

- Capacitación de usuarios (CON-11): dotar de conocimientos y herramientas específicas para la realización de ciertas actividades. Las capacitaciones proveen al usuario de seguridad y destreza para el desarrollo de sus tareas, lo que previene errores en los activos de información que maneje.

    - Dirigida a las amenazas: ERR-1, ERR-2, ERR-5
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Climatización de ambientes (CON-12): acciones para mantener los activos en una temperatura adecuada de funcionamiento, y así evitar su degradación. La instalación de los llamados aires acondicionados es uno de los recursos mayormente utilizados para la climatización de áreas.

- Dirigida a las amenazas: IND-7, IND-1
- Efecto: reduce la probabilidad de la amenaza
- Tipo de protección: preventiva

- Comprobación de identidad de usuarios (CON-13): son elementos que confirman que el usuario que está accediendo a un activo de información es el que indica ser. Para comprobar la identidad hay varios métodos y herramientas, como las preguntas personalizadas, códigos de confirmación enviados a correo o teléfono, lector de huella digital, entre otros.

  - Dirigida a las amenazas: ATA-1, ATA-10, ATA-2, ATA-21, ATA-3, ATA-8, ATA-9
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Configuración de puntos de restauración (CON-14): es una propiedad que manejan equipos como computadoras de escritorio, laptops, servidores, donde el sistema realiza una copia de seguridad del equipo completo cada cierto tiempo.

  - Dirigida a las amenazas: ATA-14, ERR-12
  - Efecto: limita el daño causado
  - Tipo de protección: recuperativa

- Conmutación por error (CON-15): consiste en tener equipos o sistemas completos de respaldo, configurados como los principales, que entran a funcionar manual o automáticamente cuando el equipo o sistema principal falla.

- Dirigida a las amenazas: ERR-13, ERR-14
- Efecto: limita el daño causado
- Tipo de protección: recuperativa

- Contrato de confidencialidad (CON-16): son contratos entre personal, usuarios, clientes, proveedores y cualquier otro socio de negocio con la organización, donde se acuerda la confidencialidad y la no difusión autorizada de cierta información. Su incumplimiento puede llevar consecuencias judiciales para quien viole el contenido del contrato.

  - Dirigido a las amenazas: ATA-13, ATA-20, ATA-7, ERR-10, ERR-7
  - Efecto: reduce la probabilidad y limita el daño de la amenaza
  - Tipo de protección: disuasoria y minimizadora

- Controles de acceso (CON-17): son dispositivos de seguridad electrónica que se colocan en las entradas a las instalaciones que se requiere sean de acceso restringido.

  - Dirigidos a las amenazas: ATA-08
  - Efecto: reducen la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Convenio de responsabilidad laboral (CON-18): son documentos administrativos donde se expresan las responsabilidades u obligaciones en cuanto al tratamiento de los activos de información por parte de los empleados.

  - Dirigido a las amenazas: ATA-5
  - Efecto: reduce la probabilidad de la amenaza

- Tipo de protección: disuasoria

- Copias de seguridad (CON-19): es un proceso técnico donde se hace una copia de la información importante de los activos, con una frecuencia determinada. Estas copias son almacenadas en dispositivos de soporte.

  - Dirigidas a las amenazas: ATA-11, ATA-12, ATA-14, ATA-15, ATA-17, ATA-18, ERR-12, ERR-15, ERR-8, ERR-9, IND-1, IND-10, IND-2, IND-3, IND-4, IND-5
  - Efecto: limitan el daño causado
  - Tipo de protección: recuperativa

- Cortafuego (firewall) (CON-20): puede ser un equipo o un software que controla los servicios que están disponibles en la red.

  - Dirigido a las amenazas: ATA-8, ATA-16
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Definición de atribuciones de puesto de empleados (CON-21): es un mecanismo de control para que los empleados tengan conocimiento preciso de las tareas, permisos y privilegios que el puesto les otorga.

  - Dirigido a las amenazas: ERR-3
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Definir las competencias del puesto (CON-22): forma parte del proceso de dotación de personal; es una herramienta administrativa para determinar

las cualidades, experiencia y conocimiento que el personal debe tener para los puestos de trabajo. Esto disminuye errores que puedan ocurrir por falta de aptitudes laborales.

- Dirigida a las amenazas: ERR-1, ERR-2
- Efecto: reduce la probabilidad de la amenaza
- Tipo de protección: preventiva

- Definir y aplicar roles de usuario (CON-23): los roles de usuario son esquemas de accesos y permisos que se autorizan a usuarios de sistemas y equipos. Estos esquemas son diferentes para cada tipo de usuario; según la naturaleza de las operaciones y privilegios que deban tener, se les asigna un esquema específico. Los roles deben aplicarse a todos los equipos, sistemas y servicios para prevenir accesos y operaciones no autorizadas y abusos de privilegios.

  - Dirigidos a las amenazas: ATA-1, ATA-11, ATA-12, ATA-13, ATA-2, ERR-10, ERR-4, ERR-8, ERR-9.
  - Efecto: reducen la probabilidad de la amenaza.
  - Tipo de protección: preventiva.

- Desarrollo de actividades de inducción al puesto (CON-24): parte del proceso de dotación de personal, donde se trasladan las indicaciones, instrucciones, y cualquier información pertinente que el personal requiera para la realización de las actividades correspondientes al puesto.

  - Dirigidas a las amenazas: ERR-1, ERR-2, ERR-5
  - Efecto: reducen la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Disponibilidad de extintores de incendio (CON-25): siguiendo las disposiciones de reglamentación de seguridad industrial, las áreas deben contar con extintores contra incendios, con mayor énfasis en aquellas donde se concentren activos de información críticos.

    - Dirigida a las amenazas: IND-1
    - Efecto: limita el daño causado
    - Tipo de protección: minimizadora

- Disponibilidad de generador eléctrico (CON-26): un generador eléctrico es un equipo que convierte la energía mecánica en energía eléctrica. Es utilizado cuando la fuente principal de suministro de energía eléctrica tiene una interrupción y el generador es puesto en funcionamiento para proveer de energía a las instalaciones y equipos.

    - Dirigida a las amenazas: IND-6
    - Efecto: limita el daño causado
    - Tipo de protección: correctiva

- Disponibilidad de equipos de reemplazo (CON-27): se refiere a disponer de equipos en condiciones funcionales para sustituir a otros que fallen. Este control es común para equipos accesibles en cuanto a costo y forma de configuración genérica o con pocos parámetros, como los equipos de red y comunicaciones.

    - Dirigida a las amenazas: ERR-13, IND-8, ATA-15, ATA-18
    - Efecto: limita el daño causado
    - Tipo de protección: recuperativa

- Establecimiento de una zona desmilitarizada (CON-28): es una red que se encuentra dentro de la red local de la organización y donde se ubican todos los recursos que deben ser accedidos desde internet, por ejemplo, servidores web o de correo. Estas zonas permiten conexiones desde internet y desde la red local, pero dichas zonas no pueden conectarse hacia la red local (donde están los recursos privados de la organización). Esta estructura hace menos probable un ataque externo debido a las restricciones entre las redes.

    - Dirigido a las amenazas: ATA-8, ATA-9, ATA-16
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Flujos de aprobación de cambios (CON-29): son flujos de trabajo en los cuales se determina el procedimiento para la aprobación de cambios en las configuraciones de servicios y sistemas. Este control previene las modificaciones no autorizadas.

    - Dirigido a las amenazas: ATA-1, ATA-2, ATA-4
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Garantía de fábrica y/o proveedor de equipos (CON-30): compromiso del proveedor para atender y resolver los inconvenientes físicos y de funcionamiento de los equipos durante un periodo. Es conveniente que los equipos en funcionamiento estén dentro del periodo de garantía y que se tengan en aquellos donde se necesite soporte especializado.

    - Dirigida a las amenazas: IND-5

- Efecto: limita el daño causado
- Tipo de protección: correctiva

- Impermeabilización de techos y paredes (CON-31): aplicación de impermeabilizantes en techos y paredes de las instalaciones para evitar las filtraciones de agua o la humedad.

  - Dirigida a las amenazas: IND-2
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Inclusión de avisos o leyendas de carácter legal (CON-32): es un texto que indica que la información recibida es de carácter confidencial y su difusión sin autorización puede tener consecuencias legales para quien infrinja esta condición. Es utilizado en los mensajes de correo electrónico.

  - Dirigido a las amenazas: ATA-7, ERR-7
  - Efecto: reduce la probabilidad y limita el daño de la amenaza
  - Tipo de protección: disuasoria y minimizadora

- Instalación de equipo deshumidificador (CON-33): equipo que reduce la humedad del ambiente. La humedad puede provocar degradación de los equipos expuestos a esta.

  - Dirigida a las amenazas: IND-07
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: eliminadora

- Instalación de pararrayos (CON-34): dispositivo que encamina la descarga producida por un rayo hacia la tierra. El pararrayos protege de daños por la descarga de un rayo a las instalaciones y sus equipos.

    - Dirigida a las amenazas: NAT-3
    - Efecto: limita el daño causado
    - Tipo de protección: minimizadora

- Licenciamiento de software (CON-35): contar con licencias de uso para todo el software utilizado en la organización. El uso de software sin licencia, o con licencia vencida, pone en riesgo la seguridad de este, debido a que el proveedor no pondrá a disposición las actualizaciones que pueden contener correcciones de errores y vulnerabilidades de seguridad.

    - Dirigido a las amenazas: ERR-11
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Llaves públicas y encriptación (CON-36): uso de certificados que identifican a los individuos y otros sistemas que quieren comunicarse con los servidores y servicios de la organización. La encriptación es la codificación de la comunicación por parte de los servidores, para que el receptor permitido sea quien pueda interpretarla.

    - Dirigida a las amenazas: ATA-9, ATA-10
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Mantenimiento de equipos (CON-37): tareas de mantenimiento preventivo de los dispositivos. Estas actividades incluyen limpieza del equipo, revisión de los parámetros de funcionamiento, inspección física, ordenamiento entre otros. El mantenimiento debe ser periódico.

    - Dirigido a las amenazas: IND-4, IND-5, IND-7
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Mantenimiento de instalaciones eléctricas (CON-38): tareas de mantenimiento preventivo de los dispositivos e instalaciones eléctricas. Estas actividades incluyen la revisión de los parámetros de funcionamiento, inspección física, ordenamiento, aislamiento, reparación de daños, entre otros. El mantenimiento debe ser periódico.

    - Dirigido a las amenazas: IND-1
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Mantenimiento de los sistemas de canalización de aguas (CON-39): tareas de revisión y mantenimiento de las canalizaciones y desagües. Estos sistemas deben estar libres de obstrucciones y roturas para evitar filtraciones hacia las instalaciones. El mantenimiento debe ser periódico.

    - Dirigido a las amenazas: IND-2
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Mantenimiento de sistemas de climatización (CON-40): el mantenimiento de los sistemas de climatización o aire acondicionado es utilizado en las instalaciones para evitar el mal funcionamiento de estas. El mantenimiento debe ser periódico.

    - Dirigido a las amenazas: IND-2
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Mantenimiento de tuberías y drenajes (CON-41): las tareas de mantenimiento preventivo de los sistemas de trasporte y distribución de agua incluyen la revisión de los parámetros de funcionamiento, inspección física, ordenamiento, reparación de daños, entre otros. El mantenimiento debe ser periódico.

    - Dirigido a las amenazas: IND-4, IND-7
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Mantenimiento y limpieza de instalaciones (CON-42): tareas de mantenimiento preventivo de las instalaciones. Entre estas actividades están: limpieza de las áreas, inspección física, ordenamiento, reparación de daños, entre otros. El mantenimiento debe ser periódico.

