UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Software

“Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27002, para fortalecer la confidencialidad e integridad de la información”.

Trabajo de grado previo a la obtención del título de Ingeniero de Software de la Universidad Técnica del Norte.

Autor:

José Dimas Castañeda Cando

Director:

PhD. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2024

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE USO

LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100392984-9		
APELLIDOS Y NOMBRES:	JOSÉ DIMAS CASTAÑEDA CANDO		
DIRECCIÓN:	LA COMPAÑÍA, OTAVALO		
EMAIL:	jdcastanedac1@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0987808606

DATOS DE LA OBRA	
TÍTULO:	DESARROLLO DE UN PLAN DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO IMBACOOP LTDA., APLICANDO EL ESTÁNDAR ISO/IEC 27002, PARA FORTALECER LA CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN.
AUTOR(ES):	JOSÉ DIMAS CASTAÑEDA CANDO
FECHA:	14/02/2024
PROGRAMA:	PREGRADO
TÍTULO POR EL QUE OPTA:	INGENIERO DE SOFTWARE
DIRECTOR:	PhD. DAISY IMBAQUINGO
ASESOR 1:	MSc. MAURICIO REA
ASESOR 2:	MSc. PEDRO GRANDA

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 15 días del mes de febrero de 2024

EL AUTOR:

ESTUDIANTE

José Dimas Castañeda Cando

C.I: 1003929849-9

CERTIFICACIÓN DIRECTOR

Ibarra 14 de febrero del 2024

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE TITULACIÓN

Por medio del presente yo PhD. Daisy Imbaquingo, certifico que el Sr. José Dimas Castañeda Cando, portador de la cédula de ciudadanía número 1003929849, ha trabajado en el desarrollo del proyecto de grado "**Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27002, para fortalecer la confidencialidad e integridad de la información",** previo a la obtención del Título de Ingeniero en Software realizado con interés profesional y responsabilidad que certifico con honor de verdad.

Es todo en cuanto puedo certificar a la verdad

Atentamente

PhD. Daisy Imbaquingo

DIRECTOR DE TRABAJO DE GRADO

Dedicatoria

El presente trabajo de titulación lo dedico a mi madre María Angelina Cando Remache, quien a lo largo de la trayectoria de mi carrera universitaria me brindo apoyo incondicional en los buenos y malos momentos durante la etapa de estudio universitario, además me ayudo con la parte económica para los gastos.

A mis hermanos Tarquino Castañeda, Leonel Castañeda, Antonio Castañeda, quienes siempre estuvieron apoyándome con la parte económica, durante el proceso educativo.

José Dimas
Castañeda Cando

Agradecimiento

En primer lugar, agradezco a Dios por brindarme la sabiduría para tener una buena experiencia en mi etapa de educación universitaria, para permitirme convertir un profesional en la carrera que tanto anhele, también a cada docente por compartir sus conocimientos para la formación en toda mi trayectoria universitaria y a mi familia por motivarme a cada momento en mis estudios.

No ha sido fácil el camino, pero gracias al amor y apoyo de Dios y de mi familia, hago presente mi gran afecto hacia ustedes.

José Dimas

Castañeda Cando

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

Resumen

El trabajo de investigación lleva por título de “DESARROLLO DE UN PLAN DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO IMBACOOP LTDA, APLICANDO EL ESTÁNDAR ISO/IEC 27002, PARA FORTALECER LA CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN”; concentrándose en el Departamento de Tecnología de la Información, en el sistema financiero y sus activos, dentro de estas 3 áreas se encontró diferentes problemas como: fuga de informaciones, desconocimiento de normas de seguridad, carencia de controles y políticas de seguridad. Para encontrar el estado actual y sus vulnerabilidades se llevó a cabo una entrevista al jefe de Departamento de Tecnología de la Información, se aplicó la metodología Magerit v3 junto con la herramienta Pilar obteniendo amenazas de origen industrial, errores y fallos no identificados, y ataques intencionados; para mitigar los riesgos se seleccionó los controles de la Norma ISO/IEC 27002, posteriormente se realizó las políticas adecuadas con el objetivo de fortalecer la confidencialidad e integridad de la información mediante un Plan de SGSI, para la validez de instrumento de encuesta realizado se utilizó método Delphi con 3 expertos de seguridad informática; los resultados obtenidos determinó la madurez de seguridad que se encuentra en un estado crítico ante las amenazas internas con respecto a la manipulación de la información, la investigación presente revelo que es fundamental aplicar la metodología magerit v3 para el analices de gestión de riesgos de la información en la identificación y valoración de activos, identificación amenazas, tratamiento de riesgos, para determinar la toma de decisiones y medidas de seguridad.

Abstract

The research work is entitled "DEVELOPMENT OF AN INFORMATION SECURITY MANAGEMENT SYSTEM PLAN IN THE SAVINGS AND CREDIT COOPERATIVE IMBACOOP LTDA, APPLYING THE ISO/IEC 27002 STANDARD, TO STRENGTHEN THE CONFIDENTIALITY AND INTEGRITY OF INFORMATION"; concentrating on the Information Technology Department, the financial system and its assets, within these 3 areas different problems were found such as: information leakage, lack of knowledge of security standards, lack of controls and security policies. To find the current state and its vulnerabilities, an interview was conducted with the head of DTI, the Magerit v3 methodology was applied together with the Pilar tool, obtaining threats of industrial origin, unidentified errors and failures, and intentional attacks; to mitigate the risks, the controls of the ISO/IEC 27002 Standard were selected, then the appropriate policies were made with the objective of strengthening the confidentiality and integrity of the information through an ISMS Plan, for the validity of the survey instrument, the Delphi method was used with 3 information security experts; The results obtained determined the security maturity that is in a critical state in the face of internal threats with respect to the manipulation of information, the present investigation revealed that it is fundamental to apply the magerit v3 methodology for the analysis of risk management of the company.

Introducción

Tema

Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27002, para fortalecer la confidencialidad e integridad de la información.

Problema

Antecedentes

La Cooperativa de Ahorro y Crédito Imbacoop Ltda., ubicada en la ciudad de Otavalo, tiene 23 años de funcionamiento en el cual requiere un Plan de Sistema de Gestión de seguridad con la finalidad de garantizar la confidencialidad e integridad de la información, en el Departamento de Tecnología de información, para mitigar: fuga de información, no posee política de seguridad, errores de administrativos por no poseer un personal calificado, no conocen normativas de seguridad.

Y de acuerdo con las disposiciones establecidas, por la Secretaría Nacional de la Administración Pública (SNAP), exige a todas las empresas públicas del Ecuador implementar un sistema que gestione la seguridad de la información (Erazo, 2016). Y al ser un activo importante de la empresa, se pretende brindar solución a este requerimiento tecnológico.

La ISO 27002 nos entrega un catálogo de controles con las directrices necesarios para asegurar de una u otra forma la seguridad de la organización, también se enfoca en la protección de información contra las vulnerabilidades y riesgos que amenazan la integridad, confidencialidad de la información para gestionar la Seguridad de la información. (Masaquiza, 2011).

Situación Actual

Actualmente, la Cooperativa de Ahorro y Crédito Imbacoop Ldta., cuenta con una matriz y nueve sucursales, la organización posee un Departamento de Tecnología de Información, donde almacenan una gran cantidad de información de clientes, usuarios, ya que es un activo primordial, que se debe ser gestionada. La información se maneja mediante VPN, por lo que se encuentra vulnerable, lo cual es ocasionado por falta de controles, políticas de seguridad, los exempleados hacen mal uso de información, no cuenta con normativa interna para ejecutar un sistema de seguridad de la información, por lo cual esto puede llevar a ocasionar malas prácticas, o gestionar modificaciones en informaciones críticas de la empresa ocasionando a fuga de información, riesgos, amenazas, en los activos.

Prospectiva

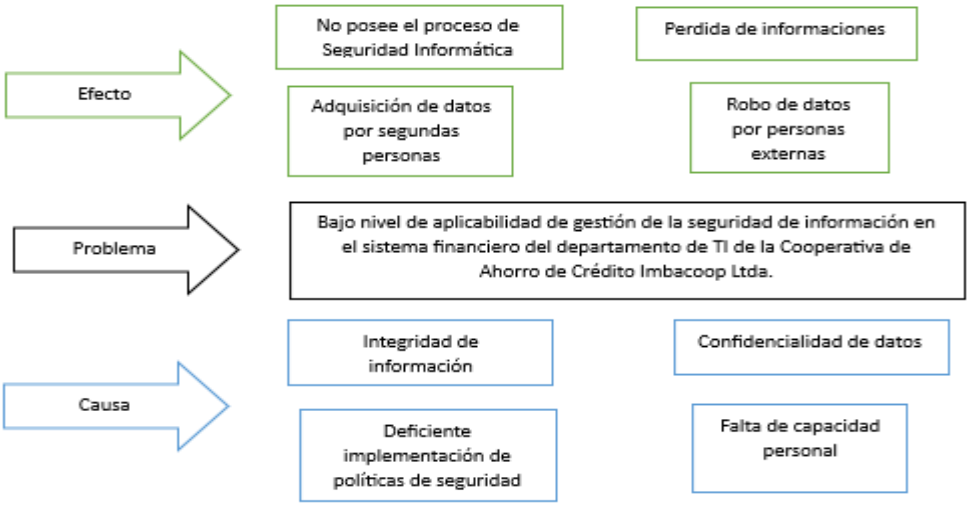
Con el presente trabajo de titulación se plantea realizar un plan de Sistema de Gestión de la seguridad de la información para la mejora del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., con el fin de disminuir las vulnerabilidades en las siguientes áreas: accesos al sistema y los activos, tal manera se basará con el estándar de Seguridad de Información ISO/IEC 27002 que dan una solución a los problemas detectados, permitiendo una buena toma de decisiones para el aseguramiento de información, el propósito es la de minimizar los riesgos, lo que permite evitar pérdida económica, ambiental, humanas, los cuales ocasionan el buen funcionamiento de los activos.

Planteamiento del problema

El control de la información que lleva el Departamento de la Tecnología Informática de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., refleja problemáticas de la vulnerabilidad. Según (Romero et al., 2018) menciona que las vulnerabilidades son fallas en los sistemas, no son puertas abiertas diseñadas deliberadamente, sino errores de diseño, configuración o implementación que generan oportunidades de ataque, es decir que hacen viable una amenaza, ya que día a día se ve expuesto las informaciones contra las amenazas, lo que causa es poner en riesgo las informaciones, lo que se tiene que llevar un buen manejo de información, con la finalidad de llevar la integridad, confidencialidad. Se llevó a cabo un diagrama de causa y efecto, para lo cual se utilizó Matriz de Vester para clasificar los problemas planteados en el proyecto.

Figura 1

Diagrama de Vester



Nota. Elaboración propia.

Objetivos

Objetivo General

Desarrollar un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27002, para fortalecer la confidencialidad e integridad de la información.

Objetivos Específicos

- Diagnosticar la situación actual de la seguridad de información, en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.
- Proponer un plan de seguridad de la información basado en la norma ISO/IEC 27002.
- Validar los resultados de la implementación de la información.

Alcance

Como alcance se desea realizar un Plan de Sistema de la Seguridad de la Información (SGSI) que será establecido en el Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., como primer objetivo se llevará a cabo el diagnóstico de la situación actual), con el segundo objetivo se propondrá un plan de seguridad de la información basado en la norma ISO/IEC 27002, las cuales brindan una implementación de mejores prácticas, orientación sobre procesos y controles clave de seguridad de la información, como tercero y último objetivo es validar los resultados de la implementación de propuestos con el fin de aumentar la seguridad de la información mediante encuesta a los expertos.

Figura 2

Gráfica de representación del alcance del proyecto

Nota. Elaboración propia.

Diagnosticar la situación actual: En la Cooperativa de Ahorro y Crédito Imbacoop Ltda., no cuenta con un Sistema de Gestión de seguridad de información, no existe un control adecuado en la empresa.

Desarrollar un Sistema de Gestión de Seguridad de la Información: Se llevará mediante herramientas tecnológicas con la finalidad de mejorar la seguridad de la información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Validar resultados: Se planificará un ambiente de pruebas, donde se puedan evaluar las vulnerabilidades encontradas, con la finalidad de mostrar la socialización de la propuesta a la gerencia para sugerir mejoras en los procesos ya implementados en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Metodología

Se llevará a cabo una investigación documental referente a la norma que se ha propuesto con el fin de obtener información necesaria. Además, se utilizará técnicas de investigación para justificar la situación actual de la empresa.

A continuación, se analizarán metodologías para evaluación de vulnerabilidades en las TI, considerando tanto los temas organizacionales como los técnicos, examinando detalladamente cómo los usuarios emplean la infraestructura en su entorno.

Implica una práctica fundamental porque genera una visión. para la Cooperativa de Ahorro y Crédito Imbacoop Ltda., acerca de las vulnerabilidades, proporcionando una base para futuras mejoras.

Según (Nqa, 2013), el auditor examinará el liderazgo al llevar a cabo entrevistas con uno o más integrantes del equipo directivo y valorando el grado de implicación que tienen en:

- Evaluación de riesgos y oportunidades.
- Establecimiento y comunicación de políticas.

Para cumplir el objetivo 1: Se utilizarán herramientas tecnológicas con el fin de diagnosticar la situación actual en la que se encuentra la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Según (Implantación et al., 2013), el auditor evaluará entrevistando a uno o más miembros de la gerencia y evaluando su nivel de participación en:

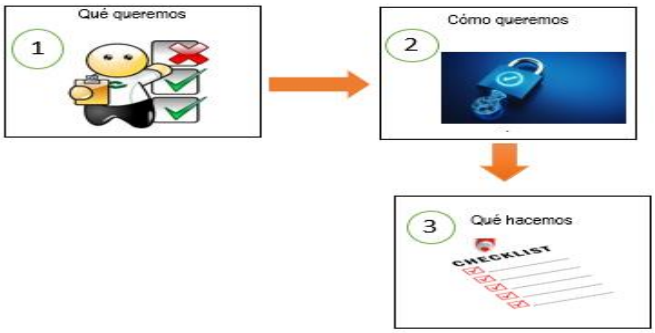
- Evaluación de riesgos y oportunidades.
- Establecimiento y comunicación de políticas.
- Establecimiento y comunicación de objetivos.

Para cumplir el objetivo 2: Se realizará una planificación de los procesos necesarios con el fin de disminuir las vulnerabilidades utilizando la norma ISO/IEC 27002.

Para cumplir el objetivo 3: Se validará los resultados propuestos mediante encuesta a expertos en seguridad.

Figura 3

Gráfico de representación de la metodología del proyecto.



Nota. Elaboración propia.

Justificación

Según Pilla, (2019) la evaluación que se va a realizar se enfoca en dar solución a uno de los Objetivos de Desarrollo Sostenible (ODS), el objetivo N.º 8 ¨ Trabajo Decente y Crecimiento Económico¨, ya que se prevé reducir los riesgos en cuanto a la seguridad de información, con el fin de mejorar la calidad de trabajo tanto de los trabajadores de la empresa y de los clientes. También para que la empresa pueda disponer de mayor disponibilidad de trabajo para las personas, dando mayor confianza de seguridad a la cooperativa.

El proyecto debe tener una o varios tipos de justificaciones que deben ser especificadas como:

Justificación Tecnológica. - El presente anteproyecto tiene como objetivo resolver el manejo de la información en el área de tecnología social y financiera de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Justificación Metodológica. - Se efectuará una investigación científica, para el estudio profundo del estándar y mixta, que permitirá conocer sobre el manejo de la información, además elaborar planes con los cuales se alcanzará el objetivo y por último validar la información obtenidos para poder plantear nuevas formas de gestionar la información.

Justificación Social. - Con el presente proyecto busca minimizar los niveles de vulnerabilidad que existe en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., para lo cual se aplicará un breve diagnóstico con el fin de mejorar la situación en la que se encuentra la empresa. Es necesario que las instituciones fortalezcan sus estrategias de gestión y análisis de riesgos administrativos y financieros (Cárdenas, 2023).

CAPÍTULO 1

Marco Teórico

1.1. Antecedentes Investigación

A nivel nacional e internacional se han realizado varias investigaciones relacionadas con la investigación que se llevará a cabo, de las cuales se hará referente para el aporte del proyecto:

La norma ISO/IEC 27002 es aquella que establece el código de mejores prácticas para la fase de la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones, mediante una guía que describe cómo se pueden establecer los controles (Rodríguez, 2019).

Por medio del diagnóstico y estudio de la norma internacional ISO/IEC 27002:2013 se diseñó una política de seguridad de la información para el área de TI de la Cooperativa de Ahorro y Crédito Chibuleo Ltda. Por lo cual se tomó en cuenta los tres pilares de la información: la confidencialidad, integridad y disponibilidad de los datos que posee la institución. Con base en estos elementos se realizó un control de la situación actual de las medidas de seguridad que el área de tecnología ha implementado, además de plasmar en una matriz los incidentes de seguridad (Pilla, 2019).

En el proyecto de investigación realizado por Criollo, (2017) en la Universidad Técnica de Ambato, afirma que “es importante que la información y centros de procesamiento tengan restringido el acceso, estableciendo lineamientos de seguridad para la información con base en la norma ISO 27002, ya que ayuda a protegerla, puesto que las políticas de seguridad minimizan el riesgo de pérdida de información garantizando el correcto funcionamiento de los procesos”.

La seguridad informática tiene como objetivo salvaguardar la integridad y confidencialidad de la información contenida en los sistemas informáticos. En esencia, implica la implementación de medidas técnicas destinadas a proteger tanto las infraestructuras de hardware como el software utilizado por una empresa, que son fundamentales para el funcionamiento de la organización (ISOTools Excelente, 2017).

Universidad Pablo de Olavide, (2020) menciona de la seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, abarca un conjunto integral de recursos que incluyen políticas, conceptos de seguridad, medidas de protección, directrices, enfoques de gestión de riesgos, prácticas recomendadas, seguros y

tecnologías. Su finalidad es resguardar la infraestructura informática de una organización, que incluye los activos, así como proteger a los usuarios involucrados en su funcionamiento.

1.1.1. Información

La información es un conjunto o un gran volumen de datos que son ordenados y seleccionados que describen elementos con la finalidad de tomar decisiones para llegar a un resultado específico.

Según Camargo, (2018) menciona que la información es un conjunto de elementos que dan significado a las cosas, para la informática la información hace referencia a datos organizados y procesados que forman mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que se relacione con un ordenador.

La información que se maneja en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se centra en la seguridad e integridad de la información de los clientes.

1.1.2. Seguridad Informática

Según varios investigadores de seguridad, menciona lo siguiente de la seguridad informática como la ciencia encargada de los procesos, técnicas y métodos que buscan procesar, almacenar y transmitir la información, por lo tanto, se puede decir, que se debe implementar los controles adecuados para salvaguardar las informaciones en las siguientes áreas: infraestructura, soporte de la empresa (hardware y software) o de la organización (Romero, 2018).

1.1.3. Seguridad de la información

La seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información, es decir, que se enfoca en la implementación de métodos o técnicas para la protección de información, con la finalidad de que no haya ningún riesgo, amenazas (Romero, 2018).

También se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información, así como a la protección de los sistemas, redes y datos contra amenazas y ataques no autorizados. La seguridad de la información es esencial para garantizar la privacidad, confidencialidad y confiabilidad de la información almacenada, procesada y transmitida en diferentes entornos, como sistemas informáticos, redes, sistemas en la nube.

Características de seguridad de la información

En la Tabla 1 se detalla algunas características muy esenciales de la seguridad de la información.

Tabla 1

Características de seguridad de la información

Numeración	Características	Definición
1	Confidencialidad	Protección de información: garantizar acceso autorizado mediante control de acceso, cifrado y políticas de privacidad.
2	Integridad	Se refiere a garantizar que la información sea precisa, completa y confiable.
3	Disponibilidad	Se refiere a asegurar que la información esté disponible para las personas autorizadas cuando la necesiten.
4	Autenticación	Se refiere a verificar la identidad de las personas o sistemas que acceden a la información.
5	Autorización	Se refiere a otorgar los permisos adecuados a las personas o sistemas autorizados para acceder a la información.
6	Auditoría	Monitoreo y registro de actividades para detectar amenazas o violaciones de seguridad en la información.
7	Gestión de riesgos	Identificar, evaluar y mitigar riesgos de seguridad de información.
8	Concientización y capacitación	Educación y capacitación en seguridad de información para personal.
9	Cumplimiento normativo	Cumplir con leyes y regulaciones de seguridad de información, como Protección de Datos y regulaciones financieras.
10	Seguridad física	Protección de activos físicos de información: centros de datos, servidores, dispositivos de almacenamiento.

Nota. Elaboración Propia.

1.2. Pilares de la seguridad de la información

Son principios fundamentales que guían la protección de la información en entornos digitales. Los elementos fundamentales que sustentan y garantizan la protección de la información en entornos digitales.

1.2.1. Dimensiones de la Seguridad Informática

Según (Eumed, 2019) menciona de norma ISO/IEC 27000 se enfoca “Requisitos para la especificación de Sistemas de Gestión de la Seguridad de la Información (SGSI)" establece un marco de estandarización destinado a la seguridad de la información, con el propósito de su implementación en una organización o empresa, e incluye un conjunto de pautas que abordan diversas áreas, tales como:

- Sistemas de gestión de la seguridad de la información.
- Valoración de riesgos.
- Controles.

Un Sistema de Gestión de Seguridad de Información (SGSI) debe fundamentarse en tres metas esenciales que aseguren la protección de los datos que gestiona, y estas son:

- La confidencialidad.
- La integridad.
- La disponibilidad.

En lo que se conoce como el triángulo de la seguridad de los datos, con el acrónimo de CID, Confidencialidad, Integridad y Disponibilidad, se puede observar en la Figura 4:

Figura 4

Pilares de la seguridad de información

Nota. Fuente: (Prez, 2022).

1.2.2. Confidencialidad

Debe garantizar que el acceso al sistema está limitado solamente a los usuarios que tengan el nivel de autorización pertinente, evitando así que la información importante pueda ser accedida por alguien que no tiene el nivel de acceso autorizado (Vázquez, 2018).

La Organización para la Cooperación y el Desarrollo Económico en sus guías para la seguridad de la información define la confidencialidad como garantizar que los datos o información solo estén disponibles para usuarios, organización o sistemas que estén autorizados, en los momentos y de la manera apropiada (Aguilera, 2020).

1.2.3. Integridad

Esto implica garantizar que únicamente los usuarios con la autorización adecuada puedan realizar modificaciones o eliminar registros del sistema. Se asegura de que no haya alteraciones no autorizadas y que solo se lleven a cabo cambios por usuarios o procesos con las debidas autorizaciones, preservando la integridad de los registros tal como se generaron originalmente (ISOTools Excellence, 2018).

1.2.4. Disponibilidad

Este elemento está vinculado con la preservación de la privacidad de la información, incluyendo los procedimientos tomados para asegurar la seguridad de información confidencial y sigilosa permanezca protegida, evitando su sustracción mediante ciberataques, actos de espionaje u otros delitos informáticos(DocuSign, 2021).

1.2.5. Sistema de Gestión de la Seguridad de la Información (SGSI)

Sistema de Gestión de la Seguridad de la información se enfoca en establecer la política y objetivos de una organización y lograrlos, mediante una estructura organizativa donde las actividades, cargos de los usuarios, están definidas. Un enfoque de medición y evaluación que permite valorar los resultados en comparación con los objetivos, incorporando la retroalimentación de los resultados para la planificación de mejoras en el sistema(Alvaro, 2018).

Según Regina, (2019) menciona que apoya de la adopción de un Sistema de Gestión de Seguridad de la Información, existe la norma ISO 27000 que fue realizada para ser conjunto de estándares internacionales relacionadas con la Seguridad de la Información, esta norma ofrece una serie de pautas de mejores prácticas para establecer, preservar y mejorar al mismo tiempo que uniformiza estos procedimientos para regular los Sistemas de Gestión de Seguridad de la Información (SGSI).

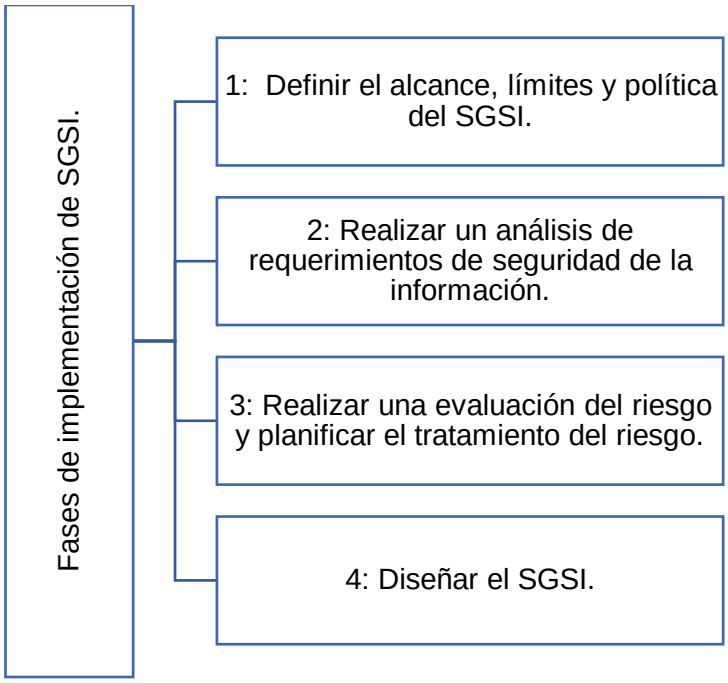
Sistema de Gestión de la Seguridad de la Información es un gran conjunto de datos que contiene una organización que se encuentra guardada o que se pueda transmitir el origen de la información.

Fases de implementación de SGSI

Según Teórico, (2012) menciona las fases de implementación de SGSI y en la Figura 5 se puede observar dicho proceso.

Figura 5

Fases de implementación de SGSI



Nota. Fuente: (Teórico, 2012).

- **Definir el alcance, límites y política del SGSI:** El propósito de esta etapa es precisar minuciosamente la extensión y las restricciones del Sistema de Gestión de Seguridad de la Información (SGSI) y elaborar la política del SGSI, asegurando la aprobación de la alta dirección.
- **Llevar a cabo un análisis de requerimientos de seguridad de la información:** En la fase de inicio del SGSI se busca definir los requerimientos relevantes para el sistema, identificar los activos de información y obtener el estado actual de la seguridad en el alcance del proyecto.
- **Hacer una evaluación del riesgo y planificar el tratamiento del riesgo:** En la fase de evaluación de riesgos del SGSI se identifican y analizan los riesgos de seguridad de la información, se define una metodología de evaluación de riesgos y se seleccionan opciones de tratamiento de riesgos, objetivos y controles de seguridad.
- **Diseñar el SGSI:** En la fase final del SGSI se completa el plan de implementación, diseñando la seguridad de la organización basada en las opciones seleccionadas para el tratamiento de riesgos. También se diseña la documentación, los controles y los requisitos específicos del SGSI.

La finalidad de la documentación es desarrollar un plan de seguridad de la información para la cooperativa, con los controles de SGSI para que puedan realizar la siguiente fase de la implementación.

1.3 Definiciones importantes de un SGSI

Para una comprensión adecuada de tareas relacionadas con SGSI y gestión de riesgos, es necesario familiarizarse con las siguientes definiciones claves vinculadas a este procedimiento para tomar las decisiones informadas y aplicar estrategias efectivas en este ámbito.

1.3.1. Activos

Los activos son recursos muy importantes de una empresa u organización que deben ser bien protegidos. Hay dos tipos de activos, primero los elementos esenciales que se enfocan a una relación lógica y la información, en segundo lugar, activos de apoyo, en su mayoría son sistemas, infraestructura tecnológica, redes, personal(Sevilla, 2023).

1.3.2. Amenaza

Hace referencia a cualquier situación que tenga la facilidad de aprovechar las debilidades o vulnerabilidades, aquellas que pueden ocasionar problemas no deseados, con el fin de provocar perjuicios a sistemas, infraestructura tecnológica, individuos, entidades, sin importar su naturaleza o actividad(Cortés, 2023).

1.3.3. Vulnerabilidades

Son debilidades o fallos en un sistema informático que pueden ser explotados por una amenaza para comprometer la seguridad de los activos. Estas vulnerabilidades pueden ser el resultado de configuraciones incorrectas, falta de parches de seguridad, errores de programación, los ciberdelincuentes pueden aprovechar la situación para ingresar en los activos y sacar informaciones de la entidad u organización(Guamán, 2019).

1.3.4. Riesgo

El riesgo de seguridad informática se refiere como la probabilidad de que una amenaza ocasione o aproveche de una vulnerabilidad de los activos y que cause un daño o pérdida. Una amenaza no se considera riesgo cuando no existe una vulnerabilidad correspondiente, ni una vulnerabilidad se considera riesgo si no existe una amenaza que la pueda explotar(Aldas, 2017).

1.3.5. Ataques Informáticos

Son aquellas acciones maliciosas que son realizados por individuos o grupos que atacan la seguridad de sistemas informáticos que poseen informaciones, como tales datos,

hardware, software, redes, ocasionando destrucción de archivos, robar, exponer, interrumpir, acceso no autorizado a sistemas, explotación de vulnerabilidades de los activos(Guaña, 2022).

Para evitar los ataques se debe conocer las debilidades y riesgos de los activos de información y sistemas, con la finalidad de realizar una estrategia eficaz para salvaguardar la seguridad y tomar buenas decisiones para proteger los activos y datos de manera efectiva.

1.4. Normas de la seguridad de la información

Las normas de la seguridad de la información son pautas y prácticas establecidas para proteger los pilares de la seguridad de la información. Estas normas son muy importantes para proteger la información contra amenazas, riesgos, y continuidad de las operaciones de la organización.

Las normas ISO son un conjunto de estándares de la seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de ayudar a las empresas, para facilitar el servicio, gestión, control y el intercambio de información para desarrollar productos de mejor calidad en la parte de la seguridad (Gobierno de España, 2018).

1.4.1. Norma ISO/IEC 27000

Aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua) (ISO/IEC 27000, 2018).

La norma ISO 27000 es una norma internacional y abierta, cuyo objetivo es establecer los requisitos mínimos con los que debe cumplir un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización, se enfoca a la seguridad de información en las siguientes áreas: confidencialidad, integridad y disponibilidad.

En la Tabla 2 se menciona la composición de la Norma ISO/IEC 27000 con cada una de las ISO que se utilizan en la seguridad y sus enfoques en cada área.

Tabla 2

Detalle de cada uno de los estándares que están incluidos en la ISO 27000

Detalle de cada uno de los estándares que están incluidos en la ISO 27000	
ISO 27000	Es una norma que permite que las demás normas se basen, porque

	aporta a la implantación de un SGSI.
ISO 27001	Es un conjunto de estándares para implementar un SGSI en una empresa.
ISO 27002	Buenas prácticas para la SGSI, también se enfoca en describir los 14 dominios, 33 objetivos de control y 112 controles.
ISO 27003	Esta norma ayuda a guiar a la implementación de SGSI, es un apoyo para la norma ISO 27001, posee directivas e instrucciones para la buena implementación de SGSI para una empresa.
ISO 27004	Ofrece directrices para evaluar la eficacia de un SGSI y sus controles, conforme a ISO/IEC 27001.
ISO 27005	Su propósito es respaldar los principios fundamentales de ISO 27001 y facilitar la implementación efectiva de la seguridad de la información mediante un enfoque de gestión de riesgos.
ISO 27006	Ofrece orientación para entender los criterios de acreditación de ISO/IEC 17021 cuando se aplican a las entidades de certificación de ISO 27001, si bien no posee la condición de ser una norma de acreditación en sí misma.
ISO 27007	Se presenta como una guía de auditoría para un SGSI, además de las directrices detalladas en ISO 19011.

Nota: Elaboración propia información basada en Intedys,2015. Fuente*: (Intedya, 2015).*

1.4.2. Norma ISO/IEC 27001

Es el estándar global que establece un marco de referencia para la Gestión de Sistemas de Seguridad de la Información (SGSI) con el propósito de garantizar la confidencialidad, integridad, disponibilidad continua de la información y el cumplimiento de requisitos legales de las organizaciones privadas o públicas.

La norma ISO 27001 sobresale como el principal marco de referencia en el campo de la seguridad de la información, puesto que facilita la creación de un Sistema de Gestión de Seguridad de la Información (SGSI) que puede ser certificado. Esto implica la selección típica de áreas críticas o vulnerables en la seguridad de la información. Una vez que se ha definido el alcance, se vuelve esencial desarrollar una política de seguridad de la información que guíe a la organización en la gestión de los riesgos relacionados con la información, abarcando aspectos legales, contractuales y específicos de la empresa(Torres, 2020).

Ventajas y Desventajas de la ISO/IEC 27001

La Norma ISO/IEC 27001 es un estándar internacional que determina los requisitos para realizar un Sistema de Gestión de la Seguridad de la Información (SGSI). Posteriormente, en la Tabla 3 se detallan algunas ventajas y desventajas asociadas a la implementación de la ISO.

Tabla 3

Ventajas y Desventajas de la Norma ISO/IEC 27001

Norma ISO/IEC 27001	
Ventajas	**Desventajas**
Proporciona una metodología de gestión de seguridad clara y bien organizada.	Elevado costo y desafíos iniciales para pequeñas empresas.
Reducción de riesgo de pérdida, robo o corrupción de información.	Resistencia al cambio en las actividades diarias de los empleados.
Reducción de costos y mejora de los procesos de servicio.	Mantenimiento continuo, lo cual puede ocasionar cargar para la organización.
Los riesgos y sus controles son continuamente revisados.	Falta de flexibilidad puede ocasionar en las actividades diarias.
Se integra con otros sistemas de gestión.	Poseer las actividades centradas en enfoque a la documentación.
Aumento de la motivación y satisfacción del personal al contar con unas directrices claras.	Respaldo del departamento de recursos humanos, que dedicará tiempo a la implementación de medidas y formación.

Nota: Elaboración propia información basada en Ctma, 2021. *Fuente:(Ctma, 2021).*

1.4.3. Norma ISO/IEC 27002:2013.

La norma ISO 27002 en años pasados se llamaba ISO 17799, es un estándar para la seguridad de la información de cualquier empresa, la norma fue publicado por la organización internacional de normalización y la comisión electrotécnica internacional. La edición más actual de la norma ISO 27002, publicada en 2013.

La norma ISO/IEC 27002:2013, la cual establece un conjunto de prácticas recomendadas, objetivos de control y controles específicos para asegurar la seguridad de la información. El propósito de aplicar esta norma es garantizar la integridad y confidencialidad de la información, promoviendo así el funcionamiento normal de las organizaciones en diversos ámbitos y áreas. Mantener la seguridad de la información no solo es esencial para las

operaciones actuales, sino que también sienta las bases para el éxito sostenible de una organización en el futuro.

Según (Cordero, 2022), la norma ISO 27002 es la más indicada para la cooperativa, ya que hoy en día en el país se ha observado que las instituciones financieras son un objetivo importante para los ataques cibernéticos y con la normativa ISO 27002, se busca minimizar los riesgos de la gran variedad de amenazas internas y externas a las que está expuesta la información, esta norma también nos permite identificar y enmendar puntos débiles en la seguridad de la información y está enfocada en la preservación de la confidencialidad, integridad y disponibilidad de los activos de información.

Ventajas y desventajas de aplicar de la Norma ISO/IEC 27002:2013

A continuación, en la Tabla 4 se representa algunas ventajas y desventajas de la Norma ISO/IEC 27002:2013:

Tabla 4

Ventajas y desventajas de aplicar de la Norma ISO/IEC 27002:2013

Norma ISO/IEC 27002:2013	
Ventajas	**Desventajas**
Detallar los controles de la normativa.	Complejidad de Implementación y requiere de recursos considerables.
Identificar y corregir puntos débiles en la seguridad de la información.	Costos significativos en capacitación e implantación.
Permite el normal funcionamiento de la organización, por ende, mejora la reputación entre proveedores y clientes.	Se necesita un personal capacitado en seguridad de los controles.
Una de las fortalezas es el control de acceso a la información.	Se necesita una actualización periódica por razón de que las amenazas asechan constantemente.
Optimización de los procedimientos para aumentar la eficiencia.	Falta de adaptación a cambios rápidos.
Eficiencia operativa con una significativa reducción de gastos.	Puede ser demasiado general para abordar adecuadamente los riesgos específicos de diferentes sectores o industrias.
Adecuación a los requisitos legales y reglamentarios vigentes.	
Reducir los riesgos que afectan con la no	

implementación de SGSI.

Nota: Elaboración propia.

1.4.4. Estructura de la Norma ISO/IEC 27002:2013

La norma está formada por 14 dominios, 35 objetivos de control y 114 controles los cuales permiten a realizar las buenas prácticas de la SGSI, en la tabla 2 se puede observar las composiciones (Iso 27000, 2013).

Dominios de la ISO/IEC 27002:2013

En la Tabla 5 se presenta los dominios y número de controles de la ISO/IEC 27002:2013.

Tabla 5

Dominios y controles

Numeración	Dominio	N.- Controles
5	Políticas de seguridad.	2
6	Aspectos organizativos de la seguridad de la información.	7
7	Seguridad ligada a los recursos humanos.	6
8	Gestión de activos.	10
9	Control de accesos.	14
10	Cifrado.	2
11	Seguridad física y ambiental.	15
12	Seguridad en la operativa.	14
13	Seguridad en las telecomunicaciones.	7
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	13
15	Relaciones con suministradores.	5
16	Gestión de incidentes en la seguridad de la información.	7
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	4

18	Cumplimiento	8

Nota: Elaboración propia información basada en Iso, 2013. *Fuente:* (Iso, 2013)

A continuación, se detallará cada uno de los controles que conforma la norma ISO/IEC 27002/2013.

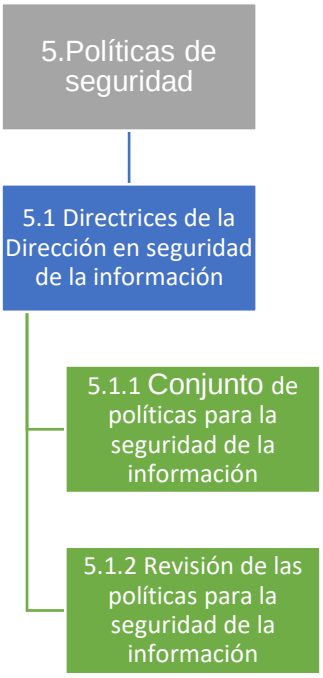
Políticas de la seguridad

Su objetivo es dirigir y dar soporte a la gestión de la seguridad de la información; debe ser redactada, documentada, aprobada y concientizada de tal manera que sea clara y comprensible para todos los usuarios.

En la Figura. 6, se puede observar que está compuesta la política de seguridad por un objetivo de control y dos controles:

Figura 6

Esquema del primer dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

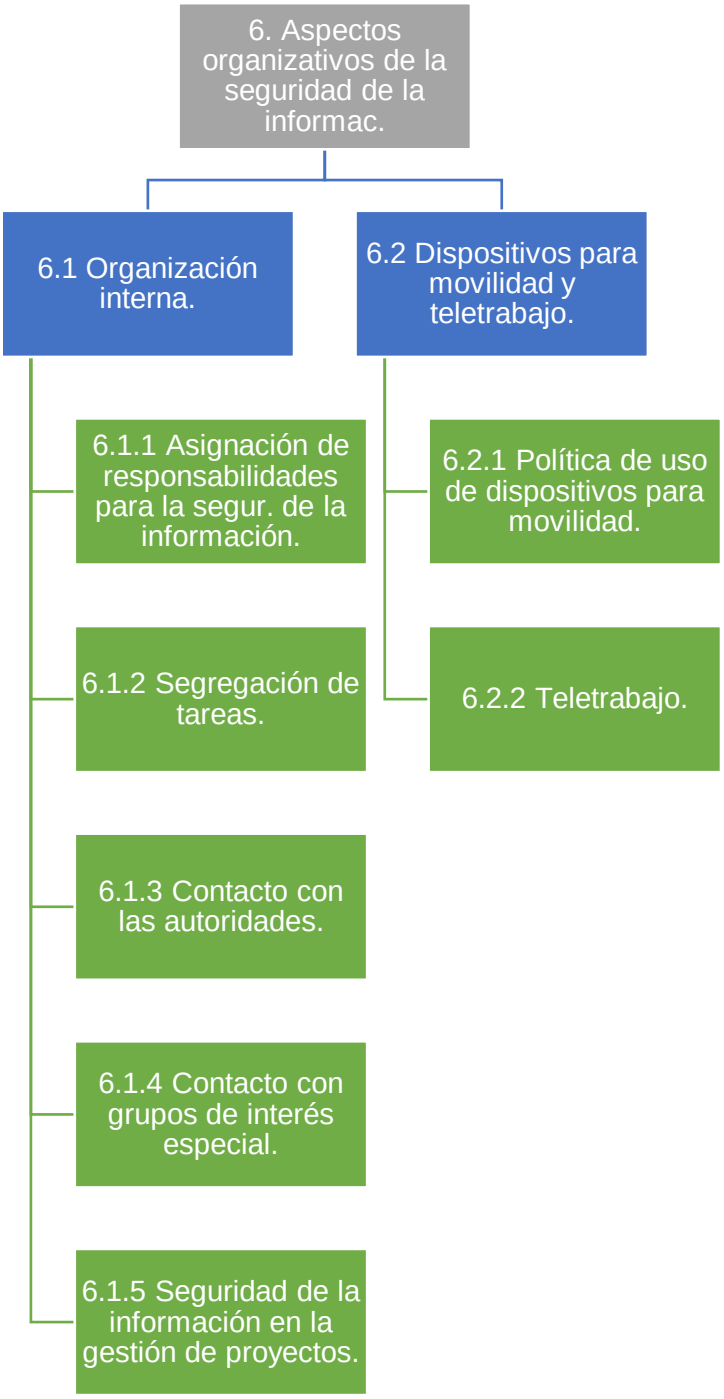
Aspectos organizativos de la seguridad de la información

Establece una estructura organizacional que identifique las responsabilidades de cada usuario o área de trabajo relacionadas con la seguridad del sistema de información.

En la Figura 7 se puede observar que está compuesto el aspecto organizativo de la seguridad de la información por dos objetivos de control y siete controles:

Figura 7

Esquema del segundo dominio de la ISO 27002:2013.



Nota. Fuente: (ISO/IEC 27002, 2013).

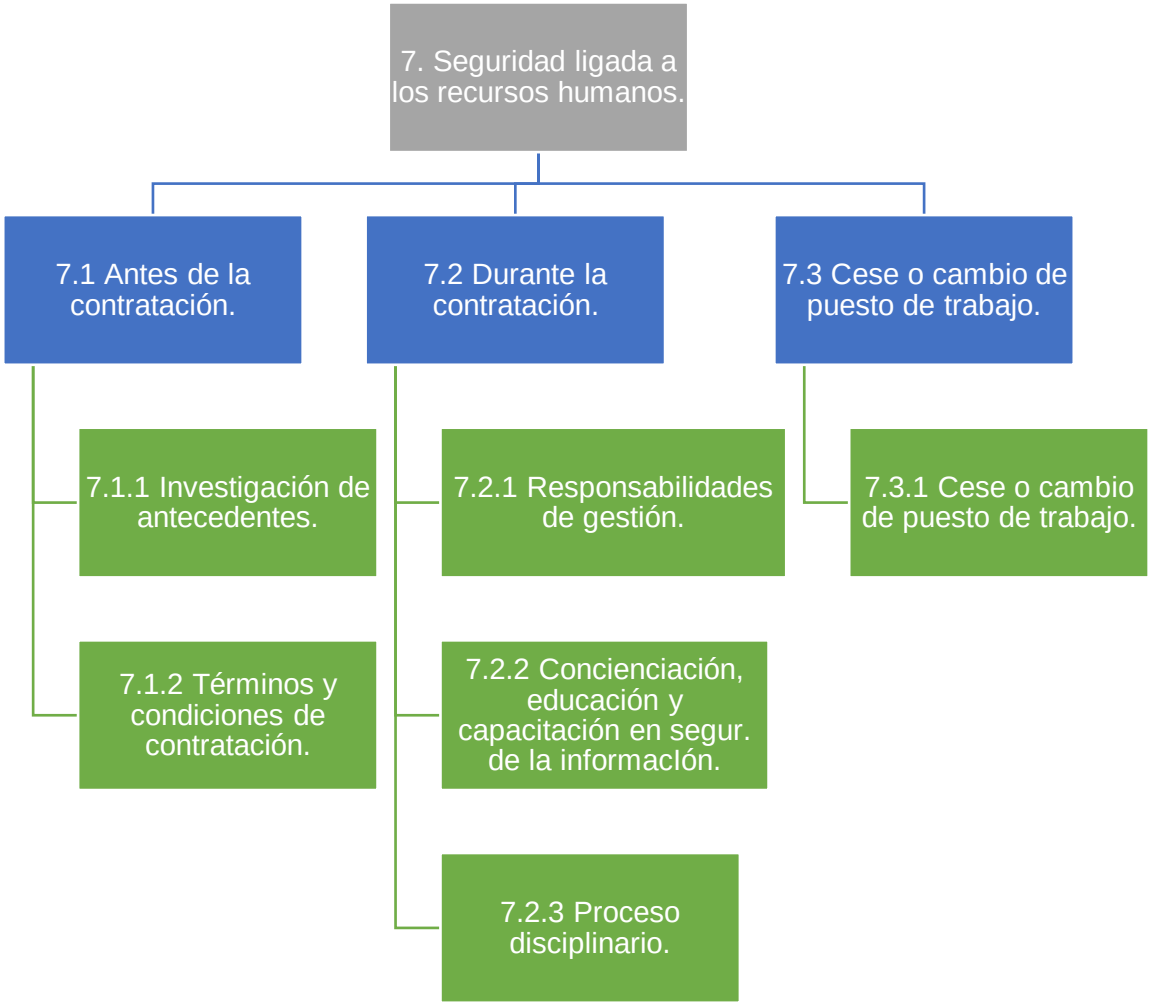
Seguridad ligada a los recursos humanos

Se enfoca en caer en cuenta a los empleados o trabadores de la empresa los riesgos que pueden ocasionar al momento utilizar incorrectamente los sistemas de información.

En la Figura 8 se puede observar que está compuesta la seguridad ligada a los recursos humanos por tres objetivos de control y seis controles:

Figura 8

Esquema de tercer dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

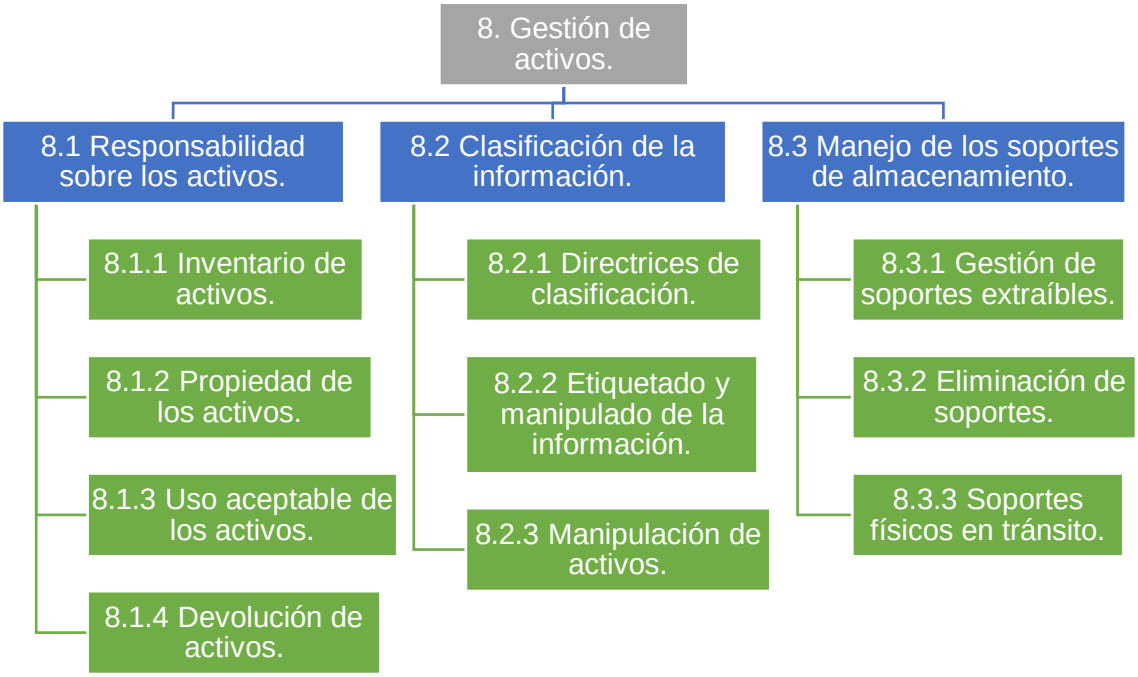
Gestión de activos

Su propósito es proteger adecuadamente los activos de una organización, clasificarlos, mantener un inventario actualizado y proporcionar protección correspondiente.

En la Figura 9 se puede observar que está compuesta la gestión de activos por tres objetivos de control y diez controles:

Figura 9

Esquema de cuarto dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

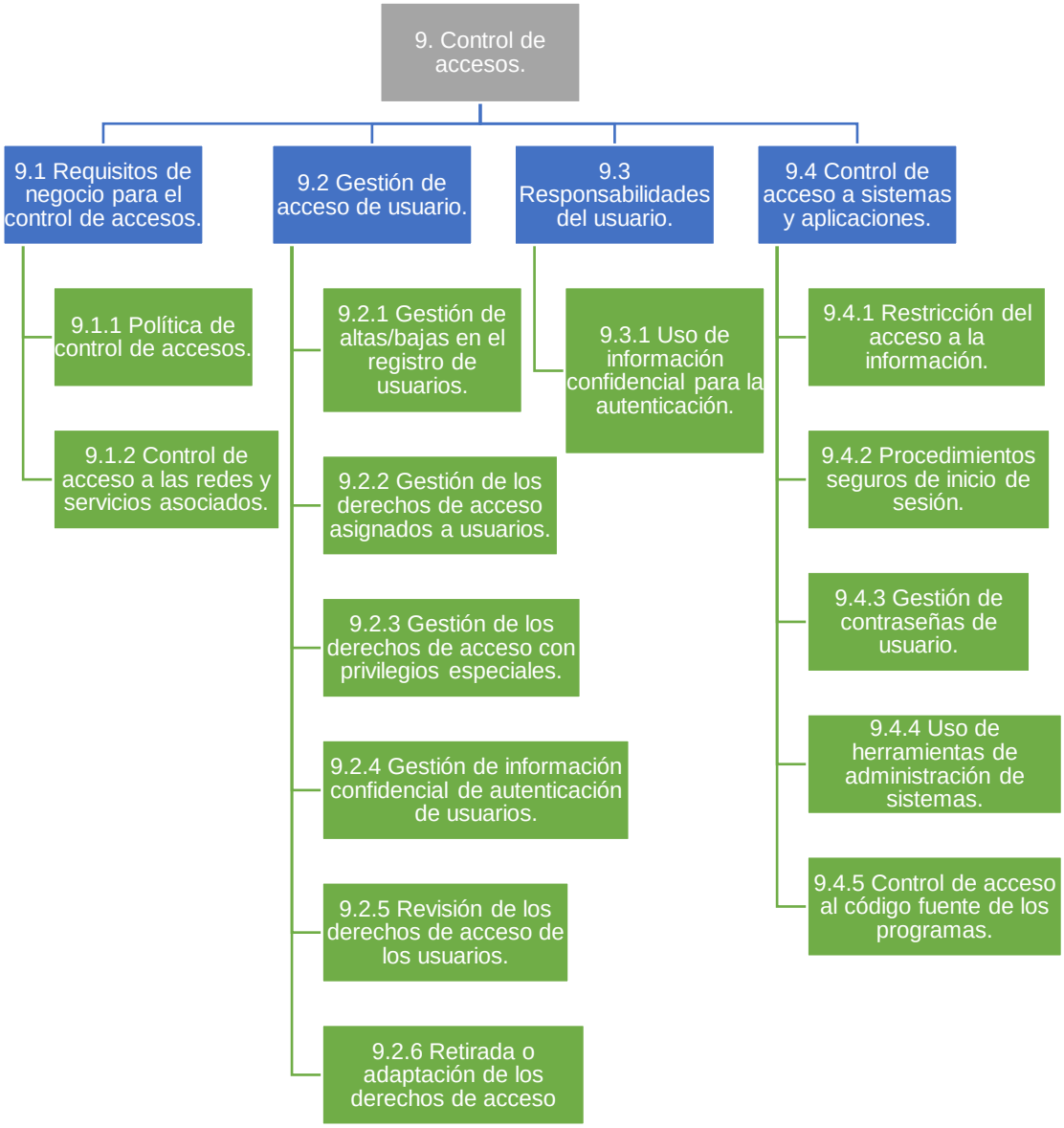
Control de accesos

No permite al acceso de las informaciones, equipos, servicios de la organización o de la empresa con la finalidad de salvaguardar la información.

En la Figura 10 se puede observar que está compuesto control de accesospor cuatro objetivos de control y catorce controles:

Figura 10

Esquema de quinto dominio de la ISO 27002:2013



Nota. Fuente:(ISO/IEC 27002, 2013).

Cifrado

En este dominio se trata de la protección de datos mediante criptografías para poder ingresar a diferentes sistemas de información de la empresa, por ello no habrá fuga de informaciones.

En la Figura 11 se puede observar que está compuesto cifrado: por un objetivo de control y dos controles:

Figura 11

Esquema de sexto dominio de la ISO 27002:2013

Nota. Fuente: (ISO/IEC 27002, 2013).

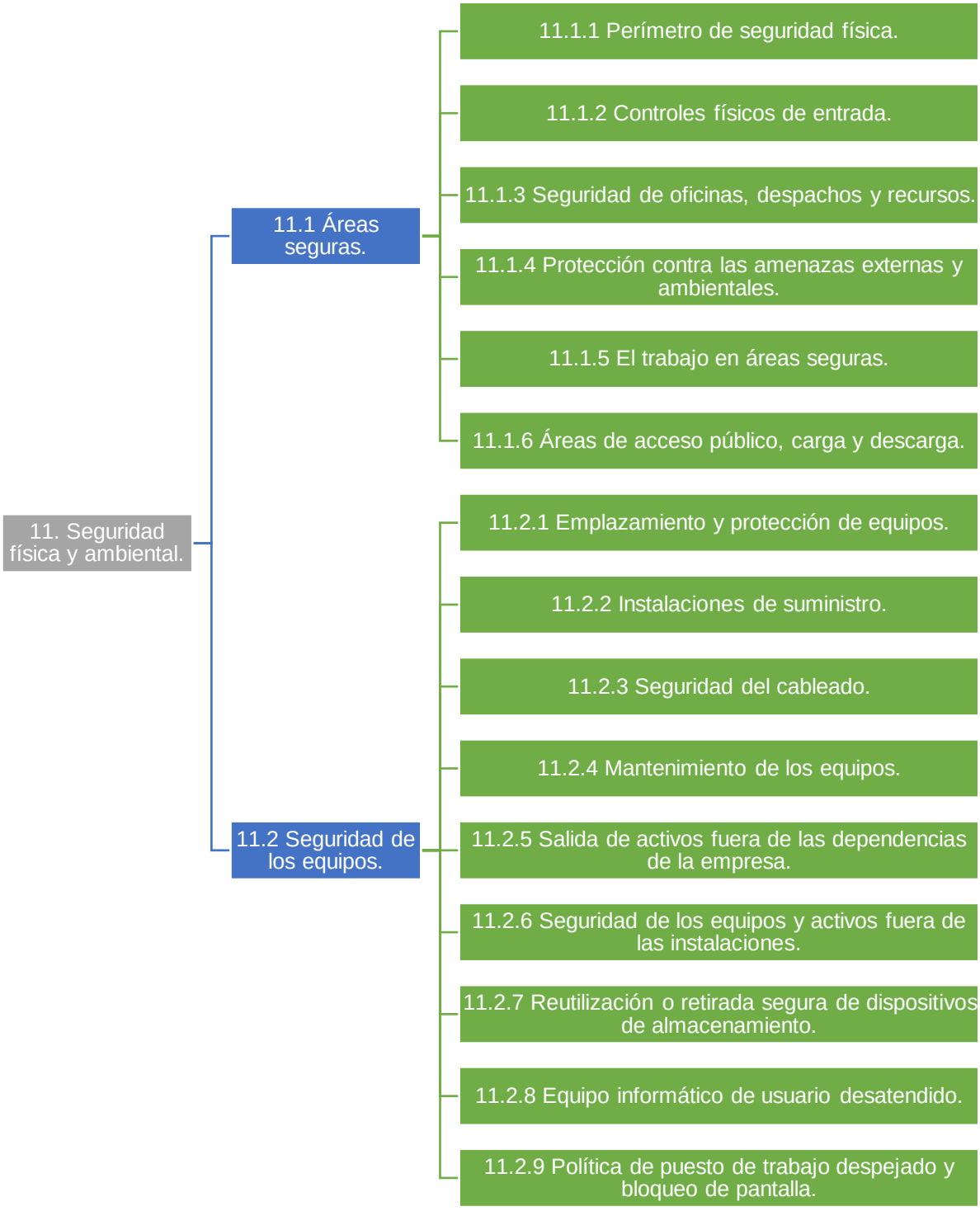
Seguridad física y ambiental.

El fin de este dominio es proteger y controlar al ingreso de diferentes áreas de trabajo, también se enfoca a la protección de amenazas contra el medio ambiente.

En la Figura 12 se puede observar que está compuesto seguridad física y ambiental por: dos objetivos de control y quince controles:

Figura 12

Esquema de séptimo dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

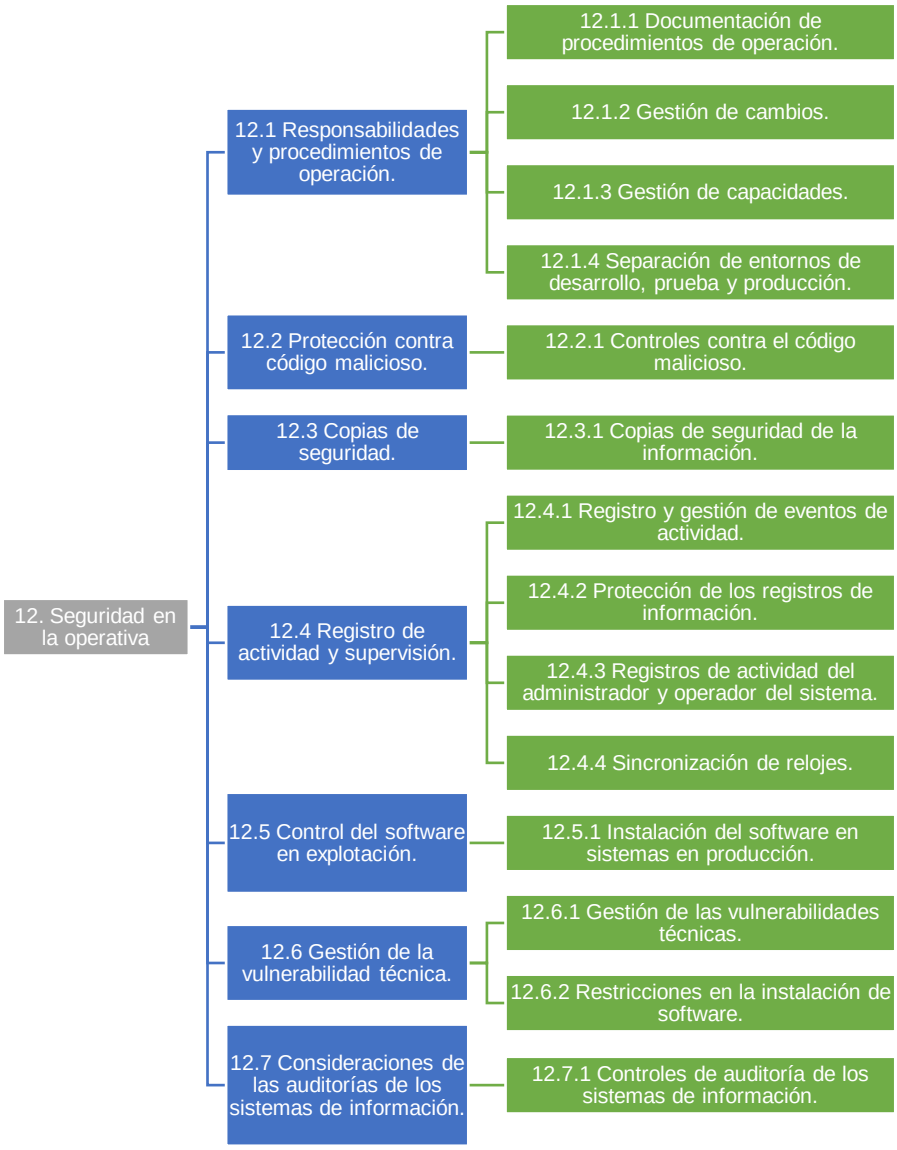
Seguridad en la operativa

El objetivo es manejo adecuado de la operación dentro de la empresa, ya sea en protección de documentos, protección de datos en el sistema para que no haya ninguna vulnerabilidad.

En la Figura 13 se puede observar que está compuesto la seguridad en la operativa por: siete objetivos de control y catorce controles:

Figura 13

Esquema de octavo dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

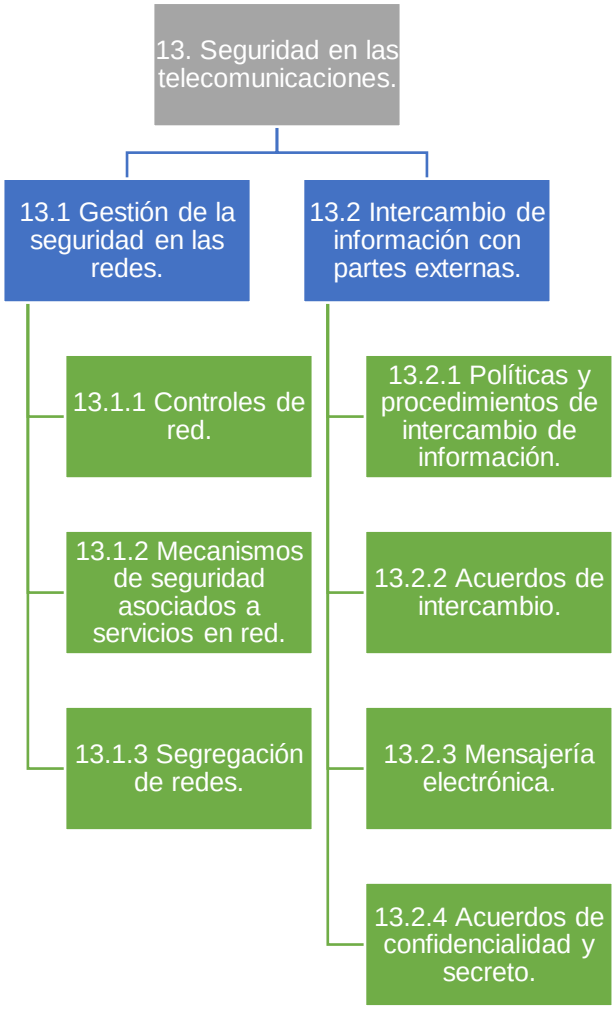
Seguridad en las telecomunicaciones

Su objetivo es a enfocar a la integridad y disponibilidad de los servicios de información y telecomunicación, para proteger la red y la infraestructura.

En la Figura14 se puede observar que está compuesta la seguridad en las telecomunicaciones por dos objetivos de control y siete controles:

Figura 14

Esquema de noveno dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

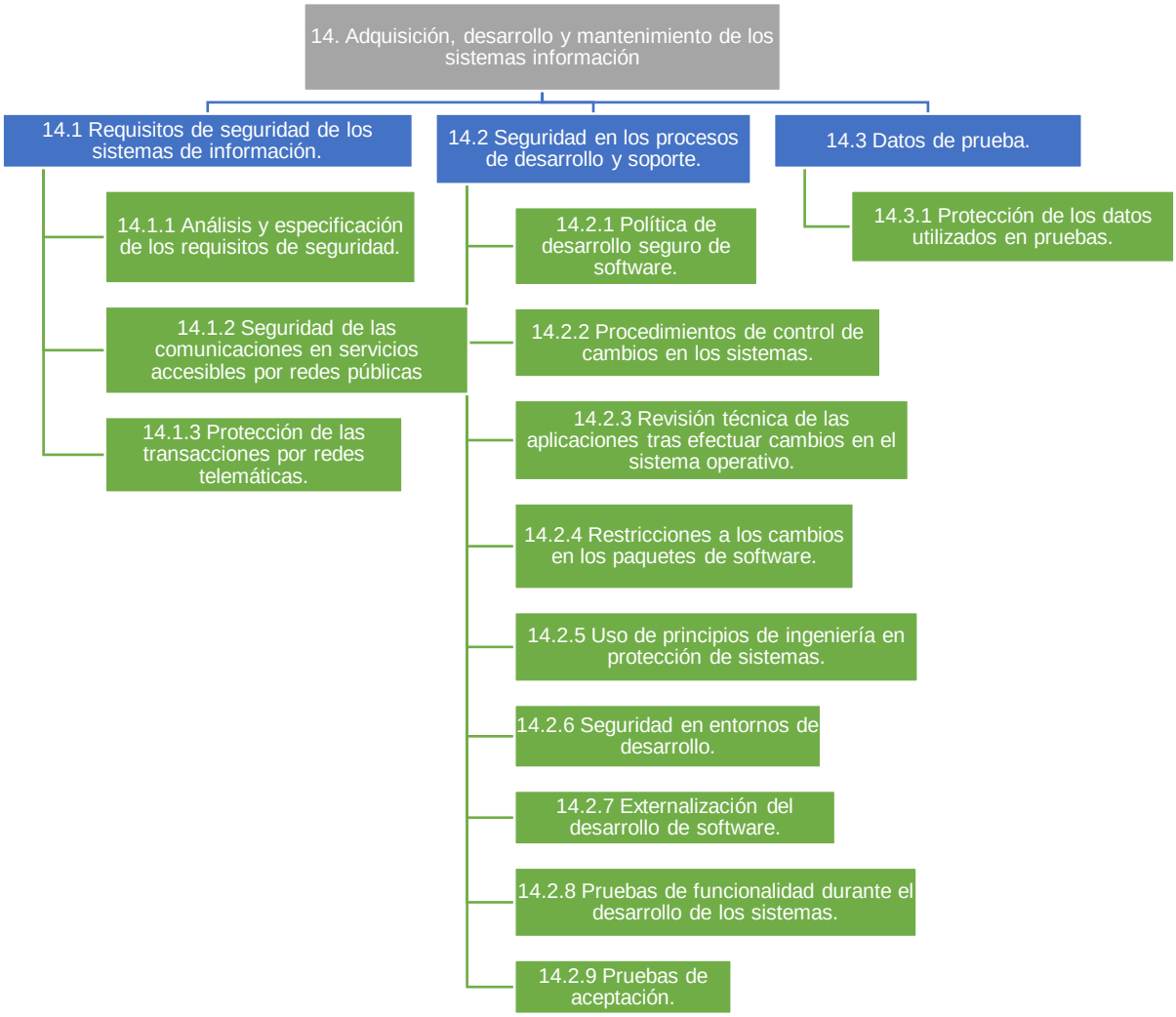
Adquisición, desarrollo y mantenimiento de los sistemas de información

Se enfoca en gestionar la seguridad en desarrollo, operación del sistema, mantenimiento del sistema para que no haya ninguna pérdida, mal uso de datos por el empleado de la empresa.

En la Figura 15 se puede observar que está compuesta la adquisición y mantenimiento de los sistemas de información por tres objetivos de control y trece controles:

Figura 15

Esquema de décimo dominio de la ISO 27002:2013



Nota. Fuente:(ISO/IEC 27002, 2013).

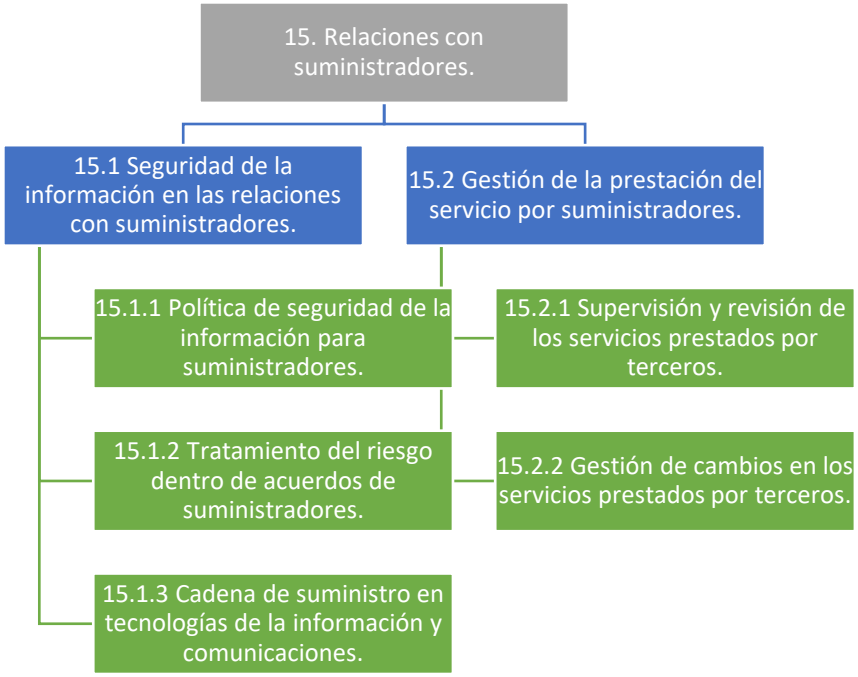
Relaciones con suministradores

Su principal objetivo es al enfoque de requisitos para tener una buena seguridad en la empresa u organización, evitando los riesgos que se puede exponer al momento de permitir al ingreso de proveedores a activos.

En la Figura 16 se puede observar que están compuestas las relaciones con suministradores por dos objetivos de control y cinco controles:

Figura 16

Esquema de undécimo dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

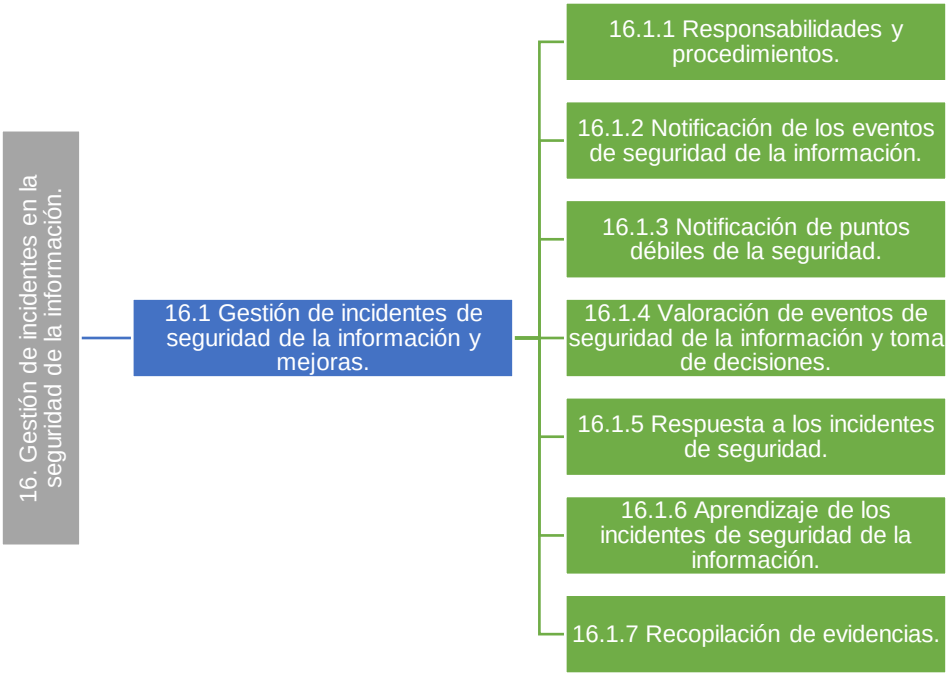
Gestión de incidentes en la seguridad de la información

Se enfoca al procedimiento y responsabilidad de algún evento que ocasiono algún problema que pueda ocasionar riesgo en la seguridad de la información, para lo cual se coge pruebas con la finalidad de tomar decisiones.

En la Figura 17 se puede observar que está compuesta la gestión de incidentes en la seguridad de la información por: un objetivo de control y siete controles:

Figura 17

Esquema de doceavo dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

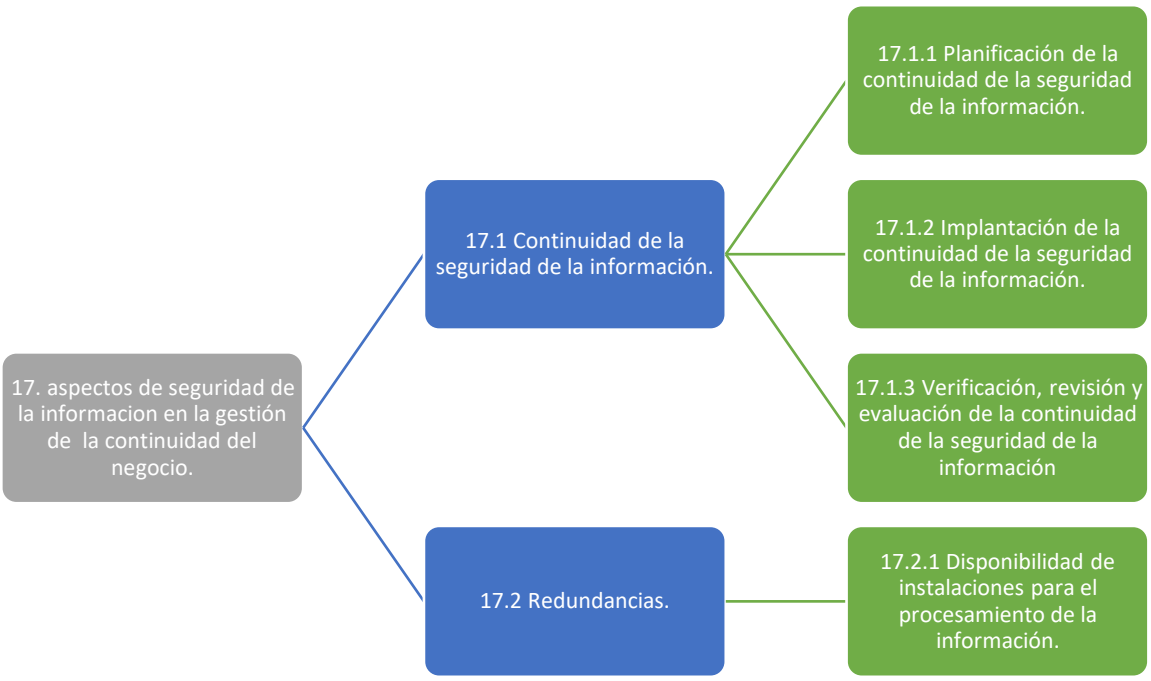
Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Se enfoca en actuar inmediatamente ante la suspensión de alguna actividad de negocios o desastres naturales, para evitar la pérdida de información, tiempo y dinero.

En la Figura 18 se puede observar que están compuestos los aspectos de seguridad de la información en la gestión de la continuidad de negocio por dos objetivos de control y cuatro controles:

Figura 18

Esquema de treceavo dominio de la ISO 27002:2013



Nota. Fuente:(ISO/IEC 27002, 2013)

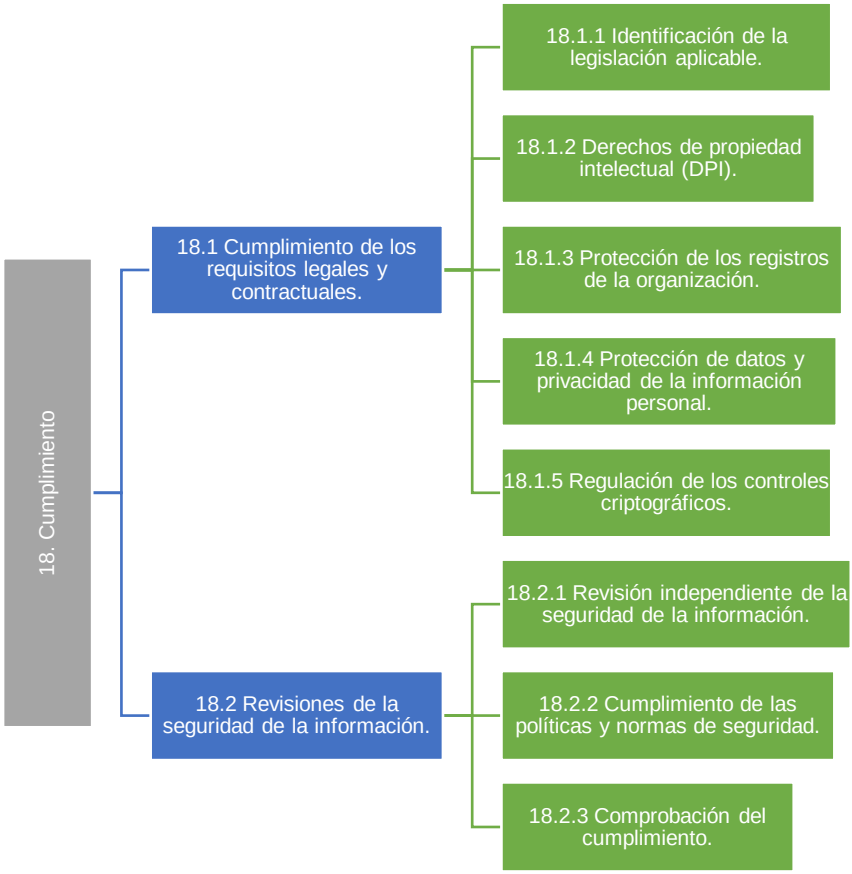
Cumplimiento

Su principal objetivo es la de cumplimiento de cualquier ley, estatuto, y cualquier requisito de la organización.

En la Figura 19 se puede observar que está compuesto el cumplimiento por: dos objetivos de control y ocho controles:

Figura 19

Esquema de catorceavo dominio de la ISO 27002:2013



Nota. Fuente: (ISO/IEC 27002, 2013).

1.5. Metodologías para gestión de riesgos

Hoy en día, mantener la seguridad de los sistemas informáticos es muy importante y requiere enfocarse en una etapa fundamental: la identificación, gestión y tratamiento de riesgos en toda la organización. Esto implica detectar y comprender las oportunidades y amenazas que pueden afectar los objetivos de negocio y adoptar un enfoque proactivo. Es esencial aplicar metodologías de análisis de seguridad informática relevantes para contextualizar y concienciar a las organizaciones sobre la importancia de utilizar estas metodologías para establecer mecanismos de seguridad adecuados según los riesgos y amenazas identificados. Además, es necesario integrar esta etapa en los Sistemas de Gestión de Seguridad Informática (SGSI) conforme a las normas y estándares establecidos.

En el proceso de la seguridad de la información existen diversas metodologías de gestión de riesgos, los cuales son:

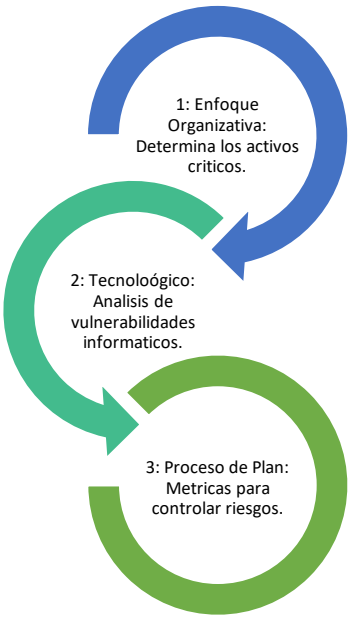
1.5.1. Octave

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) es una metodología realizada en el año 2001 por el CERT/CC, permite analizar las prácticas a la protección de seguridad para la decisión estratégica de información, es referente a los riesgos de integridad, confidencialidad, disponibilidad a los que pueden estar sometidos los activos con información crítica. También es distinto a las demás metodologías por el motivo de que no se restringe a análisis de riesgo informático, de la misma manera se enfoca al riesgo de la organización y estrategias de ámbito práctico (García& Moreta, 2019).

En la Figura 20 se puede ver las etapas que se debe seguir para el análisis de riesgos de la seguridad de la información con la metodología menciona anteriormente.

Figura 20

Etapas para el análisis de riesgo con la Metodología Octave



Nota. Elaboración propia

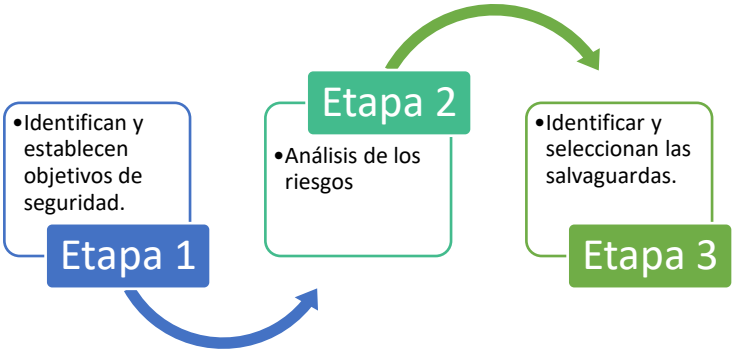
1.5.2. Cramm

La metodología se enfoca a detectar y realizar el control de riesgos que se puede presentar en sistema de la información, lo cual permite reconocer, evaluar y reducir los incidentes de seguridad que pueden estar expuestos en las organizaciones. Lleva a cabo un análisis de riesgo cualitativo y cuantitativo, conocido como metodología mixta, con el fin de tener un enfoque definido de las amenazas. Para llevar a cabo este análisis, es necesario crear una matriz para representar los activos y riesgos que pueden afectar adversamente la

disponibilidad, integridad y confidencialidad de la información. En la tabla de la matriz, los elementos o activos son muy valiosos, que se deben ser organizados en filas, mientras que los riesgos se organizan en columnas. (Miranda, 2021). En la Figura 21 se pueden observar las etapas de implementación de la metodología para detectar el análisis de riesgos.

Figura 21

Etapas de Cramm



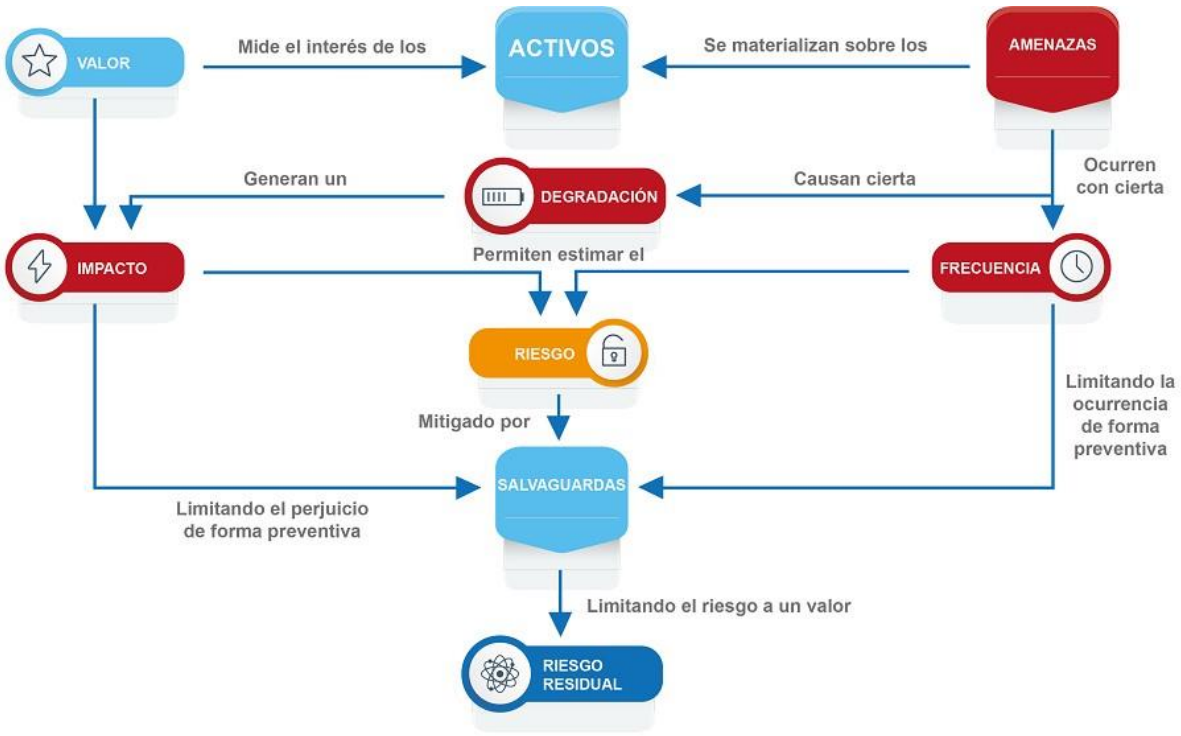
Nota. Elaboración propia

1.5.3. Magerit v3

La metodología de Margerit v3 es la de otorgar un marco de trabajo para identificar los activos, identificar amenazas, evaluar y gestionar los riesgos. Es una metodología de gestión de riesgos de la información, la que permite estudiar los riesgos que soporta un sistema de información y el entorno asociado al mismo, la metodología detalla desde tres perspectivas: describir los paso para efectuar un análisis del estado del riesgo y gestionar su mitigación, describe tareas básicas para realizar un proyecto de análisis y gestión de riesgos. Permite descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación y los resultados se expresan en valores económicos (Crespo, 2018). En la Figura 22 se puede observar el proceso para la implementación de la metodología de Magerit V3.

Figura 22

Implementación de la metodología Magerit



Nota. Fuente: (CCN-CERT, 2023)

La metodología Margerit v3 se enfoca en los siguientes objetivos:

- Fortalecer la capacidad de gestión de riesgos dentro sistema de la información de organización.
- Determinar un proceso metódico para identificar los riesgos que pueda tener la organización.
- Colaborar en la identificación y la estrategia de tratamiento adecuado para mantener bajo control los riesgos.
- Alistar a la organización, para futuros planes de certificación o acreditación, según lo que sea relevante en cada circunstancia particular.

Estructura de la metodología Magerit

La metodología está conformada por 3 libros (Libro I-Método, Libro II- Catálogo de Elementos, Libro III- Guía de técnicas), que componen la documentación de MAGERIT V3, fue desarrollado por el Centro Criptológico Nacional de España. Los libros ayudan a analizar, realizar control y gestión de los riesgos de la organización.

Libro I Método: Hace referencia a las tareas involucradas en el análisis y la gestión de riesgos como parte de un proceso global. Asimismo, proporciona alternativas y estándares para abordar de manera efectiva los riesgos.

Libro II Catálogo de Elementos: Ofrece una categorización de los recursos, variados aspectos y estándares para llevar a cabo la evaluación. Además, se mencionan las amenazas comunes que afectan a los sistemas de información y las medidas de protección correspondientes.

Libro III Guía de Técnicas: Este libro presenta las metodologías empleadas en la evaluación y administración de riesgos, detalla el propósito detrás de su aplicación, identifica los componentes esenciales vinculados a ellas y expone los principios fundamentales para su desarrollo.

1.5.4. Comparación de metodología de gestión de riesgos

En la tabla 6 se ha realizado una comparativa de cada una de las metodologías de análisis de riesgo.

Tabla 6

Metodologías de análisis de riesgos

Metodología	Octave	Cramm	Magerit V3
País	EE.UU	Francia	España
Idioma	Inglés	Inglés	Español e inglés
Año	2011	2005	2013
Enfoque	Desarrollo propietario	Basado en estándares	Basado en estándares
Tipo de enfoque	Cualitativo	Cualitativo	Cuantitativo y cualitativo.
Dimensiones	Disponibilidad, confidencialidad, integridad	Disponibilidad, confidencialidad, integridad	Disponibilidad, confidencialidad, integridad, autenticación, trazabilidad
Área de aplicación	Pymes	Organizaciones gubernamentales, empresas privadas.	Organizaciones gubernamentales, empresas privadas, pequeñas y medianas empresas (pymes).
Ventajas	Documentación disponible. Involucra a todos los actores de la organización. En torno de colaboración. En el modelo de análisis se incluyen los siguientes componentes: procesos, activos, conexiones, recursos, debilidades, riesgos y medidas de protección.	Documentación disponible. Reconoce y organiza los recursos de tecnología de la información	Documentación disponible. Concientiza la sensibilización a los usuarios de la existencia de riesgos. Evalúa los activos desde diversas perspectivas. Dispone de una vasta colección de registros de inventario relacionados con amenazas y la naturaleza de los recursos

	Se ajusta según las dimensiones de la entidad, proporcionando una variante adecuada para cada situación específica.		Se encuentra adecuadamente registrada en lo que respecta a las categorías de activos de información y amenazas. Ofrece diversos métodos para calcular riesgos. Es la más actual a comparación de otras metodologías. La versión original se encuentra en español. Utilizada en una gran cantidad de entidades en España y Latinoamérica.
Desventajas	No ofrece una descripción pormenorizada de la categorización de los activos de la seguridad de la información. Muestra una cantidad excesiva de anexos. No detecta de manera oportuna los riesgos significativos para la entidad	No incluye aspectos clave como los procedimientos y los activos esenciales	No considera procesos, recursos ni debilidades como componentes del modelo propuesto. Carece de un inventario exhaustivo en lo que respecta a políticas.

Nota: Elaboración propia

CAPÍTULO 2

Desarrollo del proyecto

2.1. Consideraciones generales

Para determinar la importancia de los riesgos, es necesario llevar a cabo una evaluación. Mediante este proceso analítico, se establecerá si la información está en riesgo de ser expuesta, ya sea dentro de la organización o fuera. El éxito se basará en la adecuada implementación de las políticas de seguridad vigentes en el departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Para ello, se detallarán las consideraciones generales que existen en el departamento de Tecnología de Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., ya que cada una de ellas reviste una gran importancia.

2.1.1. Misión

Ejecutar y coordinar la ejecución de las actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones.

2.1.2. Visión

Generar la planeación estratégica para el Departamento de Tecnologías de la Información, para el establecimiento y materialización de metas y objetivos, y, que están directamente alineados a la Planeación Estratégica Institucional de la Cooperativa, identificando la situación actual de la cooperativa, proponer un modelo negocio (de ser el caso), y la implementación de estrategias de TI.

2.1.3. Objetivo del departamento de Tecnología de información

Planificar, administrar los recursos de hardware, software, información y personas del Departamento de Tecnología de la Información coordinar con el resto de las áreas, la ejecución operativa de los procesos de la institución, implementación de soluciones de software.

2.1.4. Valores

Los valores de mayor relevancia para el Departamento de Tecnologías de la Información (DTI) de la Cooperativa de Ahorro y Crédito Imbacoop Ltda. incluyen:

- **Integridad:** En el departamento de Tecnologías de la Información, nos regimos por la integridad en todas nuestras acciones y decisiones, asegurando que la ética y la honestidad sean fundamentales en nuestro trabajo.
- **Seguridad:** La seguridad de la información es nuestra prioridad. Mantenemos la confidencialidad, integridad y disponibilidad de los datos y sistemas para proteger a la cooperativa y sus socios.