    - Dirigido a las amenazas: IND-4
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Manuales de actualización de hardware (CON-43): recursos documentales que dan las instrucciones para la actualización de los equipos. Estos manuales pueden estar basados en buenas prácticas o en documentación e indicaciones dadas por el proveedor de los equipos.

    - Dirigidos a las amenazas: ERR-13
    - Efecto: reducen la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Manuales de actualización de software (CON-44): recursos documentales que incluyen instrucciones para la actualización de software. Estos manuales pueden estar basados en buenas prácticas o en documentación e indicaciones dadas por el proveedor del software.

    - Dirigidos a las amenazas: ERR-12
    - Efecto: reducen la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Manuales de procedimientos (CON-45): recursos documentales que indican la forma en que deben realizarse los procedimientos de la organización. En estos documentos se indica también quiénes son los responsables, las unidades organizativas a cargo, funciones y demás información detallada de los procesos internos.

    - Dirigidos a las amenazas: ERR-5, ERR-16
    - Efecto: reducen la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Monitoreo de accesos (CON-46): actividades de revisión de los accesos a instalaciones, software, servicios y equipos, y que son realizadas por personal o sistemas especializados. Cumplen un rol de vigilancia ante accesos que pueden considerarse sospechosos e iniciar con acciones preventivas o correctivas.

    - Dirigido a las amenazas: ERR-5, ERR-16.
    - Efecto: reduce la probabilidad y limita el daño causado por la amenaza.
    - Tipo de protección: preventiva y minimizadora.

- Perfilación de puestos (CON-47): parte del proceso de dotación de personal; es una técnica administrativa que define las características, aptitudes, destrezas, experiencia y demás requisitos que debe cumplir una persona para optar a un puesto de trabajo. Este control previene un mal manejo de los activos de información por desconocimiento o falta de competencias.

    - Dirigida a las amenazas: ERR-5
    - Efecto: reduce la probabilidad de la amenaza
    - Tipo de protección: preventiva

- Políticas de contraseñas (CON-48): es el establecimiento de normas en cuanto a la creación, contenido, forma y vigencia de las contraseñas utilizadas en los equipos, aplicaciones y servicios. Su objetivo es reducir los accesos no autorizados o suplantaciones, debido a debilidades en las contraseñas.

    - Dirigidas a las amenazas: ATA-2, ATA-3, ATA-8

- Efecto: reducen la probabilidad de la amenaza
- Tipo de protección: preventiva

- Políticas de navegación en internet (CON-49): es el establecimiento de normas en el acceso a sitios y servicios de internet. Su objetivo es evitar sitios malintencionados o poco seguros, donde puedan crearse puntos de acceso y dañar los activos del sistema de información. Se crean listas blancas y negras de los sitios.

  - Dirigidas a las amenazas: ATA-21, ATA-5, ATA-6, ERR-6
  - Efecto: reducen la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Redundancia de servicios (CON-50): sucede cuando se tiene más de un servicio contratado del mismo tipo. Es común su uso en servicios de internet y telefonía, si hay un fallo en el servicio principal, se puede conectar al servicio redundante para continuar con la operación.

  - Dirigida a las amenazas: IND-8, IND-9
  - Efecto: limita el daño causado
  - Tipo de protección: correctiva

- Redundancia y balanceo de cargas para servicios (CON-51): estructura de operación de servicios web en la que se colocan varios servidores para un mismo servicio; uno funciona como principal o por defecto, mientras que los demás sirven de auxiliares en caso el principal deje de funcionar. Este esquema permite un funcionamiento continuo de los servicios web y también el balance de la carga de trabajo entre todos los servidores disponibles.

- Dirigida a las amenazas: ATA-16
- Efecto: limita el daño causado
- Tipo de protección: correctiva

- Renovación de equipos (CON-52): es cambiar el hardware o equipos por otros más modernos o de mejores prestaciones. Esto conlleva a la compra de equipo nuevo y su integración en el sistema de información. Este control busca mejorar las prestaciones de los dispositivos, los servicios y la eficiencia de los usuarios.

  - Dirigida a las amenazas: ERR-14, IND-10, IND-5
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Renovación de software (CON-53): adquirir y utilizar un software con mejores capacidades o prestaciones. Esto conlleva la inversión en la compra del software y su integración con los equipos que lo utilicen y con el sistema de información. Este control busca mejorar las prestaciones de los dispositivos, los servicios y la eficiencia de los usuarios.

  - Dirigida a las amenazas: ERR-11
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Respaldos en la nube (CON-54): adquirir y utilizar un espacio de alojamiento en la nube, en el que se almacenen copias de seguridad de servidores, equipos, software, digitaciones de documentos y cualquier clase de fichero digital que la organización considere importante para

conservar un respaldo. Los respaldos se realizan manualmente o de manera automática con una programación periódica.

- Dirigidos a las amenazas: ATA-11, ATA-12, ATA-15, ATA-17, ATA-18, ERR-15, ERR-8, ERR-9, IND-1, IND-10, IND-2, IND-3, IND-4, IND-5, NAT-1, NAT-2, NAT-3.
- Efecto: limitan el daño causado.
- Tipo de protección: recuperativa.

- Restricción de acceso a documentación y lugares de archivo (CON-55): limitación o restricción de acceso a las instalaciones o lugares donde se tenga almacenada información física confidencial.

  - Dirigida a las amenazas: ATA-13, ERR-10
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: preventiva

- Restricción de acceso por contraseña a disco duro (CON-56): configuración de unidades de discos duros que restringen el acceso a su lectura por medio de contraseña.

  - Dirigida a las amenazas: ATA-17, ERR-15
  - Efecto: limita el daño causado
  - Tipo de protección: minimizadora

- Revisión de los recursos del equipo (CON-57): consiste en obtener información de los equipos y servicios respecto del estado de sus recursos. Es una tarea de vigilancia periódica, con base en la

retroalimentación; se toman acciones preventivas si alguno de los recursos está llegando a su punto de agotamiento.

- Dirigida a las amenazas: ERR-14
- Efecto: reduce la probabilidad de la amenaza
- Tipo de protección: preventiva

- Seguro de daños a hardware (CON-58): deben utilizarse seguros para dispositivos electrónicos o hardware, ya que estos pueden llegar a cubrir daños, destrucción, o cualquier otro siniestro cubierto por la póliza.

  - Dirigido a las amenazas: NAT-1, NAT-2, NAT-3, ATA-18
  - Efecto: limita el daño causado
  - Tipo de protección: recuperativa

- Seguro de daños a instalaciones (CON-59): seguros contra daños que puedan sufrir las instalaciones por actividades naturales o por las actividades propias de los procesos que se realicen en estas.

  - Dirigido a las amenazas: NAT-1, NAT-2, NAT-3
  - Efecto: limita el daño causado
  - Tipo de protección: recuperativa

- Seguros por robo de equipos (CON-60): seguros que cubren el robo de equipos.

  - Dirigidos a las amenazas: NAT-1, NAT-2, NAT-3
  - Efecto: limitan el daño causado
  - Tipo de protección: recuperativa

- Sensibilización y concientización en seguridad de la información (CON-61): actividades para hacer conciencia en el personal de la organización, sobre la importancia en la seguridad de la información. Es un complemento de los otros controles técnicos como los procedimientos, las políticas y normas, para generar una cultura integral de protección hacia los activos de información que las personas manejan.

    - Dirigidas a las amenazas: ATA2, ATA-5, ATA-6, ATA-21, ERR-6, ERR-21.
    - Efecto: reducen la probabilidad de la amenaza.
    - Tipo de protección: de concientización.

- Sistema de alimentación ininterrumpida (CON-62): comúnmente conocidos por sus siglas en ingles UPS; son equipos que alimentan con energía eléctrica almacenada a los dispositivos conectados a este, cuando hay interrupciones en la fuente principal de energía eléctrica. Todo equipo que se considere crítico para el sistema de información debe estar conectado a uno de estos equipos, para prevenir daños o pérdida de información.

    - Dirigido a las amenazas: IND-6
    - Efecto: limita el daño causado
    - Tipo de protección: minimizadora

- Sistemas activos y pasivos de detección de fugas (CON-63): son dispositivos que cuentan con sensores que indican la presencia de fugas de agua en los sistemas. Sirven como mecanismos de alerta.

    - Dirigidos a las amenazas: IND-2

- Efecto: limitan el daño causado
- Tipo de protección: minimizadora

- Sistemas contra incendios (CON-64): son sistemas que detectan la presencia de fuego (humo, temperatura) en una zona determinada, emiten una alerta y se activan los dispositivos de supresión que aplican agua y otras sustancias para extinguir el incendio. Los sistemas de incendio pueden estar ubicados en puntos clave de las instalaciones; para el caso de la protección de los sistemas de información, debe priorizarse su presencia en las áreas donde se ubiquen o concentren los activos críticos del sistema, como el centro de datos y otros archivos.

  - Dirigidos a las amenazas: IND-1
  - Efecto: limitan el daño causado
  - Tipo de protección: minimizadora

- Sistemas de detección de intrusos (CON-65): software que analiza y monitorea las redes y servicios, determina y alerta sobre actividades no autorizadas o sospechosas. Su base de funcionamiento es la auditoría de archivos de actividades, con lo que puede determinar si el comportamiento de una red o sistema ha cambiado.

  - Dirigidos a las amenazas: ATA-9, ATA-10, ATA-16
  - Efecto: reducen la probabilidad de la amenaza
  - Tipo de protección: minimizadora

- Software antivirus (CON-66): es un software especializado en buscar y prevenir ataques de virus informáticos. Los virus informáticos pueden estar presentes tanto en dispositivos infectados que se introduzcan en el

sistema, como en internet; por ello el software debe ser capaz de analizar las amenazas del equipo y la que los sitios en internet puedan contener.

- Dirigido a las amenazas: ATA-6, ATA-16, ATA-21, ERR-6
- Efecto: reduce la probabilidad de la amenaza
- Tipo de protección: preventiva y minimizadora

- Subcontratación de personal (CON-67): es una práctica común en las organizaciones actuales que contratan los servicios de una empresa que se encarga de proveer el personal calificado para los puestos que se requieran. En este esquema la responsabilidad de las acciones del personal es compartida con la empresa proveedora.

  - Dirigida a las amenazas: ATA-19
  - Efecto: reduce la probabilidad de la amenaza
  - Tipo de protección: eliminatoria

- Supervisión y revisión de actividades del personal (CON-68): actividades de revisión y vigilancia de las actividades en los activos de información efectuadas por el personal. Por ejemplo, cambios en la configuración de un servidor, deberán ser revisados y probarse antes de ser aplicados; una revisión de las operaciones realizadas en los sistemas puede determinar la existencia de malas operaciones que deban corregirse.

  - Dirigidas a las amenazas: ATA-19.
  - Efecto: reducen la probabilidad y limitan el daño causado por la amenaza.
  - Tipo de protección: preventiva y correctiva.

- Teletrabajo (CON-69): es la capacidad de la organización y de su personal de poder realizar sus actividades laborales a distancia. En ocasiones la indisposición del personal o de situaciones y condiciones de entorno, impiden que las labores se efectúen en las instalaciones de la organización, lo que compromete el normal funcionamiento de los sistemas de información.

    - Dirigido a las amenazas: ATA-19, ERR-16
    - Efecto: limita el daño causado
    - Tipo de protección: minimizadora

- Términos y condiciones de trabajo (CON-70): para que el personal tenga claro cuáles son las obligaciones y responsabilidad de su trabajo, debe existir documentación donde se hagan explícitos los términos y condiciones del trabajo, con énfasis en los compromisos adquiridos respecto de la seguridad de los activos de información de la organización.

    - Dirigidos a las amenazas: ATA-5, ERR-7, ATA-20, ERR-7
    - Efecto: reducen la probabilidad de la amenaza.
    - Tipo de protección: preventiva.