- **Colaboración:** Fomentamos la colaboración estrecha, trabajando en equipo con otros departamentos y nuestros socios para impulsar la innovación y la eficiencia.
- **Innovación:** Abrazamos la innovación como parte de nuestra cultura, manteniéndonos al día con las últimas tendencias tecnológicas y buscando soluciones creativas a los desafíos.
- **Orientación al cliente:** Nos centramos en las necesidades y expectativas de nuestros socios, brindando soluciones tecnológicas que satisfagan sus requerimientos.
- **Eficiencia:** Gestionamos nuestros recursos y procesos de manera eficiente, optimizando costos y maximizando el valor de TI para la cooperativa.
- **Adaptabilidad:** Siendo conscientes de la constante evolución tecnológica, somos flexibles y adaptables para afrontar los cambios.
- **Transparencia:** Mantenemos la transparencia en todas nuestras comunicaciones y decisiones, fomentando la confianza y la claridad en nuestro trabajo.
- **Responsabilidad:** Asumimos la responsabilidad de nuestras acciones y de los resultados de nuestros proyectos y tareas, garantizando un enfoque de calidad y cumplimiento.

2.1.5. Funciones y encargados

A continuación, se describe la función desempeñada por el personal dentro de la siguiente tabla 7:

Tabla 7

Responsables

Responsables de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.	Responsable del Departamento de TI Cooperativa de Ahorro y Crédito Imbacoop Ltda.
Asamblea General Consejos Administrativos Gerente General	Director de desarrollo tecnológico e informático

Nota: Elaboración propia

Fuente: Propia

2.2. Entorno Organizacional

2.2.1. Identificación del problema

La matriz de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., ubicada en la ciudad de Otavalo, comunidad La Compañía, en la Figura 23, se puede mirar la dirección. Es una

organización muy relevante por la calidad de servicio que brindad, por tal razón ha mejorado los componentes tecnológicos, está excelentemente preparada en cuanto a la infraestructura tecnológica en los últimos años.

También los procesos que necesita realizar en cada actividad se lo hacen por medio del sistema financiero y los activos relacionados, lo cual ocasiona mayor manipulación de información por parte de los usuarios, esto lleva a la presencia de vulnerabilidades en los activos de la información ocasionados por: errores humanos, falta de capacidad, acceso no autorizado, falta de actualización de parches; estas amenazas pueden causar un alto riesgo dentro del sistema de información.

A pesar de llevar todos los procesos necesarios de cada actividad por medio de sistema financiero que posee dentro de la organización, no cuenta con un Plan de Sistema de Gestión de Seguridad de la Información, por lo tanto, puede incrementar las vulnerabilidades dentro de seguridad de la información. El departamento de Tecnología de Información tiene la obligación de implementar controles, políticas de seguridad de la información en sistema financiero y los demás activos.

Figura 23

Dirección de la Cooperativa Imbacoop.

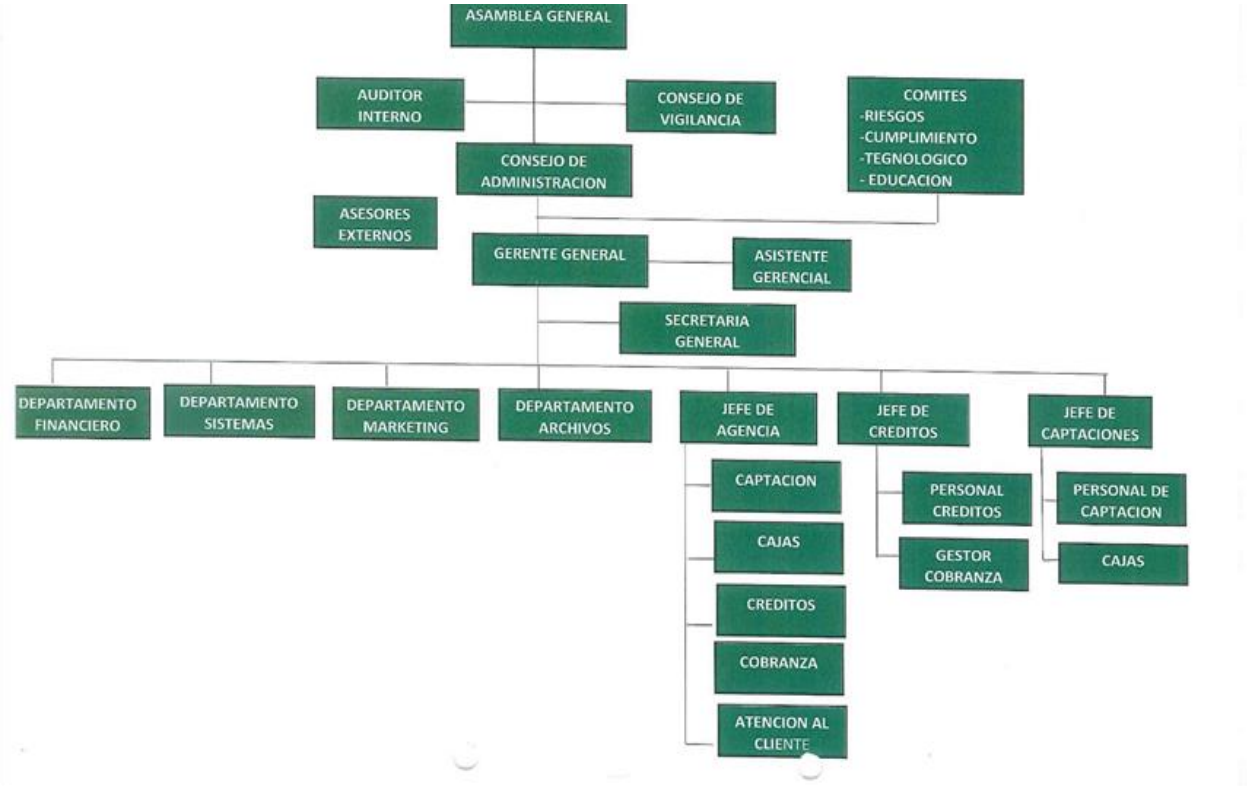
Nota. Fuente: (Google Maps, 2023)

2.2.2. Estructura Organizacional de la Cooperativa de Imbacoop Ltda

La Cooperativa de Ahorro y Crédito Imbacoop Ltda. se compone de los siguientes niveles administrativos, tal y como se describe en la Figura 24.

Figura 24

Organigrama estructural de la Cooperativa.



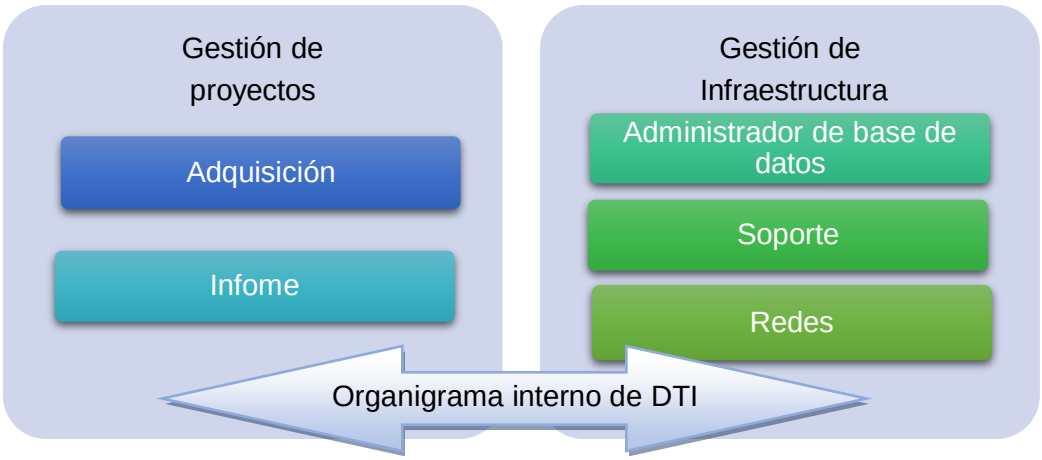
Nota. Fuente: (Imbacoop, 2023).

2.2.3. Organigrama interno del Departamento de Tecnológico de Información Coop. Imbacoop

Para la Cooperativa de Ahorro y Crédito Imbacoop Ltda., el Departamento de Tecnología de Información (DTI) es muy necesario para su correcto funcionamiento. El nivel de importancia de este departamento radica en su composición, que incluye lo siguiente: redes, administrador de base de datos, desarrollo, informe. De igual manera, se puede presenciar en la Figura 25.

Figura 25

Organigrama de DTI



Nota. Elaboración propia

2.3. Departamento de Tecnología de Información

2.3.1. Funciones Cruciales

Las funciones cruciales son aquellas que aportan valor y están alineadas con la dirección estratégica de la organización, garantizando así su continuidad empresarial, en el Departamento de Tecnología de la información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se han identificado como funciones cruciales lo siguiente:

Redes: Es un sistema de unidades, personas o entidades conectadas electrónica o físicamente para facilitar la comunicación, la colaboración y el intercambio de información, recursos y servicios. Gracias a las redes, la tecnología funciona ahora en Internet, lo que permite actividades a distancia como video llamadas y otras formas de trabajo a distancia.

Base de datos: Una base de datos se utiliza para facilitar la gestión eficaz de la cooperativa, ayudándola a registrar con precisión sus actividades, tomar decisiones informadas y servir a sus miembros de forma eficaz. Puede gestionarse mediante un software especializado de gestión de bases de datos o un sistema de información diseñado para satisfacer las necesidades específicas de la cooperativa.

Sistema Financiero: Varían en tamaño y complejidad, desde los ordenadores personales utilizados en casa hasta los sistemas integrados en servidores corporativos, centros de datos y dispositivos electrónicos utilizados en entornos corporativos. El diseño y la implantación de sistemas informáticos dependen de las necesidades específicas de la aplicación y de los recursos disponibles.

2.3.2. Nivel de seguridad actual.

Con el propósito de obtener información sobre el nivel de seguridad actual, se llevó a cabo una entrevista al jefe de Departamento de Tecnología de Información de la Cooperativa

de Ahorro y Crédito Imbacoop Ltda., en el Anexo 1 se halla las preguntas que se realizó en la entrevista, por medio ello se obtuvo los siguientes resultados que se detalla a continuación:

En el departamento de Tecnología de la información y en el ámbito del sistema financiero, se observa un grado sustancial de desviación en lo que respecta a regulaciones que se mencionan en la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013. Los puntos destacados que ilustran esta condición son los siguientes:

- Los servidores operan con cuatro discos, cada uno con una capacidad de un terabyte. La base de datos es de pequeño tamaño, y el respaldo diario de datos se sitúa en 400 MB por día.
- La información que gestionamos en formato digital se considera un activo de la Cooperativa de Ahorro y Crédito Imbacoop Ltda. Por lo tanto, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es esencial.
- Actualmente, no se han implementado medidas de seguridad de la información.
- En cuanto al personal, cuentan con formación en informática y algunas disciplinas relacionadas. No obstante, es crucial resaltar la necesidad de contar con un equipo que posea y se ajuste al perfil requerido para la gestión de la seguridad de la información.
- Las políticas internas que se aplican brindan protección al sistema financiero, no obstante, es importante enfatizar que la seguridad no es absoluta, por lo que continuamos perfeccionando nuestras políticas.
- Se lo hace cada trimestral o cada 6 meses, depende al comité de tecnologías que se tiene a menudo, por ellos se lo lleva a las directrices, se va formando, enumerando de acuerdo con vulnerabilidades o problemas que tenga nuestro sistema financiero, tanto de acceso o como de salida del servidor desde la matriz.
- Esto no significa que estemos completamente seguros en todo momento; es fundamental seguir mejorando y aplicando nuevos métodos de seguridad de manera constante.
- Se utilizan servidores dedicados para cada aplicación, incluyendo servidores de aplicaciones y servidores de bases de datos. La información de la base de datos se almacena en un servidor NAS que es altamente confiable.
- No tiene unas políticas y directrices bien documentadas para poner en marcha si se detecta este tipo de incidentes.
- Poseen controles internos que se manejan en el Departamento de Tecnología de Información, y esos controles son aprobados por la parte administrativa de la

cooperativa y eso es lo que se maneja actualmente, sin embargo, no están bien establecidas.

2.3.3. Controles existentes

A pesar de que no se lleva a cabo una documentación de control de manera exhaustiva, la organización implementa algunas actividades de control internas con el propósito de reducir y prevenir los riesgos que puedan afectar a sus activos. Estas medidas internas se diseñan y ejecutan de manera proactiva para garantizar la seguridad de los recursos y bienes de la organización, así como para mantener la continuidad de las operaciones en un entorno en constante evolución. Estas actividades se detallan en la Tabla 8.

Tabla 8

Controles Existentes

Amenazas	Controles
Físicas y naturales.	Sistema de energía. Climatización. Permiso Individual Aprobado. Medidas de seguridad física para el acceso. Backups.
Humanos.	Antivirus. Firewall.
Personal.	Personal con la formación necesaria para soporte.

Nota: Elaboración propia

2.4. Aspectos iniciales

2.4.1. Alcance y Objetivos de SGSI

El departamento de Tecnología de Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., es necesario definir los límites y la importancia de los sistemas de gestión de la seguridad de la información.

Alcance de SGSI: El propósito del trabajo creado es con la finalidad de desarrollar un Plan de Sistema de Gestión de la Seguridad de la Información para lograr la conservación de información del sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ldta, el desarrollo de un Plan de SGSI establece controles para mantener a salvo los activos que conforma al sistema financiero, que los elementos son fundamentales para el correcto funcionamiento de sus actividades.

Objetivos de SGSI:

- Obj 1: Garantizar la seguridad del sistema financiero y sus activos relacionados que poseen informaciones del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

- Obj 2: Contribuir al logro de los objetivos establecidos en la Cooperativa a través de una gestión eficiente de los riesgos relacionados con la seguridad de la información.
- Obj 3: Determinar medidas de seguridad eficaces con el propósito de resguardar los activos de información y sistema financiero, con la finalidad de fortalecer la confidencialidad e integridad.

2.4.2. Partes Interesadas

Las partes conformadas en el desarrollo de un Plan de SGSI se detallan a continuación:

Cooperativa de Ahorro y Crédito Imbacoop Ltda: Se ha observado un notable progreso en el sistema financiero y sus infraestructuras tecnológicas, lo cual ha permitido ofrecer una amplia gama de servicios. Sin embargo, la falta de un plan adecuado de Sistema de Gestión de la Seguridad de la Información (SGSI), controles, políticas de seguridad de la información podría aumentar la probabilidad de enfrentar amenazas que pongan en riesgo la seguridad de los recursos financieros.

DTI: En la actualidad, el Departamento de Tecnología de la Información es el encargado de establecer las normas de la seguridad de la información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Autor del trabajo: El estudiante de la carrera de ingeniería en software de la Universidad Técnica del Norte, se encuentra realizando un Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27002:2013 que pueda satisfacer las necesidades de Cooperativa de Ahorro y Crédito Imbacoop Ltda.

2.4.3. Requerimientos para establecer controles de SGSI

El personal que se encarga de tecnologías de la información a diario se enfrenta con problemas con recursos que poseen en la empresa para llevar una gran cantidad de informaciones muy importantes de la identidad. Es por ello que la empresa necesita proteger la información porque es su activo muy valioso, estableciendo controles adecuados.

Al establecer los controles de SGSI basados en la Norma ISO 27002:2013, en la identidad, puede mejorar en protección, mantenimiento de sistema financiero y los demás activos de la información. El Sistema de Gestión de la Seguridad de la Información se realiza mediante políticas de seguridad, para que se cumplan con las necesidades requeridas de la organización con el fin de cumplir sus objetivos.

El proceso de desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información (SGSI) se centra en lograr una gestión eficaz y en la mejora continua de la gestión de riesgos. La implementación de estos controles contribuirá a salvaguardar y gestionar la

información de manera adecuada, garantizando la seguridad y un seguimiento apropiado. Esto, a su vez, permitirá mantener los controles actualizados y funcionando correctamente.

2.4.4. Elementos disponibles

Las posibilidades existentes para desarrollar un Plan de Sistema de Gestión de Seguridad de la Información enfocado a los controles de la ISO/IEC 27002:2013, a continuación, se listan:

Cooperación de la organización: La organización respalda de manera íntegra la realización del trabajo de grado. Las identidades que respaldan son las siguientes:

- Respaldo de la carrera de software.
- Respaldo de las autoridades de la Cooperativa de Ahorro y Crédito Imbacoop Ldta.
- Respaldo de DTI.

Metodología: La elección de la metodología, basada en investigaciones de otros autores, contribuye a la identificación y desarrollo de la investigación que se está llevando a cabo para el trabajo, también es una metodología flexible y completa que aborda los aspectos técnicos y organizativos de la seguridad de la información, permitiendo a la organización la identificación, evaluación y gestión de los riesgos de cada uno de los activos que poseen informaciones muy importantes de la empresa:

- Metodología para la gestión de riesgos (Magerit v3).

Herramienta: La herramienta escogida ayuda en la gestión y análisis de riesgos, lo cual permite llevar gran cantidad de información para que sea más didáctica y ágil en la realización de las actividades necesarias. Además, la elección se basa en la colaboración estrecha con la metodología Magerit v3.

- La herramienta Pilar facilita para realizar la gestión de riesgos.

2.4.5. Elemento crítico identificado

Dado que la función principal del Departamento de Tecnología de la Información se centra en brindar apoyo mediante sistema financiero, se ha determinado que la automatización de ciertas tareas es de suma importancia para ofrecer una atención de alta calidad. La automatización de estas actividades posibilitará a la institución ahorrar tiempo, mejorar la experiencia del usuario y reducir la probabilidad de errores en las tareas cotidianas de la Cooperativa. Por lo tanto, es fundamental asignar esfuerzos y recursos a este proceso prioritario, en aras del éxito sostenible a largo plazo del Departamento de Tecnología de la Información.

En consecuencia, la cooperativa ha implementado un sistema denominado 'sistema financiero' que facilita un registro detallado tanto de los usuarios como del personal empleado y administrativo, así como la provisión de una amplia gama de servicios a través de esta plataforma.

Por lo tanto, se puede observar que este proceso es altamente complejo y afecta a numerosas áreas de la institución, debido a la gran cantidad de datos que genera, los cuales deben ser protegidos de manera integral.

2.5. Metodología Magerit v3 para la gestión de riesgos

Para determinar la gestión de riesgos, se eligió el método Magerit v3, que permite evaluar en profundidad las necesidades y requisitos específicos de la cooperativa. Este método se caracteriza por la capacidad de estimar con precisión el valor del servicio o la información analizada y determinar así el nivel de protección necesario.

Sus principales objetivos son identificar, analizar y gestionar los riesgos relacionados con la seguridad de la información y los sistemas de información. Esto incluye la evaluación de amenazas, vulnerabilidades y activos de información y la forma de mitigar o afrontar adecuadamente los riesgos.

Lo que hace único a esta metodología Magerit es su enfoque objetivo, que evita depender de juicios subjetivos que pueden dar lugar a decisiones improvisadas. Además de sus objetivos principales, MAGERIT también incluye otros objetivos que enriquecen su planteamiento, creando un enfoque completo y exhaustivo:

- Fortalecer la capacidad de gestión de riesgos dentro del sistema de la información de organización.
- Determinar un proceso metódico para identificar los riesgos que pueda tener la organización.
- Colaborar en la identificación y la estrategia de tratamiento adecuado para mantener bajo control los riesgos.
- Alistar a la organización para futuros planes de certificación o acreditación, según lo que sea relevante en cada circunstancia particular.

2.5.1. Pilar

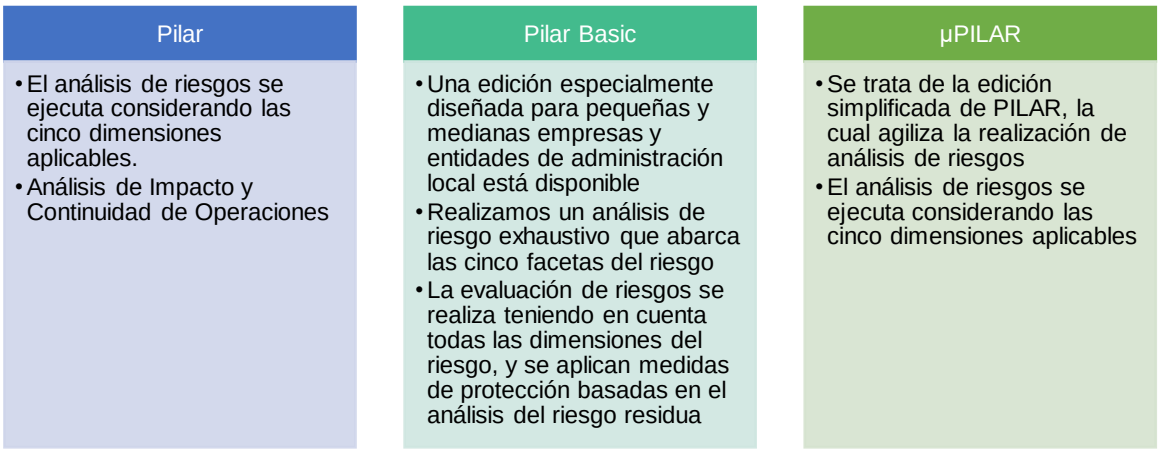
El software Pilar, que constituye la columna vertebral del método MAGERIT, se utiliza para automatizar y facilitar el proceso de análisis de riesgos en los sistemas de información, lo que ayuda a gestionar la seguridad de la información de manera más eficaz y a tomar decisiones informadas sobre la implementación de medidas de protección(Centro Criptológico Nacional, 2023).

Según Celis (2018) afirma que el software Pilar, en la mayoría de las versiones, ofrece seguridad y contramedidas eficaces para la gestión del riesgo basadas en el análisis del riesgo residual en las distintas fases del proceso.

En la Figura 26 se detallan diferentes pilares que existen y cada una de sus características:

Figura 26

Versiones del software Pilar.



Nota. Elaboración propia

2.6. Activos

2.6.1. Identificación de los activos

En esta etapa, se llevó a cabo la identificación de activos críticos en el contexto de los procesos internos de la organización. Se define como activo cualquier recurso que posea un valor significativo para el funcionamiento y la continuidad de la organización. A fin de garantizar su preservación y disponibilidad, se empleó la metodología MAGERIT y se presenta la clasificación de estos activos en la Tabla 9, según el segundo apartado de la metodología, denominado Catálogo de Elementos.

Tabla 9

Clasificación de activos de acuerdo con la Metodología MAGERIT

Tipo de Activos.	Descripción
Datos / Información	Se refiere a informaciones relevantes de la organización, como, por ejemplo: informes, guías, procesos, etc.
Servicios	Mantenimiento de computadoras, soporte. Sistema financiero, herramientas tecnológicas, base de datos, etc.

Software	Sistema financiero, herramientas tecnológicas, base de datos, etc.
Hardware	La parte, infraestructura de la empresa, por ejemplo: servidor, computadoras.
Redes de comunicación	Son aquellos servicios de comunicación como: teléfonos, radio, celular.
Soportes de información	Se refiere al medio físico o tecnológico que es utilizado para almacenar y respaldar datos, archivos como, por ejemplo: documentos impresos, discos duros, memoria, USB, CD, nube.
Equipamiento auxiliar	Son dispositivos o herramienta para apoyar un equipo o sistema principal para su funcionamiento, estos son los siguientes: computadora (teclado, mouse), componentes electrónicos (cables, adaptador, cargadores).
Instalaciones	Se refiere a los espacios físicos, estructuras donde se encuentra los sistemas de información como, por ejemplo: departamento, vehículos, empresa
Personal	Es un miembro de la organización donde trabaja, por ejemplo: usuarios, desarrolladores, secretaria, técnicos, etc.

Nota: Elaboración propia, información basada en Dirección General de Modernización Administrativa, 2012. *Fuente: (Dirección General de Modernización Administrativa, 2012a).*

La determinación de activos se llevó a cabo utilizando el documento proporcionado por el director del Departamento de Tecnología de la Información y siguiendo la clasificación establecida por la metodología MAGERIT. En la Tabla 10, se detallan los 34 activos identificados.

Tabla 10

Identificación de activos y su código

Tipo de activos	Activo	Código
	Base de datos	D-01
Datos/Información	Documentación interna	D-02
	Servidor NAS	S-01
	Electricidad	S-02
Servicios	Internet	S-03
	Telefonía	S-04
	Mantenimiento	S-05
	Correo	S-06
	Desarrollo a media	SW-01

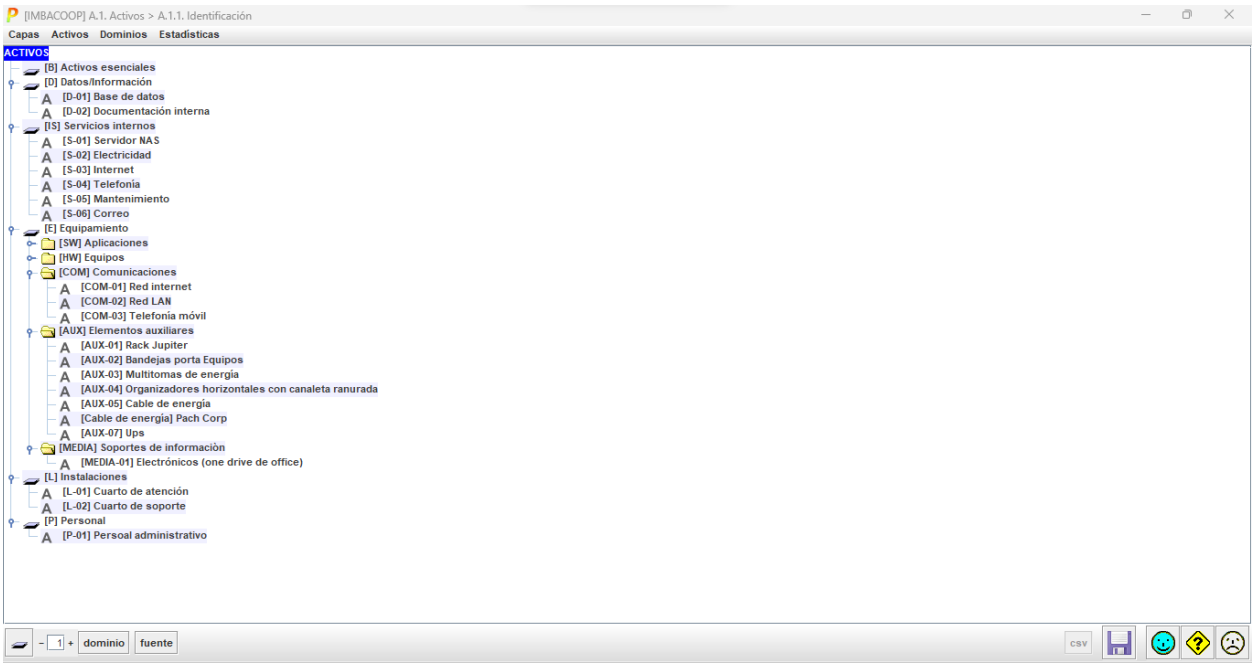
Software	Antivirus	SW-02
	Firewall	SW-03
	Licencias	SW-04
	Sistemas operativos	SW-05
Hardware	Laptop	HW-01
	Monitor	HW-02
	HPE Smart Buy	HW-03
	Impresora	HW-04
	Router Board Microtik 3011	HW-05
	Switch 24 puertos Cat. 5E	HW-06
	Unifi Uap-ac-lite	HW-07
Redes de comunicación	red internet	COM-01
	red digital	COM-02
	telefonía móvil	COM-03
Soportes de información	Electrónicos (one drive de office)	MEDIA-01
Equipamiento auxiliar	Rack Jupiter – Puerta de acero y vidrio	AUX-01
	Bandejas porta Equipos	AUX-02
	Multitomas de energía	AUX-03
	Organizadores horizontales con canaleta ranurada	AUX-04
	Cable de energía	AUX-05
	Pach Corp	AUX-06
	Ups	AUX-07
Instalaciones	Cuarto de atención	L-01
	Cuarto de soporte	L-02
Personal	Personal administrativo	P-01

Nota: Elaboración propia, 2023

En la Figura 27 se puede visualizar la identificación de los activos en software pilar.

Figura 27

Identificación de los activos de Sistema Financiero



Nota. Elaboración propia

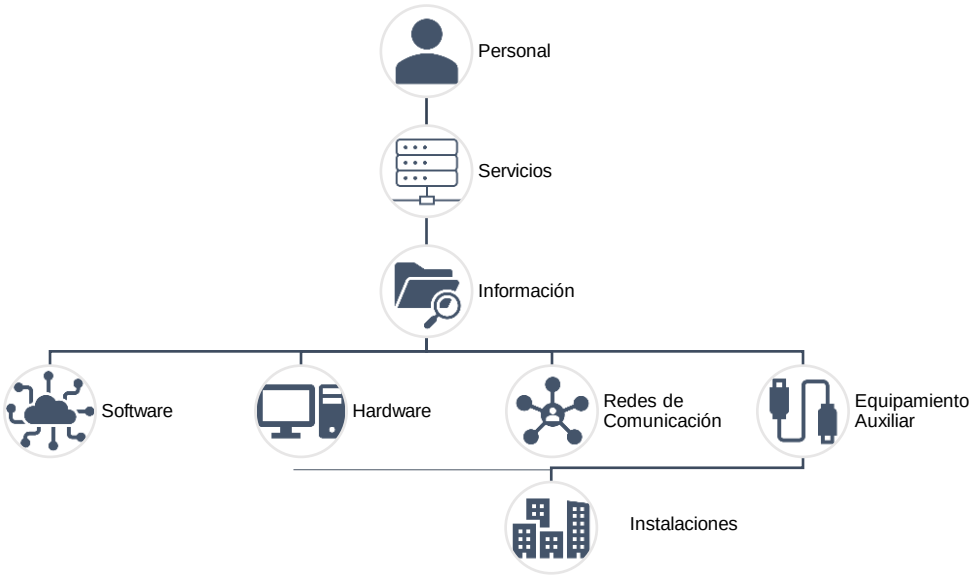
2.6.2. Dependencia entre activos

Tras identificar los activos relacionados con el funcionamiento de sistema financiero del Departamento de Tecnología de Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., es vital considerar sus relaciones entre sí. Aunque no se hayan abordado explícitamente en el análisis de riesgos para simplificarlo, es esencial reconocer que un riesgo alto en los activos inferiores puede desencadenar efectos en cadena en los superiores. En este contexto, es crucial reconocer la importancia del factor humano en todas las categorías de activo; por lo tanto, cada grado de los activos depende de uno y del otro. Si un activo falla,puede ser perjudicial para la organización.

En el siguiente Figura 28, se encuentra un resumen de las conexiones entre las diferentes categorías de activos.

Figura 28

Dependencia entre activos



Nota. Elaboración propia

2.6.3. Valoración de activos

La valoración de activos se puede hacerse cuantitativamente, especificando valores numéricos. Una comprensión detallada del proceso de tasación es esencial para obtener una valoración precisa de los activos. Esto incluye un análisis minucioso de todos los documentos pertinentes de la organización y llevar a cabo una encuesta al director de departamento de Tecnologías de la Información (DTI). La Metodología Magerit evalúa, la relevancia de los activos se manifiesta en siguientes dimensiones, como se detalla en la Tabla 11.

Tabla 11

Definiciones de las dimensiones de valoración de activos

Dimensión de valoración	Definición
Confidencialidad(C)	Atributo que implica que la información no es compartida ni revelada a personas, entidades o procesos no autorizados
Integridad(I)	Atributo o propiedad que se refiere a que el recurso de información no ha experimentado modificaciones no permitidas.

Nota. Elaboración propia, información basada en la Dirección General de Modernización Administrativa, 2012.

Fuente: (Dirección General de Modernización Administrativa, 2012a)

Para llevar a cabo la valoración de los activos, se han formulado las preguntas pertinentes con el objetivo de recopilar información en relación con los valores atribuidos a cada activo por parte del director de Tecnologías de la Información (DTI).

- **Confidencialidad**

¿Cómo afectaría al departamento de tecnología de información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda. que los datos que se obtiene en el sistema financiero fueran conocidos por usuarios no autorizados?

¿El acceso no autorizado a la información puede perjudicar la imagen de la organización?

¿La divulgación no autorizada podría revelar datos sensibles de la empresa críticos para las decisiones criticas para la estrategia y financiera?

- **Integridad**

¿Qué impacto tendría para el departamento de tecnología de información que los datos del sistema financiero si fueran falsos, alterados o estuvieran incompletos?

¿Si la información que se maneja por medio del sistema financiero es alterada sin autorización, puede perjudicar la imagen de la identidad?

¿Si la información que se maneja por medio del sistema financiero es alterada sin autorización puede provocar sanciones de entes de control?

Según Magerit versión 3, la evaluación cuantitativa depende del criterio y se basa en la escala de la Tabla 12. En el Anexo 2, se encuentra la información detallada sobre la herramienta utilizada y la evaluación obtenida para cada activo en función de los parámetros evaluados, las cifras que se extraen de esta tabla representan la evaluación del impacto para la organización en el supuesto de que el activo experimente daños en dicha dimensión.

Tabla 12

Criterios de Valoración de activos

Nivel	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

Nota. Elaboración propia, información basada en Dirección General de Modernización Administrativa, 2012.

Fuente: (Dirección General de Modernización Administrativa, 2012a)

En la Tabla 13 se encuentra la asignación de cada uno de los pilares de seguridad (Integridad, confidencialidad) y la valoración de los activos del sistema financiero del DTI de la Cooperativa.

Tabla 13

Valoración de activos

Tipo de activos	Activo	Código	I	C	Peso ponderado	Valor
Datos/Información	Base de datos	D-01	10	10	10	Extremo
	Documentación interna	D-02	9	8	9	Muy Alto
Servicios	Servidor NAS	S-01	8	10	9	Muy Alto
	Electricidad	S-02	7	7	7	Alto
	Internet	S-03	8	8	8	Alto
	Telefonía	S-04	7	7	7	Alto
	Mantenimiento	S-05	7	7	7	Alto
	Correo	S-06	8	8	8	Alto
Software	Desarrollo a media	SW-01	10	10	10	Extremo
	Antivirus	SW-02	7	7	7	Alto
	Firewall	SW-03	7	8	8	Alto
	Licencias	SW-04	8	6	7	Alto
	Sistemas operativos	SW-05	8	8	8	Alto
Hardware	Laptop	HW-01	8	8	8	Alto
	Monitor	HW-02	7	8	8	Alto
	HPE Smart Buy	HW-03	10	10	10	Extremo
	Impresora	HW-04	5	5	5	Medio
	Router Board Microtik 3011	HW-05	8	7	8	Alto
	Switch 24 puertos Cat. 5E	HW-06	8	7	8	Alto
	Unifi Uap-ac-lite	HW-07	7	7	7	Alto
Redes de comunicación	red internet	COM-01	8	8	8	Alto
	red LAN	COM-02	8	8	8	Alto
	Telefonía móvil	COM-03	6	7	7	Alto
Soportes de información	Electrónicos (one drive de office)	MEDIA-01	8	7	8	Alto
Equipamiento auxiliar	Rack Jupiter	AUX-01	5	5	5	Medio
	Bandejas porta Equipos	AUX-02	5	5	5	Medio
	Multitomas de energía	AUX-03	5	7	6	Alto
	Organizadores horizontales con canaleta ranurada	AUX-04	5	5	5	Medio
	Cable de energía	AUX-05	7	6	7	Alto
	Cable de red-Patch Cord	AUX-06	8	7	8	Alto
	Ups	AUX-07	8	8	8	Alto
	Cuarto de atención	L-01	9	9	9	Muy Alto

Instalaciones	Cuarto de soporte	L-02	9	9	9	Muy Alto
Personal	Personal administrativo de DTI	P-01	9	9	9	Muy Alto

Nota: Elaboración propia, 2023.

2.6.4. Identificación de amenazas

Después de haber realizado la valoración de los activos, es muy necesario identificar las amenazas potenciales que pueden incidir en los activos. Es una tarea esencial en la gestión de riesgos. La metodología Magerit V3 en su libro II de catálogo de elementos detalla los siguientes tipos de amenazas:

- [N] Desastres Naturales
- [I] Origen industrial
- [E] Errores y fallos no identificados
- [A] Ataques intencionales

En la Tabla 14 se puede detallar cada una de las amenazas por activos; por ende, se han identificado 28 amenazas distribuidas por 34 activos, pertenecientes a la relación de sistema financiero de DTI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., las demás amenazas se encuentran en el Anexo 3.

Tabla 14

Identificación de amenazas por activos

Activo	Amenaza
Datos/Información	
Base de datos	[E.15] Alteración de la información
Base de datos	[E.19] Fugas de información
Base de datos	[A.5] Suplantación de la identidad
Base de datos	[A.6] Abuso de privilegios de acceso
Base de datos	[A.11] Acceso no autorizado
Documentación interna	[E.15] Alteración de la información
Documentación interna	[E.19] Fugas de información
Documentación interna	[A.5] Suplantación de la identidad
Documentación interna	[A.6] Abuso de privilegios de acceso
Documentación interna	[A.11] Acceso no autorizado
Servicios	
Servidor NAS	[E.1] Errores de los usuarios
Servidor NAS	[E.2] Errores del administrador del sistema / de la seguridad
Servidor NAS	[E.15] Alteración de la información
Servidor NAS	[E.19] Fugas de información
Servidor NAS	[A.5] Suplantación de la identidad

Servidor NAS	[A.6] Abuso de privilegios de acceso
Servidor NAS	[A.7] Uso no previsto
Servidor NAS	[A.11] Acceso no autorizado
Servidor NAS	[A.15] Modificación de la información
Electricidad	[E.1] Errores de los usuarios
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad
Electricidad	[E.15] Alteración de la información
Electricidad	[E.19] Fugas de información
Electricidad	[A.5] Suplantación de la identidad
Electricidad	[A.6] Abuso de privilegios de acceso
Electricidad	[A.7] Uso no previsto
Electricidad	[A.11] Acceso no autorizado
Electricidad	[A.15] Modificación de la información
Internet	[E.1] Errores de los usuarios
Internet	[E.2] Errores del administrador del sistema / de la seguridad
Internet	[E.15] Alteración de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad
Internet	[A.6] Abuso de privilegios de acceso
Internet	[A.7] Uso no previsto
Internet	[A.11] Acceso no autorizado
Internet	[A.15] Modificación de la información
Telefonía	[E.1] Errores de los usuarios
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad
Telefonía	[E.15] Alteración de la información
Telefonía	[E.19] Fugas de información
Telefonía	[A.5] Suplantación de la identidad
Telefonía	[A.6] Abuso de privilegios de acceso
Telefonía	[A.7] Uso no previsto
Telefonía	[A.11] Acceso no autorizado
Telefonía	[A.15] Modificación de la información
Mantenimiento	[E.1] Errores de los usuarios
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad
Mantenimiento	[E.15] Alteración de la información
Mantenimiento	[E.19] Fugas de información
Mantenimiento	[A.5] Suplantación de la identidad
Mantenimiento	[A.6] Abuso de privilegios de acceso
Mantenimiento	[A.7] Uso no previsto
Mantenimiento	[A.11] Acceso no autorizado
Mantenimiento	[A.15] Modificación de la información
Correo	[E.1] Errores de los usuarios

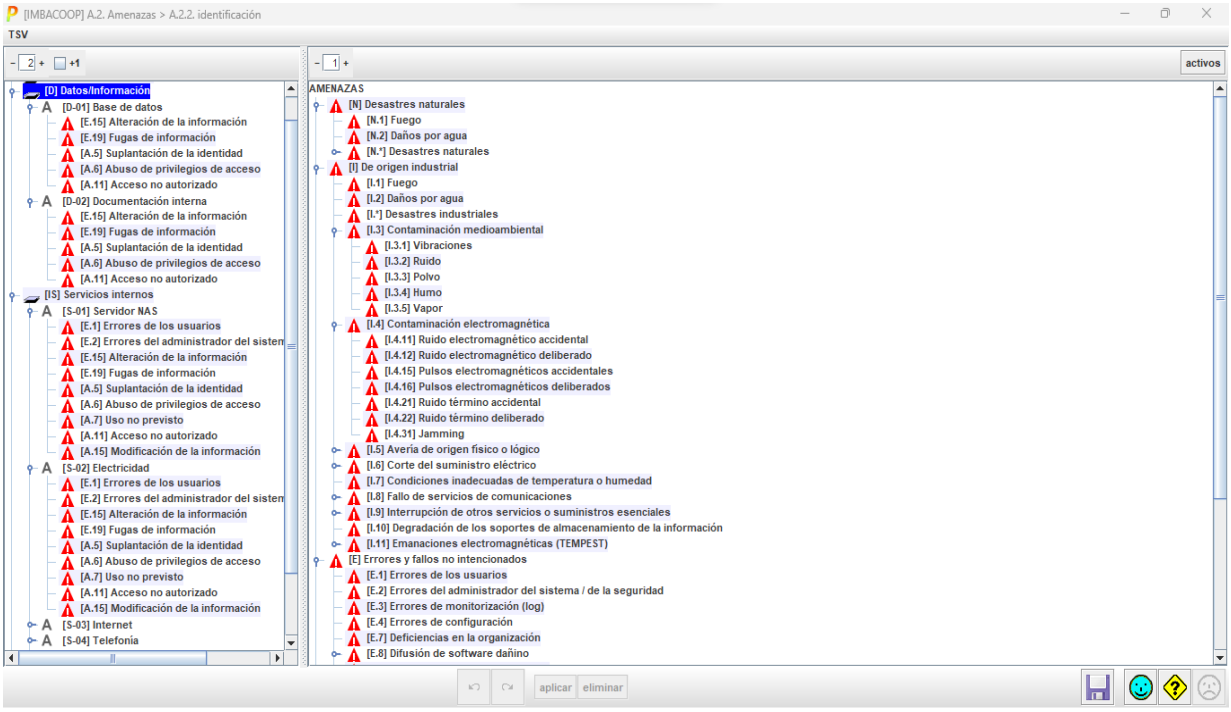
Correo	[E.2] Errores del administrador del sistema / de la seguridad
Correo	[E.15] Alteración de la información
Correo	[E.19] Fugas de información
Correo	[A.5] Suplantación de la identidad
Correo	[A.6] Abuso de privilegios de acceso
Correo	[A.7] Uso no previsto
Correo	[A.11] Acceso no autorizado
Correo	[A.15] Modificación de la información

Nota: Elaboración propia, 2023.

También la herramienta Pilar puede identificar cada una de las amenazas de manera automáticamente en relación con los activos, como se presenta en la Figura 29

Figura 29

Identificación de amenazas por activos



Nota. Elaboración propia

2.6.5. Valoración de amenazas

Una vez identificado las amenazas entre activos, el siguiente paso es la valoración de amenazas en dos elementos claves:

Impacto o Degradación: Analiza el impacto potencial en el activo si la amenaza relacionada se materializa. Esta valoración se basa en la escala proporcionada en la Tabla 15. Sin embargo, para valorar en la herramienta del Pilar, es esencial representar los valores de manera numérica, utilizando un intervalo de 0 a 100 en formato porcentual.

Tabla 15

Escala Degradación del valor de un activo

MA	100%	Muy alta	Casi seguro	Fácil
A	75%	Alta	Muy alto	Medio
M	50%	Media	Posible	Difícil
B	25%	Baja	Poco Probable	Muy difícil
MB	0%	Muy baja	Muy raro	Extremadamente difícil

Nota. Elaboración propia, información basada en la Dirección General de Modernización Administrativa, 2012. *Fuente: (DirecciónGeneral de Modernización Administrativa, 2012).*

Frecuencia o Probabilidad: Se alude a la frecuencia a la materialización de una amenaza, específicamente mediante la tasa anual de ocurrencia detallada en la Tabla 16.

Tabla 16

Valores de probabilidad de ocurrencia de una amenaza

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco Frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Nota. Elaboración propia, información basada en la Dirección General de Modernización Administrativa, 2012.*Fuente:(Dirección General de Modernización Administrativa, 2012).*

Para la valoración de las amenazas se ha tomado en cuenta la ayuda del director del Departamento de Tecnología de la Información de la Cooperativa de Ahorro Crédito Imbacoop Ltda. La valoración se determinó con base en la Tabla 15 y Tabla 16.

Por consiguiente, en la Tabla 17 se detalla la valoración de las amenazas respecto a cada uno de los activos de la organización y las demás valoraciones de amenazas adicionales se describen en el Anexo 4.