- Uso de redes privadas virtuales (CON-71): es una conexión segura entre equipos remotos, funcionando como si estuvieran dentro de una red local; son habilitadas para que servidores y usuarios específicos se puedan comunicar de forma privada y segura. Su uso evita que los equipos (servidores y sus servicios) tengan que estar públicos en internet, y que cualquier persona o sistema pueda atacarlos.

    - Dirigidas a las amenazas: ATA-10, ATA-9

- Efecto: reducen la probabilidad de la amenaza
- Tipo de protección: preventiva

3.2.2. Valoración de la eficacia

La eficacia de los controles indica el nivel de protección ante la amenaza; su objetivo es disminuir la probabilidad de que la amenaza se presente, o limitar el daño si llega a ocurrir; en algunos casos el control ayuda reduciendo ambos factores; esto se define como el efecto del control sobre la amenaza. Como consecuencia de su efecto existe una correlación sobre la probabilidad y la degradación de la amenaza, según la función del control, que hará que estos valores pasen a niveles más bajos. Para la valoración de la eficacia se utiliza la misma escala usada en la valoración de activos y amenazas, y se tomaron en cuenta los distintos factores que cada control ofrece:

- Funcionalidad técnica ante la amenaza específica
- Capacidad de operación y deficiencias o restricciones de uso
- Resultados esperados o garantías de funcionamiento
- Uso en otras organizaciones
- Experiencias y recomendaciones de uso

Tabla XVII. **Valoración de la eficacia de los controles**

Valor	Símbolo	Descripción
Muy alto	MA	Solución integral ante las amenazas.
Alto	A	Protege ante la mayoría de las amenazas, pero pueden existir casos no contemplados.
Medio	M	Es una solución parcial a las amenazas debido a su naturaleza, condiciones o aplicación.

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

La tabla siguiente muestra la eficacia en la probabilidad y la degradación de cada control.

Tabla XVIII. **Valoración de la eficacia de los controles**

Código	Amenazas	Eficacia	
		Prob.	Deg.
CON-1	ERR-1, ERR-2, ERR-5	M	
CON-2	ATA-20	M	
CON-3	IND-7	A	
CON-4	ATA-16, ERR-11	A	
CON-5	IND-1	MA	
CON-6	ATA-3, ATA-8		A
CON-7	ATA-1, ATA-2		A
CON-8	ERR-14	A	
CON-9	ATA-4	M	M
CON-10	ATA-7, ATA-8	M	M
CON-11	ERR-1, ERR-2, ERR-5	A	
CON-12	IND-7, IND-1	A	
CON-13	ATA-1, ATA-10, ATA-2, ATA-21, ATA-3, ATA-8, ATA-9	MA	
CON-14	ATA-14, ERR-12		A
CON-15	ERR-13, ERR-14		MA
CON-16	ATA-13, ATA-20, ATA-7, ERR-10, ERR-7	A	M
CON-17	ATA-08	MA	
CON-18	ATA-5	M	
CON-19	ATA-11, ATA-12, ATA-14, ATA-15, ATA-17, ATA-18, ERR-12, ERR-15, ERR-8, ERR-9, IND-1, IND-10, IND-2, IND-3, IND-4, IND-5		MA
CON-20	ATA-8, ATA-16	A	
CON-21	ERR-3	M	
CON-22	ERR-1, ERR-2	M	
CON-23	ATA-1, ATA-11, ATA-12, ATA-13, ATA-2, ERR-10, ERR-4, ERR-8, ERR-9	MA	
CON-24	ERR-1, ERR-2, ERR-5	M	
CON-25	IND-1		M
CON-26	IND-6		A

Continuación de la tabla XVIII.

CON-27	ERR-13, IND-8, ATA-15, ATA-18		MA
CON-28	ATA-8, ATA-9, ATA-16	MA	
CON-29	ATA-1, ATA-2, ATA-4	A	
CON-30	IND-5		M
CON-31	IND-2	A	
CON-32	ATA-7, ERR-7	M	A
CON-33	IND-07	A	
CON-34	NAT-3	MA	A
CON-35	ERR-11	A	
CON-36	ATA-9, ATA-10	MA	
CON-37	IND-4, IND-5, IND-7	A	
CON-38	IND-1	A	
CON-39	IND-2	A	
CON-40	IND-2	A	
CON-41	IND-4, IND-7	A	
CON-42	IND-4	A	
CON-43	ERR-13	A	
CON-44	ERR-12	A	
CON-45	ERR-5, ERR-16	A	
CON-46	ERR-5, ERR-16	A	A
CON-47	ERR-5	M	
CON-48	ATA-2, ATA-3, ATA-8	MA	
CON-49	ATA-21, ATA-5, ATA-6, ERR-6	A	
CON-50	IND-8, IND-9		MA
CON-51	ATA-16		MA
CON-52	ERR-14, IND-10, IND-5	MA	
CON-53	ERR-11	MA	
CON-54	ATA-11, ATA-12, ATA-15, ATA-17, ATA-18, ERR-15, ERR-8, ERR-9, IND-1, IND-10, IND-2, IND-3, IND-4, IND-5, NAT-1, NAT-2, NAT-3		MA
CON-55	ATA-13, ERR-10	A	
CON-56	ATA-17, ERR-15		A
CON-57	ERR-14	A	
CON-58	NAT-1, NAT-2, NAT-3, ATA-18		M

Continuación de tabla XVIII.

CON-59	NAT-1, NAT-2, NAT-3		M
CON-60	NAT-1, NAT-2, NAT-3		M
CON-61	ATA2, ATA-5, ATA-6, ATA-21, ERR-6, ERR-21	A	
CON-62	IND-6		MA
CON-63	IND-2		A
CON-64	IND-1		A
CON-65	ATA-9, ATA-10, ATA-16	MA	A
CON-66	ATA-6, ATA-16, ATA-21, ERR-6	A	
CON-67	ATA-19	M	
CON-68	ATA-19	A	
CON-69	ATA-19, ERR-16		A
CON-70	ATA-5, ERR-7, ATA-20, ERR-7	M	
CON-71	ATA-10, ATA-9	MA	

Fuente: elaboración propia utilizando Microsoft Excel 2016.

3.2.3. Nueva valoración de las amenazas

Ya que se conoce el valor de la eficacia de los controles y utilizando el método de análisis por tablas, se obtienen los nuevos valores para la degradación y probabilidad de las amenazas:

Tabla XIX. **Valoración de probabilidad y degradación de las amenazas**

Eficacia	**Probabilidad / degradación**				
	Muy baja	**Baja**	**Media**	**Alta**	**Muy alta**
Muy alto	MB	MB	MB	B	B
Alto	MB	MB	B	B	M
Medio	MB	B	B	M	M

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Para cada amenaza, y casi en su mayoría, existen varios controles con diferentes valores de eficacia; en estos casos se identifica el mayor valor de eficacia para cada factor (probabilidad y degradación) del conjunto de controles, y estos valores máximos de eficacia son los que se utilizarán para el nuevo cálculo del valor de los factores de las amenazas.

Tabla XX. **Valores nuevos de probabilidad y degradación**

Amenaza	Controles	Valores iniciales		Eficacia controles		Valores nuevos	
		P	D	P	D	P	D
NAT-1	CON-54, CON-58, CON-59	B	MA		A	B	M
NAT-2	CON-54, CON-58, CON-59	M	MA		A	M	M
NAT-3	CON-54, CON-58, CON-59	M	MA		A	M	M
IND-1	CON-19, CON-25, CON-38, CON-5, CON-54, CON-64	M	MA	MA	MA	MB	B
IND-2	CON-19, CON-31, CON-39, CON-40, CON-41, CON-54, CON-63	B	MA	A	MA	MB	B
IND-3	CON-19, CON-34, CON-38, CON-54	M	MA	MA	MA	MB	B
IND-4	CON-19, CON-42, CON-54	M	M	A	MA	B	MB
IND-5	CON-19, CON-30, CON-37, CON-52, CON-54	A	A	MA	MA	B	B
IND-6	CON-26, CON-62	M	A		MA	M	B
IND-7	CON-12, CON-3, CON-33	B	A	A		MB	A
IND-8	CON-27, CON-50	B	MB		MA	B	MB
IND-9	CON-50	MB	MB		MA	MB	MB
IND-10	CON-19, CON-52, CON-54	A	A	A	MA	B	B
ERR-1	CON-1, CON-11, CON-22, CON-24, CON-68	A	M	A		B	M
ERR-2	CON-1, CON-11, CON-22, CON-24, CON-68	M	A	A		B	A
ERR-3	CON-21, CON-68	B	M	A		MB	M
ERR-4	CON-23	B	A	MA	M	MB	M
ERR-5	CON-1, CON-11, CON-24, CON-45, CON-47	B	M	A		MB	M

Continuación de la tabla XX.

ERR-6	CON-49, CON-61, CON-66	A	MA	A		B	MA
ERR-7	CON-16, CON-32, CON-70	MB	M	A	A	MB	B
ERR-8	CON-19, CON-23, CON-54	M	A	MA	MA	MB	B
ERR-9	CON-19, CON-23, CON-54	B	MA	MA	MA	MB	B
ERR-10	CON-16, CON-23, CON-55, CON-61	B	M	MA	M	MB	B
ERR-11	CON-35, CON-4, CON-53	M	A	A		B	A
ERR-12	CON-14, CON-19, CON-44	B	A	A	A	MB	B
ERR-13	CON-15, CON-27, CON-43	B	M	A	MA	MB	MB
ERR-14	CON-15, CON-52, CON-57, CON-8	MB	M	MA	MA	MB	MB
ERR-15	CON-19, CON-54, CON-56, CON-60	M	A		MA	M	B
ERR-16	CON-45, CON-69	B	M	A	A	MB	B
ATA-1	CON-13, CON-20, CON-23, CON-29, CON-7	M	A	MA	A	MB	B
ATA-2	CON-13, CON-20, CON-23, CON-29, CON-48, CON-7	M	A	MA	A	MB	B
ATA-3	CON-13, CON-48, CON-6, CON-61	B	A	MA	A	MB	B
ATA-4	CON-29, CON-9	M	A	A	M	B	M
ATA-5	CON-18, CON-49, CON-61, CON-70	M	M	A		B	M
ATA-6	CON-49, CON-61, CON-66	A	MA	A		B	MA
ATA-7	CON-10, CON-16, CON-32, CON-70	B	M	A	A	MB	B
ATA-8	CON-10, CON-13, CON-17, CON-46, CON-48, CON-6	M	A	MA	A	MB	B
ATA-9	CON-13, CON-36, CON-65, CON-71	MB	M	MA	A	MB	B
ATA-10	CON-13, CON-36, CON-65, CON-71	MB	MB	MA	A	MB	MB
ATA-11	CON-19, CON-23, CON-54	B	MA	MA	MA	MB	B
ATA-12	CON-19, CON-23, CON-54	B	MA	MA	MA	MB	B
ATA-13	CON-16, CON-23, CON-55	B	A	MA	M	MB	M
ATA-14	CON-14, CON-19	M	A		MA	M	B
ATA-15	CON-19, CON-54	M	A		MA	M	B
ATA-16	CON-28, CON-4, CON-51, CON-65, CON-66	B	M	MA	MA	MB	MB
ATA-17	CON-19, CON-54, CON-56, CON-60	B	A		MA	B	B
ATA-18	CON-19, CON-54	MB	A		MA	MB	B
ATA-19	CON-67, CON-69	B	M	M	A	B	B

Continuación de la tabla XX.

ATA-20	CON-16, CON-2, CON-70	MB	M	A	M	MB	B
ATA-21	CON-13, CON-49, CON-61, CON-66	B	M	MA		MB	M

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

3.3. Estimación del impacto y riesgo residual

El impacto y riesgo residuales indican el estado de riesgo del sistema, considerando los controles desplegados en los activos para protegerlos de las amenazas identificadas. El objetivo de los controles es llevar a niveles más bajos de impacto y riesgo al sistema de información.

3.3.1. Estimación del impacto residual

Para estimar el impacto residual se toman los valores del activo en cada dimensión de seguridad, y los nuevos valores de degradación de la amenaza en cada dimensión de seguridad; utilizando el análisis de tablas, se determina el valor del impacto residual. Las referencias a la valoración serán las mismas que se utilizaron durante la estimación del impacto potencial (tabla IX); así también la metodología.

Tabla XXI. **Impacto residual en la dimensión de integridad de los activos**

Amenaza	Impacto	Activos afectados en su dimensión de integridad
ERR-1	Alto	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Medio	INF-1, INF-5, INF-6, INF-7, INF-8, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4

Continuación de la tabla XXI.

ERR-2	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	SW-1, SW-2
ERR-3	Alto	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11
	Medio	INF-1, INF-5, INF-6, INF-7, INF-8
ERR-4	Alto	INF-2, INF-3, INF-4, INF-9
	Medio	INF-1, INF-5, INF-6, INF-7, INF-8
ERR-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ERR-8	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	SW-1, SW-2
ERR-11	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ERR-12	Medio	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-1, SW-2
ATA-1	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-2	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12
ATA-3	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31
	Bajo	SW-1, SW-2
ATA-4	Alto	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31
	Medio	INF-1, INF-5, INF-6, INF-7, INF-8, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SW-1, SW-2, SW-8, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-32, HW-33

Continuación de la tabla XXI.

ATA-5	Alto	SEI-1, SEI-2, SEI-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, INS-1, INS-2, INS-3, INS-6, INS-7, INS-8
	Medio	SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SW-1, SW-2, SW-8, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-4, INS-5, INS-9
ATA-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ATA-8	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9
	Bajo	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-10	Medio	HW-28, HW-29, HW-30, HW-31
	Bajo	HW-32, HW-33
ATA-11	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	SW-1, SW-2
ATA-14	Medio	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-1, SW-2
ATA-20	Medio	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Alto	PER-2, PER-3, PER-4, PER-5, PER-17, PER-18
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XXII. **Impacto residual en la dimensión de confidencialidad de los activos**

Amenaza	Impacto	Activos afectados en su dimensión de confidencialidad
ERR-1	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	INF-6, INF-7, INF-11, SEI-2, SEI-7
	Bajo	SW-1, SW-2
ERR-2	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	SW-1, SW-2
ERR-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-1, SW-2
ERR-7	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SW-1, SW-2
ERR-10	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4, PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Bajo	PER-1
	Muy bajo	SW-1, SW-2
ERR-11	Alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-1, SW-2
ERR-15	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-2	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12

Continuación de la tabla XXII.

ATA-3	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31
	Muy bajo	SW-1, SW-2
ATA-4	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-32, HW-33
	Medio	INF-6, INF-7, INF-11, SEI-2, SEI-7, HW-15, HW-16, HW-28, HW-29, HW-30, HW-31
	Bajo	SW-1, SW-2
ATA-5	Alto	SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-8, INS-9
	Medio	SEI-2, SEI-7, HW-15, HW-16, HW-28, HW-29, HW-30, HW-31, INS-5
	Bajo	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
ATA-7	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
	Muy bajo	SW-1, SW-2
ATA-8	Medio	INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9
	Muy bajo	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-9	Medio	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-10	Medio	HW-32, HW-33
	Bajo	HW-28, HW-29, HW-30, HW-31

Continuación de la tabla XXII.

ATA-13	Alto	INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	INF-6, INF-7, INF-11, SEI-2, SEI-7, SW-1, SW-2
ATA-14	Medio	SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Muy bajo	SW-1, SW-2
ATA-15	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-17	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-20	Medio	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Alto	PER-2, PER-3, PER-4, PER-5, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Medio	PER-6, PER-7

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XXIII. **Impacto residual en la dimensión de disponibilidad de los activos**

Amenaza	Impacto	Activos afectados en su dimensión de disponibilidad
NAT-1	Alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9

Continuación de la tabla XXIII.

NAT-2	Alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
NAT-3	Alto	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Medio	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
IND-1	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-9
	Bajo	INS-5, INS-8
IND-2	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-9
	Bajo	INS-5, INS-8
IND-3	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-9
	Bajo	INS-5, INS-8
IND-4	Medio	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4

Continuación de la tabla XXIII.

IND-5	Medio	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
	Bajo	SW-2
IND-6	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-1, AUX-2, AUX-3, AUX-4
IND-7	Alto	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
IND-8	Medio	HW-28, HW-29, HW-30, HW-31
	Bajo	HW-32, HW-33
IND-9	Medio	AUX-1, AUX-3
	Bajo	AUX-2, AUX-4
IND-10	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ERR-1	Alto	INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7
	Medio	INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
ERR-2	Alto	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4
	Medio	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2

Continuación de la tabla XXIII.

ERR-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ERR-9	Medio	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ERR-11	Alto	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Medio	SW-2
ERR-12	Medio	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-2
ERR-13	Medio	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4
ERR-14	Medio	SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31
	Bajo	SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33
ERR-15	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ERR-16	Medio	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-18
	Bajo	PER-17
ATA-2	Medio	SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12
	Bajo	SEI-7, SEI-8, SEI-10
ATA-3	Medio	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, HW-28, HW-29, HW-30, HW-31
	Bajo	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2

Continuación de la tabla XXIII.

ATA-4	Alto	INF-2, INF-3, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31
	Medio	INF-1, INF-4, INF-5, INF-6, INF-7, INF-8, INF-11, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33
ATA-5	Alto	SEI-1, SEI-2, SEI-3, SEI-11, SEI-12, SW-3, SW-4, SW-5, SW-6, SW-7, HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, AUX-1, AUX-3, INS-1, INS-2, INS-3, INS-6
	Medio	SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, SEI-10, SW-1, SW-2, SW-8, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9
ATA-6	Muy alto	SW-3, SW-4, SW-5, SW-6, SW-7
	Alto	SW-1, SW-2, SW-8
ATA-10	Medio	HW-28, HW-29, HW-30, HW-31
	Bajo	HW-32, HW-33
ATA-12	Medio	INF-1, INF-2, INF-3, INF-8, INF-9, INF-10, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-9, SEI-11, SEI-12, SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8, SOP-1, SOP-2, SOP-3, SOP-4
	Bajo	INF-4, INF-5, INF-6, INF-7, INF-11, SEI-7, SEI-8, SEI-10, SW-2
ATA-14	Medio	SW-1, SW-3, SW-4, SW-5, SW-6, SW-7, SW-8
	Bajo	SW-2
ATA-15	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ATA-16	Medio	HW-1, HW-2, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31
	Bajo	HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-32, HW-33

Continuación de la tabla XXIII.

ATA-17	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4
ATA-18	Medio	HW-1, HW-2, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-6, INS-7, INS-9
	Bajo	INS-5, INS-8
ATA-19	Medio	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-18
	Bajo	PER-17
ATA-20	Medio	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-18
	Bajo	PER-17
ATA-21	Alto	PER-2, PER-3, PER-4, PER-5
	Medio	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

3.3.2. Estimación del riesgo residual

Para estimar el riesgo residual se toman los valores del impacto residual en cada dimensión de seguridad, y los nuevos valores de probabilidad de la amenaza; utilizando el análisis de tablas, se determina el valor del riesgo residual. Las referencias a la valoración serán las mismas usadas durante la estimación del impacto potencial (tabla XIII), así como la metodología.

Tabla XXIV. **Riesgo residual en la dimensión de integridad de los activos**

Amenaza	Riesgo	Activos afectados
ERR-1	Bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, SOP-1, SOP-2, SOP-3, SOP-4, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ERR-2	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-1, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ERR-3	Bajo	INF-2, INF-3, INF-4, INF-9, INF-10, INF-11
	Muy bajo	INF-1, INF-5, INF-6, INF-7, INF-8
ERR-4	Bajo	INF-2, INF-3, INF-4, INF-9
	Muy bajo	INF-1, INF-5, INF-6, INF-7, INF-8
ERR-6	Medio	SW-5, SW-6, SW-7, SW-3, SW-4
	Bajo	SW-8, SW-1, SW-2
ERR-8	Muy bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SOP-1, SOP-2, SOP-3, SOP-4, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ERR-11	Bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3
ERR-12	Muy bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3
ATA-1	Muy bajo	SEI-9, SEI-10, SEI-11, SEI-12, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ATA-2	Muy bajo	SEI-9, SEI-10, SEI-11, SEI-12, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ATA-3	Muy bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-28, HW-29, HW-30, HW-31, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ATA-4	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22

Continuación de la tabla XXIV.

ATA-5	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ATA-6	Medio	SW-5, SW-6, SW-7, SW-3, SW-4
	Bajo	SW-8, SW-1, SW-2
ATA-8	Muy bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
ATA-10	Muy bajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-11	Muy bajo	SW-5, SW-6, SW-7, SW-8, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, SOP-2, SOP-3, SOP-4, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9
ATA-14	Bajo	SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3, SW-4
ATA-20	Muy bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Bajo	PER-2, PER-3, PER-4, PER-5, PER-17, PER-18
	Muy bajo	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XXV. **Riesgo residual en la dimensión de confidencialidad de los activos**

Amenaza	Riesgo	Activos afectados
ERR-1	Bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SOP-1, SOP-2, SOP-3, SOP-4, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
	Muy bajo	SW-1, SW-2
ERR-2	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-1, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
	Muy bajo	SW-1, SW-2
ERR-6	Medio	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Bajo	SW-1, SW-2
ERR-7	Muy bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ERR-10	Muy bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SOP-1, SOP-2, SOP-3, SOP-4, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, PER-1, PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ERR-11	Bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SW-3
	Muy bajo	SW-1, SW-2
ERR-15	Bajo	HW-1, HW-2, HW-3, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, SOP-1, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-2	Muy bajo	SEI-9, SEI-10, SEI-11, SEI-12, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ATA-3	Muy bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-28, HW-29, HW-30, HW-31, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8

Continuación de la tabla XXV.

ATA-4	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
	Muy bajo	SW-1, SW-2
ATA-5	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, SOP-1, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
	Muy bajo	SW-1, SW-2, AUX-1, AUX-2, AUX-3, AUX-4
ATA-6	Medio	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Bajo	SW-1, SW-2
ATA-7	Muy bajo	SEI-1, SW-5, SW-6, SW-7, SW-8, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9
ATA-8	Muy bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
ATA-9	Muy bajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-10	Muy bajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33
ATA-13	Bajo	SEI-9, SW-5, SW-6, SW-7, SW-8, SEI-10, SEI-11, SEI-12, SW-3, SW-4, SOP-2, SOP-3, SOP-4, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-8, INF-9, INF-10, SEI-1, SEI-3, SEI-4, SEI-5, SEI-6, SEI-8
	Muy bajo	SW-1, SW-2, INF-6, INF-7, INF-11, SEI-2, SEI-7
ATA-14	Bajo	SW-5, SW-6, SW-7, SW-8, SW-3, SW-4
	Muy bajo	SW-1, SW-2

Continuación de la tabla XXV.