Tabla 17

Valoración de amenazas por activos

Activo	Amenaza	F	I	C
	Datos/Información			
Base de datos	[E.15] Alteración de la información	1	1%	
Base de datos	[E.19] Fugas de información	1		10%
Base de datos	[A.5] Suplantación de la identidad	10	10%	50%
Base de datos	[A.6] Abuso de privilegios de acceso	10	10%	50%
Base de datos	[A.11] Acceso no autorizado	100	10%	50%
Documentación interna	[E.15] Alteración de la información	1	1%	

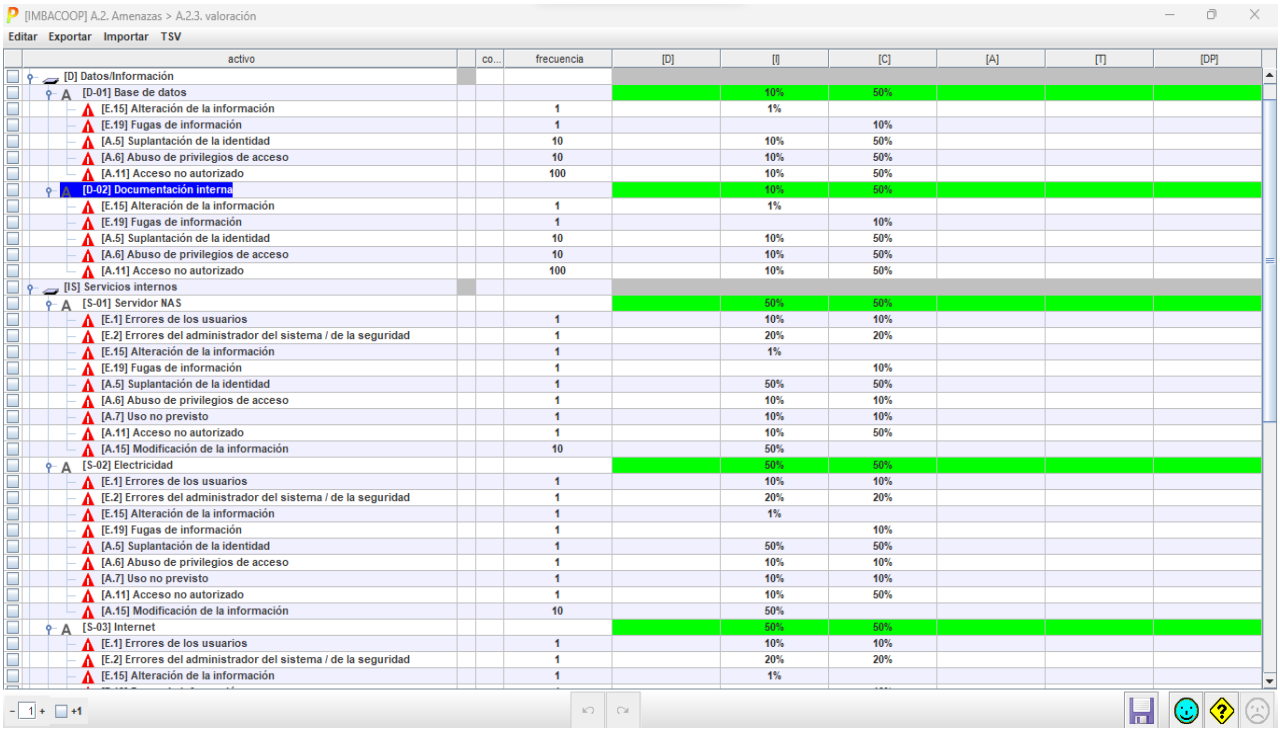
Documentación interna	[E.19] Fugas de información	1		10%
Documentación interna	[A.5] Suplantación de la identidad	10	10%	50%
Documentación interna	[A.6] Abuso de privilegios de acceso	10	10%	50%
Documentación interna	[A.11] Acceso no autorizado	100	10%	50%
	Servicios			
Servidor NAS	[E.1] Errores de los usuarios	1	10%	10%
Servidor NAS	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Servidor NAS	[E.15] Alteración de la información	1	1%	
Servidor NAS	[E.19] Fugas de información	1		10%
Servidor NAS	[A.5] Suplantación de la identidad	1	50%	50%
Servidor NAS	[A.6] Abuso de privilegios de acceso	1	10%	10%
Servidor NAS	[A.7] Uso no previsto	1	10%	10%
Servidor NAS	[A.11] Acceso no autorizado	1	10%	50%
Servidor NAS	[A.15] Modificación de la información	10	50%	
Electricidad	[E.1] Errores de los usuarios	1	10%	10%
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Electricidad	[E.15] Alteración de la información	1	1%	
Electricidad	[E.19] Fugas de información	1		10%
Electricidad	[A.5] Suplantación de la identidad	1	50%	50%
Electricidad	[A.6] Abuso de privilegios de acceso	1	10%	10%
Electricidad	[A.7] Uso no previsto	1	10%	10%
Electricidad	[A.11] Acceso no autorizado	1	10%	50%
Electricidad	[A.15] Modificación de la información	10	50%	
Internet	[E.1] Errores de los usuarios	1	10%	10%
Internet	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Internet	[E.15] Alteración de la información	1	1%	
Internet	[E.19] Fugas de información	1		10%
Internet	[A.5] Suplantación de la identidad	1	50%	50%
Internet	[A.6] Abuso de privilegios de acceso	1	10%	10%
Internet	[A.7] Uso no previsto	1	10%	10%
Internet	[A.11] Acceso no autorizado	1	10%	50%
Internet	[A.15] Modificación de la información	10	50%	
Telefonía	[E.1] Errores de los usuarios	1	10%	10%

Nota: Elaboración propia,2023

En la Figura 30 se presenta la evaluación de amenazas utilizando la herramienta Pilar. En este análisis, se ha llevado a cabo la valoración considerando la función de degradación de los activos y la probabilidad de ocurrencia.

Figura 30

Valoración de amenazas por activos



activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[DP]
[D] Datos/Información								
[D-01] Base de datos				10%	50%			
[E.15] Alteración de la información		1		1%				
[E.19] Fugas de información		1			10%			
[A.5] Suplantación de la identidad		10		10%	50%			
[A.6] Abuso de privilegios de acceso		10		10%	50%			
[A.11] Acceso no autorizado		100		10%	50%			
[D-02] Documentación interna				10%	50%			
[E.15] Alteración de la información		1		1%				
[E.19] Fugas de información		1			10%			
[A.5] Suplantación de la identidad		10		10%	50%			
[A.6] Abuso de privilegios de acceso		10		10%	50%			
[A.11] Acceso no autorizado		100		10%	50%			
[IS] Servicios internos								
[S-01] Servidor NAS				50%	50%			
[E.1] Errores de los usuarios		1		10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1		20%	20%			
[E.15] Alteración de la información		1		1%				
[E.19] Fugas de información		1			10%			
[A.5] Suplantación de la identidad		1		50%	50%			
[A.6] Abuso de privilegios de acceso		1		10%	10%			
[A.7] Uso no previsto		1		10%	10%			
[A.11] Acceso no autorizado		1		10%	50%			
[A.15] Modificación de la información		10		50%				
[S-02] Electricidad				50%	50%			
[E.1] Errores de los usuarios		1		10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1		20%	20%			
[E.15] Alteración de la información		1		1%				
[E.19] Fugas de información		1			10%			
[A.5] Suplantación de la identidad		1		50%	50%			
[A.6] Abuso de privilegios de acceso		1		10%	10%			
[A.7] Uso no previsto		1		10%	10%			
[A.11] Acceso no autorizado		1		10%	50%			
[A.15] Modificación de la información		10		50%				
[S-03] Internet				50%	50%			
[E.1] Errores de los usuarios		1		10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1		20%	20%			
[E.15] Alteración de la información		1		1%				

Nota: *Elaboración propia*

2.6.6. Evaluación de riesgos

Después de culminar la actividad de inventariar los activos, identificado y evaluado las amenazas del sistema financiero y activos relacionados del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se procede a calcular los riesgos, siguiendo los siguientes puntos.

Impacto potencial: El término impacto se refiere a una estimación del daño que sufrirá un activo como resultado de la materialización de la amenaza. Conociendo el valor de los activos en cada dimensión (integridad, confidencialidad) y comprendiendo la degradación causada por las amenazas, se puede calcular directamente este impacto en el sistema.

Criterios de valoración

- **Muy Alto (10):** Si se materializa la amenaza, tendría desastrosas
- consecuencias en la organización.
- **Alto (9):** Si se materializa la amenaza, tendría altas consecuencias sobre la organización.
- **Medio (6-8):** Si se materializa la amenaza, tendría medianas consecuencias sobre la organización.

- **Bajo (3-5):** Si se materializa la amenaza, tendría bajas consecuencias sobre la organización.
- **Muy Bajo (1-2):** Si se materializa la amenaza, tendría efectos mínimos sobre la organización.
- **Despreciable (0):** Si se materializa la amenaza, no tendría efectos sobre la organización.

La evaluación de este impacto puede llevarse a cabo desde dos perspectivas distintas:

Impacto potencial acumulado: Abarca el valor global del activo bajo consideración, englobando tanto su propio valor como la suma acumulada de los activos directamente dependientes de él, junto con la evaluación de las amenazas a las que está expuesto. Esta evaluación se lleva a cabo a través de la aplicación de una ecuación específicamente diseñada con este fin.

$$Impacto\ potencial\ acumulado = \%\ degradación\ de\ amenaza \times Valor\ acumulado\ del\ activo$$

Después de calcular el impacto potencial acumulado, se han obtenido los siguientes resultados, los cuales se muestran en la Tabla 18. Los demás resultados se encuentran detallados en el Anexo 5.

Tabla 18

Impacto potencial acumulado de afectación de activos

	Impacto potencial acumulado		Peso ponderado
Activos-Amenazas	**I**	**C**	
Datos/Información	7	9	8
Base de datos	7	9	8
[E.15] Alteración de la información	4		4
[E.19] Fugas de información		7	7
[A.5] Suplantación de la identidad	7	9	8
[A.6] Abuso de privilegios de acceso	7	9	8
[A.11] Acceso no autorizado	7	9	8
Documentación interna	6	7	6,5
[E.15] Alteración de la información	3		3
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	6	7	6,5
[A.6] Abuso de privilegios de acceso	6	7	6,5
[A.11] Acceso no autorizado	6	7	6,5
Servicios	7	9	8
Servidor NAS	7	9	8

[E.1] Errores de los usuarios	5	7	6
[E.2] Errores del administrador del sistema / de la seguridad	6	8	7
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		7	7
[A.5] Suplantación de la identidad	7	9	8
[A.6] Abuso de privilegios de acceso	5	7	6
[A.7] Uso no previsto	5	7	6
[A.11] Acceso no autorizado	5	9	7
[A.15] Modificación de la información	7		7
Electricidad	6	6	6
[E.1] Errores de los usuarios	4	4	4
[E.2] Errores del administrador del sistema / de la seguridad	5	5	5
[E.15] Alteración de la información	1		1
[E.19] Fugas de información		4	2
[A.5] Suplantación de la identidad	6	6	6
[A.6] Abuso de privilegios de acceso	4	4	4
[A.7] Uso no previsto	4	4	4
[A.11] Acceso no autorizado	4	6	5
[A.15] Modificación de la información	6		1
Internet	7	7	7
[E.1] Errores de los usuarios	5	5	5
[E.2] Errores del administrador del sistema / de la seguridad	6	6	6
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	7	7	7
[A.6] Abuso de privilegios de acceso	5	5	5
[A.7] Uso no previsto	5	5	5
[A.11] Acceso no autorizado	5	7	6
[A.15] Modificación de la información	7		7
Telefonía	6	6	6
[E.1] Errores de los usuarios	4	4	4
[E.2] Errores del administrador del sistema / de la seguridad	5	5	5
[E.15] Alteración de la información	1		1
[E.19] Fugas de información		4	4
[A.5] Suplantación de la identidad	6	6	6
[A.6] Abuso de privilegios de acceso	4	4	4
[A.7] Uso no previsto	4	4	4
[A.11] Acceso no autorizado	4	6	5
[A.15] Modificación de la información	6		6

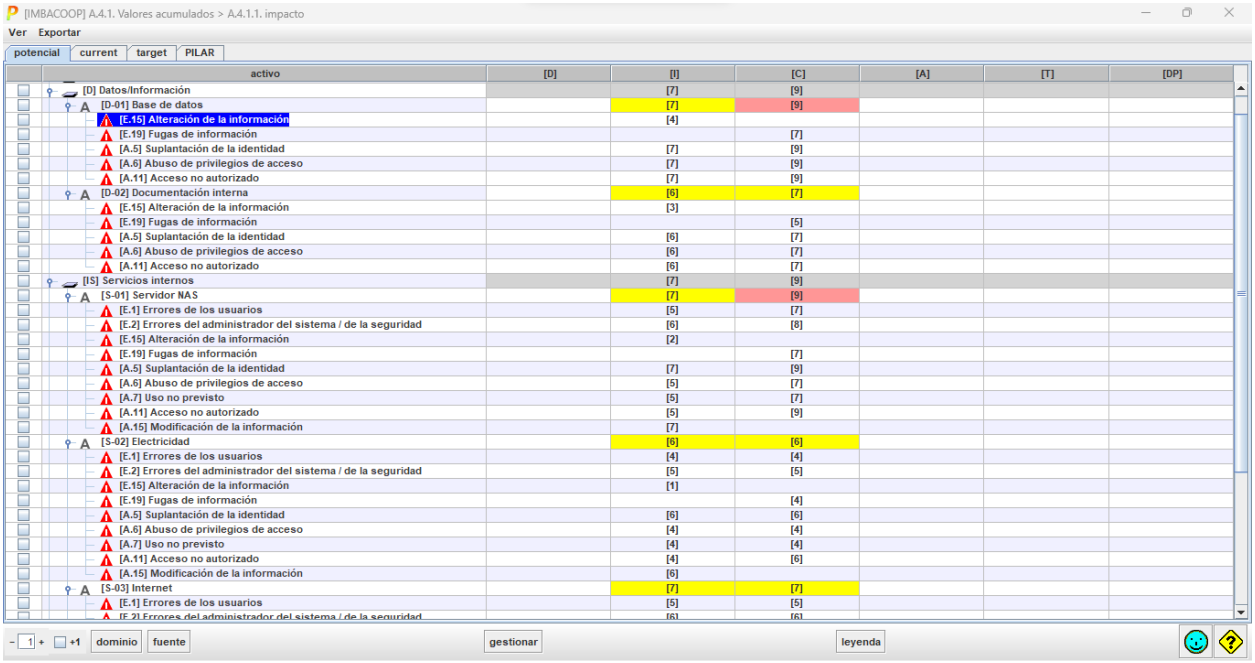
Mantenimiento	6	6	6
[E.1] Errores de los usuarios	4	4	4
[E.2] Errores del administrador del sistema / de la seguridad	5	5	5
[E.15] Alteración de la información	1		1
[E.19] Fugas de información		4	4
[A.5] Suplantación de la identidad	6	6	6
[A.6] Abuso de privilegios de acceso	4	4	4
[A.7] Uso no previsto	4	4	4
[A.11] Acceso no autorizado	4	6	5
[A.15] Modificación de la información	6		6

Nota: Elaboración propia, 2023

En la Figura 31 se presenta Impacto potencia acumulado de afectación de activos en la herramienta Pilar.

Figura 31

Impacto potencia acumulada de afectación de activos



Nota. Elaboración propia.

Impacto potencial repercutido: Se considera la evaluación integral del activo que considere tanto el impacto directo en activo, posibles amenazas a las que podrían estar expuestos los activos que dependen de él. Para el cálculo se basó en la siguiente ecuación.

$$Impacto\ potencial\ repercutivo = \%\ Degradación\ de\ amenaza \times Valor\ propio\ del\ activo$$

En la Tabla 19 se detalla el cálculo de impacto potencial repercutido de cada uno de los activos.

Tabla 19

Impacto potencial repercutido de afectación de activos

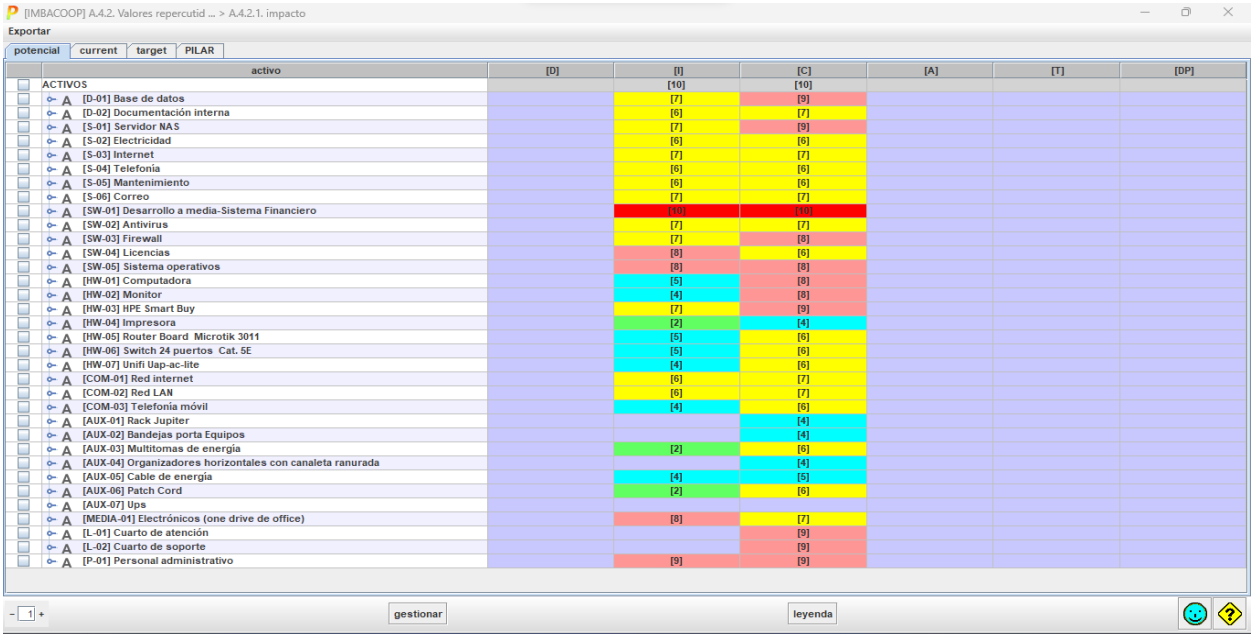
	Impacto potencial repercutido		Peso ponderado
Activos	**I**	**C**	
Base de datos	7	9	8
Documentación interna	6	7	6,5
Servidor NAS	7	9	8
Electricidad	6	6	6
Internet	7	7	7
Telefonía	6	6	6
Mantenimiento	6	6	6
Correo	7	7	7
Desarrollo a media	10	10	10
Antivirus	7	7	7
Firewall	7	8	7,5
Licencias	8	6	7
Sistemas operativos	8	8	8
Computadora	5	8	7
Monitor	4	8	6
HPE Smart Buy	7	9	8
Impresora	2	4	3
Router Board Microtik 3011	5	6	6
Switch 24 puertos Cat. 5E	5	6	5,5
Unifi Uap-ac-lite	4	6	5
red internet	6	7	6,5
red LAN	6	7	7
telefonía móvil	4	6	5
Electrónicos (one drive de office)	8	7	7,5
Rack Jupiter		4	4
Bandejas porta Equipos		4	4
Multitomas de energía	2	6	4
Organizadores horizontales con canaleta ranurada		4	4
Cable de energía	4	5	5
Cable de red-Patch Cord	2	6	4
Ups	8	8	8
Cuarto de atención		9	9
Cuarto de soporte		9	9
Personal administrativo de DTI	9	9	9

Nota: Elaboración propia, 2023

En la Figura 32 se presenta el impacto potencial repercutido para cada activo de sistema financiero en la herramienta Pilar.

Figura 32

Impacto potencial repercutido de afectación de activos



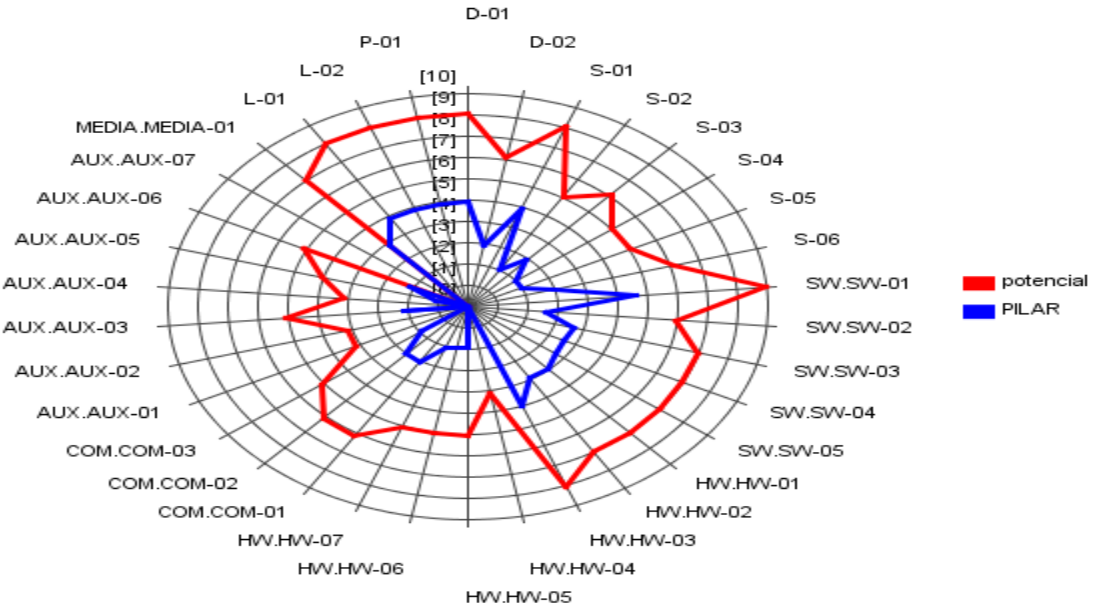
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS		[10]	[10]			
[D-01] Base de datos		[7]	[9]			
[D-02] Documentación interna		[6]	[7]			
[S-01] Servidor NAS		[7]	[9]			
[S-02] Electricidad		[6]	[6]			
[S-03] Internet		[7]	[7]			
[S-04] Telefonía		[6]	[6]			
[S-05] Mantenimiento		[6]	[6]			
[S-06] Correo		[7]	[7]			
[SW-01] Desarrollo a media-Sistema Financiero		[10]	[10]			
[SW-02] Antivirus		[7]	[7]			
[SW-03] Firewall		[7]	[8]			
[SW-04] Licencias		[8]	[6]			
[SW-05] Sistema operativos		[8]	[8]			
[HW-01] Computadora		[5]	[8]			
[HW-02] Monitor		[4]	[8]			
[HW-03] HPE Smart Buy		[7]	[9]			
[HW-04] Impresora		[2]	[4]			
[HW-05] Router Board Microtik 3011		[5]	[6]			
[HW-06] Switch 24 puertos Cat. 5E		[5]	[6]			
[HW-07] Unifi Uap-ac-lite		[4]	[6]			
[COM-01] Red internet		[6]	[7]			
[COM-02] Red LAN		[6]	[7]			
[COM-03] Telefonía móvil		[4]	[6]			
[AUX-01] Rack Jupiter			[4]			
[AUX-02] Bandejas porta Equipos			[4]			
[AUX-03] Multitomas de energía		[2]	[6]			
[AUX-04] Organizadores horizontales con canaleta ranurada			[4]			
[AUX-05] Cable de energía		[4]	[5]			
[AUX-06] Patch Cord		[2]	[6]			
[AUX-07] Ups						
[MEDIA-01] Electrónicos (one drive de office)		[8]	[7]			
[L-01] Cuarto de atención			[9]			
[L-02] Cuarto de soporte			[9]			
[P-01] Personal administrativo		[9]	[9]			

Nota. Elaboración propia

La Figura 33 exhibe un gráfico que representa el impacto acumulado potencial para cada activo, delineado por la línea roja, junto con los valores recomendados por la herramienta Pilar, los cuales están representados por la línea azul.

Figura 33

Gráfico de valores de impacto potencial acumulado de los activos



Nota. Elaboración propia

Es esencial llevar a cabo una evaluación integral del impacto potencial acumulado de las amenazas en los activos del sistema para lograr una gestión de riesgos eficaz. Este enfoque permite identificar las medidas de control necesarias. En cambio, limitarse a evaluar el impacto potencial de las amenazas solo en el valor propio de los activos proporciona información insuficiente sobre las posibles consecuencias de las incidencias.

2.6.7. Determinación de riesgo potencial

Después de evaluar el impacto potencial, se estableció el riesgo correspondiente como la evaluación del daño considerando la probabilidad de que ocurra. La magnitud del riesgo guarda una relación proporcional directa con tanto el impacto como la probabilidad asociada, y dicha relación se detalla en la Tabla 20.

Tabla 20

Nivel de riesgo

IMPACTO						
	MA	Media	Alta	Muy alta	Critico	Critico
	A	Baja	Media	Alta	Muy alta	Critico
	M	Muy baja	Baja	Media	Alta	Muy alta
	B	Aceptable	Muy baja	Baja	Media	Alta
	MB	Aceptable	Aceptable	Muy baja	Baja	Media
		MB	B	M	A	MA
		PROBABILIDAD				

Nota: Fuente: (Hermoso-Orzáez, 2021).

Se llevó a cabo el cálculo del riesgo para cada activo, considerando cada amenaza y en todas las dimensiones de valoración. La evaluación de este riesgo puede realizarse mediante dos enfoques distintos:

Riesgo potencial acumulado: Se examina minuciosamente la acumulación del impacto sobre un activo a consecuencia de una amenaza, mientras se calcula simultáneamente la probabilidad vinculada a esa amenaza. La fórmula que rige este proceso es la herramienta clave para cuantificar este análisis complejo**:**

$$Riesgo\ potencial\ acumulada = Probabilidad\ de\ amenaza \times Valor\ acumulado\ del\ impacto$$

La evaluación completa del riesgo potencial acumulado se encuentra minuciosamente descrita en el Anexo 6, donde se presenta de manera exhaustiva la matriz que abarca todos los aspectos relevantes. Para ofrecer una visión más detallada, se presenta a continuación un ejemplo concreto de dicha matriz en la Tabla 21, que ilustra de manera específica cómo se aplican los criterios y factores de evaluación en el contexto del riesgo potencial acumulado. Este recurso visual en la Tabla 21 facilita la comprensión y análisis de la evaluación completa del riesgo en el contexto del proyecto o situación en consideración.

Tabla 21

Riesgo potencial acumulado de afectación de activos

	Riesgo potencial acumulado		**Peso ponderado**
Activos-Amenazas	**I**	**C**	
Datos/Información	6,8	8,1	7,5
Base de datos	6,8	8,1	7,5
[E.15] Alteración de la información	3,3		3,3
[E.19] Fugas de información		5,1	5,1
[A.5] Suplantación de la identidad	5,9	7,2	6,6
[A.6] Abuso de privilegios de acceso	5,9	7,2	6,6
[A.11] Acceso no autorizado	6,8	8,1	7,5
Documentación interna	6,2	6,9	6,6
[E.15] Alteración de la información	2,7		2,7
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	5,4	6	5,7
[A.6] Abuso de privilegios de acceso	5,4	6	5,7
[A.11] Acceso no autorizado	6,2	6,9	6,6
Servicios	6	6,3	6,2
Servidor NAS	6	6,3	6,2
[E.1] Errores de los usuarios	3,9	5,1	4,5
[E.2] Errores del administrador del sistema / de la	4,4	5,6	5

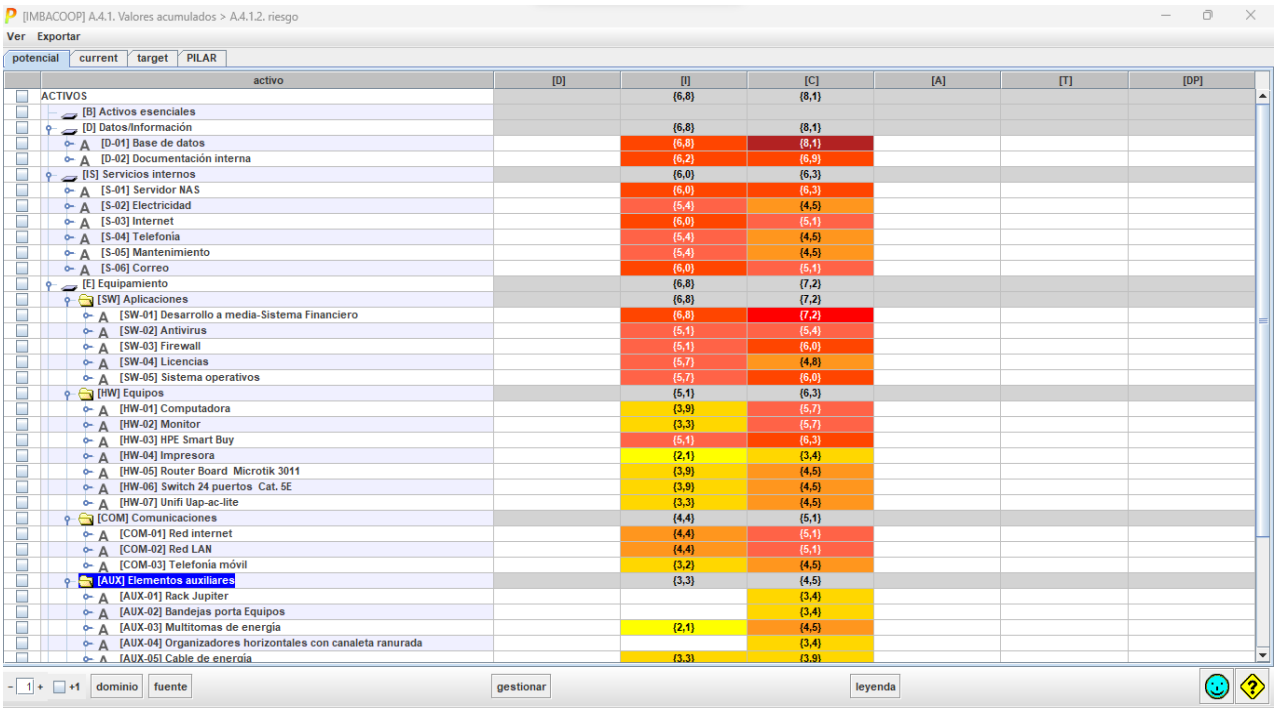
seguridad			
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		5,1	5,1
[A.5] Suplantación de la identidad	5,1	6,3	5,7
[A.6] Abuso de privilegios de acceso	3,9	5,1	4,5
[A.7] Uso no previsto	3,9	5,1	4,5
[A.11] Acceso no autorizado	3,9	6,3	5,1
[A.15] Modificación de la información	6		6
Electricidad	5,4	4,5	5
[E.1] Errores de los usuarios	3,3	3,3	6,6
[E.2] Errores del administrador del sistema / de la seguridad	3,8	3,8	7,6
[E.15] Alteración de la información	1,5		1,5
[E.19] Fugas de información		3,3	3,3
[A.5] Suplantación de la identidad	4,5	4,5	4,5
[A.6] Abuso de privilegios de acceso	3,3	3,3	3,3
[A.7] Uso no previsto	3,3	3,3	3,3
[A.11] Acceso no autorizado	3,3	4,5	3,9
[A.15] Modificación de la información	5,4		5,4
Internet	6	5,1	5,6
[E.1] Errores de los usuarios	3,9	3,9	3,9
[E.2] Errores del administrador del sistema / de la seguridad	4,4	4,4	4,4
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	5,1	5,1	5,1
[A.6] Abuso de privilegios de acceso	3,9	3,9	3,9
[A.7] Uso no previsto	3,9	3,9	3,9
[A.11] Acceso no autorizado	3,9	5,1	4,5
[A.15] Modificación de la información	6		6

Nota. Elaboración propia, 2023.

En la Figura 34, se exhiben los datos relativos al riesgo potencial acumulado utilizando la herramienta Pilar, proporcionando una visualización detallada de los niveles de riesgo asociados a cada activo. Este conjunto de información permite una comprensión más profunda de la distribución y magnitudes del riesgo en el contexto del análisis realizado mediante Pilar.

Figura 34

Riesgo potencial acumulado de afectación de activos



Nota. Elaboración propia

Riesgo potencial acumulado: Se considera la magnitud impactante del efecto sobre el activo originado por una amenaza, junto con la probabilidad asociada a dicha amenaza. La fórmula utilizada para llevar a cabo este cálculo es la siguiente:

$$Riesgo\ potencial\ repercutido = Probabilidad\ de\ amenaza\ \times Valor\ repercutido\ del\ impacto$$

En la Tabla 22 se encuentra consignado el cálculo del riesgo potencial repercutido de cada uno de los activos.

Tabla 22

Riesgo potencial repercutido de afectación de activos

	Riesgo potencial repercutido		Peso ponderado
Activos	**I**	**C**	
Base de datos	6,8	8,1	7,5
Documentación interna	6,2	6,9	6,6
Servidor NAS	6	6,3	6,2
Electricidad	5,4	4,5	5
Internet	6	5,1	5,6
Telefonía	5,4	4,5	5
Mantenimiento	5,4	4,5	5

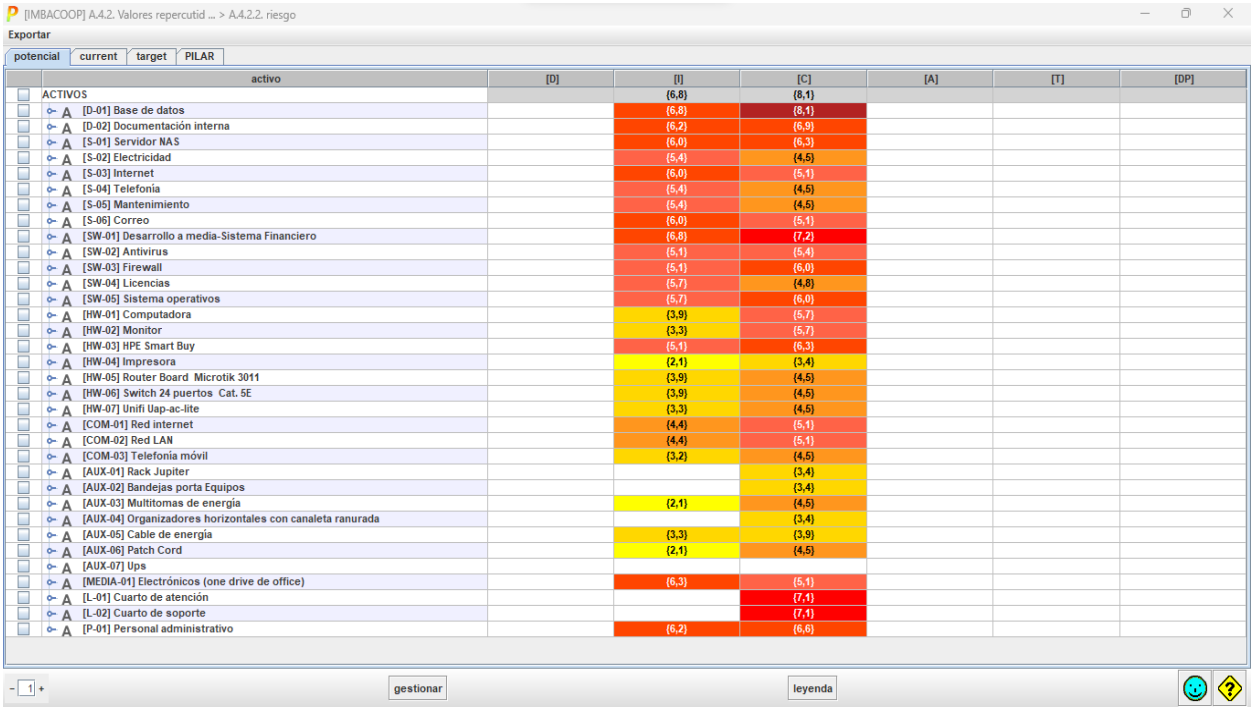
Correo	6	5,1	5,6
Desarrollo a media	6,8	7,2	7
Antivirus	5,1	5,4	5,3
Firewall	5,1	6	5,6
Licencias	5,7	4,8	5,3
Sistemas operativos	5,7	6	5,9
Computadora	3,9	5,7	4,8
Monitor	3,3	5,7	4,5
HPE Smart Buy	5,1	6,3	5,7
Impresora	2,1	3,4	2,8
Router Board Microtik 3011	3,9	4,5	4,2
Switch 24 puertos Cat. 5E	3,9	4,5	4,2
Unifi Uap-ac-lite	3,3	4,5	3,9
red internet	4,4	5,1	4,8
red LAN	4,4	5,1	4,8
telefonía móvil	3,2	4,5	3,9
Electrónicos (one drive de office)	6,3	5,1	5,7
Rack Jupiter		3,4	3,4
Bandejas porta Equipos		3,4	3,4
Multitomas de energía	2,1	4,5	3,3
Organizadores horizontales con canaleta ranurada		3,4	3,4
Cable de energía	3,3	3,9	3,6
Cable de red-Patch Cord	2,1	4,5	3,3
Ups		7,7	7,7
Cuarto de atención		7,1	7,1
Cuarto de soporte		7,1	7,1
Personal administrativo de DTI	6,2	6,6	6,4

Nota. Elaboración propia,2023

En la Figura 35, se proporcionan detalladamente los valores que reflejan el riesgo potencial que podría derivarse para cada activo, utilizando la herramienta de software PILAR. Esta representación visual ofrece una visión exhaustiva de la evaluación de riesgos, destacando la influencia específica de cada activo en el panorama general.

Figura 35

Riesgo potencial repercutido de afectación de activos



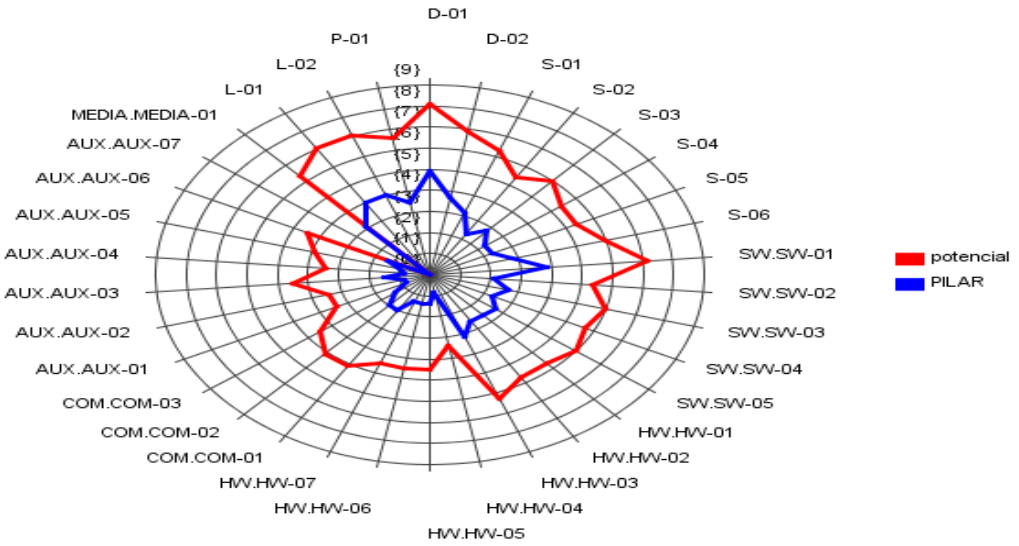
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS		{6,8}	{8,1}			
[D-01] Base de datos		{6,8}	{8,1}			
[D-02] Documentación interna		{6,2}	{6,9}			
[S-01] Servidor NAS		{6,0}	{6,3}			
[S-02] Electricidad		{5,4}	{4,5}			
[S-03] Internet		{6,0}	{5,1}			
[S-04] Telefonía		{5,4}	{4,5}			
[S-05] Mantenimiento		{5,4}	{4,5}			
[S-06] Correo		{6,0}	{5,1}			
[SW-01] Desarrollo a media-Sistema Financiero		{6,8}	{7,2}			
[SW-02] Antivirus		{5,1}	{5,4}			
[SW-03] Firewall		{5,1}	{6,0}			
[SW-04] Licencias		{5,7}	{4,8}			
[SW-05] Sistema operativos		{5,7}	{6,0}			
[HW-01] Computadora		{3,9}	{5,7}			
[HW-02] Monitor		{3,3}	{5,7}			
[HW-03] HPE Smart Buy		{5,1}	{6,3}			
[HW-04] Impresora		{2,1}	{3,4}			
[HW-05] Router Board Microtik 3011		{3,9}	{4,5}			
[HW-06] Switch 24 puertos Cat. 5E		{3,9}	{4,5}			
[HW-07] Unifi Uap-ac-lite		{3,3}	{4,5}			
[COM-01] Red internet		{4,4}	{5,1}			
[COM-02] Red LAN		{4,4}	{5,1}			
[COM-03] Telefonía móvil		{3,2}	{4,5}			
[AUX-01] Rack Jupiter			{3,4}			
[AUX-02] Bandejas porta Equipos			{3,4}			
[AUX-03] Multitomas de energía		{2,1}	{4,5}			
[AUX-04] Organizadores horizontales con canaleta ranurada			{3,4}			
[AUX-05] Cable de energía		{3,3}	{3,9}			
[AUX-06] Patch Cord		{2,1}	{4,5}			
[AUX-07] Ups						
[MEDIA-01] Electrónicos (one drive de office)		{6,3}	{5,1}			
[L-01] Cuarto de atención			{7,1}			
[L-02] Cuarto de soporte			{7,1}			
[P-01] Personal administrativo		{6,2}	{6,6}			

Nota. Elaboración propia

En la Figura 36, se visualiza la línea roja que refleja los niveles actuales de riego potencial acumulado para cada activo. Contrapuesta a esta, la línea azul representa los valores de riesgo potencial acumulado recomendados por la herramienta Pilar.

Figura 36

Gráfico de valores de riesgo acumulado de los activos



Nota. Elaboración propia.

El riesgo potencial acumulado, al ser calculado sobre el valor total de los activos del sistema, facilita la identificación de las medidas de protección en el proceso de gestión de riesgos. Por otro lado, al calcular el riesgo potencial repercutido sobre el valor intrínseco de los activos, se logra evaluar exclusivamente las repercusiones derivadas de incidentes relacionados con amenazas específicas.

2.6.8. Tratamiento de riesgos

La mitigación de riesgos es un proceso que implica la implementación de medidas y estrategias para reducir la probabilidad de que ocurran eventos adversos o para minimizar sus impactos en caso de que se produzcan. La mitigación de riesgos en el sistema financiero y sus activos relacionados del DTI de Cooperativa de Ahorro y Crédito Imbacoop Ltda., implica elegir e implementar medidas apropiadas con el objetivo de modificar los riesgos, con el fin de evitar posibles daños a los activos.

2.6.9. Pautas para tratamiento de riesgos

Después de identificar los niveles de riesgo asociados con las amenazas que podrían impactar cada activo de información, se definen los estándares para aceptar esos riesgos. Estos criterios no solo ayudan a clasificar el tipo de riesgo, sino que también orientan la aplicación de controles específicos. Para obtener información detallada sobre las medidas a seguir, se recomienda referirse a la Figura. 37

Figura 37

Niveles de Tratamiento de riesgos

ZONA DE RIESGO RESIDUAL	NIVEL DE RIESGO ACEPTABLE	OPCIÓN O ESTRATEGIA DE TRATAMIENTO A SEGUIR
Bajo	Aceptable	Asumir/Aceptar
Moderado	Aceptable	Asumir/Aceptar
Alto	No Aceptable	Reducir/Mitigar
Extremo	No Aceptable	Reducir/Mitigar

Nota. Fuente: (Unidad Nacional para la Gestión del Riesgo de Desastres, 2022)

- **Aceptar:** Se aceptan riesgos si ocurren con menos frecuencia, tienen menos impacto y no amenazan la estabilidad de la organización.
- **Transferir:** Se produce cuando el riesgo se transfiere a otra empresa mediante un contrato de subcontratación o un seguro.
- **Reducir**: Si el riesgo se considera inaceptable, es importante implementar medidas adicionales. Estas medidas deben diseñarse para fortalecer los controles existentes o agregar nuevos controles para reducir el riesgo a un nivel aceptable.
- **Evitar:** Cambiar las actividades o decisiones para eliminar la posibilidad de que un riesgo específico se materialice.

Es fundamental que la institución lleve a cabo una evaluación periódica de los riesgos identificados. Esto permitirá identificar los factores subyacentes y facilitará la asignación adecuada de recursos para abordarlos de manera efectiva

Se proporciona una muestra de la matriz de tratamiento de riesgo en la Tabla 23, la matriz completa se encuentra en el Anexo 7.

Tabla 23

Matriz de tratamiento de riesgos

		Peso ponderado	Tratamiento
Activos-Amenazas			
Base de datos	[A.11] Acceso no autorizado	7,5	Reducir
Cuarto de atención	[A.25] Robo de equipos	7,1	Evitar
Cuarto de atención	[A.25] Robo de equipos	7,1	Evitar
Desarrollo a media-Sistema Financiero	[A.8] Difusión de software dañino	6,8	Evitar
Desarrollo a media-Sistema Financiero	[A.22] Manipulación de programas	6,8	Evitar
Personal administrativo de DTI	[A.19] Revelación de información	6,6	Evitar
Base de datos	[A.5] Suplantación de la identidad	6,6	Evitar

Base de datos	[A.6] Abuso de privilegios de acceso	6,6	Evitar
Documentación interna	[A.11] Acceso no autorizado	6,6	Reducir
Desarrollo a media-Sistema Financiero	[E.21] Errores de mantenimiento / actualización de programas (software)	6,6	Reducir
HPE Smart Buy	[E.25] Pérdida de equipos	6,3	Reducir
Electrónicos (one drive de office)	[A.15] Modificación de la información	6,3	Evitar
Personal administrativo de DTI	[A.29] Extorsión	6,2	Evitar
Servidor NAS	[A.15] Modificación de la información	6	Evitar
Internet	[A.15] Modificación de la información	6	Evitar
Correo	[A.15] Modificación de la información	6	Evitar
HPE Smart Buy	[A.23] Manipulación del hardware	6	Evitar
HPE Smart Buy	[A.25] Robo de equipos	6	Evitar
Personal administrativo de DTI	[A.30] Ingeniería social (picaresca)	6	Evitar
Documentación interna	[A.5] Suplantación de la identidad	5,7	Evitar
Documentación interna	[A.6] Abuso de privilegios de acceso	5,7	Evitar
Sistemas operativos	[A.8] Difusión de software dañino	5,7	Evitar
Sistemas operativos	[A.22] Manipulación de programas	5,7	Evitar
Computadora	[E.25] Pérdida de equipos	5,7	Reducir
Monitor	[E.25] Pérdida de equipos	5,7	Reducir

Nota. Elaboración propia, 2023

2.7. Controles de la Norma ISO/IEC 27002/2013

Al identificar, analizar las amenazas y riesgos, se lleva a cabo el proceso de mapeo de controles según las pautas establecidas en la norma ISO/IEC 27002:2013. Esta norma proporciona directrices para asegurar la información en las organizaciones, abarcando la selección, implementación y gestión de controles, teniendo en cuenta el contexto del riesgo de seguridad de la información.