ATA-15	Bajo	HW-1, HW-2, HW-3, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, SOP-1, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-17	Bajo	HW-1, HW-2, HW-3, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, SOP-1, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
ATA-20	Muy bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Bajo	PER-2, PER-3, PER-4, PER-5, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
	Muy bajo	PER-6, PER-7

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Tabla XXVI. **Riesgo residual en la dimensión de disponibilidad de los activos**

Amenaza	Riesgo	Activos afectados
NAT-1	Bajo	HW-1, HW-2, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
NAT-2	Medio	HW-1, HW-2, HW-26, HW-27, HW-28, AUX-1, AUX-3, HW-29, HW-30, HW-31, INS-1, INS-2, INS-3, INS-6, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14
	Bajo	HW-23, HW-24, HW-25, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, HW-32, HW-33, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22

Continuación de la tabla XXVI.

NAT-3	Medio	HW-1, HW-2, HW-26, HW-27, HW-28, AUX-1, AUX-3, HW-29, HW-30, HW-31, INS-1, INS-2, INS-3, INS-6, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14
	Bajo	HW-23, HW-24, HW-25, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, HW-32, HW-33, AUX-4, INS-4, INS-5, INS-7, INS-8, INS-9, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-1	Muy bajo	HW-1, HW-2, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-2	Muy bajo	HW-1, HW-2, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-3	Muy bajo	HW-1, HW-2, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-4	Bajo	HW-1, HW-2, HW-26, HW-27, HW-28, AUX-1, AUX-3, HW-29, HW-30, HW-31, HW-3, HW-4, HW-11, HW-12, HW-13, HW-14
	Muy bajo	HW-23, HW-24, HW-25, SOP-1, SOP-2, SOP-3, SOP-4, AUX-2, HW-32, HW-33, AUX-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-5	Bajo	SW-4, SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, SW-1, SW-3, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-3, AUX-4, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
	Muy bajo	SW-2

Continuación de la tabla XXVI.

IND-6	Bajo	HW-1, HW-2, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, AUX-1, AUX-2, HW-29, HW-30, HW-31, HW-32, HW-33, AUX-3, AUX-4, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-7	Bajo	HW-1, HW-2, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, HW-29, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-3, AUX-4, HW-3, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
IND-8	Bajo	HW-28, HW-29, HW-30, HW-31
	Muy bajo	HW-32, HW-33
IND-9	Muy bajo	AUX-1, AUX-2, AUX-3, AUX-4
IND-10	Bajo	HW-1, HW-2, HW-3, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-1, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, AUX-4, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ERR-1	Bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, SOP-1, SOP-2, SOP-3, SOP-4, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ERR-2	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-1, SOP-2, SOP-3, SOP-4, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ERR-5	Bajo	PER-2, PER-3, PER-4, PER-5
	Muy bajo	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ERR-6	Medio	SW-5, SW-6, SW-7, SW-3, SW-4
	Bajo	SW-8, SW-1, SW-2
ERR-9	Muy bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SOP-1, SOP-2, SOP-3, SOP-4, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ERR-11	Bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3
ERR-12	Muy bajo	SW-4, SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3

Continuación de la tabla XXVI.

ERR-13	Muy bajo	HW-1, HW-2, HW-3, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ERR-14	Muy Bajo	HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ERR-15	Bajo	HW-1, HW-2, HW-3, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ERR-16	Muy bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-2	Muy bajo	SEI-9, SEI-10, SEI-11, SEI-12, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ATA-3	Muy bajo	SW-5, SW-6, SW-7, SW-8, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-28, HW-29, HW-30, HW-31, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8
ATA-4	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ATA-5	Bajo	SW-5, SW-6, SW-7, SW-8, HW-1, HW-2, HW-3, SEI-9, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ATA-6	Medio	SW-5, SW-6, SW-7, SW-3, SW-4
	Bajo	SW-8, SW-1, SW-2
ATA-10	Muy bajo	HW-28, HW-29, HW-30, HW-31, HW-32, HW-33

Continuación de la tabla XXVI.

ATA-12	Muy bajo	SW-5, SW-6, SW-7, SW-8, SEI-10, SEI-11, SEI-12, SW-1, SW-2, SW-3, SW-4, SOP-2, SOP-3, SOP-4, SOP-1, INF-1, INF-2, INF-3, INF-4, INF-5, INF-6, INF-7, INF-8, INF-9, INF-10, INF-11, SEI-1, SEI-2, SEI-3, SEI-4, SEI-5, SEI-6, SEI-7, SEI-8, SEI-9
ATA-14	Bajo	SW-5, SW-6, SW-7, SW-8, SW-1, SW-2, SW-3, SW-4
ATA-15	Bajo	HW-1, HW-2, HW-3, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
ATA-16	Muy bajo	HW-1, HW-2, HW-3, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, HW-30, HW-31, HW-32, HW-33, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
ATA-17	Bajo	HW-1, HW-2, HW-3, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22, HW-23
ATA-18	Muy bajo	HW-1, HW-2, HW-3, HW-23, HW-24, HW-25, HW-26, HW-27, HW-28, HW-29, SOP-2, SOP-3, SOP-4, AUX-1, AUX-2, AUX-3, HW-30, HW-31, HW-32, HW-33, SOP-1, AUX-4, INS-1, INS-2, INS-3, INS-4, INS-5, INS-6, INS-7, INS-8, INS-9, HW-4, HW-5, HW-6, HW-7, HW-8, HW-9, HW-10, HW-11, HW-12, HW-13, HW-14, HW-15, HW-16, HW-17, HW-18, HW-19, HW-20, HW-21, HW-22
ATA-19	Bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-18
	Muy bajo	PER-17
ATA-20	Muy bajo	PER-2, PER-3, PER-4, PER-5, PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18
ATA-21	Bajo	PER-2, PER-3, PER-4, PER-5
	Muy bajo	PER-6, PER-7, PER-8, PER-9, PER-10, PER-11, PER-12, PER-13, PER-14, PER-15, PER-16, PER-17, PER-18

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

4. GESTIÓN DE RIESGOS

La gestión de riesgo indica las acciones que la organización debe tomar para llevar los niveles de riesgo hacia valores fijados como aceptados. En el presente capítulo se analiza e interpreta el estado de riesgo del sistema de información con el que se genera un conjunto de guías que ayudarán a la organización en la toma de decisiones para la gestión de los riesgos.

4.1. Interpretación del estado de riesgo

El estado de riesgo se origina del análisis del impacto y riesgo potenciales y residuales. En el capítulo anterior se utilizó el método de análisis mediante tablas para determinar los valores mencionados, cuyos resultados requieren una interpretación con el fin de dar a conocer a la organización del estado de seguridad del sistema de información.

4.1.1. Impacto y riesgo potencial

Los valores de impacto potencial indican la gravedad del daño ocasionado por la amenaza al valor de un activo en sus diferentes dimensiones de seguridad. Se debe realizar esta valoración en cada dimensión, puesto que cada activo es importante en alguna o varias de estas propiedades. Los valores potenciales no consideran la existencia de controles; es el escenario extremo donde el sistema de información está expuesto a cualquier amenaza posible. Las tablas X, XI y XII muestran para cada amenaza el valor de impacto (asignado también con un color) y el conjunto de activos afectados.

Se puede apreciar que la mayoría de las amenazas tendrán un impacto alto sobre una gran cantidad de activos; esto indica que los daños causados serán graves en su mayoría debido al valor otorgado a los activos. También se observa que la dimensión con mayores amenazas es la de la disponibilidad.

Los valores de riesgo potencial son una medida del impacto potencial y la probabilidad de que ocurra en sus distintas dimensiones de seguridad. Las tablas XIII, XIV y XV muestran para cada amenaza el valor de riesgo y el conjunto de activos afectados; se observa que estos valores están mayormente distribuidos en los niveles medios. La disponibilidad es la dimensión con mayor cantidad de amenazas, por consiguiente, también de activos afectados.

Potencialmente, las amenazas identificadas para el sistema tienen impactos altos y riesgos que van de bajos a medios. Esto indica que el sistema está compuesto por muchos activos valorados como altos o muy altos, que es un parámetro de confianza sobre el análisis, el cual se ha enfocado en aquellos activos que se consideran más importantes para la organización.

El estado de riesgo potencial del sistema es considerado medio, es decir, sus elementos se consideran de alto valor, y hay presencia de una cantidad considerable de amenazas en el sistema, pero las probabilidades de materialización son medias o bajas mayormente, teniendo en cuenta que se deben considerar los casos con niveles de riesgo altos y muy altos presenten en algunos activos, ya que estos indican valores de impacto (activos de gran valor) y probabilidad alta.

4.1.2. Impacto y riesgos residuales

En los valores residuales se consideran los controles propuestos; estos tienen una valoración de eficacia que reduce el daño o disminuye la probabilidad de ocurrencia de la amenaza, lo que conlleva a una reducción en el impacto potencial y una disminución en el riesgo potencial. Las tablas XXI, XXII y XXIII muestran cada amenaza con sus valores de impacto residual y el conjunto de activos afectados en cada dimensión de seguridad. Los nuevos valores de impacto se reducen o mantienen (debido a la ausencia de controles de impacto en algunas amenazas), se observan niveles medios y bajos en comparación con los iniciales, lo que indica que los controles cumplen con su función de minimización de los daños para la mayoría de las amenazas.

El riesgo residual, después de aplicar la eficacia de los controles, se detalla en las tablas XXV, XXVI y XXVII; las cuales muestran por cada dimensión de seguridad del activo, cada amenaza con sus valores de riesgo residual y el conjunto de activos afectados. Se observa que los niveles de riesgo cambian a niveles más bajos (en su mayoría de niveles bajos y muy bajos); esto es un indicador de que gran parte de los controles tiene una característica preventiva ante las amenazas. Los controles, en su característica preventiva o correctiva, deben ser complementarios entre sí, es decir, que si no se cuenta con un control preventivo se debe buscar un control correctivo o que disminuya el impacto y en caso contrario, si no se cuentan o no existen controles correctivos se deben buscar controles preventivos.

En la interpretación de los valores residuales, el sistema se ve afectado positivamente con la inclusión de los controles propuestos, notándose que los valores potenciales que en su mayoría son altos y medios, cambian a niveles más b2ajos y manejables para la organización.

Es viable la aplicación del conjunto de controles y tendrá una repercusión de aumento de la seguridad y protección del sistema de información de la organización.

4.2. Aceptación del riesgo

La organización, a través de sus directivos, debe tomar las decisiones respecto del nivel de riesgo que desean asumir. Los valores de impacto y riesgo residuales son parámetros para determinar el nivel de aceptación de los riesgos con base en sus factores institucionales como objetivos, políticas, metas, contratos y otros que se consideren relevantes. La organización puede establecer estos niveles analizando individualmente los activos por agrupaciones o áreas de prioridad como los departamentos, enfocándose en una dimensión específica o cualquier otro enfoque de análisis para la aceptación.

4.2.1. Criterios

Es un conjunto de reglas para las decisiones de aceptación que se toman en función del nivel de riesgo. Sirven como guía para la organización sobre qué planteamiento debe utilizar frente a un estado de riesgo. La organización puede hacer uso de los criterios que mejor se adecuen a sus objetivos de seguridad, a manera simple se proponen los siguientes:

- El nivel de riesgo se considera aceptable si el riesgo es bajo o muy bajo.
- El nivel de riesgo se considera aceptable y susceptible a mejora si el riesgo es medio.
- No se considera aceptable el nivel de riesgo si es alto y no se implementan medidas de protección específicas.
- Si es muy alto, no se considera aceptable el nivel de riesgo.

La dirección de la organización será quien conozca y tome la decisión de la aceptación de los niveles de riesgo.

4.3. Modificación de los niveles de riesgo

Posterior al proceso de aceptación de los riesgos, se determina qué hacer para llegar a los niveles deseados tomando como base dos principios:

- Reducción del valor del riesgo residual: cuando se determina que el riesgo aceptado debe ser menor al residual. Considerado cuando se tienen valores de riesgo, altos o muy altos, donde no es conveniente mantener el nivel actual y deba reducirse hasta niveles aceptables.