En consecuencia, la selección de controles se realiza teniendo en cuenta los riesgos asociados a los activos previamente identificados. Posteriormente, se verifica la pertinencia del dominio y control mediante una revisión de la norma.

2.7.1. Controles para implementar en sistema financiero de la Cooperativa

La Tabla 24 presenta una descripción detallada de los controles, los cuales establecen criterios para señalar las medidas necesarias destinadas a mitigar el riesgo o el nivel residual de riesgo. En el Anexo 8 se puede encontrar el detalle completo de los controles para la implementación en el sistema financiero del DTI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

Tabla 24

Identificación de dominios, Objetivos, controles

Activos	Amenazas	Dominio	Objetivos	Controles
Base de datos	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Cuarto de atención	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Cuarto de atención	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Desarrollo a media-Sistema Financiero	[A.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
Desarrollo a media-Sistema Financiero	[A.22] Manipulación de programas	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Personal administrativo de DTI	[A.19] Revelación de información	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Base de datos	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Base de datos	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Documentación interna	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Desarrollo a media-Sistema Financiero	[E.21] Errores de mantenimiento / actualización de programas (software)	12. Seguridad en la operativa.	12.1 Responsabilidades y procedimientos de operación.	12.1.2 Gestión de cambios
HPE Smart Buy	[E.25] Pérdida de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Electrónicos (one	[A.15] Modificación de la	13. Seguridad en las	13.1 Gestión de la	13.1.1 Controles de red

drive de office)	información	telecomunicaciones.	seguridad en las redes.	
Personal administrativo de DTI	[A.29] Extorsión	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Servidor NAS	[A.15] Modificación de la información	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Internet	[A.15] Modificación de la información	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Correo	[A.15] Modificación de la información	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
HPE Smart Buy	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
HPE Smart Buy	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Personal administrativo de DTI	[A.30] Ingeniería social (picaresca)	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Documentación interna	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso

Nota. Elaboración propia.

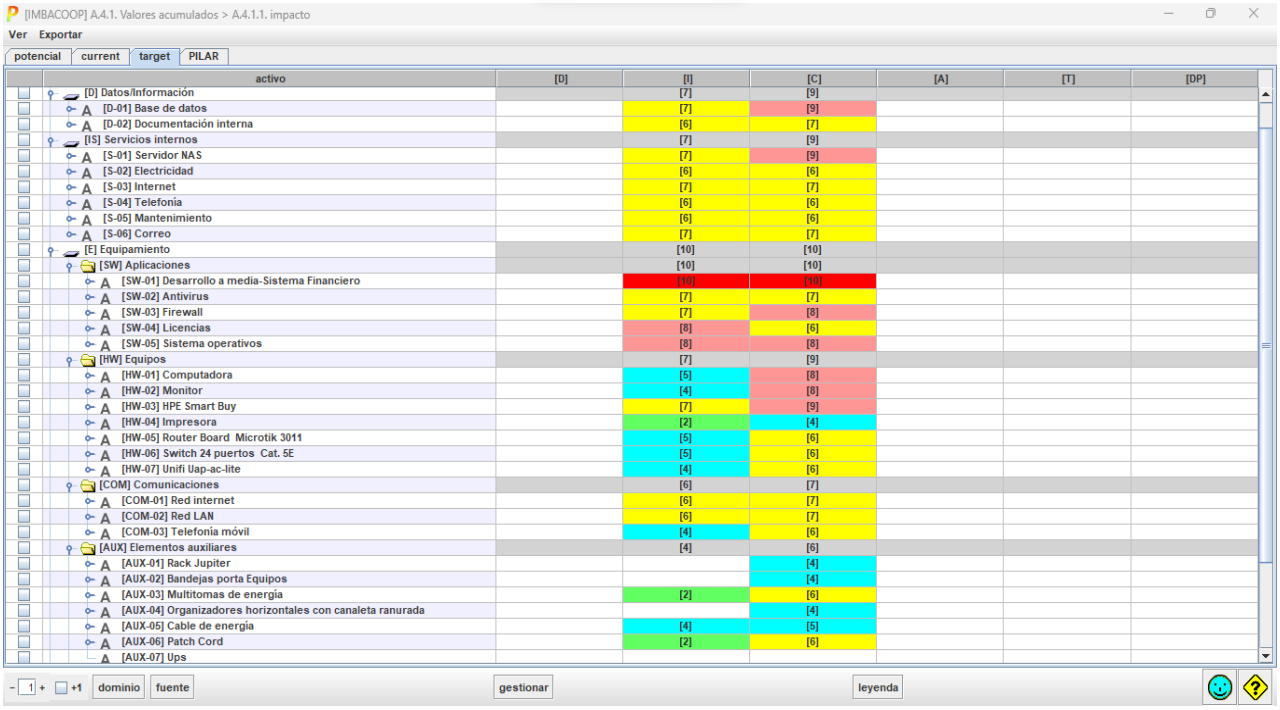
2.7.2. Estimación de impacto residual

Si se ejecutan las actividades propuestas para llevar a cabo los controles, el sistema modifica su posible impacto original a un impacto residual. Esto se debe a que la herramienta Pilar simula la implementación de los controles, proporcionando una evaluación del impacto residual acumulado y el impacto residual resultante.

La Figura 38 se presenta la acumulación del impacto residual, mientras que en la Figura 39 se visualiza cómo este impacto residual se refleja o repercute.

Figura 38

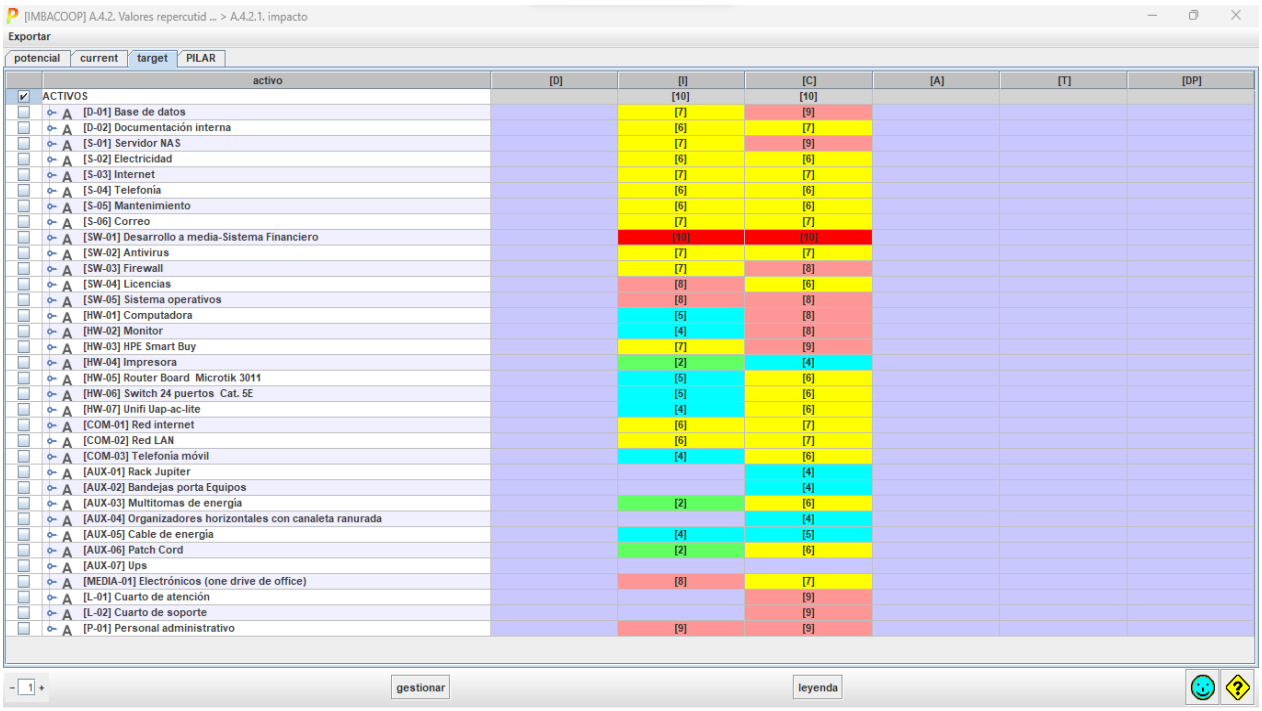
Impacto residual acumulado de los activos



Nota. Elaboración propia

Figura 39

Impacto residual repercutido de los activos

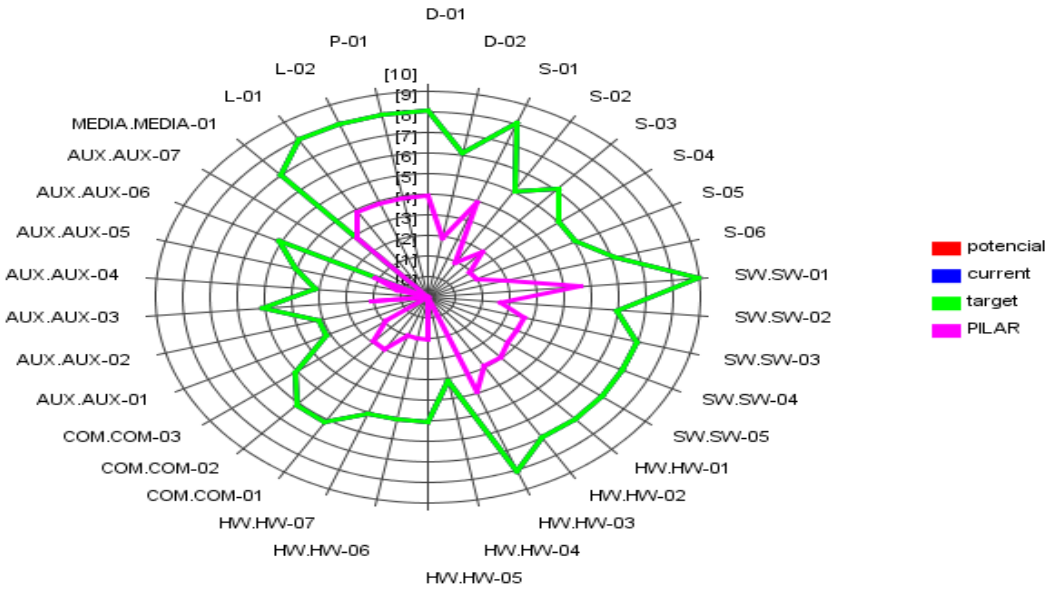


Nota. Elaboración propia.

La Figura 40 exhibe de manera concisa y gráfica los efectos posibles, actuales, deseados y sugeridos por el programa PILAR.

Figura 40

Gráfico de valores de impacto de activos



Nota. Elaboración propia.

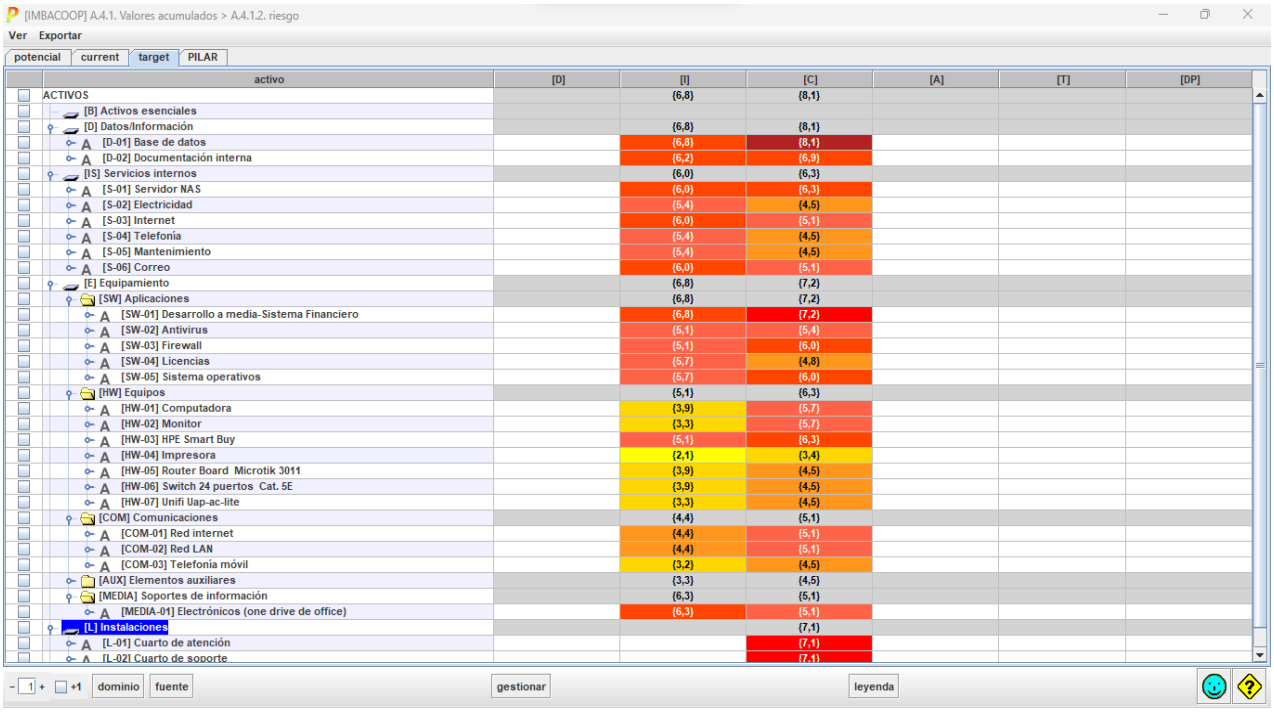
2.7.3. Estimación del impacto residual

Similar al efecto residual, la herramienta Pilar simula la implementación de controles y proporciona una evaluación del riesgo residual acumulado y del riesgo residual repercutido.

En la siguiente Figura 41 se ilustra la acumulación del riesgo residual, mientras que en la Figura 42 se presenta la manifestación de dicho riesgo residual.

Figura 41

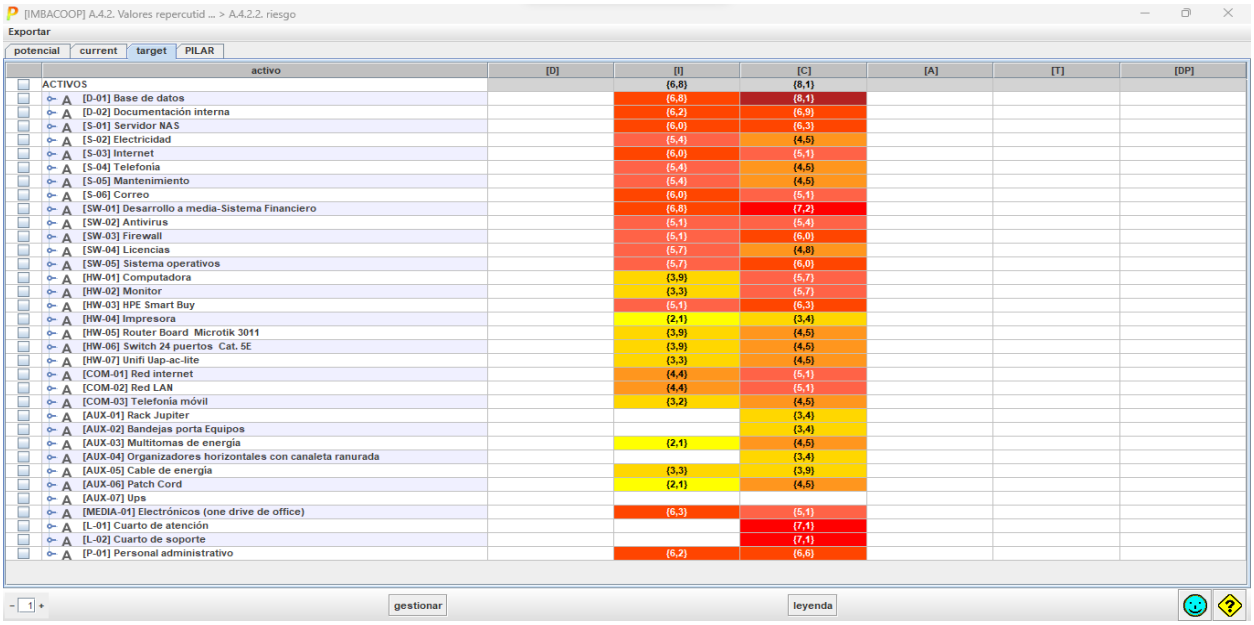
Riesgo residual acumulado de afectación de activos



Nota. Elaboración propia

Figura 42

Riesgo residual repercutido de afectación de activos



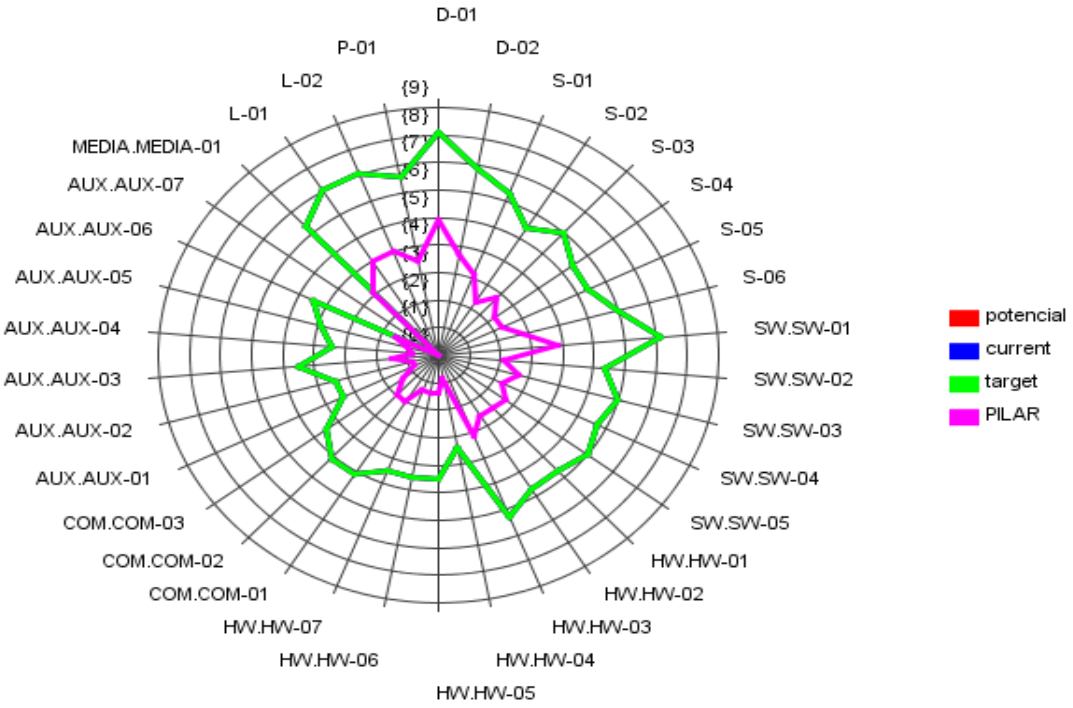
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS		{6,8}	{8,1}			
[D-01] Base de datos		{6,8}	{8,1}			
[D-02] Documentación interna		{6,2}	{6,9}			
[S-01] Servidor NAS		{6,0}	{6,3}			
[S-02] Electricidad		{5,4}	{4,5}			
[S-03] Internet		{6,0}	{5,1}			
[S-04] Telefonia		{5,4}	{4,5}			
[S-05] Mantenimiento		{5,4}	{4,5}			
[S-06] Correo		{6,0}	{5,1}			
[SW-01] Desarrollo a media-Sistema Financiero		{6,8}	{7,2}			
[SW-02] Antivirus		{5,1}	{5,4}			
[SW-03] Firewall		{5,1}	{6,0}			
[SW-04] Licencias		{5,7}	{4,8}			
[SW-05] Sistema operativos		{5,7}	{6,0}			
[HW-01] Computadora		{3,9}	{5,7}			
[HW-02] Monitor		{3,3}	{5,7}			
[HW-03] HPE Smart Buy		{5,1}	{6,3}			
[HW-04] Impresora		{2,1}	{3,4}			
[HW-05] Router Board Microtik 3011		{3,9}	{4,5}			
[HW-06] Switch 24 puertos Cat. 5E		{3,9}	{4,5}			
[HW-07] Unifi Uap-ac-lite		{3,3}	{4,5}			
[COM-01] Red internet		{4,4}	{5,1}			
[COM-02] Red LAN		{4,4}	{5,1}			
[COM-03] Telefonia móvil		{3,2}	{4,5}			
[AUX-01] Rack Jupiter			{3,4}			
[AUX-02] Bandejas porta Equipos			{3,4}			
[AUX-03] Multitomas de energia		{2,1}	{4,5}			
[AUX-04] Organizadores horizontales con canaleta ranurada			{3,4}			
[AUX-05] Cable de energia		{3,3}	{3,9}			
[AUX-06] Patch Cord		{2,1}	{4,5}			
[AUX-07] Ups						
[MEDIA-01] Electrónicos (one drive de office)		{6,3}	{5,1}			
[L-01] Cuarto de atención			{7,1}			
[L-02] Cuarto de soporte			{7,1}			
[P-01] Personal administrativo		{6,2}	{6,6}			

Nota. Elaboración propia.

En la siguiente Figura 43, se muestra un gráfico donde se representa los riesgos potenciales, actuales, objetivos y orientaciones según la herramienta Pilar.

Figura 43

Gráfico de valores de riesgo de activos del sistema financiero



Nota. Elaboración propia

2.8. Políticas de seguridad

2.8.1. Objetivo de la política de la seguridad

Establecer las políticas, prácticas y lineamientos internos de Seguridad de la Información para la Cooperativa de Ahorro y Crédito Imbacoop Ltda., con el fin de asegurar la protección de los activos de información del sistema financiero en todas sus formas y medios contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de modo de garantizar su confidencialidad, integridad.

De tal manera, las políticas de seguridad de la información son documentos formales que establecen las directrices, principios y prácticas que una organización debe seguir para garantizar la seguridad de la información que maneja. Estas políticas son parte integral de un programa de seguridad de la información y buscan proteger la confidencialidad e integridad de la información crítica para la organización.

Dicho eso, las políticas de la seguridad de la información se enfocan en todos los riesgos y amenazas encontradas en cada uno de los activos. Algunas de las ventajas al implementar la política en la organización son:

- Ayuda a asegurar la integridad de los datos financieros, evitando manipulaciones no autorizadas.
- Proporciona una base para adaptarse a nuevas tecnologías y amenazas emergentes, asegurando que los controles de seguridad estén actualizados.
- También abordan la gestión de incidentes y la planificación para la continuidad del negocio. Esto significa que la Cooperativa de Ahorro y Crédito Imbacoop Ltda., será adecuadamente preparada para enfrentar y recuperarse de interrupciones, ya sean causadas por eventos naturales, errores humanos o ataques cibernéticos.

2.8.2. Responsabilidades

Jefe de DTI

- Responsable de liderar y supervisar todas las actividades del sistema financiero y de DTI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.
- Encargado de la gestión y mantenimiento de la infraestructura de hardware y redes.
- Colabora con otros departamentos para entender sus necesidades y desarrollar soluciones tecnológicas efectivas.
- Administra las bases de datos utilizadas por la Cooperativa de Ahorro y Crédito Imbacoop Ltda.
- Coordina la planificación y ejecución de proyectos tecnológicos.

2.8.3. Desarrollo de las políticas de seguridad de la información

En la Tabla 25 se detallan las políticas y procedimientos cruciales que deben implementarse para garantizar la ausencia de riesgos en el proceso. Estas directrices son fundamentales para mitigar cualquier posibilidad de riesgo y asegurar un funcionamiento seguro y eficiente de los activos.

Tabla 25

Políticas de la seguridad de la información

Dominio	Resumen de objetivo y control	Detalle de Políticas
5. Políticas de seguridad.	**5.1 Directrices de la Dirección en seguridad de la información.** 5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información.	Política general, definido y aprobado. Definir y documentar todos los requisitos legales, regulatorios o contractuales.
6. Aspectos organizativos de la seguridad de la información.	**6.1 Organización interna.** 6.1.1 Asignación de responsabilidades para la segur. de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial 6.1.5 Seguridad de la información en la gestión de proyectos. **6.2 Dispositivos para movilidad y teletrabajo.** 6.2.1 Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo.	Experto en seguridad de la información del DTI de la Cooperativa de Ahorro y Crèdito Imbacoop Ltda., con enfoque en gestión y desarrollo de políticas de seguridad. Destacada capacidad para aprobar, implementar y asignar responsabilidades. Prioriza asesoramiento externo para un desempeño exitoso en seguridad.

7. Seguridad ligada a los recursos humanos.	**7.1 Antes de la contratación.** 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. **7.2 Durante la contratación.** 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la información. **7.2.3 Proceso disciplinario.** 7.3 Cese o cambio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo.	Plan de capacitación alineado a las políticas más relevantes. Evaluar el historial del candidato para asegurar su adecuación

Nota. Elaboración propia, 2023.

2.9. Mejora Continua

La optimización continua del SGSI realizado con la Norma ISO/IEC 27002:2013 implica revisar los resultados de la evaluación de los controles, políticas para ajustar los componentes de contramedidas del plan actual. Estas contramedidas tienen como objetivo mitigar los riesgos. Proponemos implementar nuevas tareas encaminadas a mitigar de manera más efectiva los riesgos que puedan persistir en los activos de la información.

- Realizar revisiones regulares de la efectividad del SGSI para identificar áreas de mejora y oportunidades de fortalecimiento.
- Asegurarse de que las políticas y procedimientos relacionados con la seguridad de la información estén actualizados para abordar las amenazas actuales y los cambios en el entorno operativo.
- Llevar a cabo análisis de riesgos continuos para evaluar nuevas amenazas y vulnerabilidades, y ajustar los controles de seguridad según sea necesario.
- Proporcionar formación continua en seguridad de la información a los empleados para mantenerlos informados sobre las mejores prácticas y las amenazas emergentes.

- Establecer sistemas de monitoreo continuo para identificar y responder a eventos de seguridad de manera proactiva.

2.9.1. Plan de implementación

Para la implementación de Plan de Desarrollo de SGSI para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se debe seguir algunos pasos que se detallara a continuación en la Tabla 26:

Tabla 26

Pasos para el plan de implementación de SGSI

Implementación de Sistema de Gestión de Seguridad de la Información	
Ejecutar los controles definidos de la ISO 27002:2013 de acuerdo con las políticas de seguridad que se hayan realizado en el Desarrollo de Plan de Sistema de gestión de la Seguridad de la Información.	Es muy importante la ejecución de las políticas mencionadas en el Desarrollo de Plan SGSI del sistema financiero de DTI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., con el fin de evitar inconvenientes o inferencias con las actividades institucionales. Se recomienda una revisión previa a la implementación utilizando una lista de verificación acompañada de un análisis de activos, identificación de amenazas, tratamiento de riesgos, controles, políticas de seguridad. Este enfoque garantiza una implementación perfecta que se alinea con las operaciones actuales, mejorando la seguridad de la información.

Implementación de controles	Como primer punto se realizó la identificación de sistema financiero y los activos relacionados con el fin de realizar la valoración de cada uno de ellos, luego para realizar la identificación de amenazas, y como siguiente punto tratamiento de riesgo. Como resultado se ha definido los controles en Desarrollo de Plan de SGSI. En la implementación se recomienda detallar cada control con el fin de determinar los recursos necesarios y desarrollar un plan de desarrollo efectivo. Establecer áreas y comités de seguridad de la información para manejar incidentes y definir responsabilidades y cronogramas son críticos para implementar los controles propuestos en el proyecto.
Ejecución de plan de gestión de incidentes	Es importante que el DTI lleve un documento de registro de incidentes ocurridos, con el fin de tratar y reducir los futuros incidentes, mediante las políticas establecidas. Se debe tener un manual de actividades o procesos que se debe seguir para incidentes: Crear un protocolo de notificación de incidentes. Designar responsabilidades de reporte de áreas afectadas Desarrollar un plan de contingencia. Presentar informes trimestrales.
Manejo de recursos para Plan de Sistema de Gestión de la Seguridad de la Información.	La gestión eficaz del SGSI implica una asignación eficiente de recursos mediante el análisis de prioridades dentro de DTI. Cree un plan que cumpla con la política de seguridad y garantice que los controles se prioricen y validen en función de los informes.

Revisión, evaluación y aprobación de Desarrollo de Plan de Sistema de Gestión de la Seguridad de la Información por el jefe de Departamento de Tecnología de la Información.	El Departamento de Tecnología de la Información ha recibido los documentos resultantes del Desarrollo de Plan de Sistema de Gestión de Seguridad de la Información (SGSI).

Nota. Elaboración propia

2.9.2. Socialización y Capacitación

Es muy importante la socialización y capacitación para finalizar la implementación de SGSI, para lo cual hay que tomar en cuenta los siguientes puntos:

- Dar a conocer la importancia de la seguridad de la información en las identidades financieras.
- Difundir el conocimiento adquirido a lo largo de totalidad del procedimiento de concepción de SGSI con la Norma ISO/IEC 27002:2013.
- Comunicar las tareas que se ha realizado al desarrollar un plan de SGSI con la ISO/IEC 27002:2013.
- Detallar en que consiste cada una de las tareas realizadas para la ejecución de controles, políticas de seguridad de la información.
- Aclaras dudas que tengan.

También se han realizado algunos materiales para la socialización que se encuentran en el Anexo 10, los interesados son gerente general, jefe del Departamento de Tecnología de la Información, área de riesgo, de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., para la capacitación a que demorar no más de 2 horas.

De igual manera, se presentará el Desarrollo de Plan de Sistema de Gestión de Seguridad de la Información. El documento, junto con las actividades realizadas en el archivo de Excel (gestión de riesgos).

Finalmente, la organización debe utilizar plataformas en línea para llevar a cabo evaluaciones o encuestas que confirmen la eficacia y la satisfacción de las actividades de concientización. Esto garantizará que se incluya a quienes no participaron en la evaluación presencial. Las siguientes preguntas del Anexo 11 servirán como guía para que utilice en la institución.

CAPÍTULO 3

Resultados

3.1. Evaluación de Desarrollo de Plan de Sistema de Gestión de la Seguridad de la Información con el método Delphi

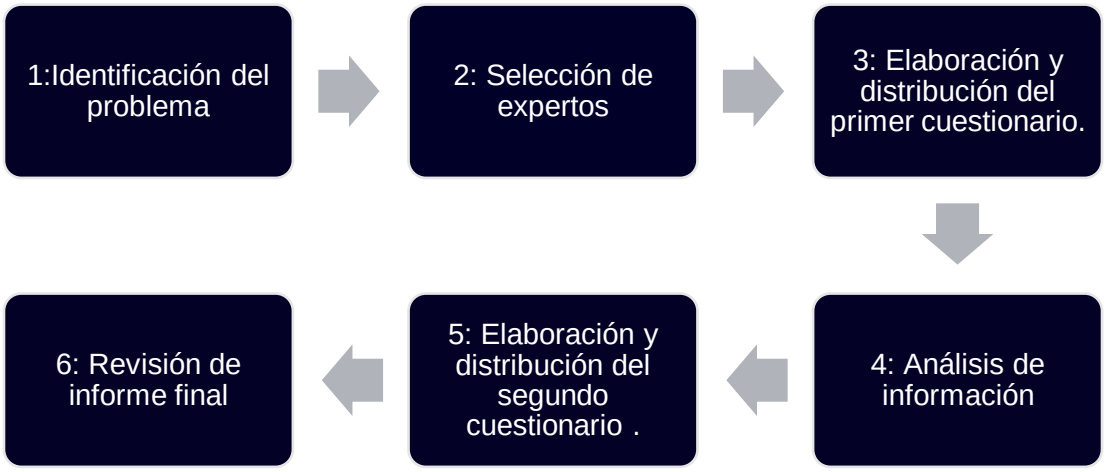
Tras culminar Desarrollar un Plan de Sistema de Gestión de la seguridad de la Información, es muy importante comprobar la eficacia del proceso realizado para comprobar la calidad y el éxito de estas iniciativas, se decidió utilizar el método Delphi de evaluación. Este enfoque participativo proporciona información de expertos para garantizar una evaluación exhaustiva y coherente.

El método Delphi es un método para consultar repetidamente con expertos en el área que se ha investigado hasta llegar a un consenso, cada experto responde las preguntas de cuestionario enviado en cada ronda por el investigador, con el fin de obtener un resultado esperado(Ureba et al., 2019).

Se debe seguir los siguientes pasos para la validación con el método de Delphi, como se detalla en la siguiente Figura 44.

Figura 44

Pasos a seguir para el método Delphi



Nota. Fuente: *(Quezada et al., 2020)*.

3.1.1. Identificación del problema

Lo primero que hay que realizar es la identificación del problema u objetivo de estudio como lo manifiesta en el método Delphi, en esta instancia se trata de evaluar la eficiencia de Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en el sistema

financiero y los demás activos del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., un documento de informe realizado con base en la metodología Magerit versión 3 y teniendo en cuenta las consideraciones de la Norma ISO/IEC 27003:2013 con respecto a análisis y gestión de riesgos tecnológicos en el sistema.

3.1.2. Selección de expertos

La Identificación y selección de un grupo relevante de expertos en áreas relacionadas con el campo de investigación que se investiga, los cuales deben tener conocimiento, estos expertos pueden ser profesionales, académicos, investigadores. Todos deben participar de manera voluntariamente, sin depender unos de otros y sin prejuicios ni condicionamientos de respuesta(Sánchez, 2022).

Además, para determinar el tamaño y la estructura del grupo de expertos hay que tener en cuenta la naturaleza de la investigación, los posibles resultados y los recursos de que disponen los investigadores, no obstante, la validez y la fiabilidad de este método se puede ver afectado por el tamaño del grupo expertos, ya que grupos de expertos demasiado grandes o pequeños pueden afectar negativamente a la calidad de los resultados(Cañizares & Suárez, 2022).

Inicialmente, se contactó con un grupo específico de expertos de diversas instituciones enviando email por medio de correos electrónicos a las siguientes direcciones, de todos los expertos únicamente participaron un número ilimitado de 3 expertos de diferentes organizaciones.

3.1.3. Elaboración y distribución del primer cuestionario

Después de haber definido el objetivo de investigación, se realizó un cuestionario de 11 preguntas, que se centrarán en el objetivo de investigación con un enfoque a los puntos relevantes de Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27002:2013. El cuestionario inicial está disponible en el Anexo 10. La recolección de información fue realizada mediante email de correo electrónico y la participación de los expertos. Se determinó que el tiempo previsto entre el envío de la información y la recepción de una respuesta era de una semana, en la información enviada se adjuntó Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27002:2013 y un vínculo para que pueda acceder al cuestionario en Google Forms.

Exceptuando la pregunta 11, lo cual es opinión personal y los demás son opcionales, se propuso las demás preguntas mediante la escala de Likert de 5 puntos, detallada en la Tabla 27.

Tabla 27

Escala de Likert para la valoración de cuestionarios

Valor	Escala de Likert
1	Totalmente de acuerdo
2	De acuerdo
3	Indiferente o neutro
4	En desacuerdo
5	Totalmente en desacuerdo

Nota. Elaboración Propia, 2023.

3.1.4. Análisis de información

Las informaciones analizadas utilizando medos descriptivos, cualitativos y cuantitativos para comprender los resultados obtenidos durante el estudio.

Para calcular el índice de validez de contenido que representa cada elemento, se utilizó la siguiente fórmula:

$$CVI = \frac{número\ rto\ de\ respuestas\ positivas}{número\ total\ de\ respuestas}$$

$$CVITotal = \frac{número\ de\ respuestas\ positivas}{(número\ de\ expertos\ \times\ número\ de\ items)}$$

Según con la investigación revisada, la validez de un instrumento de evaluación se determina considerando el índice de validez de contenido (IVC). Para que cada ítem se considere globalmente efectivo, su CVI total es igual o superior al 90%. Además, cada proyecto debe tener un CVI igual o superior al 75% para ser considerado válido. Si se verifican estas condiciones, se concluye un consenso. Por otro lado, si no están satisfechos, se les puede pedir opiniones o sugerencias para ajustar y/o eliminar las preguntas (Silva& Montilha, 2021).

Además, se optó por utilizar métodos adicionales como:

- **Estadística descriptiva:** Promover la comprensión de la estructura de los datos para identificar patrones generales de comportamiento y sus desviaciones. Una forma de lograrlo es mediante gráficos fáciles de crear e interpretar. Al emplear variables cuantitativas (como escalas Likert), optamos por utilizar medidas de tendencia central, incluidas la media aritmética, la mediana y la moda.
- **Alfa de Cronbach:** Es una medida de la fiabilidad o consistencia interna de una escala de medida. Suele utilizarse en investigación para evaluar la coherencia de las respuestas de los participantes a cuestionarios o pruebas. Los valores del alfa de

Cronbach oscilan entre 0 y 1, y los valores mínimos aceptables se debe estar entre 0,70 y 0,90.

Como primer punto, se debe efectuar un análisis de las 11 preguntas obtenidas del cuestionario enviado a los expertos, lo cual se muestra en la Tabla 28.

Tabla 28

Primer cuestionario proporcionado a los expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
E1	1	1	2	2	2	1	2	2	2	2	No
E2	2	2	2	2	2	2	2	2	2	2	No
E3	1	2	2	1	1	2	2	1	1	1	Ampliar la descripción en lo referente a mejora continua

Nota. La tabla indica los datos tabulados del primer cuestionario, donde P son preguntas y E expertos. Elaboración propia

Con el propósito de evaluar la validez del contenido, se precisa una tabla que incluya las respuestas para cada pregunta y el valor correspondiente en la escala Likert. Se puede hallar esta matriz en la Tabla 29, y visualizarla de manera gráfica en la Figura 45.

Tabla 29

Tabulación de respuestas del primer cuestionario realizado a expertos por pregunta y valor

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
TA	2	1	0	1	1	1	0	1	1	1	-
A	1	2	3	2	2	2	3	2	2	2	-
N	0	0	0	0	0	0	0	0	0	0	-
D	0	0	0	0	0	0	0	0	0	0	-
TD	0	0	0	0	0	0	0	0	0	0	-

Nota. TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, P: Preguntas de cuestionario. Elaboración propia

Figura 45

Respuesta de por ítem de 1er cuestionario a expertos

Nota. P: Interrogantes del cuestionario, TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo. Elaboración propia

Una vez tabuladas las respuestas, el índice de validez de contenido se puede calcular utilizando la fórmula descrita anteriormente. Consulte la Tabla 30 para obtener más detalles.

Tabla 30

Índice de Validez de Contenido (CVI) del primer cuestionario a expertos

Preguntas	TD	D	N	A	TA	IVC ÍTEM
1: ¿Considera usted que es muy imprescindible Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información con la ISO/27002:2013 en el sistema financiero del departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda?	-	-	-	33%	67%	100%
2: ¿Cómo evalúa el Desarrollo de Plan de Sistema de Gestión de Seguridad de la Información con la ISO/27002:2013 para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., es un informe comprensible de manera simple?	-	-	-	67%	33%	100%
3: ¿A su criterio el informe de Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información con la ISO/27002:2013 para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., cuenta con la información necesaria?	-	-	-	100%	-	100%

4: ¿Está de acuerdo con la elección de la Metodología Magerit v3 y la ISO/IEC 27002:2013 para Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda?	-	-	-	67%	33%	100%
5: ¿Considera usted que los procedimientos realizados en el Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., fueron los necesarios?	-	-	-	67%	33%	100%
6: ¿Considera usted que la utilización de la herramienta Pilar y las hojas de cálculo de Excel resultaron han demostrado ser eficientes y acertadas en el manejo de información en el Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda.?	-	-	-	67%	33%	100%
7: ¿En su opinión las tareas propuestas a manera de controles para la mitigación de riesgos en el Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., fueron adecuadas?	-	-	-	100%	-	100%
8: ¿Cree que el Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información con la norma ISO/IEC 27002:2013, realizada para el sistema financiero del Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., puede ser aplicado con éxito en otras entidades financieras?	-	-	-	67%	33%	100%
9: ¿Considera usted que las políticas de seguridad realizadas para el Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en sistema financiero del Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda fueron las más adecuadas?	-	-	-	67%	33%	100%
10: ¿Considera usted que a través de la acción del plan de tratamiento riesgo realizada se asegura la confidencialidad e integridad de la información del sistema financiero en el Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información del Departamento	-	-	-	67%	33%	100%

de Tecnología de la información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.?											
11: ¿Haría ajustes a algún elemento del Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda?	-	-	-	-	-	-					
									Total IVC	100%	

Nota. TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, IVC: índice de Validez de Contenido. Elaboración propia

En la primera ronda de cuestionario se recopiló el Índice de validez de contenido (IVC) Total de 93%. Lo que menciona en la literatura es un puntaje apropiado para que sea válido el cuestionario. Cada una de las preguntas tiene un IVC de ítem superior o igual al 75% dado el consenso sobre los resultados, se concluyó que no fueron necesarios ajustes ni eliminación de ítems.

Para probar la validez del cuestionario, se aplicó el método estadístico alfa de Cronbach a todo el instrumento utilizando la siguiente fórmula:

$$\alpha = \frac{k}{k-1} \times \left[1 - \frac{\sum vi}{vt}\right]$$

En donde,

$\alpha = Alfa\ de\ cronbach$

$K = Número\ de\ Items$

$Vi = Varianza\ de\ cada\ item$

$Vt = Varianza\ Total$

Los resultados de la varianza se presentan en la Tabla 31, mientras que los cálculos del alfa de Cronbach están detallados en la Tabla 32.

Tabla 31

Varianza de ítems del primer cuestionario a expertos

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Suma Total
E1	1	1	2	2	2	1	2	2	2	2	17
E2	2	2	2	2	2	2	2	2	2	2	20
E3	1	2	2	1	1	2	2	1	1	1	14
Varianza	0,22	0,22	0,00	0,22	0,22	0,22	0,00	0,22	0,22	0,22	51

Nota. E: Número de Expertos, P: Preguntas del cuestionario. Elaboración propia

Tabla 32

Alfa de Cronbach del primer cuestionario a expertos

k	10
Suma de varianza (Vi)	1,78
Varianza total (Vt)	6,00
Cronbach	0,78

Nota. Elaboración propia

El valor alfa de Cronbach es de 0,78 lo que indica que la confiabilidad del cuestionario se encuentra dentro de un rango aceptable. La literatura sugiere que valores en el rango de 0,72 a 0,99 indican una excelente confiabilidad del instrumento.

En relación con lo anterior, en el punto 11 se analiza el controvertido tema de la posibilidad de realizar cambios o mejoras en el Desarrollo de Plan de Sistema de Gestión de la Seguridad de la Información. Estas recomendaciones quedaron reflejadas en la revisión del informe y el desarrollo de la segunda ronda de preguntas Delphi.

3.1.5. Elaboración y distribución del segundo cuestionario

Para tomar la decisión de modificar el actual informe sobre el Desarrollo de Plan de Sistema de Gestión de Seguridad de la Información, es necesario analizar las respuestas recogidas en el punto 11 del primer cuestionario. Estas respuestas se resumen en la Tabla 33.

Tabla 33

Resumen de las respuestas obtenidas en la pregunta 11 del cuestionario inicial

11: ¿Haría ajustes a algún elemento del Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda? ¿cuál sería?	
Expertos	**Respuesta**
E1	No
E2	No
E3	Ampliar la descripción en lo referente a mejora continua

Nota: E: Es número de expertos. Elaboración Propia

Solamente el experto 3 brinda retroalimentación que podría ayudar a aumentar la efectividad del Sistema de Gestión de la Seguridad de la Información.

Con el fin de abordar de manera efectiva cada uno de estos comentarios, se implementaron las siguientes adaptaciones:

1. **Mejora Continua:** La optimización continua del SGSI realizado con la Norma ISO/IEC 27002:2013 implica revisar los resultados de la evaluación de los controles, políticas para ajustar los componentes de contramedidas del plan actual. Estas contramedidas

tienen como objetivo mitigar los riesgos. Proponemos implementar nuevas tareas encaminadas a mitigar de manera más efectiva los riesgos que puedan persistir en los activos de la información.

Respecto a la mejora continua, el DTI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., dará atención a los siguientes puntos:

- Realizar revisiones regulares de la efectividad del SGSI para identificar áreas de mejora y oportunidades de fortalecimiento.
- Asegurarse de que las políticas y procedimientos relacionados con la seguridad de la información estén actualizados para abordar las amenazas actuales y los cambios en el entorno operativo.
- Realizar análisis de riesgos continuos para evaluar nuevas amenazas y vulnerabilidades, y ajustar los controles de seguridad según sea necesario.
- Proporcionar formación continua en seguridad de la información a los empleados para mantenerlos informados sobre las mejores prácticas y las amenazas emergentes.
- Establecer sistemas de monitoreo continuo para identificar y responder a eventos de seguridad de manera proactiva.

Plan de implementación: Para la implementación de Plan de Desarrollo de SGSI para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se debe seguir algunos pasos que se detallara a continuación:

- Ejecutar los controles definidos de la ISO 27002:2013 de acuerdo con las políticas de seguridad que se hayan realizado en el Desarrollo de Plan de Sistema de gestión de la Seguridad de la Información.
- Implementación de controles.
- Ejecución de plan de gestión de incidentes.
- Manejo de recursos para Plan de Sistema de Gestión de la Seguridad de la Información.
- Revisión, evaluación y aprobación de Desarrollo de Plan de Sistema de Gestión de la Seguridad de la Información por el jefe de Departamento de Tecnología de la Información.