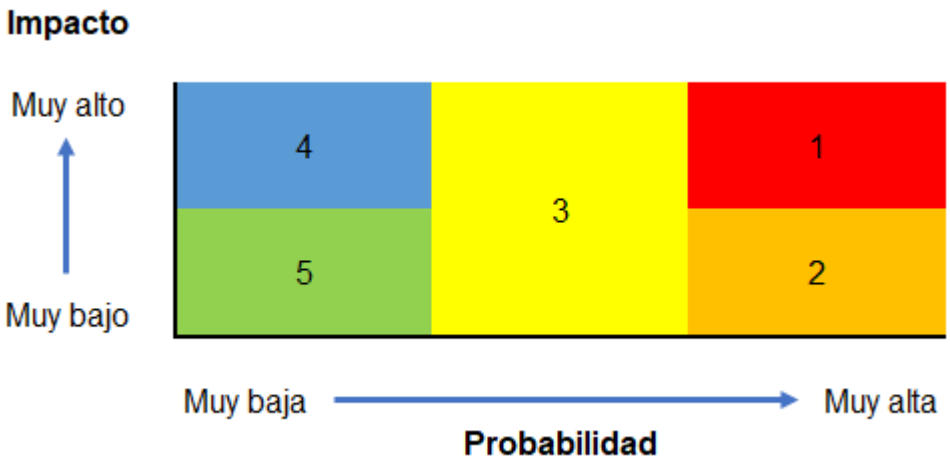
- Aumento del valor del riesgo residual: cuando se determina que el riesgo aceptado podrá ser mayor al riesgo residual. Considerado en situaciones donde el valor del riego es bajo o muy bajo y no es conveniente mantener niveles bajos si el valor del activo o los objetivos de la organización no lo justifican.

Para cada caso es conveniente considerar factores de interés para la organización como sus políticas internas, contratos con los socios de negocios, implicaciones legales, imagen y reputación, competitividad en el mercado entre otros más que podrán tomarse en cuenta durante el análisis de las modificaciones.

4.3.1. Regiones de riesgo

Colocando los valores de riesgo en una gráfica de impacto y probabilidad, se observan 4 regiones:

Figura 17. **Regiones de riesgo**



Fuente: elaboración propia, utilizando Microsoft Excel 2016.

En cada región se tomarán consideraciones para la modificación del nivel de riesgo:

- Región 1: probabilidades e impactos altos, esta región es la más crítica y debe trasladarse a regiones de menor riesgo.

- Región 2: probabilidades altas e impactos bajos, las opciones de traslado pueden realizarse a regiones medias o considerarse dejar el riesgo en esta región, el valor del activo podría no justificar su modificación.

- Región 3: probabilidades medias, las opciones de manejo son relativas al valor del impacto.

- Región 4: probabilidades bajas e impactos altos, el traslado a regiones de menor riesgo podría no justificarse, pero la organización debe prever acciones correctivas o de minimización de los daños.

- Región 5: probabilidades e impactos bajos, puede trasladarse a regiones de mayor riesgo si las acciones de control podrían invertirse en otras amenazas, o no se toma ninguna acción de modificación y se dejan en esta región.

4.4. Estudio costo-beneficio

El objetivo del estudio es cuantificar el costo para la organización de la implementación de los controles propuestos y compararlo con los beneficios obtenidos de estos para determinar si la solución es factible para la organización. El proyecto no tiene una valoración cuantitativa o monetaria de los beneficios, no se puede determinar un posible ingreso o retorno de la inversión debido a que estos son intangibles, pero su implementación puede tener beneficios tangibles potenciales si el aumento de la seguridad de sus sistemas de información son un aspecto relevante en las relaciones comerciales presentes y futuras, pero no es conveniente cuantificar estos supuestos.

Si es posible determinar una aproximación del costo de la solución, en algunos casos, el costo será monetario y en otros serán recursos administrativos u operativos de la organización, es decir los recursos con los que cuenta son capaces de realizar esas actividades. Se define entonces un análisis costo-beneficio de tipo mixto, cuantitativo y cualitativo, presentado en la siguiente tabla:

Tabla XXVII. **Costos y beneficios**

Control	Costo	Beneficios
CON-1	Actividades administrativas	Mejora la productividad y eficiencia del personal
		Previene conflictos laborales
		Fortalecimiento en la toma de decisiones de jefes
		Procesos con trasparencia y justicia para los empleados
		Mejora del ambiente y clima laboral
CON-2	Actividades administrativas	Previene conflictos laborales
		Disuade a las personas de realizar actos indebidos
CON-3	Q 10 000,00	Mejora las condiciones de operaciones de los activos
		Prolonga la vida útil de los activos
		Previene accesos no autorizados
		Previene el deterioro de los activos
CON-4	Actividades técnicas	Aumenta la seguridad del software, equipos e información que utiliza
		Mejora el rendimiento de los equipos
		Evita utilizar software innecesario u obsoleto
		Satisfacen nuevas necesidades de la organización
CON-5	Actividades operativas	Previene incendios
CON-6	Actividades operativas	Previene actividades no autorizadas
		Previene daños a los activos
CON-7	Actividades operativas	Asegura la continuidad y correcto funcionamiento de los servicios
CON-8	Q 5 000,00	Asegura la continuidad y correcto funcionamiento de los servicios
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
CON-9	Actividades operativas	Previene daños a los activos
		Ordena y mejora los controles y procesos internos
		Genera confianza a los usuarios internos y externos
CON-10	Actividades operativas	Asegura la continuidad y correcto funcionamiento de los servicios
		Genera confianza a los usuarios externos de los servicios
CON-11	Q 2 000,00	Incremento de la productividad
		Minimiza los errores de los usuarios
		Aumenta la confianza en la ejecución de tareas
CON-12	Q 8 000,00	Evita sobrecalentamiento y deterioro de los equipos
		Mejora el rendimiento de los equipos

Continuación de la tabla XXVII.

CON-13	Actividades técnicas	Reduce la posibilidad de fraudes
		Mejora la percepción de la seguridad en usuarios internos y externos
		Mayor confianza en los servicios
CON-14	Actividades técnicas	Evita la pérdida total de información
		Reduce los tiempos de restablecimiento de servicios
		Aumento de la competitividad en el mercado
CON-15	Q 30 000,00	Asegura la continuidad y correcto funcionamiento de los servicios
		Reduce los tiempos de restablecimiento de servicios
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
CON-16	Q 5 000,00	Protege información delicada del negocio de uso malintencionado o divulgación
		Evita problemas legales con las partes
		Disuade a las personas de realizar actos indebidos
CON-17	Q 4 000,00	Evita daños malintencionados
		Privacidad de los activos de información
		Genera confianza a los usuarios internos y externos
CON-18	Actividades administrativas	Previene conflictos laborales
		Limita las acciones de las personas de la organización
		Mejor uso de los recursos disponibles
		Mejora la productividad y eficiencia del personal
		Determina los compromisos que se adquieren para la protección de la información
CON-19	Actividades técnicas	Disponibilidad inmediata de restauración de información, equipos y servicios
		Evita la pérdida total de información
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
CON-20	Q 6 000,00	Previene o alerta intentos de ataques a los activos por usuarios externos
		Controlar los flujos de información de las operaciones
		Optimiza el rendimiento de la red
		Incremento de la productividad de los usuarios
CON-21	Actividades administrativas	Optimiza el proceso de reclutamiento y selección
		Minimiza los errores en la ejecución de las tareas
		Ayuda a definir una estructura organizacional

Continuación de la tabla XXVII.

CON-22	Actividades administrativas	Ayuda a la medición del desempeño del personal
		Asegura tener a las personas competentes para los puestos correctos
		Minimiza los errores en la ejecución de las tareas
		Mejora la productividad y eficiencia del personal
CON-23	Actividades técnico-administrativas	Se tiene el control de quién tiene acceso a los activos de información
		Se tiene control de las acciones permitidas a realizar en los activos de información
		Genera confianza a los usuarios internos y externos
		Evita errores involuntarios y ataques intencionados
CON-24	Actividades administrativas	Reduce el tiempo de integración del empleado con el puesto de trabajo
		El personal conocerá los objetivos de la organización sobre los que debe guiar sus funciones
		Mejora el rendimiento del personal
		Aumenta la confianza en la ejecución de tareas
		Evita errores del personal al proporcionar la información necesaria del puesto y organización
CON-25	Q 6 000,00	Reduce accidentes en el personal
		Reduce daños a los activos de información
		Reduce los daños a las instalaciones de la organización
		Evita daños a instalaciones de terceros
CON-26	Q 9 000,00	Asegura la continuidad de las operaciones del negocio
		Asegura la continuidad operativa de los equipos y servicios
		Aumento de la competitividad en el mercado
CON-27	Q 10 000,00	Asegura la continuidad de las operaciones del negocio
CON-28	Actividades técnicas	Evita ataques a activos críticos de información, principalmente a los servicios públicos
		Restricción de acceso de usuarios no autorizados a las redes de la organización
		Evita el robo de información
CON-29	Actividades administrativas	La estructura de aprobación de cambios evita acciones no autorizadas a los activos de información
		Genera confianza a los usuarios internos y externos
		Aumenta la confianza en la ejecución de tareas
CON-30	Actividades técnico - administrativas	Se trasladan los costos de reparación al proveedor

Continuación de la tabla XXVII.

CON-31	Q 12 000,00	Evita costos correctivos o de reparación
		Evita daños a los activos de información
		Previene daños en las instalaciones a largo plazo
CON-32	Actividades administrativas	Disuade a las personas de realizar actos indebidos
CON-33	Q 6 000,00	Mantiene los ambientes libres de humedad en exceso
		Previene la corrosión de los equipos, superficies metálicas y tuberías.
		Evita la degradación de las estructuras de las instalaciones
CON-34	Q 2 000,00	Protege los equipos eléctricos por sobrevoltajes
		Evita accidentes eléctricos en las instalaciones
		Protege a las personas dentro de las instalaciones
CON-35	Q 6 800,00	Evita problemas legales
		Mejora el rendimiento de los equipos
		Mejora la productividad y eficiencia del personal
		Refuerza la seguridad de la información manejada por el software
CON-36	Actividades técnicas	Previene o alerta intentos de ataques y robo de información de usuarios externos
		Asegura que los receptores de la información sean correctos
		Si la información es interceptada no podrá ser interpretada ni utilizada
CON-37	Q 6 000, 00	Prolonga la vida útil de los activos
		Mejora el rendimiento de los equipos
		Mejora la productividad y eficiencia de los usuarios
		Evita costos correctivos o de reparación
CON-38	Q 4 000, 00	Previene daños a equipos eléctricos
		Previene incendios
		Evita accidentes eléctricos en las instalaciones
		Evita costos correctivos o de reparación
CON-39	Q 4 000,00	Aumenta la vida útil de los sistemas de canalización de aguas
		Previene accidentes ocasionados por agua
		Evita costos correctivos o de reparación

Continuación de la tabla XXVII.