Tras confirmar la idoneidad del informe, se creó un segundo cuestionario para el método de validación Delphi. Este nuevo cuestionario tiene el mismo estilo que el cuestionario

anterior y constaba de 5 ítems directamente relacionados con los cambios en las respuestas al primer cuestionario. Puede encontrar esta información en el Anexo 11.

3.1.6. Revisión final de información

Tras recopilar las respuestas de los 3 expertos, se pueden observar los resultados como se muestra en la Tabla 34.

Tabla 34

Respuesta de segundo cuestionario a Expertos

	P1	P2	P3	P4	P5
E1	1	1	1	2	2
E2	2	2	1	2	2
E3	1	1	1	1	1

Nota. La tabla muestra los datos de tabulación del segundo cuestionario, donde E: Es número de expertos, P: Preguntas de cuestionario. Elaboración propia

La lista requerida de respuestas para cada pregunta junto con la asignación de valores en la escala Likert se muestra la tabulación en la Tabla 35 y de forma gráficamente en la Figura46. Esta información es esencial para calcular el índice de efectividad del contenido.

Tabla 35

Tabulación de respuestas obtenidas del segundo cuestionario a expertos por pregunta y valor en la escala de Likert

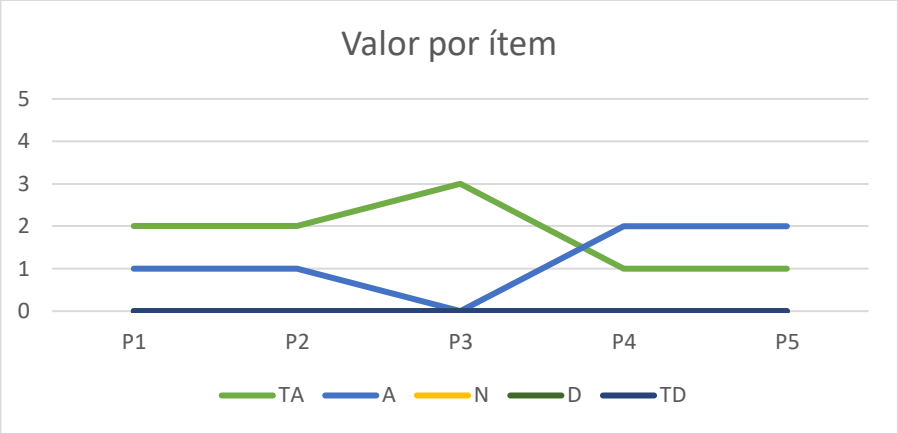
	P1	P2	P3	P4	P5
TA	2	2	3	1	1
A	1	1	0	2	2
N	0	0	0	0	0
D	0	0	0	0	0
TD	0	0	0	0	0

Nota: TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, P: Preguntas de cuestionario. Elaboración propia

Figura 46

Respuestas por ítem del segundo cuestionario a expertos

Los resultados de la tabulación de los resultados se muestran a continuación y la fórmula anterior se puede utilizar para calcular el índice de validez del contenido. En la Tabla 36 para obtener más detalles.



Nota. P: Interrogantes del cuestionario, TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo. Elaboración propia

Tabla 36

Índice de Validez de Contenido del segundo cuestionario a expertos

Preguntas	TD	D	N	A	TA	IVC ÍTEM
1: ¿Considera que las políticas de Mejora Continua que se han establecido en el desarrollo de Plan Sistema de Gestión de la Seguridad de la Información están acordes con el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda?	-	-	-	33%	67%	100%
2: ¿Considera usted que, en respuesta al enfoque de Mejora Continua, sea acertado plantear un seguimiento por trimestral o por lo menos una vez al año sistema financiero del Departamento de Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda?	-	-	-	33%	67%	100%
3: ¿Considera usted que la optimización de proceso de respuesta a incidentes contribuiría a una mejora continua en la detección y mitigación de riesgos?	-	-	-	-	100%	100%
4: ¿Estaría de acuerdo en que el uso la norma ISO/IEC 27002:2013 fue acertada para la selección de controles?	-	-	-	67%	33%	100%
5: ¿Cree que las modificaciones en el Informe de Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información para el sistema financiero del departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda mejoraron la calidad según las observaciones del primer cuestionario?	-	-	-	67%	33%	100%
					Total, IVC	100%

Nota: TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, IVC: índice de Validez de Contenido. Elaboración propia

En la segunda ronda de cuestionario se recopilo el Índice de validez de contenido (IVC) Total de 100%, lo que menciona en la literatura es un puntaje apropiado para que sea válido el cuestionario. Cada una de las preguntas tiene un IVC de ítem de 100% dado el consenso sobre los resultados, se concluyó que no fueron necesarios ajustes ni eliminación de ítems.

Se aplicó nuevamente el método estadístico alfa de Cronbach a todo el conjunto de cuestionarios para probar su fiabilidad.

Los resultados obtenidos de las varianzas se detallan en la Tabla 37, en tanto que los resultados de la evaluación de alfa de Cronbach se encuentran en la Tabla 38.

Tabla 37

Varianza de ítems del cuestionario final (información) a expertos

	P1	P2	P3	P4	P5	Suma Total
E1	1	1	1	2	2	7
E2	2	2	1	2	2	9
E3	1	1	1	1	1	5
Varianza	0,22	0,22	0,00	0,22	0,22	21

Nota. TA: Totalmente de acuerdo, A: Acuerdo, N: Neutro, D: Desacuerdo, TD: Totalmente desacuerdo, P: Preguntas de cuestionario. Elaboración propia

Tabla 38

Alfa de Cronbach del segundo cuestionario a expertos

k	5
Suma de varianza (Vi)	0,89
Varianza total (Vt)	2,67
Cronbach	0,83

Nota: Elaboración propia

El resultado de Alfa de Cronbach da un valor de 0,83 lo cual indica que se encuentra en un rango de excelente fiabilidad el cuestionario realizado para la segunda ronda a expertos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Al examinar las teorías fundamentales relacionadas con el Sistema de Gestión de la Seguridad de la Información de la Información, se ha sentado una base conceptual robusta. La comprensión de los principios de confidencialidad, integridad ha permitido identificar áreas específicas del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., puede mejorar la seguridad de los activos de la información.
2. La revisión de la literatura desempeñó un papel fundamental al proporcionar una comprensión sólida de los conceptos vinculados a un Sistema de Gestión de la Seguridad de la Información en un enfoque a activos de la información lo cual llevó a una elección y comparación de la norma y metodología adecuada para la gestión de riesgos para el Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.
3. El Departamento de Tecnología de la Información debe implementar controles sólidos, políticas de acceso basadas en roles, monitoreo de actividad de usuarios y medidas de seguridad. Estas medidas no solo protegen a la cooperativa de amenazas, sino que también generan confianza entre los clientes y demuestran el compromiso de la cooperativa con la protección de datos sensibles.
4. El uso de metodología Magerit v3 para la gestión de riesgos tuvo un papel muy importante para realizar los procesos de identificación y valoración de activos, identificación de amenazas, tratamiento de riesgos, con la finalidad de fortalecer de manera robusta al Departamento Tecnología de la Información contra desafíos que se puede presentar.
5. Organizar los activos según su riesgo y mantener un registro actualizado se convierte en un elemento esencial para potenciar su seguridad y protección. Para valorar los activos se consideraron las dimensiones de confidencialidad, integridad. En el ámbito del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., se identificaron 8 activos críticos.
6. La inexistencia de políticas de seguridad personalizadas ha limitado la eficacia de la implementación de controles basados en ISO/IEC 27002:2013, al realizar las políticas de seguridad específicas han proporcionado directrices claras, mejorando la conciencia

y responsabilidad que se debe llevar en Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

7. La evaluación de SGSI mediante método Delphi proporciona una visión integral al recopilar las aportaciones de los expertos seleccionados sobre el informe realizado, los expertos manifiestan que es comprensible, confiable, y aceptable con los métodos, herramienta, métodos, estándares seleccionados.
8. El índice de validez de contenido final dio como resultado 100% indica que el contenido de las preguntas o ítems es apropiado y refleja de manera precisa, lo cual demostró que no hay más necesidad de cambiar los ítems.
9. El análisis del alfa de Cronbach, con un resultado del 0.83, confirma la consistencia interna del cuestionario, esto significa que las preguntas están correlacionadas de manera positiva entres sí, lo que refuerza la validez y confiabilidad del instrumento, este hallazgo refuerza la calidad de desarrollo de investigación que se ha realizado.

Recomendaciones

1. Es importante llevar una evaluación exhaustiva, identificar vulnerabilidades y actualizar los protocolos de seguridad, incluyendo la capacitación continua del personal. Estas medidas asegurarán una protección más efectiva de la información y fortalecerán la seguridad general de la cooperativa.
2. Es conveniente que la Cooperativa de Ahorro y Crédito Imbacoop Ltda., priorice la implementación de Sistema de Gestión de la Seguridad de la Información. Dado que la elección de la Norma y Metodología adecuadas desempeña un papel crucial, con la finalidad de realizar una evaluación exhaustiva de las opciones disponibles, teniendo en cuenta las características específicas y las necesidades de la organización.
3. El Departamento de Tecnología de la Información debe reforzar una información sencible mediante la implementación de políticas y controles específicos. Esto incluye el cifrado de datos en reposo y en tránsito, la revisión regular de políticas de acceso y permisos, y la implementación de sistemas de detección de intrusiones. Además, se debe fomentar una cultura de seguridad en toda la cooperativa, donde todos los empleados entiendan la importancia de proteger los datos y sepan cómo actuar en caso de incidentes de seguridad.
4. Se sugiere una capacitación continua al personal en la metodología para garantizar una implementación efectiva y un entendimiento profundo de los principios para la gestión

de riesgo de los activos del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

5. Se debe actualizar o revisar las políticas de seguridad de manera trimestralmente con el fin de prevenir los riesgos, los cuales evolucionan constantemente de acuerdo los avances tecnológicos, asegurando así un enfoque preventivo y flexible en la protección del sistema financiero y los demás activos de la información.
6. Para futuras investigaciones proponer la utilización de herramientas de automatización Gobierno, gestión de riesgo y cumplimiento (GRC) para toda la gestión del Sistema de Gestión de la Información y utilizando el método Delphi, el SGSI es un sistema vivo que debe estar en constante evolución y mejora, esto implica abordar todas las áreas de la organización empezando por el Liderazgo.
7. Aunque el índice de validez de contenido actual es excelente, se recomienda realizar revisiones periódicas del instrumento. Los contextos y las áreas de interés pueden cambiar con el tiempo, y es importante asegurarse de que el instrumento siga siendo relevante y representativo.
8. Se sugiere aumentar más preguntas en el cuestionario y más expertos para futuros trabajos con el fin de llegar a mayor nivel de confiabilidad de instrumento más cercana a 1, fortaleciendo la validez y exhaustividad del instrumento de medición en la evaluación del SGSI.

REFERENCIAS Y BIBLIOGRAFÍA

Bibliografía

Aguilera, P. (2020, June). *Introducción a la seguridad informática (Seguridad informática)*. https://books.google.com.ec/books?id=jofTAwAAQBAJ&lpg=PA10&ots=lsQs1roWRd&pg=PA10#v=onepage&q&f=false

Aldas, C. (2017). *Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.* https://repositorio.uta.edu.ec/bitstream/123456789/27124/1/Tesis_%20t1359si.pdf

Alvaro, C. V. (2018). *Sistema de gestión de seguridad de la información: qué es y sus etapas*. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Camargo, J. (2018). *Diagnóstico de la Seguridad de la Información para la división de investigación y extensión de la Universidad Francisco de Paula Santander Ocaña, basado en la norma ISO/IEC 27002:2013*. http://repositorio.ufpso.edu.co/xmlui/bitstream/handle/123456789/2905/32699.pdf?sequence=1

Cañizares, E., & Suárez, K. (2022). El Método Delphi Cualitativo y su Rigor Científico: Una revisión argumentativa. *Sociedad & Tecnología*, *5*(3), 533. https://doi.org/10.51247/st.v5i3.261

Cárdenas, J. (2023). *Estrategias para mitigar riesgos financieros en la Cooperativa de Ahorro y Crédito Kisapincha Ltda.* https://repositorio.pucesa.edu.ec/bitstream/123456789/4228/1/MCA%20Cardenas%20Zu%C3%B1iga%20Joana%20Elizabeth.pdf

CCN-CERT. (2023). *Implementación de la metodología Magerit*. https://pilar.ccn-cert.cni.es/index.php/metodologia/implementacion

Celis, L. (2018). *Plan de Seguridad de la Información aplicado Central Hidroeléctrica Carhuaquero*. https://tesis.usat.edu.pe/bitstream/20.500.12423/1615/1/TL_CelisFigueroaLeonardo.pdf

Centro Criptológico Nacional. (2023). *Pilar*. https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar

Cordero, M. (2022). *Políticas de seguridad de la información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el*

departamento de tecnología de la Cooperativa de Ahorro y Crédito San Francisco Ltda. https://repositorio.uta.edu.ec/bitstream/123456789/34814/1/t1959si.pdf

Cortés, J. (2023). *Modelo de Seguridad basado en Blockchain para la Interoperabilidad de Datos Clínicos entre Sistemas de Información de IPS en Colombia*. https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5904/JaimeAlberto_CortesCalle_2023.pdf?sequence=1&isAllowed=y

Crespo, E. (2018). *Estudio comparativo entre las metodologías cramm y magerit para la gestión de riesgo de ti en las mpymes*. https://dspace.uazuay.edu.ec/bitstream/datos/10433/1/Akadem1_4.pdf

Criollo, S. (2017). Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo. *Seguridad de Unidades Informáticas*. https://repositorio.uta.edu.ec/bitstream/123456789/26537/1/Tesis_%20t1318si.pdf

Ctma. (2021). *Estas son las ventajas y desventajas de la ISO 27001*. https://ctmaconsultores.com/ventajas-y-desventajas-de-la-iso-27001/

Dirección General de Modernización Administrativa, P. e I. de la A. E. (2012a). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos*. http://administracionelectronica.gob.es/

Dirección General de Modernización Administrativa, P. e I. de la A. E. (2012b). *MAGERIT-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I-Método*. http://administracionelectronica.gob.es/

DocuSign. (2021). *¿Cuáles son los pilares de la seguridad de la información?* https://www.docusign.mx/blog/seguridad-de-la-informacion

Erazo, A. (2016). *Análisis y planteamiento de políticas de acuerdo al esquema gubernamental de seguridad de la información (EGSI) para la empresa pública Yachay.* [UTN]. http://repositorio.utn.edu.ec/bitstream/123456789/9001/1/05%20FECYT%20213%20TRABAJO%20DE%20GRADO.pdf

Eumed. (2019). *Importancia de la Norma ISO/IEC 27000 en la implementación de un Sistema de Gestión de la Seguridad de la Información*. https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html

García, F. Y. H., & Moreta, L. M. L. (2019). *Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras*. https://doi.org/10.17013/risti.31.1-17

Gobierno de España. (2018). *Normas ISO sobre gestión de seguridad de la información*. http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Gobierno Electrónico de Ecuador. (2020). *Ciclo de Deming*. Gobierno Electrónico de Ecuador. https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

Google Maps. (2023). *Dirección de la Cooperativa Imbacoop*. https://maps.app.goo.gl/xo78Ax4y4bYQ3b8SA

Guamán, V. (2019). *Evaluación de seguridad de la información Aplicado al Sistema de evaluación de docentes de la Universidad Técnica del Norte basado en la ISO 27002:2017 con la Metodología Magerit v3*. http://repositorio.utn.edu.ec/bitstream/123456789/9535/2/04%20ISC%20524%20TRABAJO%20DE%20GRADO.pdf

Guaña, J. (2022). *Ataques informáticos más comunes en el mundo digitalizado*. https://media.proquest.com/media/hms/PFT/1/rjdZR?_s=dvWakK9%2F4bsrimGrSdqocjwdw38%3D

Hermoso-Orzáez, G. (2021). *Risk management methodology in the supply chain: a case study applied*. https://doi.org/https://doi.org/10.1007/s10479-021-04220-y

Imbacoop. (2023). *Organigrama estructural de la Cooperativa*. Organigrama estructural de la Cooperativa

Implantaci, D. E., La, P., & La, S. D. E. (2013). *Guía De Implantación Para La Seguridad De La Información*.

Intedya. (2015, September 1). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

Iso 27000. (2013). *ISO/IEC 27002:2013. 14 dominios, 35 objetivos de control y 114 controles*. https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

Iso, 27002:2013. (2013). *ISO/IEC 27002:2013. 14 dominios, 35 objetivos de control y 114 controles*. https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

ISO/IEC 27000. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. www.iso.org

ISO/IEC 27002. (2013). *ISO/IEC 27002:2013. 14 dominios, 35 objetivos de control y 114 controles*. https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

ISOTools Excellence. (2017). *¿Seguridad informática o seguridad de la información?* https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

ISOTools Excellence. (2018). *Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad*. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Jeklin, A. (2016). *済無No Title No Title No Title*. *July*, 1–23.

Martínez, J. (2017). Instituto de Acceso a la Información Pública. *Iaip*, *88*. https://www.transparencia.gob.sv/institutions/iaip/documents/309603/download

Masaquiza, C. (2011). Facultad De Ingeniería En Sistemas, Electrónica E Industrial. *Estudent*, *5*(54), 453544. http://repo.uta.edu.ec/bitstream/123456789/8595/1/Tesis_t953si.pdf

Miranda, J. (2021). *Mapeo Sistemático de Metodologías de Seguridad de la Información para el control de la Gestión de riesgos informáticos*. https://dspace.ups.edu.ec/bitstream/123456789/20966/4/UPS-GT003401.pdf

Nqa. (2013). *ISO 27001:2013 Guía de implantación para la seguridad de la información*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Pérez, S. (2022, March 13). *Metodologías de Seguridad en la nube*. https://forum.huawei.com/enterprise/es/metodolog%C3%ADas-de-seguridad-en-la-nube-parte-2-final/thread/838381-100261

Pilla, J. (2019). *Diseño de una Política de Seguridad de la Información para el área de tecnología de la Información de la Cooperativa de Ahorro y Crédito Chibuleo Ltda., basado en la norma ISO/IEC 27002:2013*. https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%C3%91O%20DE%20UNA%20POL%C3%8DTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20PARA%20EL%20%C3%81REA%20DE%20TECNOLOG%C3%8DA%20DE%20LA%20INFORMACI%C3%93.pdf

Quezada, G., Oliva, J., & Gallo, C. (2020). *Método Delphi como estrategia didáctica en la formación de semilleros de investigación*. https://doi.org/10.35622/j.rie.2020.01.005

Regina, G., Mendoza, R., Coronado, J., & Dorantes, E. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. *Contribuciones a La Economía*, *junio*. https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html

Rodríguez, H. (2019). *Importancia de controlar todas las amenazas detectadas a través de Magerit v.3 e ISO/IEC 27002 según análisis de ataques informáticos en Latinoamérica*.

https://repository.unad.edu.co/bitstream/handle/10596/31879/harodriguezar.pdf?sequence=1&isAllowed=y

Romero, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., & Álava, C. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. In *Introducción a la seguridad informática y el análisis de vulnerabilidades*. https://doi.org/10.17993/ingytec.2018.46

Sánchez, L. (2022). Aplicación del método Delphi en el diseño de un marco para el aprendizaje por competencias. *Revista de Investigacion Educativa*, *40*(1), 219–235. https://doi.org/10.6018/rie.463611

Sevilla, E. (2023). *Diseño De Un Plan De Gestión De Riesgos Tecnológicos Con La Metodología Magerit V3 Basada En La Norma ISO/IEC 31000, Para Fortalecer La Gestión De Amenazas Y Riesgos En Los Laboratorios De Informática De La Facultad De Ingeniería En Ciencias De La Universidad Técnica Del Norte*. http://repositorio.utn.edu.ec/bitstream/123456789/13866/2/04%20ISC%20672%20TESIS%20GRADO.pdf

Silva, M., & Montilha, R. de C. I. (2021). Contribuições da técnica Delphi para a validação de uma avaliação de terapia ocupacional em deficiência visual. *Cadernos Brasileiros de Terapia Ocupacional*, *29*. https://doi.org/10.1590/2526-8910.ctoao2163

Teorico, P. I. M. (2012). *Seguridad de la Información ISO 27003 técnicas de seguridad. directrices para la implementación de un sistema de Gestión de la Seguridad de la Información*. https://1library.co/document/y8rwgmwq-seguridad-de-la-informacion-iso-v.html

Torres, C. (2020). *Plan de Seguridad Informática basado En La Norma ISO 27001, para proteger la información y activos de la empresa privada MEGAPROFER S.A*. https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

Unidad Nacional para la Gestión del Riesgo de Desastres. (2022). *Plan de Tratamiento de Riesgos*. https://portal.gestiondelriesgo.gov.co/Documents/GTI/Plan-de-Tratamiento-de-Riesgos-2022.pdf

Universidad Pablo de Olavide. (2020). *Seguridad informática*. https://rio.upo.es/xmlui/bitstream/handle/10433/8991/Seguridad%20informatica.pdf?sequence=1&isAllowed=y

Ureba, S. F., Agudo, L., & Menéndez, J. (2019). *El método Delphi aplicado al diseño de un modelo de financiación de transporte urbano*. https://doi.org/10.22136/est20191364

Vazquez, A. (2018). *Los Pilares de la Seguridad Corporativa: presente y futuro*. https://www.recercat.cat/bitstream/handle/2072/338148/TFG_Abel_Vazquez_Gutierrez.pdf?sequence=1

Anexos

Anexo 1: Entrevista para la situación actual

Entrevista al Directo del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN SOFTWARE

Situación Actual

1. ¿Qué capacidad de almacenamiento de datos tiene el sistema financiero?
2. ¿Dentro en la organización es importante la implementación de un Plan de Sistema de Gestión de Seguridad de la información?
3. ¿Se han implementado medidas de seguridad en el departamento y cuáles son esas medidas?
4. ¿El recurso humano de DTI cuenta con la formación apropiada en cuanto a seguridad?
5. ¿En el departamento cuenta con políticas de seguridad de información para el sistema financiero?
6. ¿Con qué frecuencia se realiza revisiones de las directrices de seguridad?
7. ¿Se realiza análisis de vulnerabilidades del sistema financiero?
8. ¿Qué acciones preventivas y correctivas tiene implementada para garantizar la confidencialidad y la integridad de la información que se gestionan dentro del DTI?
9. ¿Existe un plan de respuesta a incidentes en caso de que se detecte una violación de seguridad de información en el sistema financiero?
10. ¿En la actualidad la organización cuenta con procesos y políticas debidamente establecidos y documentados? Si es así, ¿quién o quiénes son los responsables de su aprobación?
11. ¿Cuáles son las personas encargadas de diferentes áreas del departamento?

Anexo 2: Encuesta para la valoración de los activos

Encuesta al Directo del departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda, sobre la de valoración de los activos del sistema financiero.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN SOFTWARE

Encuesta sobre la concientización de gestión de riesgo

La siguiente encuesta tiene el objetivo de conocer el nivel de riesgo existente para el Sistema Financiero del departamento de tecnología de información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda, le pido de manera cordialmente que comparta la información solicitada en las siguientes preguntas, lo cual se realizaran en base a la siguiente escala de valoraciones y de preguntas.

Nivel	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

Dimensión de valoración	Preguntas
Confidencialidad	¿Cómo afectaría al departamento de tecnología de información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda que los datos que se obtiene en el sistema financiero fueran conocido por usuarios no autorizados? ¿El acceso no autorizado a la información puede perjudicar la imagen de la organización? ¿La divulgación no autorizada podría revelar datos sensibles de la

	empresa críticos para las decisiones criticas para la estrategia y financiera?
Integridad	¿Qué impacto tendría para el departamento de tecnología de información que los datos del sistema financiero si fueran falsos, alterados o estuvieran incompletos? ¿Si la información que se maneja por medio del sistema financiero es alterada sin autorización puede perjudicar la imagen de la identidad? ¿Si la información que se maneja por medio del sistema financiero es alterada sin autorización puede provocar sanciones de entes de control?

Activos relacionados al sistema financiero.

Tipo de activos	Activo	Código	C	I
Datos/Información	Base de datos	D-01		
	Documentación interna	D-02		
Servicios	Servidor NAS	S-01		
	Electricidad	S-02		
	Internet	S-03		
	Telefonía	S-04		
	Mantenimiento	S-05		
	Correo	S-06		
Software	Desarrollo a media	SW-01		
	Antivirus	SW-02		
	Firewall	SW-03		
	Licencias	SW-04		
	Sistemas operativos	SW-05		
Hardware	Laptop	HW-01		
	Monitor	HW-02		
	HPE Smart Buy	HW-03		
	Impresora	HW-04		
	Router Board Microtik 3011	HW-05		
	Switch 24 puertos Cat. 5E	HW-06		
	Unifi Uap-ac-lite	HW-07		
Redes de comunicación	red internet	COM-01		
	red LAN	COM-02		
	telefonía móvil	COM-03		
Soportes de información	Electrónicos (one drive de office)	MEDIA-01		
	Rack Jupiter	AUX-01		
	Bandejas porta Equipos	AUX-02		
	Multitomas de energía	AUX-03		

Equipamiento auxiliar	Organizadores horizontales con canaleta ranurada	AUX-04
	Cable de energía	AUX-05
	Cable de red-Patch Cord	AUX-06
	Ups	AUX-07
Instalaciones	Cuarto de atención	L-01
	Cuarto de soporte	L-02
Personal	Personal administrativo de DTI	P-01

Anexo 3: Identificación de amenazas del sistema financiero y los demás activos

Activo	Amenaza
Datos/Información	
Base de datos	[E.15] Alteración de la información
Base de datos	[E.19] Fugas de información
Base de datos	[A.5] Suplantación de la identidad
Base de datos	[A.6] Abuso de privilegios de acceso
Base de datos	[A.11] Acceso no autorizado
Documentación interna	[E.15] Alteración de la información
Documentación interna	[E.19] Fugas de información
Documentación interna	[A.5] Suplantación de la identidad
Documentación interna	[A.6] Abuso de privilegios de acceso
Documentación interna	[A.11] Acceso no autorizado
Servicios	
Servidor NAS	[E.1] Errores de los usuarios
Servidor NAS	[E.2] Errores del administrador del sistema / de la seguridad
Servidor NAS	[E.15] Alteración de la información
Servidor NAS	[E.19] Fugas de información
Servidor NAS	[A.5] Suplantación de la identidad
Servidor NAS	[A.6] Abuso de privilegios de acceso
Servidor NAS	[A.7] Uso no previsto
Servidor NAS	[A.11] Acceso no autorizado
Servidor NAS	[A.15] Modificación de la información
Electricidad	[E.1] Errores de los usuarios
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad
Electricidad	[E.15] Alteración de la información
Electricidad	[E.19] Fugas de información
Electricidad	[A.5] Suplantación de la identidad
Electricidad	[A.6] Abuso de privilegios de acceso
Electricidad	[A.7] Uso no previsto
Electricidad	[A.11] Acceso no autorizado

Electricidad	[A.15] Modificación de la información
Internet	[E.1] Errores de los usuarios
Internet	[E.2] Errores del administrador del sistema / de la seguridad
Internet	[E.15] Alteración de la información
Internet	[E.19] Fugas de información
Internet	[A.5] Suplantación de la identidad
Internet	[A.6] Abuso de privilegios de acceso
Internet	[A.7] Uso no previsto
Internet	[A.11] Acceso no autorizado
Internet	[A.15] Modificación de la información
Telefonía	[E.1] Errores de los usuarios
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad
Telefonía	[E.15] Alteración de la información
Telefonía	[E.19] Fugas de información
Telefonía	[A.5] Suplantación de la identidad
Telefonía	[A.6] Abuso de privilegios de acceso
Telefonía	[A.7] Uso no previsto
Telefonía	[A.11] Acceso no autorizado
Telefonía	[A.15] Modificación de la información
Mantenimiento	[E.1] Errores de los usuarios
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad
Mantenimiento	[E.15] Alteración de la información
Mantenimiento	[E.19] Fugas de información
Mantenimiento	[A.5] Suplantación de la identidad
Mantenimiento	[A.6] Abuso de privilegios de acceso
Mantenimiento	[A.7] Uso no previsto
Mantenimiento	[A.11] Acceso no autorizado
Mantenimiento	[A.15] Modificación de la información
Correo	[E.1] Errores de los usuarios
Correo	[E.2] Errores del administrador del sistema / de la seguridad
Correo	[E.15] Alteración de la información
Correo	[E.19] Fugas de información
Correo	[A.5] Suplantación de la identidad
Correo	[A.6] Abuso de privilegios de acceso
Correo	[A.7] Uso no previsto
Correo	[A.11] Acceso no autorizado
Correo	[A.15] Modificación de la información
	Software
Desarrollo a media-Sistema	[E.8] Difusión de software dañino

Financiero	
Desarrollo a media-Sistema Financiero	[E.20] Vulnerabilidades de los programas (software)
Desarrollo a media-Sistema Financiero	[E.21] Errores de mantenimiento / actualización de programas (software)
Desarrollo a media-Sistema Financiero	[A.8] Difusión de software dañino
Desarrollo a media-Sistema Financiero	[A.22] Manipulación de programas
Antivirus	[E.8] Difusión de software dañino
Antivirus	[E.20] Vulnerabilidades de los programas (software)
Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software)
Antivirus	[A.8] Difusión de software dañino
Antivirus	[A.22] Manipulación de programas
Firewall	[E.8] Difusión de software dañino
Firewall	[E.20] Vulnerabilidades de los programas (software)
Firewall	[E.21] Errores de mantenimiento / actualización de programas (software)
Firewall	[A.8] Difusión de software dañino
Firewall	[A.22] Manipulación de programas
Licencias	[E.8] Difusión de software dañino
Licencias	[E.20] Vulnerabilidades de los programas (software)
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)
Licencias	[A.8] Difusión de software dañino
Licencias	[A.22] Manipulación de programas
Sistemas operativos	[E.8] Difusión de software dañino
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)
Sistemas operativos	[A.8] Difusión de software dañino
Sistemas operativos	[A.22] Manipulación de programas
	Hardware
Computadora	[I.11] Emanaciones electromagnéticas (TEMPEST)
Computadora	[E.25] Pérdida de equipos
Computadora	[A.7] Uso no previsto
Computadora	[A.11] Acceso no autorizado
Computadora	[A.23] Manipulación del hardware
Computadora	[A.25] Robo de equipos
Monitor	[I.11] Emanaciones electromagnéticas (TEMPEST)
Monitor	[E.25] Pérdida de equipos
Monitor	[A.7] Uso no previsto
Monitor	[A.11] Acceso no autorizado

Monitor	[A.23] Manipulación del hardware
Monitor	[A.25] Robo de equipos
HPE Smart Buy	[I.11] Emanaciones electromagnéticas (TEMPEST)
HPE Smart Buy	[E.25] Pérdida de equipos
HPE Smart Buy	[A.7] Uso no previsto
HPE Smart Buy	[A.11] Acceso no autorizado
HPE Smart Buy	[A.23] Manipulación del hardware
HPE Smart Buy	[A.25] Robo de equipos
Impresora	[I.11] Emanaciones electromagnéticas (TEMPEST)
Impresora	[E.25] Pérdida de equipos
Impresora	[A.7] Uso no previsto
Impresora	[A.11] Acceso no autorizado
Impresora	[A.23] Manipulación del hardware
Impresora	[A.25] Robo de equipos
Router Board Microtik 3011	[I.11] Emanaciones electromagnéticas (TEMPEST)
Router Board Microtik 3011	[E.25] Pérdida de equipos
Router Board Microtik 3011	[A.7] Uso no previsto
Router Board Microtik 3011	[A.11] Acceso no autorizado
Router Board Microtik 3011	[A.23] Manipulación del hardware
Router Board Microtik 3011	[A.25] Robo de equipos
Switch 24 puertos Cat. 5E	[I.11] Emanaciones electromagnéticas (TEMPEST)
Switch 24 puertos Cat. 5E	[E.25] Pérdida de equipos
Switch 24 puertos Cat. 5E	[A.7] Uso no previsto
Switch 24 puertos Cat. 5E	[A.11] Acceso no autorizado
Switch 24 puertos Cat. 5E	[A.23] Manipulación del hardware
Switch 24 puertos Cat. 5E	[A.25] Robo de equipos
Unifi Uap-ac-lite	[I.11] Emanaciones electromagnéticas (TEMPEST)
Unifi Uap-ac-lite	[E.25] Pérdida de equipos
Unifi Uap-ac-lite	[A.7] Uso no previsto
Unifi Uap-ac-lite	[A.11] Acceso no autorizado
Unifi Uap-ac-lite	[A.23] Manipulación del hardware
Unifi Uap-ac-lite	[A.25] Robo de equipos
Redes de comunicación	
Red internet	[E.2] Errores del administrador del sistema / de la seguridad
Red internet	[E.9] Errores de [re-]encaminamiento
Red internet	[E.10] Errores de secuencia
Red internet	[E.15] Alteración de la información
Red internet	[E.19] Fugas de información
Red internet	[A.5] Suplantación de la identidad
Red internet	[A.7] Uso no previsto
Red internet	[A.9] [Re-]encaminamiento de mensajes

Red internet	[A.10] Alteración de secuencia
Red internet	[A.11] Acceso no autorizado
Red internet	[A.12] Análisis de tráfico
Red internet	[A.14] Interceptación de información (escucha)
Red internet	[A.15] Modificación de la información
Red LAN	[E.2] Errores del administrador del sistema / de la seguridad
Red LAN	[E.9] Errores de [re-]encaminamiento
Red LAN	[E.10] Errores de secuencia
Red LAN	[E.15] Alteración de la información
Red LAN	[E.19] Fugas de información
Red LAN	[A.5] Suplantación de la identidad
Red LAN	[A.7] Uso no previsto
Red LAN	[A.9] [Re-]encaminamiento de mensajes
Red LAN	[A.10] Alteración de secuencia
Red LAN	[A.11] Acceso no autorizado
Red LAN	[A.12] Análisis de tráfico
Red LAN	[A.14] Interceptación de información (escucha)
Red LAN	[A.15] Modificación de la información
Telefonía móvil	[E.2] Errores del administrador del sistema / de la seguridad
Telefonía móvil	[E.9] Errores de [re-]encaminamiento
Telefonía móvil	[E.10] Errores de secuencia
Telefonía móvil	[E.15] Alteración de la información
Telefonía móvil	[E.19] Fugas de información
Telefonía móvil	[A.5] Suplantación de la identidad
Telefonía móvil	[A.7] Uso no previsto
Telefonía móvil	[A.9] [Re-]encaminamiento de mensajes
Telefonía móvil	[A.10] Alteración de secuencia
Telefonía móvil	[A.11] Acceso no autorizado
Telefonía móvil	[A.12] Análisis de tráfico
Telefonía móvil	[A.14] Interceptación de información (escucha)
Telefonía móvil	[A.15] Modificación de la información
Soportes de información	
Electrónicos (one drive de office)	[I.11] Emanaciones electromagnéticas (TEMPEST)
Electrónicos (one drive de office)	[E.1] Errores de los usuarios
Electrónicos (one drive de office)	[E.15] Alteración de la información
Electrónicos (one drive de office)	[E.19] Fugas de información
Electrónicos (one drive de office)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Electrónicos (one drive de office)	[E.25] Pérdida de equipos
Electrónicos (one drive de office)	[A.7] Uso no previsto

Electrónicos (one drive de office)	[A.11] Acceso no autorizado
Electrónicos (one drive de office)	[A.15] Modificación de la información
Electrónicos (one drive de office)	[A.23] Manipulación del hardware
Electrónicos (one drive de office)	[A.25] Robo de equipos
Elementos Auxiliares	
Rack Jupiter	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Rack Jupiter	[A.7] Uso no previsto
Rack Jupiter	[A.23] Manipulación del hardware
Bandejas porta equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Bandejas porta equipos	[A.7] Uso no previsto
Bandejas porta equipos	[A.23] Manipulación del hardware
Multitomas de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)
Multitomas de energía	[A.7] Uso no previsto
Multitomas de energía	[A.11] Acceso no autorizado
Multitomas de energía	[A.23] Manipulación del hardware
Organizadores horizontales con canaleta ranurada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Organizadores horizontales con canaleta ranurada	[A.7] Uso no previsto
Organizadores horizontales con canaleta ranurada	[A.23] Manipulación del hardware
Cables de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)
Cables de energía	[A.7] Uso no previsto
Cables de energía	[A.11] Acceso no autorizado
Cables de energía	[A.23] Manipulación del hardware
Patch Cord	[A.7] Uso no previsto
Patch Cord	[A.23] Manipulación del hardware
Ups	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Ups	[A.7] Uso no previsto
Ups	[A.23] Manipulación del hardware
Ups	[A.25] Robo de equipos
Ups	[A.26] Ataque destructivo
Instalaciones	
Cuarto de atención	[E.25] Pérdida de equipos
Cuarto de atención	[A.25] Robo de equipos
Cuarto de soporte	[E.25] Pérdida de equipos
Cuarto de soporte	[A.25] Robo de equipos
Personal	
Personal administrativo de DTI	[E.15] Alteración de la información
Personal administrativo de DTI	[E.19] Fugas de información

Personal administrativo de DTI	[A.15] Modificación de la información
Personal administrativo de DTI	[A.19] Revelación de información
Personal administrativo de DTI	[A.29] Extorsión
Personal administrativo de DTI	[A.30] Ingeniería social (picaresca)

Anexo 4: Valoración de amenazas entre activos del sistema financiero

Activo	Amenaza	F	I	C
	Datos/Información			
Base de datos	[E.15] Alteración de la información	1	1%	
Base de datos	[E.19] Fugas de información	1		10%
Base de datos	[A.5] Suplantación de la identidad	10	10%	50%
Base de datos	[A.6] Abuso de privilegios de acceso	10	10%	50%
Base de datos	[A.11] Acceso no autorizado	100	10%	50%
Documentación interna	[E.15] Alteración de la información	1	1%	
Documentación interna	[E.19] Fugas de información	1		10%
Documentación interna	[A.5] Suplantación de la identidad	10	10%	50%
Documentación interna	[A.6] Abuso de privilegios de acceso	10	10%	50%
Documentación interna	[A.11] Acceso no autorizado	100	10%	50%
	Servicios			
Servidor NAS	[E.1] Errores de los usuarios	1	10%	10%
Servidor NAS	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Servidor NAS	[E.15] Alteración de la información	1	1%	
Servidor NAS	[E.19] Fugas de información	1		10%
Servidor NAS	[A.5] Suplantación de la identidad	1	50%	50%
Servidor NAS	[A.6] Abuso de privilegios de acceso	1	10%	10%
Servidor NAS	[A.7] Uso no previsto	1	10%	10%
Servidor NAS	[A.11] Acceso no autorizado	1	10%	50%
Servidor NAS	[A.15] Modificación de la información	10	50%	
Electricidad	[E.1] Errores de los usuarios	1	10%	10%
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Electricidad	[E.15] Alteración de la información	1	1%	
Electricidad	[E.19] Fugas de información	1		10%
Electricidad	[A.5] Suplantación de la identidad	1	50%	50%
Electricidad	[A.6] Abuso de privilegios de acceso	1	10%	10%
Electricidad	[A.7] Uso no previsto	1	10%	10%
Electricidad	[A.11] Acceso no autorizado	1	10%	50%
Electricidad	[A.15] Modificación de la información	10	50%	
Internet	[E.1] Errores de los usuarios	1	10%	10%
Internet	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%

Internet	[E.15] Alteración de la información	1	1%	
Internet	[E.19] Fugas de información	1		10%
Internet	[A.5] Suplantación de la identidad	1	50%	50%
Internet	[A.6] Abuso de privilegios de acceso	1	10%	10%
Internet	[A.7] Uso no previsto	1	10%	10%
Internet	[A.11] Acceso no autorizado	1	10%	50%
Internet	[A.15] Modificación de la información	10	50%	
Telefonía	[E.1] Errores de los usuarios	1	10%	10%
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Telefonía	[E.15] Alteración de la información	1	1%	
Telefonía	[E.19] Fugas de información	1		10%
Telefonía	[A.5] Suplantación de la identidad	1	50%	50%
Telefonía	[A.6] Abuso de privilegios de acceso	1	10%	10%
Telefonía	[A.7] Uso no previsto	1	10%	10%
Telefonía	[A.11] Acceso no autorizado	1	10%	50%
Telefonía	[A.15] Modificación de la información	10	50%	
Mantenimiento	[E.1] Errores de los usuarios	1	10%	10%
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Mantenimiento	[E.15] Alteración de la información	1	1%	
Mantenimiento	[E.19] Fugas de información	1		10%
Mantenimiento	[A.5] Suplantación de la identidad	1	50%	50%
Mantenimiento	[A.6] Abuso de privilegios de acceso	1	10%	10%
Mantenimiento	[A.7] Uso no previsto	1	10%	10%
Mantenimiento	[A.11] Acceso no autorizado	1	10%	50%
Mantenimiento	[A.15] Modificación de la información	10	50%	
Correo	[E.1] Errores de los usuarios	1	10%	10%
Correo	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Correo	[E.15] Alteración de la información	1	1%	
Correo	[E.19] Fugas de información	1		10%
Correo	[A.5] Suplantación de la identidad	1	50%	50%
Correo	[A.6] Abuso de privilegios de acceso	1	10%	10%
Correo	[A.7] Uso no previsto	1	10%	10%
Correo	[A.11] Acceso no autorizado	1	10%	50%
Correo	[A.15] Modificación de la información	10	50%	
	Software			
Desarrollo a media-Sistema Financiero	[E.8] Difusión de software dañino	1	10%	10%
Desarrollo a media-Sistema Financiero	[E.20] Vulnerabilidades de los programas (software)	1	20%	20%
Desarrollo a media-	[E.21] Errores de mantenimiento / actualización	10	10%	50%

Sistema Financiero	de programas (software)			
Desarrollo a media-Sistema Financiero	[A.8] Difusión de software dañino	1	100%	100%
Desarrollo a media-Sistema Financiero	[A.22] Manipulación de programas	1	100%	100%
Antivirus	[E.8] Difusión de software dañino	1	10%	10%
Antivirus	[E.20] Vulnerabilidades de los programas (software)	1	20%	20%
Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software)	10	10%	50%
Antivirus	[A.8] Difusión de software dañino	1	100%	100%
Antivirus	[A.22] Manipulación de programas	1	100%	100%
Firewall	[E.8] Difusión de software dañino	1	10%	10%
Firewall	[E.20] Vulnerabilidades de los programas (software)	1	20%	20%
Firewall	[E.21] Errores de mantenimiento / actualización de programas (software)	10	10%	50%
Firewall	[A.8] Difusión de software dañino	1	100%	100%
Firewall	[A.22] Manipulación de programas	1	100%	100%
Licencias	[E.8] Difusión de software dañino	1	10%	10%
Licencias	[E.20] Vulnerabilidades de los programas (software)	1	20%	20%
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	10	10%	50%
Licencias	[A.8] Difusión de software dañino	1	100%	100%
Licencias	[A.22] Manipulación de programas	1	100%	100%
Sistemas operativos	[E.8] Difusión de software dañino	1	10%	10%
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	1	20%	20%
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	10	10%	50%
Sistemas operativos	[A.8] Difusión de software dañino	1	100%	100%
Sistemas operativos	[A.22] Manipulación de programas	1	100%	100%
	Hardware			
Computadora	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Computadora	[E.25] Pérdida de equipos	1		100%
Computadora	[A.7] Uso no previsto	1	1%	10%
Computadora	[A.11] Acceso no autorizado	1	10%	50%
Computadora	[A.23] Manipulación del hardware	0,5		50%
Computadora	[A.25] Robo de equipos	0,5		100%
Monitor	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Monitor	[E.25] Pérdida de equipos	1		100%
Monitor	[A.7] Uso no previsto	1	1%	10%

Monitor	[A.11] Acceso no autorizado	1	10%	50%
Monitor	[A.23] Manipulación del hardware	0,5		50%
Monitor	[A.25] Robo de equipos	0,5		100%
HPE Smart Buy	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
HPE Smart Buy	[E.25] Pérdida de equipos	1		50%
HPE Smart Buy	[A.11] Acceso no autorizado	1	10%	50%
HPE Smart Buy	[A.23] Manipulación del hardware	0,5		50%
HPE Smart Buy	[A.25] Robo de equipos	0,5		50%
Impresora	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Impresora	[E.25] Pérdida de equipos	1		50%
Impresora	[A.11] Acceso no autorizado	1	10%	50%
Impresora	[A.23] Manipulación del hardware	0,5		50%
Impresora	[A.25] Robo de equipos	0,5		50%
Router Board Microtik 3011	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Router Board Microtik 3012	[E.25] Pérdida de equipos	1		50%
Router Board Microtik 3013	[A.7] Uso no previsto	1		10%
Router Board Microtik 3014	[A.11] Acceso no autorizado	1	10%	50%
Router Board Microtik 3015	[A.23] Manipulación del hardware	0,5		50%
Router Board Microtik 3016	[A.25] Robo de equipos	0,5		50%
Switch 24 puertos Cat. 5E	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Switch 24 puertos Cat. 5E	[E.25] Pérdida de equipos	1		50%
Switch 24 puertos Cat. 5E	[A.7] Uso no previsto	1		10%
Switch 24 puertos Cat. 5E	[A.11] Acceso no autorizado	1	10%	50%
Switch 24 puertos Cat. 5E	[A.23] Manipulación del hardware	0,5		50%
Switch 24 puertos Cat. 5E	[A.25] Robo de equipos	0,5		50%
Unifi Uap-ac-lite	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Unifi Uap-ac-lite	[E.25] Pérdida de equipos	1		50%
Unifi Uap-ac-lite	[A.7] Uso no previsto	1		10%
Unifi Uap-ac-lite	[A.11] Acceso no autorizado	1	10%	50%
Unifi Uap-ac-lite	[A.23] Manipulación del hardware	0,5		50%
Unifi Uap-ac-lite	[A.25] Robo de equipos	0,5		50%
Redes de comunicación				
Red internet	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Red internet	[E.9] Errores de [re-]encaminamiento	1		10%