CON-40	Q 9 000,00	Aumenta la vida útil de los sistemas de climatización
		Mejora el rendimiento de los equipos
		Previene accidentes ocasionados por agua
		Previene daños colaterales a los equipos
		Evita costos correctivos o de reparación
CON-41	Q 3 000,00	Aumenta la vida útil de los sistemas de desagüe y transporte de agua
		Previene accidentes ocasionados por agua
		Previene daños colaterales a los equipos
		Evita costos correctivos o de reparación
CON-42	Q 10 000,00	Aumenta la vida útil de las instalaciones y estructuras
		Evita daños por contaminación a los equipos
		Las actividades del personal se realizan en un ambiente ordenado y limpio, lo que aumenta el rendimiento y productividad
		Evita costos correctivos o de reparación
CON-43	Actividades técnicas	Previene daños a los activos
		Asegura la continuidad operativa de los equipos y servicios
		Evita costos de personal especializado
CON-44	Actividades técnicas	Previene daños al software
		Asegura la continuidad operativa de los equipos y servicios
		Evita costos de personal especializado
		Aumento de la competitividad en el mercado
CON-45	Actividades técnicas	Disminuye las malas ejecuciones en las tareas
		Evita malentendidos en las operaciones
		Conocimiento claro de las acciones y parámetros al realizar una tarea
CON-46	Actividades operativas	Previene o minimiza daños a los activos
		Previene la divulgación de información confidencial
CON-47	Actividades administrativas	Ayuda a la medición del desempeño del personal
		Asegura tener a las personas competentes para los puestos correctos
		Minimiza los errores en la ejecución de las tareas
		Mejora la productividad y eficiencia del personal
CON-48	Actividades técnicas	Evita daños a los activos de información
		Evita accesos no autorizados, suplantaciones o robo de identidad
		Previenen la ingeniería social

Continuación de la tabla XXVII.

CON-49	Actividades técnico-administrativas	Evita daños a los activos de información
		Previene que software malintencionado ingrese en la red y equipos del sistema, y cause daños a la información.
		Mejora la productividad y eficiencia del personal
		Optimiza el rendimiento de la red
		Aumento de la competitividad en el mercado
CON-50	Q 35 000,00	Asegura la continuidad operativa de los equipos y servicios
		Asegura la continuidad de las operaciones del negocio
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
		Aumento de la competitividad en el mercado
CON-51	Q 3 000,00	Asegura la continuidad operativa de los equipos y servicios
		Asegura la continuidad de las operaciones del negocio
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
CON-52	Q 35 000,00	Mejora la productividad y eficiencia del personal
		Mejora la productividad y eficiencia de los servicios
		Aumento de la competitividad en el mercado
CON-53	Q 4 000,00	Mejora la productividad y eficiencia del personal
		Mejora la productividad y eficiencia de los servicios
		Mejora el rendimiento de los equipos
		Aumenta la seguridad del software, equipos e información que utiliza
CON-54	Q 15 000,00	Disponibilidad inmediata de restauración de información, equipos y servicios al contar con respaldos automáticos
		Evita la pérdida total de información
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
		Evita el uso de dispositivos de almacenamiento, que generan costo y son propensos a degradación, robo, perdida y daños
CON-55	Actividades técnico-administrativas	Evita la destrucción, robo, divulgación y daños a la documentación
		Cumplimientos legales de resguardo de documentos fiscales y contables
CON-56	Actividades técnicas	Evita el robo y divulgación de información contenida en los equipos
		Previenen el mal uso de la información y extorsión

Continuación de la tabla XXVII.

CON-57	Actividades operativas	Asegura la continuidad operativa de los equipos y servicios
		Asegura la continuidad de las operaciones del negocio
		Mantiene el cumplimiento de los acuerdos de servicio con los clientes
CON-58	Q 2 500,00	Se recupera parte del costo del equipo asegurado
CON-59	Q 3 000,00	Se recupera parte del costo de lo asegurado
CON-60	Q 2 000,00	Se recupera parte del costo del equipo asegurado
		Aumento de la competitividad en el mercado
CON-61	Q 8 000,00	Genera buenos hábitos en el personal sobre seguridad de la información
		Incrementa la seguridad en la organización lo que mejora su imagen
		Orienta al personal al cumplimiento de los objetivos de la empresa
		Genera acciones de vigilancia en las personas evitando que alguien más incurra en acciones riesgosas
CON-62	Q 30 000,00	Asegura la continuidad operativa de los equipos y servicios
		Disponibilidad de suministro de energía
		Protege a los equipos por sobrecargas
CON-63	Q 12 000,00	Alerta accidentes ocasionados por agua y disminuye el daño
		Minimiza costos correctivos o de reparación
CON-64	Q 8 000,00	Reduce el daño ocasionado por un incendio
		Reduce daños a los activos de información
		Reduce daños a las instalaciones de la organización
		Evita daños a instalaciones de terceros
CON-65	Q 3 000,00	Previene o alerta intentos de ataques a los activos por usuarios externos
		Asegura la continuidad y correcto funcionamiento de los servicios
		Evita ataques a activos críticos de información, principalmente a los servicios públicos
CON-66	Q 4 000,00	Evita daños a los activos de información
		Previene que software malintencionado ingrese en la red y equipos del sistema, y cause daños como robo, destrucción o secuestro de información.
		Aumenta la seguridad del software, equipos e información que utiliza

Continuación de la tabla XXVII.

CON-67	Actividades administrativas	Reduce costos por contratación de personal
		Contar con personal experimentado y capacitado, lo que minimiza los errores en el manejo de activos
		Compartir responsabilidades con la empresa proveedora
		Contar con servicios profesionales para el tratamiento de algunos aspectos de seguridad de información, permite a la organización orientar los esfuerzos a los procesos de negocio
		No es necesario modificar la estructura de la organización para introducir personal especializado
CON-68	Actividades administrativas	Genera confianza a los usuarios internos y externos
		Ordena y mejora los controles y procesos internos
		Reduce costos asociados a la corrección de errores
CON-69	Actividades administrativas	Reduce costos operativos relacionados al mantenimiento y atención del personal
		Puede mejorar la productividad y eficiencia del personal
		Mejora la percepción del personal hacia la organización
		Los accesos a activos de información son más limitados lo que evita la interceptación y divulgación.
CON-70	Actividades administrativas	Previene conflictos laborales
		Limita las acciones de las personas de la organización
		Mejor uso de los recursos disponibles
		Conocimiento de las obligaciones y responsabilidades del personal
CON-71	Actividades técnicas	Previene intentos de ataques a los activos por usuarios externos
		Aumenta la integridad y confidencialidad de la información durante la comunicación ya que viaja de forma cifrada
		La comunicación de información solo se estable entre dispositivos previamente configurados y autorizados
		Mejora la productividad y eficiencia del personal
		Posibilidad del personal para realizar sus labores en cualquier parte conectado a internet
		Aumento de la competitividad en el mercado

Fuente: elaboración propia, utilizando Microsoft Excel 2016.

Los costos no recurrentes ascienden a Q 221 800,00 y los recurrentes, correspondientes a los controles CON-37, CON-38, CON-39, CON-40, CON-41,

CON-42, CON-50, CON-51, CON-54, CON-58, CON-59 y CON-60 ascienden a Q 100 500,00 anuales.

4.5. Opciones de tratamiento

Obtenidos los valores de riesgo residual, los niveles de aceptación y los costos de los controles, se determinan las formas adecuadas en que se tratarán los riesgos para modificar su nivel. Las opciones de tratamientos propuestas son eliminación, mitigación y compartición.

4.5.1. Eliminación

Indica eliminar la fuente del riesgo, es decir prescindir del activo que motiva la presencia del riesgo. Para este tratamiento la organización puede considerar las siguientes consideraciones:

- Analizar la posibilidad de modificar la estructura del sistema de información, revisando las dependencias de activos y determinando en cuáles recae mayor valor acumulado; de esa manera se podrá definir si es viable separar algunos activos dependientes.

- Quitar elementos e integrarlos como otra forma tecnológica, por ejemplo, migrar los servidores físicos a servidores en la nube, donde algunos de los riesgos asociados podrían ser eliminados. El mismo caso podría ser utilizado en los soportes de información.

- Separar activos de información creando conjuntos de subsistemas, evitando así la interrelación de activos de gran valor acumulados con los que presentan riesgos elevados.

Cuando se eliminan elementos del sistema de información, es necesario volver a realizar el análisis de riesgo con la estructura modificada, y tomar en cuenta que la modificación del sistema conlleva un cambio organizacional y operativo.

4.5.2. Mitigación

Es el conjunto de acciones cuyo fin es la reducción de cualquiera de los dos elementos que componen el riesgo, impacto y probabilidad, y esto es realizado por los controles.

En este tratamiento se evalúa el riesgo residual contra el nivel de aceptación de la organización; los resultados definirán las acciones a tomar sobre los controles propuestos:

- El costo es asumible, los controles propuestos serán integrados.
- El costo de los controles no es asumible y se buscan controles alternativos.
- El riesgo no justifica el costo y se descartan los controles o se buscan controles alternativos de menor costo.
- El riesgo justifica la ampliación o la mejora de los controles.
- Si se reduce el nivel de riesgo, se deben ampliar los controles; si se amplía el nivel de riesgo se deben reducir los controles.

Se debe considerar que, al aprobar la integración al sistema de controles consistentes en nuevos activos de información, es necesario volver a hacer el análisis de riesgos del sistema modificado debido a que los nuevos activos estarán expuestos a amenazas y agregan valor al sistema.

4.5.3. Compartición

Es la acción de transferir parcial o totalmente el riesgo cuando el costo del tratamiento indirecto es menor al tratamiento realizado directamente por la organización. La transferencia del riesgo es posible para algunos activos del sistema, aquellos que posean características genéricas de operación o los servicios que otorgan son iguales en cualquier otro sistema. Existen dos formas de transferir el riesgo:

- Subcontratación: la organización puede contratar servicios que reemplacen las funciones realizadas por algunos de los activos de información. Recientemente las organizaciones están migrando mucha de la infraestructura de un sistema de información a soluciones en la nube ya que reducen costos de adquisición, mantenimiento y administración de los equipos.

- El anterior caso es un ejemplo de subcontratación o tercerización, de esta forma al realizar un contrato se traslada parcial o totalmente los riesgos al proveedor de servicios, puesto que este es el encargado de brindar los controles de seguridad según lo estipulado en el contrato. La organización deberá evaluar más allá de la reducción de costos directos, el aumento de controles de seguridad con mayor madurez que las que podrían ser implementadas por ellos mismos, es un factor que considerar en la elección de este tipo de tratamiento. Otros ejemplos de activos que pueden subcontratarse son:

    - Servidores
    - Almacenamiento de copias de resguardo
    - Software

- Personal o recurso humano

- Contratación de seguros: cuando se contrata un seguro, el proveedor cubrirá una parte del valor del activo asegurado, de esta forma al asegurador se le transfiere parcial o totalmente el impacto y la probabilidad de la amenaza queda en la organización. Este tratamiento servirá para recuperar parte del valor económico del activo. Para cualquier clase de activo, un reintegro de su valor cuantificable ayuda para volver a hacerse con un activo de reemplazo. La organización podrá considerar la contratación de seguros que cubra los siguientes activos y eventos:

  - Equipo electrónico

    - Daño
    - Robo
    - Pérdida

  - Bienes muebles

    - Robo
    - Destrucción
    - Incendio
    - Eventos naturales y catástrofes

Se observa que la existencia de seguros de equipo electrónico cubre una amplia lista de dispositivos en los que puede colocarse el equipo de cómputo (servidores, máquinas de escritorio y portátiles) que forman el núcleo de los sistemas de información, y los bienes muebles que lo conforman, así como las instalaciones que albergan los activos.

4.6. Comunicación y consulta

Etapa de retroalimentación de las personas involucradas en el sistema de información, respecto del proceso de gestión de riesgos que la organización desea implementar. Esta fase busca conocer aspectos importantes que durante el análisis no se consideraron, a través de la comunicación con los usuarios. Es importante que se establezcan reuniones donde participe personal de todas las áreas de la organización, con el fin de conocer sus ideas, opiniones, comentarios y dudas; con esto se reforzarán o debatirán las propuestas para la gestión de riesgos. El involucramiento del personal en la comunicación y consulta asegura que las acciones que se van a realizar no afecten la productividad de la organización y el manejo del sistema de información.

5. PLAN DE TRATAMIENTO DE RIESGOS

Es el conjunto de programas de seguridad que tienen por objetivo determinar cómo se realizarán las decisiones tomadas sobre la gestión de los riesgos. El capítulo comprende una guía para la elaboración de un plan de tratamiento de riesgos, luego que se haya definido el proceso de gestión de riesgos por parte de la dirección de la organización.

5.1. Marco referencial

En el marco de referencia para la elaboración del plan de tratamiento de riesgos de la organización se pueden considerar:

- Objetivos y metas de la organización
- Normas y políticas de la organización
- Contratos con clientes y proveedores
- Contratos y convenios con empleados

Así como cualquier otro compromiso relevante en temas de seguridad de la información adquirido por la organización.

5.2. Responsables y responsabilidades

Los responsables son personas o grupos de personas a quienes la organización les delega actividades específicas a ejecutar para la implementación del proceso de gestión de riesgos. El objetivo es determinar y documentar quién o quiénes estarán a cargo de los tratamientos de riesgos y qué

tareas deben realizar. Es importante que la dirección de la organización constituya un comité interdisciplinario que tome las decisiones y dirija todo el proceso, orientándolo a sus metas y objetivos.

5.3. Programas de seguridad

Conjunto de tareas para la implementación de los controles que modifican los valores de impacto y riesgo residual a niveles aceptados por la organización. Cada programa de seguridad debe contener como mínimo la información siguiente:

5.3.1. Objetivos

La finalidad para la que se realizan las actividades. Pueden estar enfocadas en tratamientos, activos, amenazas, y cualquier agrupación de las anteriores, que faciliten la estructuración del plan. Por ejemplo, se realiza un plan de seguridad para una amenaza específica o se realiza un programa de seguridad por tipo de tratamiento.

5.3.2. Prioridad

Indica el orden de importancia del programa. La prioridad es definida por la dirección de la organización quienes deben evaluar factores como:

- Criticidad del riesgo
- Inversión de los controles
- Complejidad de implementación de los controles
- Recursos requeridos (humanos, técnicos, infraestructura, entre otros)

Debe prevalecer como criterio básico el nivel de orientación del programa hacia las metas, objetivos y estrategias de la organización. En el caso que el programa tenga una parte importante dentro de las estrategias de la organización, deberá ser categorizado con prioridad alta. Si el programa no tiene relevancia en los objetivos del negocio, podrán utilizarse los factores anteriormente descritos.

Para asignarle un valor a la prioridad se puede hacer uso de escalas cualitativas o cuantitativas; al hacer la elección, debe usarse la misma escala para priorizar todos los programas.

5.3.3. Ubicación temporal

Estimación del tiempo en el que el programa será desarrollado. Su finalidad es establecer el tiempo necesario para asegurar que la implementación tenga un periodo viable y el resultado sea el esperado por la organización. Las prácticas que a continuación se describen ayudarán a realizar una estimación del tiempo:

- Definir un cronograma de trabajo por cada programa.
- Estimar la duración de las tareas.
- Definir la secuencia de las tareas.
- Determinar la dependencia de tareas, qué tareas deben completarse antes de iniciar otras.

Los tiempos de los programas y sus tareas deben ser medibles, razonables y realistas, si no se tiene certeza en el conocimiento de los tiempos de las tareas se buscará información histórica o se harán consultas a personal experto dedicado a dichas tareas o que ha estado involucrado en procesos de gestión en otras organizaciones.

5.3.4. Controles

Habrá un conjunto de controles que se implementará como parte del programa de seguridad, tomando en cuenta los controles que han sido aceptados o mejorados, luego del análisis de las opciones de tratamiento.

5.3.5. Unidad a cargo

Es el área de la organización que está a cargo del desarrollo del programa de seguridad. Tiene a cargo las siguientes funciones:

- Planeamiento e implementación del plan de seguridad.
- Monitorización de las actividades para asegurar que las tareas se cumplan según el cronograma, y su funcionamiento sea el esperado.
- Comunicación con la dirección y las demás unidades de la organización.
- Lanzamiento del programa que incluye actividades de información a usuarios y capacitaciones.

5.3.6. Estimación de costos económicos

En todos los costos que integren la implementación del programa de seguridad, deben tomarse en cuenta los siguientes rubros:

- Actividades de formación y capacitación: campañas de información y adiestramiento sobre las nuevas tecnologías y procedimientos.
- Asistencia especializada externa: asesoramiento de expertos para que las tareas se ejecuten de forma correcta.
- Tecnología: son los controles tangibles que se integrarán al sistema y cuya función es la reducción del riesgo.

- Tiempo del personal: tiempo que el personal dedica para la implementación del programa; en las implementaciones puede ser necesario que el personal dedique tiempo extra para el aprendizaje de las nuevas tecnologías o procedimientos.

5.3.7. Estimación de recursos

Además de los costos económicos que implica la implementación de los programas de seguridad, se deben estimar los recursos necesarios. Se requiere conocer de forma precisa las tareas y el alcance de cada una de ellas y cuándo se tiene programada su ejecución, así como el presupuesto de la organización, ya que las restricciones financieras afectarán la elección de los recursos. Para determinar los recursos deben considerarse los siguientes aspectos:

- Qué se necesita: etapa para identificar los recursos.
  - Personal
  - Equipos o dispositivos
  - Materiales
  - Herramientas
  - Instalaciones
  - Conocimientos especializados
  - Software
  - Hardware

- Cómo se obtendrán: definir las estrategias.
  - Dentro de la organización
  - Recurso externo
    - Proveedores
    - Consultores

        - Especialistas

- Cuando se necesita: planificación de los recursos.
    - Revisión de cronogramas
    - Revisión de presupuesto

5.3.8. Estimación del impacto organizacional

Se indica cuáles serán los efectos en la estructura y procedimientos de la organización. La implementación de los programas de seguridad hará que muchos de los procesos operativos, administrativos, financieros, tecnológicos, entre otros, tengan un cambio o una nueva forma de ejecutarse y debe considerarse el impacto en la productividad. Algunos aspectos de la organización que tendrán impacto son:

- Estructura organizacional, las funciones y responsabilidades.
- La cultura organizacional
- Flujos de información
- Procedimientos para la toma de decisiones
- Normas y políticas
- Alcances en las relaciones contractuales
- Rediseño de los procesos

CONCLUSIONES

1. La valoración de los activos del sistema de información muestra que los que tienen mayor valor son aquellos que almacenan información o prestan servicios. Los equipos o dispositivos por sí mismo no se consideran valiosos para la organización, es la información que contienen o los servicios que brindan lo que tienen la mayor valoración; en consecuencia, es lo más importante para la organización.

2. El sistema de información está expuesto a una cantidad considerable de amenazas, existen muy pocos controles o medidas de seguridad para los activos, lo que hace más vulnerable al sistema. Se determinaron valores de degradación altos en las amenazas, pero en su mayoría, en situación de probabilidad.

3. Los valores de impacto potencial, mayormente, se determinaron altos; quiere decir que la degradación del valor del activo provocado por la amenaza es alta. El riesgo potencial se determinó en su mayoría en valores medios, lo que indica que las consecuencias pueden llegar a ser muy perjudiciales pero las probabilidades aún son manejables, lo que provoca un estado de riesgo del sistema medio.

4. Los controles propuestos tienen gran eficacia sobre el sistema, reducen la degradación o minimizan la probabilidad de ocurrencia de las amenazas identificadas. Su implementación modificará el estado de riesgo del sistema a niveles bajos.

5. Para los valores de impacto residual se determinaron niveles medios a bajos; en los valores de riesgo residual se determinaron niveles bajos a muy bajos, lo que muestra la eficacia de los controles propuestos. Con estos resultados la dirección podrá tomar decisiones fundamentadas para la modificación de los valores de riesgo a los aceptados por la organización.

6. Es viable la aplicación del conjunto de controles propuestos, ya que tendrán un efecto de aumento de la seguridad y protección del sistema de información de la organización.

7. El aumento de la seguridad del sistema de información es un factor potencial para la competitividad en el mercado, marcando una diferenciación con la competencia y brindando mayor confianza a sus socios comerciales.

RECOMENDACIONES

1. La organización, a través de sus directivos, deberá tomar las decisiones respecto del nivel de riesgo que desea asumir. Los valores de impacto y riesgo residuales son parámetros necesarios para definir el nivel de aceptación de los riesgos, con base en sus factores institucionales como objetivos, políticas, metas, contratos y cualquier otro convenio relevante.

2. Considerar el cambio de algunos elementos físicos del sistema, principalmente servidores y dispositivos de respaldo, a soluciones de computación en la nube, las cuales ofrecen beneficios como el ahorro en costos de infraestructura y licencias, costos menores en mantenimiento y una disponibilidad casi permanente de los recursos, así como la transferencia de parte de los riesgos al proveedor.

3. Cuando la organización apruebe y ejecute los programas de seguridad e integre al sistema controles consistentes en nuevos activos de información, es necesario volver a hacer el análisis de riesgos, debido a que los nuevos activos estarán expuestos a nuevas amenazas.

4. El proceso de gestión de riesgos debe estar orientado en todo momento a las políticas, objetivos y metas de la organización.

5. Es importante que se establezcan reuniones donde participe personal de todas las áreas de la organización, con el fin de conocer sus ideas, opiniones, comentarios y dudas, para reforzar o debatir las propuestas de gestión de riesgos. Involucrar al personal en todas las etapas del

proceso asegura que las acciones que se realizarán no afecten la productividad de la organización y el manejo del sistema de información.

6. Debe prevalecer como criterio primario el nivel de orientación de los programas de seguridad hacia las estrategias de la organización. En el caso que el programa tenga una parte importante dentro de las estrategias, se debe considerar prioritaria su ejecución.

BIBLIOGRAFÍA

1. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. MAGERIT – versión 3.0. *Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I – Método.* [en línea]. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XIBt1YgzbIV>. [Consulta: 2 de marzo de 2019].

2. _____. *Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II - Catálogo de elementos.* [en línea]. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XIBt1YgzbIV>. [Consulta: 2 de marzo de 2019].

3. _____. *Metodología de análisis y gestión de riesgos de los sistemas de información. Libro III - Guía de técnicas.* [en línea]. <https://administracionelectronica.gob.es/pae_Home /pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XIBt1YgzbIV>. [Consulta: 2 de marzo de 2019].

4. GÓMEZ VIEITES, Álvaro. *Enciclopedia de la seguridad informática*. 2a ed. México: Alfaomega, 2014. 825 p.

5. IMBAQUINGO ESPARZA, Daisy Elizabeth; PUSDÁ CHULDE, Marco Remigio; JÁCOME LEÓN, José Guillermo. *Fundamentos de*

auditoría informática basada en riesgos. Ecuador: Ibarra-Ecuador, 2016. 160 p.

6. Instituto Nacional de Ciberseguridad. *Decálogo de ciberseguridad empresas.* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf>. [Consulta: 27 de abril de 2019].

7. _____. *Desarrollar cultura en seguridad.* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad. pdf>. [Consulta: 27 de abril de 2019].

8. _____. *Gestión de riesgos.* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf>. [Consulta: 27 de abril de 2019].

9. _____. *Glosario de términos de ciberseguridad* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf>. [Consulta: 27 de abril de 2019].

10. _____. *Plan director de seguridad.* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf>. [Consulta 27 de abril de 2019].

11. _____. *Protección de la información.* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/dosieres/meta

d_proteccion-de-la-informacion.pdf>. [Consulta: 27 de abril de 2019].

12. ISO27000.ES. *Sistema de Gestión de la Seguridad de la Información.* [en línea]. <http://www.iso27000.es/download/doc_sgsi_all.pdf>. [Consulta: 6 de marzo de 2019].

13. RIVAS LÓPEZ, José Luis. *Protección de la información*. España: Ediciones VirtuaLibro, 2003. 142 p.