Red internet	[E.10] Errores de secuencia	1	10%	
Red internet	[E.15] Alteración de la información	1	1%	
Red internet	[E.19] Fugas de información	1		10%
Red internet	[A.5] Suplantación de la identidad	1	10%	50%
Red internet	[A.7] Uso no previsto	1	10%	10%
Red internet	[A.9] [Re-]encaminamiento de mensajes	1		10%
Red internet	[A.10] Alteración de secuencia	1	10%	
Red internet	[A.11] Acceso no autorizado	1	10%	50%
Red internet	[A.12] Análisis de tráfico	1		2%
Red internet	[A.14] Interceptación de información (escucha)	1		10%
Red internet	[A.15] Modificación de la información	1	10%	
Red LAN	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Red LAN	[E.9] Errores de [re-]encaminamiento	1		10%
Red LAN	[E.10] Errores de secuencia	1	10%	
Red LAN	[E.15] Alteración de la información	1	1%	
Red LAN	[E.19] Fugas de información	1		10%
Red LAN	[A.5] Suplantación de la identidad	1	10%	50%
Red LAN	[A.7] Uso no previsto	1	10%	10%
Red LAN	[A.9] [Re-]encaminamiento de mensajes	1		10%
Red LAN	[A.10] Alteración de secuencia	1	10%	
Red LAN	[A.11] Acceso no autorizado	1	10%	50%
Red LAN	[A.12] Análisis de tráfico	1		2%
Red LAN	[A.14] Interceptación de información (escucha)	1		1%
Red LAN	[A.15] Modificación de la información	1	10%	
Telefonía móvil	[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%
Telefonía móvil	[E.9] Errores de [re-]encaminamiento	1		10%
Telefonía móvil	[E.10] Errores de secuencia	1	10%	
Telefonía móvil	[E.15] Alteración de la información	1	1%	
Telefonía móvil	[E.19] Fugas de información	1		10%
Telefonía móvil	[A.5] Suplantación de la identidad	1	10%	50%
Telefonía móvil	[A.7] Uso no previsto	1	10%	10%
Telefonía móvil	[A.9] [Re-]encaminamiento de mensajes	1		10%
Telefonía móvil	[A.10] Alteración de secuencia	1	10%	
Telefonía móvil	[A.11] Acceso no autorizado	1	10%	50%
Telefonía móvil	[A.12] Análisis de tráfico	1		2%
Telefonía móvil	[A.14] Interceptación de información (escucha)	1		10%
Telefonía móvil	[A.15] Modificación de la información	1	10%	
Soportes de información				
Electrónicos (one drive de office)	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%

Electrónicos (one drive de office)	[E.1] Errores de los usuarios	1	5%	10%
Electrónicos (one drive de office)	[E.15] Alteración de la información	1	1%	
Electrónicos (one drive de office)	[E.19] Fugas de información	1		10%
Electrónicos (one drive de office)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	50%
Electrónicos (one drive de office)	[E.25] Pérdida de equipos	1		50%
Electrónicos (one drive de office)	[A.7] Uso no previsto	1		1%
Electrónicos (one drive de office)	[A.11] Acceso no autorizado	1	1%	50%
Electrónicos (one drive de office)	[A.15] Modificación de la información	5	100%	
Electrónicos (one drive de office)	[A.23] Manipulación del hardware	0,1		50%
Electrónicos (one drive de office)	[A.25] Robo de equipos	1		100%
	Elementos Auxiliares			
Rack Jupiter	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1		50%
Rack Jupiter	[A.7] Uso no previsto	1		1%
Rack Jupiter	[A.23] Manipulación del hardware	1		50%
Bandejas porta equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1		50%
Bandejas porta equipos	[A.7] Uso no previsto	1		1%
Bandejas porta equipos	[A.23] Manipulación del hardware	1		50%
Multitomas de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Multitomas de energía	[A.7] Uso no previsto	1	1%	1%
Multitomas de energía	[A.11] Acceso no autorizado	1	10%	50%
Multitomas de energía	[A.23] Manipulación del hardware	1		50%
Organizadores horizontales con canaleta ranurada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1		50%
Organizadores horizontales con canaleta ranurada	[A.7] Uso no previsto	1		1%
Organizadores horizontales con canaleta ranurada	[A.23] Manipulación del hardware	1		50%
Cables de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)	1		1%
Cables de energía	[A.7] Uso no previsto	1	1%	1%
Cables de energía	[A.11] Acceso no autorizado	1	10%	50%
Cables de energía	[A.23] Manipulación del hardware	1		50%

Patch Cord	[A.7] Uso no previsto	1	1%	1%
Patch Cord	[A.23] Manipulación del hardware	1		50%
Ups	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1		
Ups	[A.7] Uso no previsto	1	1%	1%
Ups	[A.23] Manipulación del hardware	1		50%
Ups	[A.25] Robo de equipos	0,5		
Ups	[A.26] Ataque destructivo	1		
	Instalaciones			
Cuarto de atención	[E.25] Pérdida de equipos	10		10%
Cuarto de atención	[A.25] Robo de equipos	10		100%
Cuarto de soporte	[E.25] Pérdida de equipos	10		10%
Cuarto de soporte	[A.25] Robo de equipos	10		100%
	Personal			
Personal administrativo de DTI	[E.15] Alteración de la información	1	10%	
Personal administrativo de DTI	[E.19] Fugas de información	1		10%
Personal administrativo de DTI	[A.15] Modificación de la información	1	50%	
Personal administrativo de DTI	[A.19] Revelación de información	10		50%
Personal administrativo de DTI	[A.29] Extorsión	0,9	100%	100%
Personal administrativo de DTI	[A.30] Ingeniería social (picaresca)	0,5	100%	100%

Anexo 5: Impacto potencial acumulado de afectación de activos del sistema financiero

	Impacto potencial acumulado		Peso ponderado
Activos-Amenazas	**I**	**C**	
Datos/Información	7	9	8
Base de datos	7	9	8
[E.15] Alteración de la información	4		4
[E.19] Fugas de información		7	7
[A.5] Suplantación de la identidad	7	9	8
[A.6] Abuso de privilegios de acceso	7	9	8
[A.11] Acceso no autorizado	7	9	8
Documentación interna	6	7	6,5
[E.15] Alteración de la información	3		3
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	6	7	6,5
[A.6] Abuso de privilegios de acceso	6	7	6,5
[A.11] Acceso no autorizado	6	7	6,5

Servicios	7	9	8
Servidor NAS	7	9	8
[E.1] Errores de los usuarios	5	7	6
[E.2] Errores del administrador del sistema / de la seguridad	6	8	7
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		7	7
[A.5] Suplantación de la identidad	7	9	8
[A.6] Abuso de privilegios de acceso	5	7	6
[A.7] Uso no previsto	5	7	6
[A.11] Acceso no autorizado	5	9	7
[A.15] Modificación de la información	7		7
Electricidad	6	6	6
[E.1] Errores de los usuarios	4	4	4
[E.2] Errores del administrador del sistema / de la seguridad	5	5	5
[E.15] Alteración de la información	1		1
[E.19] Fugas de información		4	2
[A.5] Suplantación de la identidad	6	6	6
[A.6] Abuso de privilegios de acceso	4	4	4
[A.7] Uso no previsto	4	4	4
[A.11] Acceso no autorizado	4	6	5
[A.15] Modificación de la información	6		1
Internet	7	7	7
[E.1] Errores de los usuarios	5	5	5
[E.2] Errores del administrador del sistema / de la seguridad	6	6	6
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	7	7	7
[A.6] Abuso de privilegios de acceso	5	5	5
[A.7] Uso no previsto	5	5	5
[A.11] Acceso no autorizado	5	7	6
[A.15] Modificación de la información	7		7
Telefonía	6	6	6
[E.1] Errores de los usuarios	4	4	4
[E.2] Errores del administrador del sistema / de la seguridad	5	5	5
[E.15] Alteración de la información	1		1
[E.19] Fugas de información		4	4
[A.5] Suplantación de la identidad	6	6	6
[A.6] Abuso de privilegios de acceso	4	4	4
[A.7] Uso no previsto	4	4	4

[A.11] Acceso no autorizado	4	6	5
[A.15] Modificación de la información	6		6
Mantenimiento	6	6	6
[E.1] Errores de los usuarios	4	4	4
[E.2] Errores del administrador del sistema / de la seguridad	5	5	5
[E.15] Alteración de la información	1		1
[E.19] Fugas de información		4	4
[A.5] Suplantación de la identidad	6	6	6
[A.6] Abuso de privilegios de acceso	4	4	4
[A.7] Uso no previsto	4	4	4
[A.11] Acceso no autorizado	4	6	5
[A.15] Modificación de la información	6		6
Correo	7	7	7
[E.1] Errores de los usuarios	5	5	5
[E.2] Errores del administrador del sistema / de la seguridad	6	6	6
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	7	7	7
[A.6] Abuso de privilegios de acceso	5	5	5
[A.7] Uso no previsto	5	5	5
[A.11] Acceso no autorizado	5	7	6
[A.15] Modificación de la información	7		7
Software	10	10	10
Desarrollo a media-Sistema Financiero	10	10	10
[E.8] Difusión de software dañino	7	7	7
[E.20] Vulnerabilidades de los programas (software)	8	8	8
[E.21] Errores de mantenimiento / actualización de programas (software)	7	9	8
[A.8] Difusión de software dañino	10	10	10
[A.22] Manipulación de programas	10	10	10
Antivirus	7	7	7
[E.8] Difusión de software dañino	4	4	4
[E.20] Vulnerabilidades de los programas (software)	5	5	5
[E.21] Errores de mantenimiento / actualización de programas (software)	4	6	5
[A.8] Difusión de software dañino	7	7	7
[A.22] Manipulación de programas	7	7	7
Firewall	7	8	7,5
[E.8] Difusión de software dañino	4	5	4,5

[E.20] Vulnerabilidades de los programas (software)	5	6	5,5
[E.21] Errores de mantenimiento / actualización de programas (software)	4	7	5,5
[A.8] Difusión de software dañino	7	8	7,5
[A.22] Manipulación de programas	7	8	7,5
Licencias	8	6	7
[E.8] Difusión de software dañino	5	3	4
[E.20] Vulnerabilidades de los programas (software)	6	4	5
[E.21] Errores de mantenimiento / actualización de programas (software)	5	5	5
[A.8] Difusión de software dañino	8	6	7
[A.22] Manipulación de programas	8	6	7
Sistemas operativos	8	8	8
[E.8] Difusión de software dañino	5	5	5
[E.20] Vulnerabilidades de los programas (software)	6	6	6
[E.21] Errores de mantenimiento / actualización de programas (software)	5	7	6
[A.8] Difusión de software dañino	8	8	8
[A.22] Manipulación de programas	8	8	8
Hardware	7	9	8
Computadora	5	8	6,5
[I.11] Emanaciones electromagnéticas (TEMPEST)		2	2
[E.25] Pérdida de equipos		8	8
[A.7] Uso no previsto	2	5	3,5
[A.11] Acceso no autorizado	5	7	6
[A.23] Manipulación del hardware		7	7
[A.25] Robo de equipos		8	8
Monitor	4	8	6
[I.11] Emanaciones electromagnéticas (TEMPEST)		2	2
[E.25] Pérdida de equipos		8	8
[A.7] Uso no previsto	1	5	3
[A.11] Acceso no autorizado	4	7	5,5
[A.23] Manipulación del hardware		7	7
[A.25] Robo de equipos		8	8
HPE Smart Buy	7	9	8
[I.11] Emanaciones electromagnéticas (TEMPEST)		4	4
[E.25] Pérdida de equipos		9	9
[A.11] Acceso no autorizado	7	9	8

[A.23] Manipulación del hardware		9	9
[A.25] Robo de equipos		9	9
Impresora	2	4	3
[I.11] Emanaciones electromagnéticas (TEMPEST)		0	0
[E.25] Pérdida de equipos		4	4
[A.11] Acceso no autorizado	2	4	3
[A.23] Manipulación del hardware		4	4
[A.25] Robo de equipos		4	4
Router Board Microtik 3011	5	6	5,5
[I.11] Emanaciones electromagnéticas (TEMPEST)		1	1
[E.25] Pérdida de equipos		6	6
[A.7] Uso no previsto		4	4
[A.11] Acceso no autorizado	5	6	5,5
[A.23] Manipulación del hardware		6	6
[A.25] Robo de equipos		6	6
Switch 24 puertos Cat. 5E	5	6	5,5
[I.11] Emanaciones electromagnéticas (TEMPEST)		1	1
[E.25] Pérdida de equipos		6	6
[A.7] Uso no previsto		4	4
[A.11] Acceso no autorizado	5	6	5,5
[A.23] Manipulación del hardware		6	6
[A.25] Robo de equipos		6	6
Unifi Uap-ac-lite	4	6	5
[I.11] Emanaciones electromagnéticas (TEMPEST)		1	1
[E.25] Pérdida de equipos		6	6
[A.7] Uso no previsto		4	4
[A.11] Acceso no autorizado	4	6	5
[A.23] Manipulación del hardware		6	6
[A.25] Robo de equipos		6	6
Redes de comunicación	6	7	6,5
Red intenet	6	7	6,5
[E.2] Errores del administrador del sistema / de la seguridad	6	6	6
[E.9] Errores de [re-]encaminamiento		5	5
[E.10] Errores de secuencia	5		5
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	5	7	6
[A.7] Uso no previsto	5	5	5

[A.9] [Re-]encaminamiento de mensajes		5	5
[A.10] Alteración de secuencia	5		5
[A.11] Acceso no autorizado	5	7	6
[A.12] Análisis de tráfico		3	3
[A.14] Interceptación de información (escucha)		5	5
[A.15] Modificación de la información	5		5
Red Lan	6	7	6,5
[E.2] Errores del administrador del sistema / de la seguridad	6	6	6
[E.9] Errores de [re-]encaminamiento		5	5
[E.10] Errores de secuencia	5		5
[E.15] Alteración de la información	2		2
[E.19] Fugas de información		5	5
[A.5] Suplantación de la identidad	5	7	6
[A.7] Uso no previsto	5	5	5
[A.9] [Re-]encaminamiento de mensajes		5	5
[A.10] Alteración de secuencia	5		5
[A.11] Acceso no autorizado	5	7	6
[A.12] Análisis de tráfico		3	3
[A.14] Interceptación de información (escucha)		2	2
[A.15] Modificación de la información	5		5
Telefonía móvil	4	6	5
[E.2] Errores del administrador del sistema / de la seguridad	4	5	4,5
[E.9] Errores de [re-]encaminamiento		4	4
[E.10] Errores de secuencia	3		3
[E.15] Alteración de la información	0		0
[E.19] Fugas de información		4	0
[A.5] Suplantación de la identidad	3	6	4,5
[A.7] Uso no previsto	3	4	3,5
[A.9] [Re-]encaminamiento de mensajes		4	4
[A.10] Alteración de secuencia	3		3
[A.11] Acceso no autorizado	3	6	4,5
[A.12] Análisis de tráfico		2	2
[A.14] Interceptación de información (escucha)		4	4
[A.15] Modificación de la información	3		3
Soportes de información	8	7	7,5
Electrónicos (one drive de office)	8	7	7,5
[I.11] Emanaciones electromagnéticas (TEMPEST)		1	1
[E.1] Errores de los usuarios	4	4	4
[E.15] Alteración de la información	2		2

[E.19] Fugas de información		4	4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	6	5,5
[E.25] Pérdida de equipos		6	6
[A.7] Uso no previsto		1	1
[A.11] Acceso no autorizado	2	6	4
[A.15] Modificación de la información	8		8
[A.23] Manipulación del hardware		6	6
[A.25] Robo de equipos		7	7
Elementos Auxiliares	4	6	5
Rack Jupiter		4	4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		4	4
[A.7] Uso no previsto		0	0
[A.23] Manipulación del hardware		4	4
Bandejas porta equipos		4	4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		4	4
[A.7] Uso no previsto		0	0
[A.23] Manipulación del hardware		4	4
Multitoma de energía	2	6	4
[I.11] Emanaciones electromagnéticas (TEMPEST)		1	1
[A.7] Uso no previsto	0	1	1
[A.11] Acceso no autorizado	2	6	4
[A.23] Manipulación del hardware		6	6
Organizadores horizontales con canaleta ranurada		4	4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		4	4
[A.7] Uso no previsto		0	0
[A.23] Manipulación del hardware		4	4
Cables de energía	4	5	4,5
[I.11] Emanaciones electromagnéticas (TEMPEST)		0	0
[A.7] Uso no previsto	1	0	0,5
[A.11] Acceso no autorizado	4	5	4,5
[A.23] Manipulación del hardware		5	5
Patch Cord	2	6	4
[A.7] Uso no previsto	2	1	1,5
[A.23] Manipulación del hardware		6	6
Ups	4	9	6,5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	7		7

[A.7] Uso no previsto	6	5	5,5
[A.23] Manipulación del hardware	5	5	5
[A.25] Robo de equipos	7	7	7
Instalaciones		9	9
Cuarto de atención		9	5
[E.25] Pérdida de equipos		6	6
[A.25] Robo de equipos		9	9
Cuarto de soporte		9	9
[E.25] Pérdida de equipos		6	6
[A.25] Robo de equipos		9	9
Personal	9	9	9
Pesona administrativo de DTI	9	9	9
[E.15] Alteración de la información	6		6
[E.19] Fugas de información		6	6
[A.15] Modificación de la información	8		8
[A.19] Revelación de información		8	8
[A.29] Extorsión	9	9	9
[A.30] Ingeniería social (picaresca)	9	9	9

Anexo 6: Riesgo potencial acumulado de Amenazas

	Riesgo potencial acumulado		Peso ponderado
Activos-Amenazas	**I**	**C**	
Datos/Información	6,8	8,1	7,5
Base de datos	6,8	8,1	7,5
[E.15] Alteración de la información	3,3		3,3
[E.19] Fugas de información		5,1	5,1
[A.5] Suplantación de la identidad	5,9	7,2	6,6
[A.6] Abuso de privilegios de acceso	5,9	7,2	6,6
[A.11] Acceso no autorizado	6,8	8,1	7,5
Documentación interna	6,2	6,9	6,6
[E.15] Alteración de la información	2,7		2,7
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	5,4	6	5,7
[A.6] Abuso de privilegios de acceso	5,4	6	5,7
[A.11] Acceso no autorizado	6,2	6,9	6,6
Servicios	6	6,3	6,2
Servidor NAS	6	6,3	6,2
[E.1] Errores de los usuarios	3,9	5,1	4,5
[E.2] Errores del administrador del sistema / de la seguridad	4,4	5,6	5
[E.15] Alteración de la información	2,1		2,1

[E.19] Fugas de información		5,1	5,1
[A.5] Suplantación de la identidad	5,1	6,3	5,7
[A.6] Abuso de privilegios de acceso	3,9	5,1	4,5
[A.7] Uso no previsto	3,9	5,1	4,5
[A.11] Acceso no autorizado	3,9	6,3	5,1
[A.15] Modificación de la información	6		6
Electricidad	5,4	4,5	5
[E.1] Errores de los usuarios	3,3	3,3	6,6
[E.2] Errores del administrador del sistema / de la seguridad	3,8	3,8	7,6
[E.15] Alteración de la información	1,5		1,5
[E.19] Fugas de información		3,3	3,3
[A.5] Suplantación de la identidad	4,5	4,5	4,5
[A.6] Abuso de privilegios de acceso	3,3	3,3	3,3
[A.7] Uso no previsto	3,3	3,3	3,3
[A.11] Acceso no autorizado	3,3	4,5	3,9
[A.15] Modificación de la información	5,4		5,4
Internet	6	5,1	5,6
[E.1] Errores de los usuarios	3,9	3,9	3,9
[E.2] Errores del administrador del sistema / de la seguridad	4,4	4,4	4,4
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	5,1	5,1	5,1
[A.6] Abuso de privilegios de acceso	3,9	3,9	3,9
[A.7] Uso no previsto	3,9	3,9	3,9
[A.11] Acceso no autorizado	3,9	5,1	4,5
[A.15] Modificación de la información	6		6
Telefonía	5,4	4,5	5
[E.1] Errores de los usuarios	3,3	3,3	3,3
[E.2] Errores del administrador del sistema / de la seguridad	3,8	3,8	3,8
[E.15] Alteración de la información	1,5		1,5
[E.19] Fugas de información		3,3	3,3
[A.5] Suplantación de la identidad	4,5	4,5	4,5
[A.6] Abuso de privilegios de acceso	3,3	3,3	3,3
[A.7] Uso no previsto	3,3	3,3	3,3
[A.11] Acceso no autorizado	3,3	4,5	3,9
[A.15] Modificación de la información	5,4		5,4
Mantenimiento	5,4	4,5	5,0
[E.1] Errores de los usuarios	3,3	3,3	3,3
[E.2] Errores del administrador del sistema / de la seguridad	3,8	3,8	3,8

[E.15] Alteración de la información	1,5		1,5
[E.19] Fugas de información		3,3	3,3
[A.5] Suplantación de la identidad	4,5	4,5	4,5
[A.6] Abuso de privilegios de acceso	3,3	3,3	3,3
[A.7] Uso no previsto	3,3	3,3	3,3
[A.11] Acceso no autorizado	3,3	4,5	3,9
[A.15] Modificación de la información	5,4		5,4
Correo	6	5,1	5,6
[E.1] Errores de los usuarios	3,9	3,9	3,9
[E.2] Errores del administrador del sistema / de la seguridad	4,4	4,4	4,4
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	5,1	5,1	5,1
[A.6] Abuso de privilegios de acceso	3,9	3,9	3,9
[A.7] Uso no previsto	3,9	3,9	3,9
[A.11] Acceso no autorizado	3,9	5,1	4,5
[A.15] Modificación de la información	6		6
Software	6,8	7,2	7
Desarrollo a media-Sistema Financiero	6,8	7,2	7
[E.8] Difusión de software dañino	5,1	5,1	5,1
[E.20] Vulnerabilidades de los programas (software)	5,6	5,6	5,6
[E.21] Errores de mantenimiento / actualización de programas (software)	5,9	7,2	6,6
[A.8] Difusión de software dañino	6,8	6,8	6,8
[A.22] Manipulación de programas	6,8	6,8	6,8
Antivirus	5,1	5,4	5,3
[E.8] Difusión de software dañino	3,3	3,3	3,3
[E.20] Vulnerabilidades de los programas (software)	3,8	3,8	3,8
[E.21] Errores de mantenimiento / actualización de programas (software)	4,2	5,4	4,8
[A.8] Difusión de software dañino	5,1	5,1	5,1
[A.22] Manipulación de programas	5,1	5,1	5,1
Firewall	5,1	6	5,6
[E.8] Difusión de software dañino	3,3	3,9	3,6
[E.20] Vulnerabilidades de los programas (software)	3,8	4,4	4,1
[E.21] Errores de mantenimiento / actualización de programas (software)	4,2	6	5,1
[A.8] Difusión de software dañino	5,1	5,7	5,4
[A.22] Manipulación de programas	5,1	5,7	5,4
Licencias	5,7	4,8	5,3

[E.8] Difusión de software dañino	3,9	2,7	3,3
[E.20] Vulnerabilidades de los programas (software)	4,4	3,2	3,8
[E.21] Errores de mantenimiento / actualización de programas (software)	4,8	4,8	4,8
[A.8] Difusión de software dañino	5,7	4,5	5,1
[A.22] Manipulación de programas	5,7	4,5	5,1
Sistemas operativos	5,7	6	5,9
[E.8] Difusión de software dañino	3,9	3,9	3,9
[E.20] Vulnerabilidades de los programas (software)	4,4	4,4	4,4
[E.21] Errores de mantenimiento / actualización de programas (software)	4,8	6	5,4
[A.8] Difusión de software dañino	5,7	5,7	5,7
[A.22] Manipulación de programas	5,7	5,7	5,7
Hardware	5,1	6,3	5,7
Computadora	3,9	5,7	4,8
[I.11] Emanaciones electromagnéticas (TEMPEST)		2,1	2,1
[E.25] Pérdida de equipos		5,7	5,7
[A.7] Uso no previsto	2,1	3,9	3
[A.11] Acceso no autorizado	3,9	5,1	4,5
[A.23] Manipulación del hardware		4,9	4,9
[A.25] Robo de equipos		5,4	5,4
Monitor	3,3	5,7	4,5
[I.11] Emanaciones electromagnéticas (TEMPEST)		2,1	2,1
[E.25] Pérdida de equipos		5,7	5,7
[A.7] Uso no previsto	1,5	3,9	2,7
[A.11] Acceso no autorizado	3,3	5,1	4,2
[A.23] Manipulación del hardware		4,9	4,9
[A.25] Robo de equipos		5,4	5,4
HPE Smart Buy	5,1	6,3	5,7
[I.11] Emanaciones electromagnéticas (TEMPEST)		3,3	3,3
[E.25] Pérdida de equipos		6,3	6,3
[A.11] Acceso no autorizado	5,1	6,3	5,7
[A.23] Manipulación del hardware		6	6
[A.25] Robo de equipos		6	6
Impresora	2,1	3,4	2,8
[I.11] Emanaciones electromagnéticas (TEMPEST)		0,87	0,9
[E.25] Pérdida de equipos		3,4	3,4
[A.11] Acceso no autorizado	2,1	3,4	2,8

[A.23] Manipulación del hardware		3,1	3,1
[A.25] Robo de equipos		3,1	3,1
Router Board Microtik 3011	3,9	4,5	4,2
[I.11] Emanaciones electromagnéticas (TEMPEST)		1,5	1,5
[E.25] Pérdida de equipos		4,5	4,5
[A.7] Uso no previsto		3,3	3,3
[A.11] Acceso no autorizado	3,9	4,5	4,2
[A.23] Manipulación del hardware		4,3	4,3
[A.25] Robo de equipos		4,3	4,3
Switch 24 puertos Cat. 5E	3,9	4,5	4,2
[I.11] Emanaciones electromagnéticas (TEMPEST)		1,5	1,5
[E.25] Pérdida de equipos		4,5	4,5
[A.7] Uso no previsto		3,3	3,3
[A.11] Acceso no autorizado	3,9	4,5	4,2
[A.23] Manipulación del hardware		4,3	4,3
[A.25] Robo de equipos		4,3	4,3
Unifi Uap-ac-lite	3,3	4,5	3,9
[I.11] Emanaciones electromagnéticas (TEMPEST)		1,5	1,5
[E.25] Pérdida de equipos		4,5	4,5
[A.7] Uso no previsto		3,3	3,3
[A.11] Acceso no autorizado	3,3	4,5	3,9
[A.23] Manipulación del hardware		4,3	4,3
[A.25] Robo de equipos		4,3	4,3
Redes de comunicación	4,4	5,1	4,8
Red intenet	4,4	5,1	4,8
[E.2] Errores del administrador del sistema / de la seguridad	4,4	4,4	4,4
[E.9] Errores de [re-]encaminamiento		3,9	3,9
[E.10] Errores de secuencia	3,9		3,9
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	3,9	5,1	4,5
[A.7] Uso no previsto	3,9	3,9	3,9
[A.9] [Re-]encaminamiento de mensajes		3,9	3,9
[A.10] Alteración de secuencia	3,9		3,9
[A.11] Acceso no autorizado	3,9	5,1	4,5
[A.12] Análisis de tráfico		2,7	2,7
[A.14] Interceptación de información (escucha)		3,9	3,9
[A.15] Modificación de la información	3,9		3,9
Red Lan	4,4	5,1	4,8

[E.2] Errores del administrador del sistema / de la seguridad	4,4	4,4	4,4
[E.9] Errores de [re-]encaminamiento		3,9	3,9
[E.10] Errores de secuencia	3,9		3,9
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		3,9	3,9
[A.5] Suplantación de la identidad	3,9	5,1	4,5
[A.7] Uso no previsto	3,9	3,9	3,9
[A.9] [Re-]encaminamiento de mensajes		3,9	3,9
[A.10] Alteración de secuencia	3,9		3,9
[A.11] Acceso no autorizado	3,9	5,1	4,5
[A.12] Análisis de tráfico		2,7	2,7
[A.14] Interceptación de información (escucha)		2,1	2,1
[A.15] Modificación de la información	3,9		3,9
Telefonía móvil	3,2	4,5	3,9
[E.2] Errores del administrador del sistema / de la seguridad	3,2	3,8	3,5
[E.9] Errores de [re-]encaminamiento		3,3	3,3
[E.10] Errores de secuencia	2,7		2,7
[E.15] Alteración de la información	0,98		1
[E.19] Fugas de información		3,3	3,3
[A.5] Suplantación de la identidad	2,7	4,5	3,6
[A.7] Uso no previsto	2,7	3,3	3,0
[A.9] [Re-]encaminamiento de mensajes		3,3	3,3
[A.10] Alteración de secuencia	2,7		2,7
[A.11] Acceso no autorizado	2,7	4,5	3,6
[A.12] Análisis de tráfico		2,1	2,1
[A.14] Interceptación de información (escucha)		3,3	3,3
[A.15] Modificación de la información	2,7		2,7
Soportes de información	6,3	5,1	5,7
Electrónicos (one drive de office)	6,3	5,1	5,7
[I.11] Emanaciones electromagnéticas (TEMPEST)		1,5	1,5
[E.1] Errores de los usuarios	3,4	3,3	3,4
[E.15] Alteración de la información	2,1		2,1
[E.19] Fugas de información		3,3	3,3
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3,9	4,5	4,2
[E.25] Pérdida de equipos		4,5	4,5
[A.7] Uso no previsto		1,5	1,5
[A.11] Acceso no autorizado	2,1	4,5	3,3
[A.15] Modificación de la información	6,3		6,3
[A.23] Manipulación del hardware		3,7	3,7

[A.25] Robo de equipos		5,1	5,1
Elementos Auxiliares	3,3	4,5	3,9
Rack Jupiter		3,4	3,4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		3,4	3,4
[A.7] Uso no previsto		0,87	0,9
[A.23] Manipulación del hardware		3,4	3,4
Bandejas porta equipos		3,4	3,4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		3,4	3,4
[A.7] Uso no previsto		0,87	0,9
[A.23] Manipulación del hardware		3,4	3,4
Multitoma de energía	2,1	4,5	3,3
[I.11] Emanaciones electromagnéticas (TEMPEST)		1,5	1,5
[A.7] Uso no previsto	0,87	1,5	1,2
[A.11] Acceso no autorizado	2,1	4,5	3,3
[A.23] Manipulación del hardware		4,5	4,5
Organizadores horizontales con canaleta ranurada		3,4	3,4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		3,4	3,4
[A.7] Uso no previsto		0,87	0,9
[A.23] Manipulación del hardware		3,4	3,4
Cables de energía	3,3	3,9	3,6
[I.11] Emanaciones electromagnéticas (TEMPEST)		0,98	1
[A.7] Uso no previsto	1,5	0,98	1,2
[A.11] Acceso no autorizado	3,3	3,9	3,6
[A.23] Manipulación del hardware		3,9	3,9
Patch Cord	2,1	4,5	3,3
[A.7] Uso no previsto	2,1	1,5	1,8
[A.23] Manipulación del hardware		4,5	4,5
Ups			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3,5	6,3	4,9
[A.7] Uso no previsto	1,5	0,98	1,2
[A.23] Manipulación del hardware		3,9	3,9
[A.25] Robo de equipos		5,1	5,1
Instalaciones		7,1	7,1
Cuarto de atención		7,1	7,1
[E.25] Pérdida de equipos		5,4	5,4
[A.25] Robo de equipos		7,1	7,1
Cuarto de soporte		7,1	7,1

[E.25] Pérdida de equipos		5,4	5,4
[A.25] Robo de equipos		7,1	7,1
Personal	6,2	6,6	6,4
Personal administrativo de DTI	6,2	6,6	6,4
[E.15] Alteración de la información	4,5		4,5
[E.19] Fugas de información		4,5	4,5
[A.15] Modificación de la información	5,7		5,7
[A.19] Revelación de información		6,6	6,6
[A.29] Extorsión	6,2	6,2	6,2
[A.30] Ingeniería social (picaresca)	6	6	6

Anexo 7: Asignación de opción de tratamiento a los riesgos identificados

		Peso ponderado	Tratamiento
Activos-Amenazas			
Base de datos	[A.11] Acceso no autorizado	7,5	Reducir
Cuarto de atención	[A.25] Robo de equipos	7,1	Evitar
Cuarto de atención	[A.25] Robo de equipos	7,1	Evitar
Desarrollo a media-Sistema Financiero	[A.8] Difusión de software dañino	6,8	Evitar
Desarrollo a media-Sistema Financiero	[A.22] Manipulación de programas	6,8	Evitar
Personal administrativo de DTI	[A.19] Revelación de información	6,6	Evitar
Base de datos	[A.5] Suplantación de la identidad	6,6	Evitar
Base de datos	[A.6] Abuso de privilegios de acceso	6,6	Evitar
Documentación interna	[A.11] Acceso no autorizado	6,6	Reducir
Desarrollo a media-Sistema Financiero	[E.21] Errores de mantenimiento / actualización de programas (software)	6,6	Reducir
HPE Smart Buy	[E.25] Pérdida de equipos	6,3	Reducir
Electrónicos (one drive de office)	[A.15] Modificación de la información	6,3	Evitar
Personal administrativo de DTI	[A.29] Extorsión	6,2	Evitar
Servidor NAS	[A.15] Modificación de la información	6	Evitar
Internet	[A.15] Modificación de la información	6	Evitar
Correo	[A.15] Modificación de la información	6	Evitar
HPE Smart Buy	[A.23] Manipulación del hardware	6	Evitar
HPE Smart Buy	[A.25] Robo de equipos	6	Evitar

Personal administrativo de DTI	[A.30] Ingeniería social (picaresca)	6	Evitar
Documentación interna	[A.5] Suplantación de la identidad	5,7	Evitar
Documentación interna	[A.6] Abuso de privilegios de acceso	5,7	Evitar
Sistemas operativos	[A.8] Difusión de software dañino	5,7	Evitar
Sistemas operativos	[A.22] Manipulación de programas	5,7	Evitar
Computadora	[E.25] Pérdida de equipos	5,7	Reducir
Monitor	[E.25] Pérdida de equipos	5,7	Reducir
Personal administrativo de DTI	[A.15] Modificación de la información	5,7	Evitar
Servidor NAS	[A.5] Suplantación de la identidad	5,7	Evitar
HPE Smart Buy	[A.11] Acceso no autorizado	5,7	Reducir
Desarrollo a media-Sistema Financiero	[E.20] Vulnerabilidades de los programas (software)	5,6	Reducir
Electricidad	[A.15] Modificación de la información	5,4	Evitar
Telefonía	[A.15] Modificación de la información	5,4	Evitar
Mantenimiento	[A.15] Modificación de la información	5,4	Evitar
Firewall	[A.8] Difusión de software dañino	5,4	Evitar
Firewall	[A.22] Manipulación de programas	5,4	Evitar
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	5,4	Reducir
Computadora	[A.25] Robo de equipos	5,4	Evitar
Monitor	[A.25] Robo de equipos	5,4	Evitar
Cuarto de atención	[E.25] Pérdida de equipos	5,4	Reducir
Cuarto de atención	[E.25] Pérdida de equipos	5,4	Reducir
Base de datos	[E.19] Fugas de información	5,1	Reducir
Servidor NAS	[E.19] Fugas de información	5,1	Reducir
Servidor NAS	[A.11] Acceso no autorizado	5,1	Reducir
Internet	[A.5] Suplantación de la identidad	5,1	Evitar
Correo	[A.5] Suplantación de la identidad	5,1	Evitar
Desarrollo a media-Sistema Financiero	[E.8] Difusión de software dañino	5,1	Reducir
Antivirus	[A.8] Difusión de software dañino	5,1	Evitar
Antivirus	[A.22] Manipulación de	5,1	Evitar

	programas		
Firewall	[E.21] Errores de mantenimiento / actualización de programas (software)	5,1	Reducir
Licencias	[A.8] Difusión de software dañino	5,1	Evitar
Licencias	[A.22] Manipulación de programas	5,1	Evitar
Electrónicos (one drive de office)	[A.25] Robo de equipos	5,1	Evitar
Ups	[A.25] Robo de equipos	5,1	Evitar
Servidor NAS	[E.2] Errores del administrador del sistema / de la seguridad	5	Reducir
Computadora	[A.23] Manipulación del hardware	4,9	Evitar
Monitor	[A.23] Manipulación del hardware	4,9	Evitar
Ups	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4,9	Reducir
Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software)	4,8	Reducir
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	4,8	Reducir
Servidor NAS	[E.1] Errores de los usuarios	4,5	Reducir
Servidor NAS	[A.6] Abuso de privilegios de acceso	4,5	Evitar
Servidor NAS	[A.7] Uso no previsto	4,5	Evitar
Electricidad	[A.5] Suplantación de la identidad	4,5	Evitar
Internet	[A.11] Acceso no autorizado	4,5	Reducir
Telefonía	[A.5] Suplantación de la identidad	4,5	Evitar
Mantenimiento	[A.5] Suplantación de la identidad	4,5	Evitar
Correo	[A.11] Acceso no autorizado	4,5	Reducir
Computadora	[A.11] Acceso no autorizado	4,5	Reducir
Router Board Microtik 3013	[E.25] Pérdida de equipos	4,5	Reducir
Switch 24 puertos Cat. 5E	[E.25] Pérdida de equipos	4,5	Reducir
Unifi Uap-ac-lite	[E.25] Pérdida de equipos	4,5	Reducir
Red intenet	[A.5] Suplantación de la identidad	4,5	Evitar
Red intenet	[A.11] Acceso no autorizado	4,5	Reducir
Red Lan	[A.5] Suplantación de la identidad	4,5	Evitar
Red Lan	[A.11] Acceso no autorizado	4,5	Reducir

Electrónicos (one drive de office)	[E.25] Pérdida de equipos	4,5	Reducir
Multitoma de energía	[A.23] Manipulación del hardware	4,5	Evitar
Patch Cord	[A.23] Manipulación del hardware	4,5	Evitar
Personal administrativo de DTI	[E.15] Alteración de la información	4,5	Reducir
Personal administrativo de DTI	[E.19] Fugas de información	4,5	Reducir
Internet	[E.2] Errores del administrador del sistema / de la seguridad	4,4	Reducir
Correo	[E.2] Errores del administrador del sistema / de la seguridad	4,4	Reducir
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	4,4	Reducir
Red intenet	[E.2] Errores del administrador del sistema / de la seguridad	4,4	Reducir
Red Lan	[E.2] Errores del administrador del sistema / de la seguridad	4,4	Reducir
Router Board Microtik 3016	[A.23] Manipulación del hardware	4,3	Evitar
Router Board Microtik 3017	[A.25] Robo de equipos	4,3	Evitar
Switch 24 puertos Cat. 5E	[A.23] Manipulación del hardware	4,3	Evitar
Switch 24 puertos Cat. 5E	[A.25] Robo de equipos	4,3	Evitar
Unifi Uap-ac-lite	[A.23] Manipulación del hardware	4,3	Evitar
Unifi Uap-ac-lite	[A.25] Robo de equipos	4,3	Evitar
Router Board Microtik 3015	[A.11] Acceso no autorizado	4,2	Reducir
Switch 24 puertos Cat. 5E	[A.11] Acceso no autorizado	4,2	Reducir
Electrónicos (one drive de office)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	4,2	Reducir
Monitor	[A.11] Acceso no autorizado	4,2	Reducir
Firewall	[E.20] Vulnerabilidades de los programas (software)	4,1	Reducir
Documentación interna	[E.19] Fugas de información	3,9	Reducir
Electricidad	[A.11] Acceso no autorizado	3,9	Reducir
Internet	[E.1] Errores de los usuarios	3,9	Reducir
Internet	[E.19] Fugas de información	3,9	Reducir
Internet	[A.6] Abuso de privilegios de acceso	3,9	Evitar
Internet	[A.7] Uso no previsto	3,9	Evitar
Telefonía	[A.11] Acceso no autorizado	3,9	Reducir
Mantenimiento	[A.11] Acceso no autorizado	3,9	Reducir
Correo	[E.1] Errores de los usuarios	3,9	Reducir
Correo	[E.19] Fugas de información	3,9	Reducir

Correo	[A.6] Abuso de privilegios de acceso	3,9	Evitar
Correo	[A.7] Uso no previsto	3,9	Evitar
Sistemas operativos	[E.8] Difusión de software dañino	3,9	Reducir
Unifi Uap-ac-lite	[A.11] Acceso no autorizado	3,9	Reducir
Red intenet	[E.9] Errores de [re-]encaminamiento	3,9	Reducir
Red intenet	[E.10] Errores de secuencia	3,9	Reducir
Red intenet	[E.19] Fugas de información	3,9	Reducir
Red intenet	[A.7] Uso no previsto	3,9	Evitar
Red intenet	[A.9] [Re-]encaminamiento de mensajes	3,9	Reducir
Red intenet	[A.10] Alteración de secuencia	3,9	Evitar
Red intenet	[A.14] Interceptación de información (escucha)	3,9	Evitar
Red intenet	[A.15] Modificación de la información	3,9	Evitar
Red Lan	[E.9] Errores de [re-]encaminamiento	3,9	Reducir
Red Lan	[E.10] Errores de secuencia	3,9	Reducir
Red Lan	[E.19] Fugas de información	3,9	Reducir
Red Lan	[A.7] Uso no previsto	3,9	Evitar
Red Lan	[A.9] [Re-]encaminamiento de mensajes	3,9	Reducir
Red Lan	[A.10] Alteración de secuencia	3,9	Evitar
Red Lan	[A.15] Modificación de la información	3,9	Evitar
Cables de energía	[A.23] Manipulación del hardware	3,9	Evitar
Ups	[A.23] Manipulación del hardware	3,9	Evitar
Licencias	[E.20] Vulnerabilidades de los programas (software)	3,8	Reducir
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	3,8	Reducir
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad	3,8	Reducir
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	3,8	Reducir
Antivirus	[E.20] Vulnerabilidades de los programas (software)	3,8	Reducir
Electrónicos (one drive de office)	[A.23] Manipulación del hardware	3,7	Evitar
Telefonía móvil	[A.5] Suplantación de la identidad	3,6	Evitar
Telefonía móvil	[A.11] Acceso no autorizado	3,6	Reducir

Firewall	[E.8] Difusión de software dañino	3,6	Reducir
Cables de energía	[A.11] Acceso no autorizado	3,6	Reducir
Telefonía móvil	[E.2] Errores del administrador del sistema / de la seguridad	3,5	Reducir
Impresora	[E.25] Pérdida de equipos	3,4	Reducir
Rack Jupiter	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3,4	Reducir
Rack Jupiter	[A.23] Manipulación del hardware	3,4	Evitar
Bandejas porta equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3,4	Reducir
Bandejas porta equipos	[A.23] Manipulación del hardware	3,4	Evitar
Organizadores horizontales con canaleta ranurada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3,4	Reducir
Organizadores horizontales con canaleta ranurada	[A.23] Manipulación del hardware	3,4	Evitar
Electrónicos (one drive de office)	[E.1] Errores de los usuarios	3,4	Reducir
Electricidad	[E.1] Errores de los usuarios	3,3	Reducir
Base de datos	[E.15] Alteración de la información	3,3	Reducir
Electricidad	[E.19] Fugas de información	3,3	Reducir
Electricidad	[A.6] Abuso de privilegios de acceso	3,3	Evitar
Electricidad	[A.7] Uso no previsto	3,3	Evitar
Telefonía	[E.1] Errores de los usuarios	3,3	Reducir
Telefonía	[E.19] Fugas de información	3,3	Reducir
Telefonía	[A.6] Abuso de privilegios de acceso	3,3	Evitar
Telefonía	[A.7] Uso no previsto	3,3	Evitar
Mantenimiento	[E.1] Errores de los usuarios	3,3	Reducir
Mantenimiento	[E.19] Fugas de información	3,3	Reducir
Mantenimiento	[A.6] Abuso de privilegios de acceso	3,3	Evitar
Mantenimiento	[A.7] Uso no previsto	3,3	Evitar
Antivirus	[E.8] Difusión de software dañino	3,3	Reducir
Licencias	[E.8] Difusión de software dañino	3,3	Reducir
HPE Smart Buy	[I.11] Emanaciones electromagnéticas (TEMPEST)	3,3	Reducir
Router Board Microtik 3014	[A.7] Uso no previsto	3,3	Evitar

Switch 24 puertos Cat. 5E	[A.7] Uso no previsto	3,3	Evitar
Unifi Uap-ac-lite	[A.7] Uso no previsto	3,3	Evitar
Telefonía móvil	[E.9] Errores de [re-]encaminamiento	3,3	Reducir
Telefonía móvil	[E.19] Fugas de información	3,3	Reducir
Telefonía móvil	[A.9] [Re-]encaminamiento de mensajes	3,3	Reducir
Telefonía móvil	[A.14] Interceptación de información (escucha)	3,3	Evitar
Electrónicos (one drive de office)	[E.19] Fugas de información	3,3	Reducir
Electrónicos (one drive de office)	[A.11] Acceso no autorizado	3,3	Reducir
Multitoma de energía	[A.11] Acceso no autorizado	3,3	Reducir
Impresora	[A.23] Manipulación del hardware	3,1	Evitar
Impresora	[A.25] Robo de equipos	3,1	Evitar
Computadora	[A.7] Uso no previsto	3	Evitar
Telefonía móvil	[A.7] Uso no previsto	3,0	Evitar
Impresora	[A.11] Acceso no autorizado	2,8	Reducir
Documentación interna	[E.15] Alteración de la información	2,7	Reducir
Monitor	[A.7] Uso no previsto	2,7	Evitar
Red intenet	[A.12] Análisis de tráfico	2,7	Evitar
Red Lan	[A.12] Análisis de tráfico	2,7	Evitar
Telefonía móvil	[E.10] Errores de secuencia	2,7	Reducir
Telefonía móvil	[A.10] Alteración de secuencia	2,7	Evitar
Telefonía móvil	[A.15] Modificación de la información	2,7	Evitar
Servidor NAS	[E.15] Alteración de la información	2,1	Reducir
Internet	[E.15] Alteración de la información	2,1	Reducir
Correo	[E.15] Alteración de la información	2,1	Reducir
Computadora	[I.11] Emanaciones electromagnéticas (TEMPEST)	2,1	Reducir
Monitor	[I.11] Emanaciones electromagnéticas (TEMPEST)	2,1	Reducir
Red intenet	[E.15] Alteración de la información	2,1	Reducir
Red Lan	[E.15] Alteración de la información	2,1	Reducir
Red Lan	[A.14] Interceptación de información (escucha)	2,1	Evitar
Telefonía móvil	[A.12] Análisis de tráfico	2,1	Evitar

Electrónicos (one drive de office)	[E.15] Alteración de la información	2,1	Reducir
Patch Cord	[A.7] Uso no previsto	1,8	Evitar
Electricidad	[E.15] Alteración de la información	1,5	Reducir
Telefonía	[E.15] Alteración de la información	1,5	Reducir
Mantenimiento	[E.15] Alteración de la información	1,5	Reducir
Router Board Microtik 3012	[I.11] Emanaciones electromagnéticas (TEMPEST)	1,5	Reducir
Switch 24 puertos Cat. 5E	[I.11] Emanaciones electromagnéticas (TEMPEST)	1,5	Reducir
Unifi Uap-ac-lite	[I.11] Emanaciones electromagnéticas (TEMPEST)	1,5	Reducir
Electrónicos (one drive de office)	[I.11] Emanaciones electromagnéticas (TEMPEST)	1,5	Reducir
Electrónicos (one drive de office)	[A.7] Uso no previsto	1,5	Evitar
Multitoma de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)	1,5	Reducir
Cables de energía	[A.7] Uso no previsto	1,2	Evitar
Ups	[A.7] Uso no previsto	1,2	Evitar
Multitoma de energía	[A.7] Uso no previsto	1,2	Evitar
Telefonía móvil	[E.15] Alteración de la información	1	Reducir
Cables de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)	1	Reducir
Impresora	[I.11] Emanaciones electromagnéticas (TEMPEST)	0,9	Reducir
Rack Jupiter	[A.7] Uso no previsto	0,9	Evitar
Bandejas porta equipos	[A.7] Uso no previsto	0,9	Evitar
Organizadores horizontales con canaleta ranurada	[A.7] Uso no previsto	0,9	Evitar

Anexo 8: Selección de dominios, objetivos de controles, controles para implementar

Activos	Amenazas	Dominio	Objetivos	Controles
Base de datos	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Cuarto de	[A.25] Robo de	11.Seguridad	11.2 Seguridad	11.2.1Emplazamient

atención	equipos	física y ambiental.	de los equipos.	o y protección de equipo
Cuarto de atención	[A.25] Robo de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Desarrollo a media-Sistema Financiero	[A.8] Difusión de software dañino	12.Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
Desarrollo a media-Sistema Financiero	[A.22] Manipulación de programas	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Personal administrativo de DTI	[A.19] Revelación de información	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Base de datos	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Base de datos	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Documentación interna	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Desarrollo a media-Sistema Financiero	[E.21] Errores de mantenimiento / actualización de programas (software)	12.Seguridad en la operativa.	12.1Responsabilidades y procedimientos de operación.	12.1.2 Gestión de cambios
HPE Smart Buy	[E.25] Pérdida de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1Emplazamiento y protección de equipo
Electrónicos (one drive de office)	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Personal administrativo de DTI	[A.29] Extorsión	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Servidor NAS	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red

Internet	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Correo	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
HPE Smart Buy	[A.23] Manipulación del hardware	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
HPE Smart Buy	[A.25] Robo de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1Emplazamiento y protección de equipo
Personal administrativo de DTI	[A.30] Ingeniería social (picaresca)	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Documentación interna	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Documentación interna	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Sistemas operativos	[A.8] Difusión de software dañino	12.Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
Sistemas operativos	[A.22] Manipulación de programas	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Computadora	[E.25] Pérdida de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Monitor	[E.25] Pérdida de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Personal administrativo de DTI	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Servidor NAS	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
HPE Smart	[A.11] Acceso no	9. Control de	9.1 Requisitos	9.1.1 Política de

Buy	autorizado	accesos.	de negocio para el control de accesos	control de acceso
Desarrollo a media-Sistema Financiero	[E.20] Vulnerabilidades de los programas (software)	12.Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.
Electricidad	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Telefonía	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Mantenimiento	[A.15] Modificación de la información	13.Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Firewall	[A.8] Difusión de software dañino	12.Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
Firewall	[A.22] Manipulación de programas	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Sistemas operativos	[E.21] Errores de mantenimiento / actualización de programas (software)	12.Seguridad en la operativa.	12.1Responsabilidades y procedimientos de operación.	12.1.2 Gestión de cambios
Computadora	[A.25] Robo de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Monitor	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Cuarto de atención	[E.25] Pérdida de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1Emplazamiento y protección de equipo
Cuarto de atención	[E.25] Pérdida de equipos	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Base de datos	[E.19] Fugas de información	13.Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Servidor NAS	[E.19] Fugas de información	13.Seguridad en las telecomunica	13.2 Intercambio de información con partes	13.2.4 Acuerdos de confidencialidad y secreto.

		ciones.	externas.	
Servidor NAS	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Internet	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Correo	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Desarrollo a media-Sistema Financiero	[E.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software
Antivirus	[A.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
Antivirus	[A.22] Manipulación de programas	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Firewall	[E.21] Errores de mantenimiento / actualización de programas (software)	12. Seguridad en la operativa.	12.1 Responsabilidades y procedimientos de operación.	12.1.2 Gestión de cambios
Licencias	[A.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software.
Licencias	[A.22] Manipulación de programas	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Electrónicos (one drive de office)	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Ups	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Servidor NAS	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Computadora	[A.23] Manipulación del hardware	11. Seguridad física y	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.

		ambiental.		
Monitor	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Ups	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11.Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Antivirus	[E.21] Errores de mantenimiento / actualización de programas (software)	12.Seguridad en la operativa.	12.1 Responsabilidades y procedimientos de operación.	12.1.2 Gestión de cambios
Licencias	[E.21] Errores de mantenimiento / actualización de programas (software)	12. Seguridad en la operativa.	12.1 Responsabilidades y procedimientos de operación.	12.1.2 Gestión de cambios
Servidor NAS	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Servidor NAS	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Servidor NAS	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Electricidad	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Internet	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Telefonía	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Mantenimiento	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso

Correo	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Computadora	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Router Board Microtik 3013	[E.25] Pérdida de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Switch 24 puertos Cat. 5E	[E.25] Pérdida de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Unifi Uap-ac-lite	[E.25] Pérdida de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Red internet	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Red internet	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Red Lan	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Red Lan	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Electrónicos (one drive de office)	[E.25] Pérdida de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Multitoma de energía	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Patch Cord	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Personal administrativo	[E.15] Alteración de la información	12. Seguridad en	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la

de DTI		la operativa		información
Personal administrativo de DTI	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Internet	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Correo	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Sistemas operativos	[E.20] Vulnerabilidades de los programas (software)	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.
Red intenet	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Red Lan	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Router Board Microtik 3016	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Router Board Microtik 3017	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Switch 24 puertos Cat. 5E	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Switch 24 puertos Cat. 5E	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Unifi Uap-ac-lite	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Unifi Uap-ac-lite	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo

Router Board Microtik 3015	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Switch 24 puertos Cat. 5E	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Electrónicos (one drive de office)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Monitor	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Firewall	[E.20] Vulnerabilidades de los programas (software)	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.
Documentación interna	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Electricidad	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Internet	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Internet	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Internet	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Internet	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Telefonía	[A.11] Acceso no	9. Control de	9.1 Requisitos	9.1.1 Política de

	autorizado	accesos.	de negocio para el control de accesos	control de acceso
Mantenimiento	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Correo	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Correo	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Correo	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Correo	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Sistemas operativos	[E.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software
Unifi Uap-ac-lite	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Red internet	[E.9] Errores de [re-]encaminamiento	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
Red internet	[E.10] Errores de secuencia	12. Seguridad en la operativa	12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad
Red internet	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Red internet	[A.7] Uso no previsto	7. Seguridad ligada a los recursos	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en

		humanos.		seguridad de la información
Red internet	[A.9] [Re-]encaminamiento de mensajes	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Red internet	[A.10] Alteración de secuencia	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Red internet	[A.14] Interceptación de información (escucha)	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.2 Mecanismos de seguridad asociados a servicios en red.
Red internet	[A.15] Modificación de la información	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Red Lan	[E.9] Errores de [re-]encaminamiento	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
Red Lan	[E.10] Errores de secuencia	12. Seguridad en la operativa	12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad
Red Lan	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Red Lan	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Red Lan	[A.9] [Re-]encaminamiento de mensajes	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Red Lan	[A.10] Alteración de secuencia	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red

Red Lan	[A.15] Modificación de la información	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Cables de energía	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Ups	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Licencias	[E.20] Vulnerabilidades de los programas (software)	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.
Electricidad	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Telefonía	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Mantenimiento	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Antivirus	[E.20] Vulnerabilidades de los programas (software)	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas.
Electrónicos (one drive de office)	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Telefonía móvil	[A.5] Suplantación de la identidad	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Telefonía móvil	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Firewall	[E.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de softwa
Cables de energía	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para	9.1.1 Política de control de acceso

			el control de accesos	
Telefonía móvil	[E.2] Errores del administrador del sistema / de la seguridad	12. Seguridad en la operativa.	12.4 Registro de actividad y supervisión.	12.4.3 Registros de actividad del administrador y operador del sistema.
Impresora	[E.25] Pérdida de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Rack Jupiter	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Rack Jupiter	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Bandejas porta equipos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Bandejas porta equipos	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Organizadores horizontales con canaleta ranurada	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Organizadores horizontales con canaleta ranurada	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Electrónicos (one drive de office)	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Electricidad	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Base de datos	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Electricidad	[E.19] Fugas de información	13. Seguridad en las	13.2 Intercambio de información con partes	13.2.4 Acuerdos de confidencialidad y secreto.

		telecomunicaciones.	externas.	
Electricidad	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Electricidad	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Telefonía	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Telefonía	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Telefonía	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Telefonía	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Mantenimiento	[E.1] Errores de los usuarios	12. Seguridad en la operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
Mantenimiento	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Mantenimiento	[A.6] Abuso de privilegios de acceso	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Mantenimiento	[A.7] Uso no previsto	7. Seguridad ligada a los recursos	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en

		humanos.		seguridad de la información
Antivirus	[E.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software
Licencias	[E.8] Difusión de software dañino	12. Seguridad en la operativa.	12.6 Gestión de la vulnerabilidad técnica.	12.6.2 Restricciones en la instalación de software
HPE Smart Buy	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Router Board Microtik 3014	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Switch 24 puertos Cat. 5E	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Unifi Uap-ac-lite	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Telefonía móvil	[E.9] Errores de [re-]encaminamiento	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
Telefonía móvil	[E.19] Fugas de información	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas.	13.2.4 Acuerdos de confidencialidad y secreto.
Telefonía móvil	[A.9] [Re-]encaminamiento de mensajes	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Telefonía móvil	[A.14] Interceptación de información (escucha)	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.2 Mecanismos de seguridad asociados a servicios en red.
Electrónicos (one drive de office)	[E.19] Fugas de información	13. Seguridad en las	13.2 Intercambio de información con partes	13.2.4 Acuerdos de confidencialidad y secreto.

		telecomunicaciones.	externas.	
Electrónicos (one drive de office)	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Multitoma de energía	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Impresora	[A.23] Manipulación del hardware	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.4 Mantenimiento de los equipos.
Impresora	[A.25] Robo de equipos	11. Seguridad física y ambiental.	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipo
Computadora	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Telefonía móvil	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Impresora	[A.11] Acceso no autorizado	9. Control de accesos.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de acceso
Documentación interna	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Monitor	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Red intenet	[A.12] Análisis de tráfico	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información.
Red Lan	[A.12] Análisis de tráfico	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información.

Telefonía móvil	[E.10] Errores de secuencia	12. Seguridad en la operativa	12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad
Telefonía móvil	[A.10] Alteración de secuencia	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Telefonía móvil	[A.15] Modificación de la información	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red
Servidor NAS	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Internet	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Correo	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Computadora	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Monitor	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Red internet	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Red Lan	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Red Lan	[A.14] Interceptación de información (escucha)	13. Seguridad en las telecomunicaciones.	13.1 Gestión de la seguridad en las redes.	13.1.2 Mecanismos de seguridad asociados a servicios en red.
Telefonía móvil	[A.12] Análisis de tráfico	13. Seguridad en las telecomunicaciones.	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información.
Electrónicos (one drive de office)	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Patch Cord	[A.7] Uso no previsto	7. Seguridad	7.2 Durante la	7.2.2 Concienciación,

		ligada a los recursos humanos.	contratación.	educación y capacitación en seguridad de la información
Electricidad	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Telefonía	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Mantenimiento	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Router Board Microtik 3012	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Switch 24 puertos Cat. 5E	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Unifi Uap-ac-lite	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Electrónicos (one drive de office)	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Electrónicos (one drive de office)	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Multitoma de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Cables de energía	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Ups	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Multitoma de energía	[A.7] Uso no previsto	7. Seguridad ligada a los	7.2 Durante la contratación.	7.2.2 Concienciación, educación y

		recursos humanos.		capacitación en seguridad de la información
Telefonía móvil	[E.15] Alteración de la información	12. Seguridad en la operativa	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información
Cables de energía	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Impresora	[I.11] Emanaciones electromagnéticas (TEMPEST)	11. Seguridad física y ambiental	11.1 Áreas seguras.	11.1.4 Protección contra las amenazas externas y ambientales.
Rack Jupiter	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Bandejas porta equipos	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Organizadores horizontales con canaleta ranurada	[A.7] Uso no previsto	7. Seguridad ligada a los recursos humanos.	7.2 Durante la contratación.	7.2.2 Concienciación, educación y capacitación en seguridad de la información

Anexo 9: Políticas de seguridad de la información

Dominio	Resumen de objetivo y control	Detalle de Políticas
5. Políticas de seguridad.	**5.1 Directrices de la Dirección en seguridad de la información.** 5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información.	Política general, definido y aprobado. Definir y documentar todos los requisitos legales, regulatorios o contractuales.

6. Aspectos organizativos de la seguridad de la información.	**6.1 Organización interna.** 6.1.1 Asignación de responsabilidades para la segur. de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos. **6.2 Dispositivos para movilidad y teletrabajo.** 6.2.1 Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo.	Experto en seguridad de la información del DTI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., con enfoque en gestión y desarrollo de políticas de seguridad. Destacada capacidad para aprobar, implementar y asignar responsabilidades. Prioriza asesoramiento externo para un desempeño exitoso en seguridad.
7. Seguridad ligada a los recursos humanos.	**7.1 Antes de la contratación.** 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. **7.2Durante la contratación.** 7.2.1 Responsabilidades de gestión. 7.2.2Concienciación, educación y capacitación en segur. de la información. **7.2.3 Proceso disciplinario.** 7.3 Cese o cambio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo.	Plan de capacitación alineado a las políticas más relevantes. Evaluar el historial del candidato para asegurar su adecuación

8. Gestión de activos.	**8.1 Responsabilidad sobre los activos.** 8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. **8.1.4 Devolución de activos**. 8.2 Clasificación de la información. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos. **8.3 Manejo de los soportes de almacenamiento.** 8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito.	El encargado de DTI tiene la responsabilidad de llevar un inventario de activos, los cuales se deben actualizarse por lo menos 1 ves al año. Desarrollar y actualizar manuales para administrar instalaciones de software, realizar copias de seguridad, reiniciar sistemas e implementar procedimientos de recuperación.
9. Control de accesos.	**9.1 Requisitos de negocio para el control de accesos.** 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. **9.2 Gestión de acceso de usuario.** 9.2.1 Gestión de altas/bajas en el registro de usuarios. **9.3 Responsabilidades del usuario.** 9.3.1 Uso de información	Crear un manual de control de acceso Desarrollar políticas que regulen las interacciones con redes y servicios en línea. Desarrollar un formulario de revisión de los derechos de acceso de los usuarios.

	confidencial para la autenticación. **9.4 Control de acceso a sistemas y aplicaciones.** 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión.	
10. Cifrado.	**10.1Controles criptográficos.** 10.1.2 Gestión de claves.	Definir pautas para usar una herramienta de contraseñas.
11. Seguridad física y ambiental	**11.1 Áreas seguras.** 11.1.4 Protección contra las amenazas externas y ambientales. **11.2 Seguridad de los equipos.** 11.2.1 Emplazamiento y protección de equipos. 11.2.4 Mantenimiento de los equipos.	Establecer un protocolo de cuidado y mantenimiento de los equipos. Realizar una reunion informativa. Crear un plan de pedido de suministros de energía.
12. Seguridad en la operativa.	**12.1 Responsabilidades y procedimientos de operación.** 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción **12.4 Registro de actividad y supervisión.** 12.4.3 Registros de actividad del administrador y operador del sistema.	Establecer políticas y prácticas para monitorear la instalación de software sin licencia. Crear una política para monitorear las instalaciones de software por parte de los usuarios.

	12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software.	
13.Seguridad en las telecomunicaciones	**13.1 Gestión de la seguridad en las redes.** 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. **13.2 Intercambio de información con partes externas.** 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.4 Acuerdos de confidencialidad y secreto.	De acuerdo con la política del sistema de gestión de seguridad de la información, se establecen medidas de seguridad mediante la implementación de algoritmos de cifrado para proteger la confidencialidad de los datos de las comunicaciones electrónicas.
14. Adquisición, desarrollo y mantenimiento de los sistemas de información.	**14.1 Requisitos de seguridad de los sistemas de información.** 14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.3 Protección de las transacciones por redes telemáticas. **14.2 Seguridad en los procesos de desarrollo y soporte.** 14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de	Propuesta de política de desarrollo seguro. Crear un plan estratégico para establecer y mantener requisitos de seguridad de la información en el software existente, implementando controles de acceso y protección de datos en los servicios de red conforme a las políticas del sistema de gestión de seguridad de la información. Después de un cambio en la

	control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 14.2.6 Seguridad en entornos de desarrollo. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación. **14.3 Datos de prueba.** 14.3.1 Protección de los datos utilizados en pruebas.	plataforma, el jefe de DTI es responsable de realizar pruebas rigurosas para garantizar que los datos estén protegidos en términos de confidencialidad, integridad y cumplan plenamente con los estándares del Sistema de gestión de seguridad de la información (SGSI). Además, se deben desarrollar protocolos de prueba de aceptación en colaboración con cada proveedor de software utilizado en la organización antes de su implementación en un entorno de producción.
15. Relaciones con suministradores	**15.1 Seguridad de la información en las relaciones con suministradores.** 15.1.1 Política de seguridad de la información para suministradores.	Deberá negociar acuerdos de confidencialidad con proveedores que tengan acceso a instalaciones o equipos regulatorios del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.
16. Gestión de incidentes en la seguridad de la información.	**16.1 Gestión de incidentes de seguridad de la información y mejoras.**	Comunicar a los empleados a través de correo electrónico de la

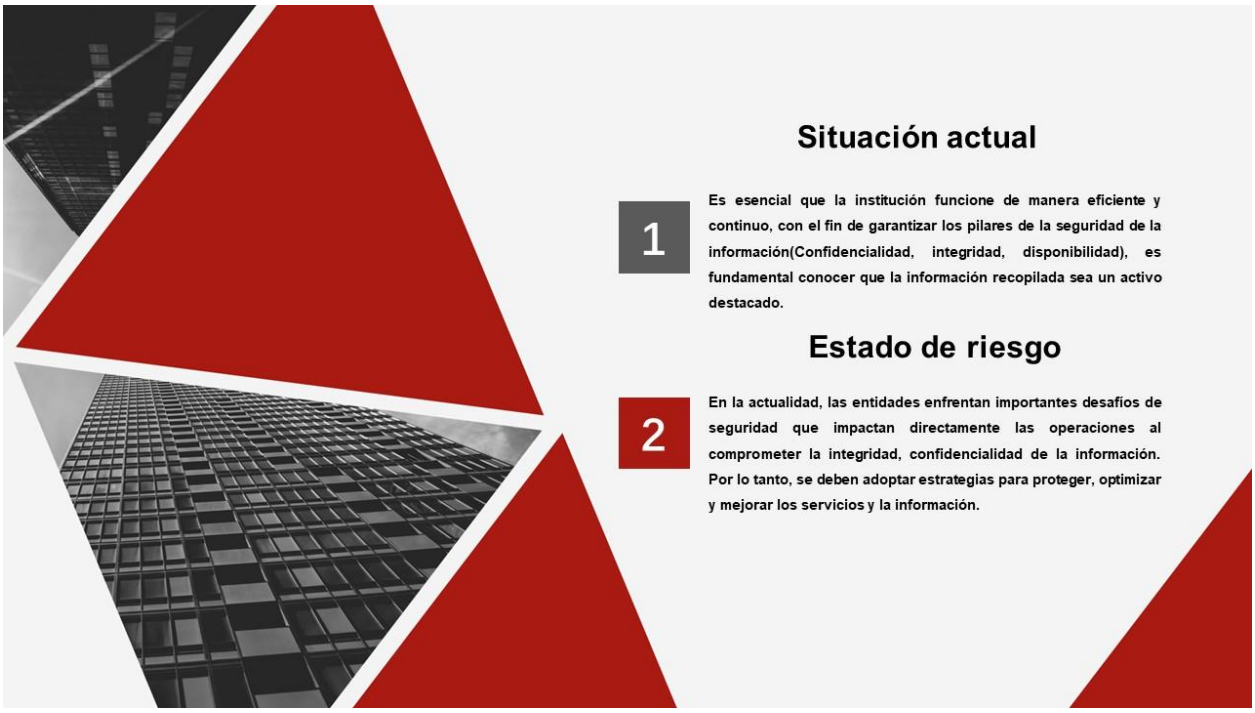
	16.1.1 Responsabilidades y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.6 Aprendizaje de los incidentes de seguridad de la información.	organización que se requiere capacitación social si los empleados no tienen conocimientos sobre el uso de estos medios. Aplicar correcciones de seguridad. Guardar notificaciones vulnerabilidades del sistema.
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	**17.1 Continuidad de la seguridad de la información.** 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. **17.2Redundancias.** 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	La planificación de la continuidad de la seguridad se basa en el concepto de crear una política de seguridad que identifique las necesidades y requisitos básicos para hacer frente a situaciones de riesgos y desastres que puedan afectar la seguridad de la información. En este contexto, la política de seguridad juega un papel fundamental en la definición de políticas y procedimientos para garantizar la resiliencia frente a eventos adversos. Determinar los requisitos de planificación y seguridad de la información de la organización para garantizar la continuidad en el

		tratamiento de eventos adversos.
18. Cumplimiento.	**18.1 Cumplimiento de los requisitos legales y contractuales.** 18.1.1 Identificación de la legislación aplicable. 18.1.2 Derechos de propiedad intelectual (DPI).	Desarrollar una estrategia integral para la protección de datos personales y garantizar el estricto cumplimiento de todas las leyes y regulaciones relevantes.

Nota. Elaboración propia.

Anexo 10: Materiales (Presentación, infografía)

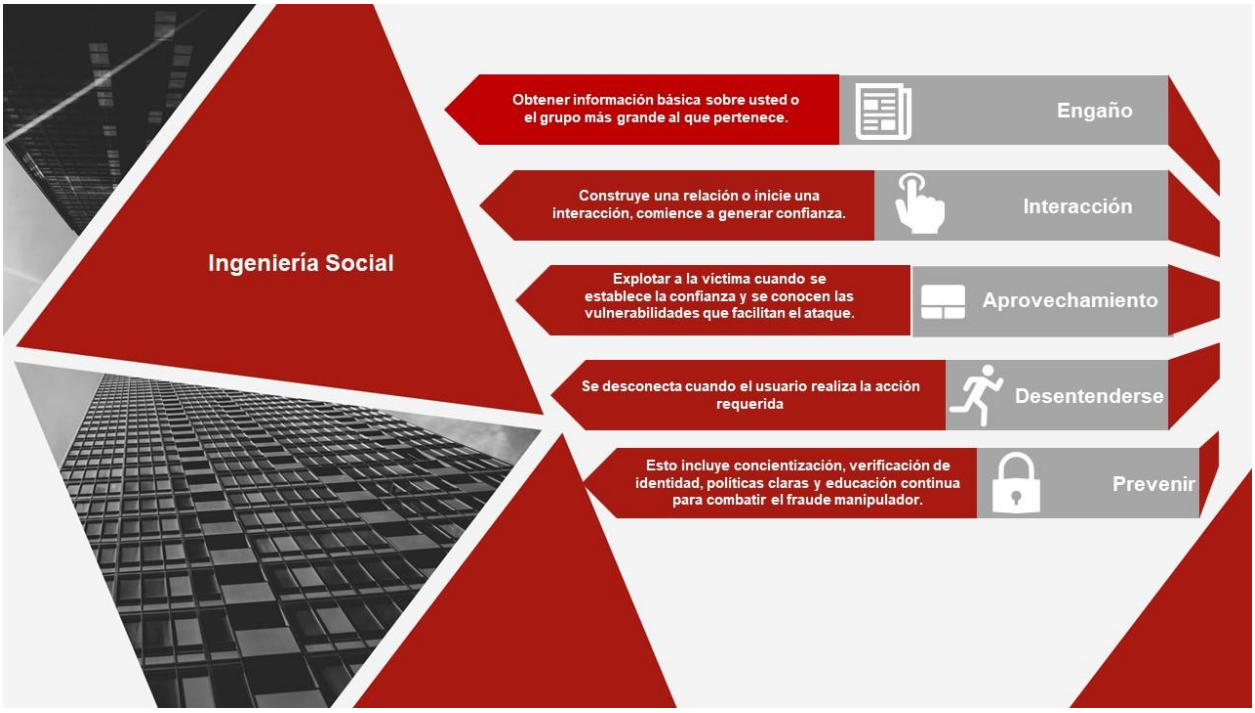
Presentación


Situación actual
1
Es esencial que la institución funcione de manera eficiente y continuo, con el fin de garantizar los pilares de la seguridad de la información(Confidencialidad, integridad, disponibilidad), es fundamental conocer que la información recopilada sea un activo destacado.
Estado de riesgo
2
En la actualidad, las entidades enfrentan importantes desafíos de seguridad que impactan directamente las operaciones al comprometer la integridad, confidencialidad de la información. Por lo tanto, se deben adoptar estrategias para proteger, optimizar y mejorar los servicios y la información.

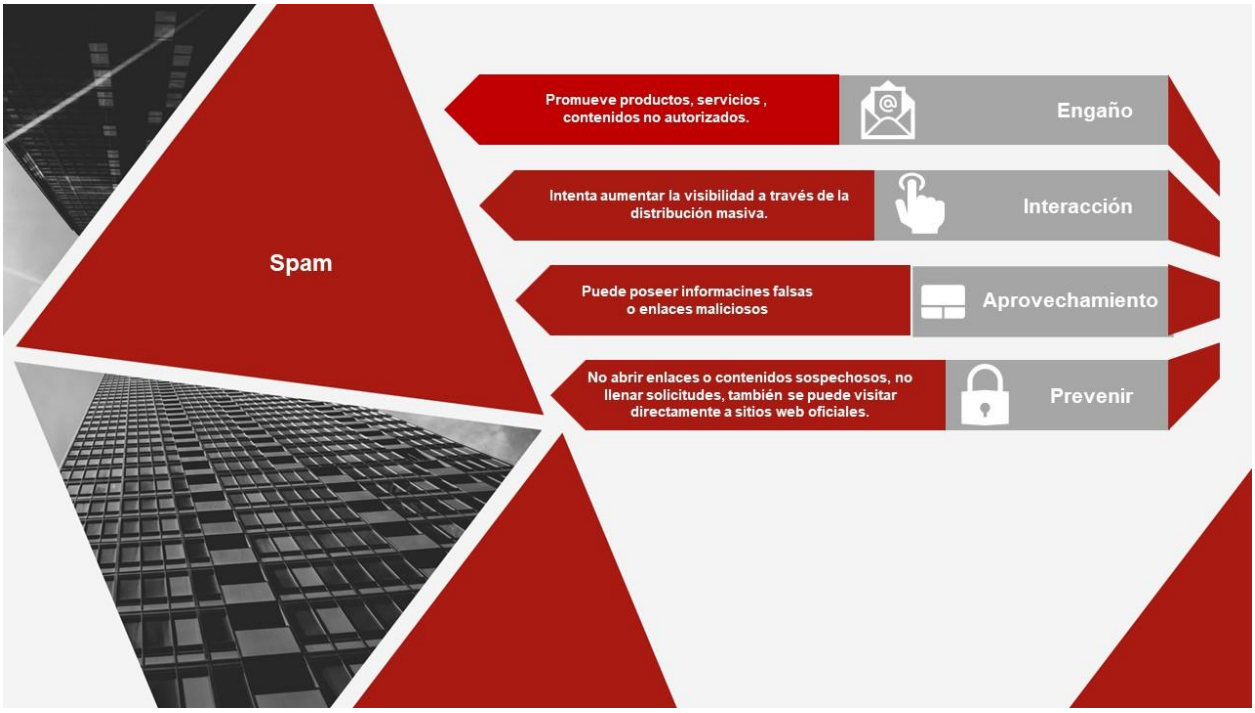

Definiciones de SGSI
Sistema de gestion de seguridad de la informacón
Es un conjunto de políticas y medidas utilizadas para proteger la seguridad de la información de una organización, garantizar la confidencialidad, integridad y disponibilidad, y gestionar los riesgos de seguridad.
Activo
Recursos valiosos, como datos, hardware, software o personas, que aportan valor a una organización y requieren protección adecuada.
Amenaza
Posibilidad de un evento perjudicial que puede explotar vulnerabilidades en sistemas o procesos, comprometiendo la seguridad de la información.
Vulnerabilidad
Debilidad en un sistema, proceso o componente que puede ser explotada por una amenaza para comprometer la seguridad.
Riesgo
Probabilidad de pérdida o daño, combinada con el impacto potencial, asociada a amenazas y vulnerabilidades en un entorno específico.


Pilares de la Seguridad de la información
Confidencialidad
Asegúrese de que la información sea accesible solo para el personal autorizado y evite el acceso no autorizado.
Integridad
Asegúrese de que la información sea precisa, completa y no haya sido manipulada. El objetivo es evitar la manipulación no autorizada de datos.
Disponibilidad
Asegure el acceso y disponibilidad de la información autorizada, previniendo resultados inesperados o ataques que puedan afectar su sistema.

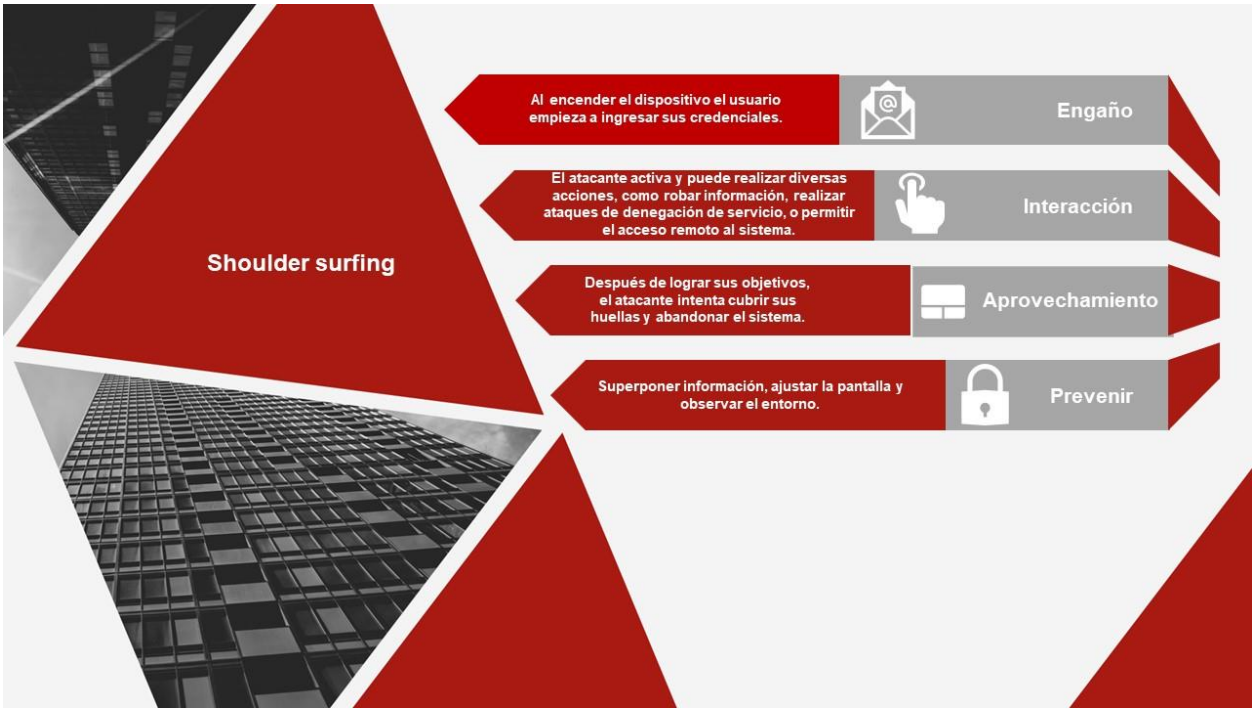

Métodos para recopilar informaciones privadas


Ingeniería Social
Obtener información básica sobre usted o el grupo más grande al que pertenece.
Engaño
Construye una relación o inicie una interacción, comience a generar confianza.
Interacción
Explotar a la víctima cuando se establece la confianza y se conocen las vulnerabilidades que facilitan el ataque.
Aprovechamiento
Se desconecta cuando el usuario realiza la acción requerida
Desentenderse
Esto incluye concientización, verificación de identidad, políticas claras y educación continua para combatir el fraude manipulador.
Prevenir


Pishing
Envío correos electrónicos de phishing con enlaces o archivos maliciosos
Engaño
Las víctimas interactúan con elementos maliciosos, lo que les provoca instalar malware o filtrar información
Interacción
Utiliza la información recopilada para cometer actividades maliciosas.
Aprovechamiento
Implementar medidas educativas, técnicas y de concientización, como verificación de correo electrónico, autenticación de dos factores y actualizaciones de software.
Prevenir


Spam
Promueve productos, servicios , contenidos no autorizados.
Engaño
Intenta aumentar la visibilidad a través de la distribución masiva.
Interacción
Puede poseer informacines falsas o enlaces maliciosos
Aprovechamiento
No abrir enlaces o contenidos sospechosos, no llenar solicitudes, también se puede visitar directamente a sitios web oficiales.
Prevenir


Malware
El malware generalmente se introduce en un sistema a través de correo electrónico, descargas o sitios web infectados.
Engaño
Realiza acciones maliciosas elaboradas como robo de datos, corrupción de archivos o toma de control del sistema.
Interacción
Intenta mantener su presencia en el sistema haciendo copias o cambiando configuraciones para evitar más actividades maliciosas.
Aprovechamiento
Mantener sistemas actualizados, utilizar software antivirus, tenga cuidado en linea y cree copias de seguridad para evitar
Prevenir



Nota. Elaboración propia

Infografía


Spam
Envío masivo de mensajes no solicitados.
Fiabilidad de la publicación
Promueve productos, servicios , contenidos no autorizados.
SCAM
Generación de tráfico
Intenta aumentar la visibilidad a través de la distribución masiva.
SCAM
Contenido engañoso
Puede poseer informacines falsas o enlaces maliciosos
SCAM
¿Qué hacer ?
Antivirus
Instalar software de antivirus que pueda detectar spam.
SCAM
Enlaces o contenidos
No abrir enlaces o contenidos sospechosos, no llenar solicitudes, también se puede visitar directamente a sitios web oficiales.
SCAM
Seguridad


Contraseñas robustas
Longitud
Utilizar contraseñas largas, cuanto más larga(12 caracteres) sea la contraseña, más difícil será para alguien descifrarla.
Combinación de caracteres
Incluir una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales (!, @, #, $, %, etc.). Esto aumenta la complejidad de la contraseña.
Evitar información personal
Se recomienda evitar el uso de información personal fácilmente accesible y palabras comunes para mejorar la seguridad
Contraseñas únicas para cada cuenta
No utilizar la misma contraseña para varias cuentas. Si una contraseña se ve comprometida, pueda que todas tus cuentas estén en peligro.
Actualización periódicaociales
Cambiar las contraseñas periódicamente. Esto reduce el riesgo en caso de que la contraseña se haya visto comprometida y aún no lo sepas.
Seguridad

Nota. Elaboración propia.

Anexo 11: Cuestionario para la capacitación

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN SOFTWARE

Cuestionario sobre Seguridad de la Información

El siguiente cuestionario tiene como objetivo de reflejar los conocimientos adquiridos durante la capacitación sobre la Seguridad de la información. Se puede elegir solo una respuesta a las siguientes preguntas.

1: ¿Qué es un activo?

a) Recursos valiosos, como datos, hardware, software o personas, que aportan valor a una organización y requieren protección adecuada.
b) Recursos no valiosos que no aportan valor a una organización y no requieren protección adecuada.
c) Recursos tangibles que no aportan valor a una organización y no requieren protección adecuada.

2: ¿Qué es una amenaza?

a) Se refiere a eventos beneficiosos que mejoran la eficiencia de sistemas y procesos, fortaleciendo la seguridad de la información.
b) Posibilidad de un evento perjudicial que puede explotar vulnerabilidades en sistemas o procesos, comprometiendo la seguridad de la información.
c) Es la certeza de que ningún evento perjudicial ocurrirá, eliminando cualquier posibilidad de comprometer la seguridad de la información.

3: ¿Qué es un riesgo?

a) Probabilidad de pérdida o daño, combinada con el impacto potencial, asociada a amenazas y vulnerabilidades en un entorno específico.
b) Son eventos favorables que mejoren la seguridad de la información y los activos de una organización.
c) La probabilidad de que ocurra una amenaza y afecte negativamente a los activos de la organización.

4: ¿Cuáles son los pilares fundamentales de la seguridad de la información?

a) Confidencialidad. integridad, disponibilidad.

b) Transparencia, colaboración. actualización

c) Seguridad, privacidad, sostenibilidad.

5: ¿Cuáles son las principales funciones del software antivirus?

a) Navegación web cómoda y mejora de la velocidad del sistema.

b) Detectar, prevenir y eliminar softwares maliciosos.

c) Optimizar el rendimiento del hardware y software.

6: ¿Cuál de las siguientes opciones describe mejor la ingeniería social?

a) Formas de aumentar la velocidad de un sistema informático.

b) Manipulación psicológica para obtener información confidencial.

c) Métodos para optimizar el rendimiento del hardware y del software.

7: ¿Cuál de las siguientes opciones describe mejor el phishing?

a) Formas de aumentar la velocidad de un sistema informático.

b) Manipulación psicológica para obtener información confidencial.

c) Envío correos electrónicos con enlaces o archivos maliciosos.

8: ¿Cuál de las siguientes opciones describe mejor el spam?

a) Tecnologías que aumentan la velocidad de los sistemas informáticos.

b) enviar mensajes masivos no solicitados debido a publicidad o actividades fraudulentas.

c) métodos para obtener información confidencial mediante manipulación psicológica.

9: ¿Cuáles son las medidas anti spam efectivas?

a) Compartir la dirección de correo electrónico en las redes sociales.

b) Utilizar software de filtrado de correo electrónico.

c) Hacer clic en un enlace de un correo electrónico desconocido.

10: ¿Cuál de las siguientes opciones describe mejor el malware?

a) Software diseñado para mejorar el rendimiento del sistema.

b) Programas informáticos que dañen o infiltren el sistema.

c) Aplicaciones que proporcionen servicios de seguridad en línea.

Anexo 12: Primer cuestionario Inicial para la validación con método Delphi

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información enfocado a la ISO/IEC 27002:2013 del sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SOFTWARE

Cuestionario Inicial

1: ¿Considera usted que es muy imprescindible Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información con la ISO/27002:2013 en el sistema financiero del departamento de TI de la Cooperativa de Ahorro y Crédito Imbacoop Ltda?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

2: ¿Cómo evalúa el Desarrollo de Plan de Sistema de Gestión de Seguridad de la Información con la ISO/27002:2013 para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., es un informe comprensible de manera simple?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

3: ¿A su criterio el informe de Desarrollo de Plan de Sistema de Gestión de Seguridad de la Información con la ISO/27002:2013 para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., cuenta con la información necesaria?

1. Totalmente de acuerdo
2. De acuerdo

3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

4: ¿Está de acuerdo con la elección de la Metodología Magerit v3 y la ISO/IEC 27002:2013 para Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

5: ¿Considera usted que los procedimientos realizados en el Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., fueron los necesarios?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

6: ¿Considera usted que la utilización de la herramienta Pilar y las hojas de cálculo de Excel resultaron han demostrado ser eficientes y acertadas en el manejo de información en el Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda.?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

7: ¿En su opinión las tareas propuestas a manera de controles para la mitigación de riesgos en el Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda., fueron adecuadas?

6. Totalmente de acuerdo
7. De acuerdo
8. Indiferente o neutro
9. En desacuerdo
10. Totalmente en desacuerdo

8: ¿Cree que el Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información con la norma ISO/IEC 27002:2013, realizada para el sistema financiero del Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., puede ser aplicado con éxito en otras entidades financieras?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

9: ¿Considera usted que las políticas de seguridad realizadas para el Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en sistema financiero del Departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda fueron las más adecuadas?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

10: ¿Considera usted que a través de la acción del plan de tratamiento riesgo realizada se asegura la confidencialidad e integridad de la información del sistema financiero en el Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información del Departamento de Tecnología de la información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

11: ¿Haría ajustes a algún elemento del Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información para el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito de Imbacoop Ltda, cual sería?

_____

_____

Anexo 12: Cuestionario Final para la validación con método Delphi

El presente cuestionario tiene como finalidad recolectar información sobre distintos puntos relevantes al Desarrollo de un Plan de Sistema de Gestión de Seguridad de la Información enfocado a la ISO/IEC 27002:2013 del sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SOFTWARE

Cuestionario Final

1: ¿Considera que las políticas de Mejora Continua que se han establecido en el desarrollo de Plan Sistema de Gestión de la Seguridad de la Información están acordes con el sistema financiero del Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

2: ¿Considera usted que, en respuesta al enfoque de Mejora Continua, sea acertado plantear un seguimiento por lo menos una vez al año sistema financiero del Departamento de Departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda?

6. Totalmente de acuerdo
7. De acuerdo
8. Indiferente o neutro
9. En desacuerdo
10. Totalmente en desacuerdo

3: ¿Considera usted que la optimización de proceso de respuesta a incidentes contribuiría a una mejora continua en la detección y mitigación de riesgos?

1. Totalmente de acuerdo
2. De acuerdo

3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

4: ¿Estaría de acuerdo en que el uso la norma ISO/IEC 27002:2013 fue acertada para la selección de controles?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

5: ¿Cree que las modificaciones en el Informe de Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información para el sistema financiero del departamento de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda mejoraron la calidad según las observaciones del primer cuestionario?

1. Totalmente de acuerdo
2. De acuerdo
3. Indiferente o neutro
4. En desacuerdo
5. Totalmente en desacuerdo

Anexo 13: Certificados

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERIA EN SOFTWARE

ACTA DE ENTREGA DEL INFORME DEL DESARROLLO DEL PLAN DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON LA ISO 27002: 2013, DE LA COOPERATIVA DE AHORRO Y CRÉDITO IMBACOOP LTDA.

En la ciudad de Ibarra a los 31 días del mes de enero del año 2024, se entrega al jefe del Departamento de Tecnología del Información de la Cooperativa de Ahorro y Crédito Imbacoop Ltda., al ing. Jeison Ramos los siguientes documentos:

- Informe de políticas de seguridad de la información
- Documento de Excel
- Presentación de la socialización

Considerando que las partes manifiestan su total conformidad, se ratifica y aceptan todo su contenido, entendiendo su alcance y significado.

Recibe conforme:

Ing. Jeison Ramos

Jefe de DTI

Entrega conforme:

José Castañeda

Estudiante

CERTIFICADO DE ENTREGA Y RECEPCION

Ingeniero Jeison Ramos, jefe del Departamento de Tecnología de la Información de la Cooperativa Ahorro y Crédito Imbacoop Ltda., apetición verbal del interesado.

CERTIFICA:

Que el señor José Dimas Castañeda Cando con número de cédula 1003929849, se realizó la entrega del CONTENIDO y FORMATO del trabajo de titulación denominado: Desarrollo de un Plan de Sistema de Gestión de la Seguridad de la Información en la Cooperativa de Ahorro y Crédito Imbacoop Ltda., aplicando el estándar ISO/IEC 27002, para fortalecer la confidencialidad e integridad de la información.

Es todo cuanto puedo certificar en honor a la verdad, pudiendo el interesado hacer uso del presente como lo estime conveniente.

Otavalo, 31 de enero del 2024

Atentamente

.....
Ing. Jeison Ramos
JEFE DE TECNOLOGIAS
COAC IMBACOOP LTDA


DETECTOR DE HUMO
IMBACOOP