UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria (SEPS).

AUTOR

Solano Chico Doris Michelle

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

Ing. SANG GUUN YOO, PhD.

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
SANG GUUN YOO .

Ing. Sang Guun Yoo, Ph.D.
TUTOR

Firmado electrónicamente por:
JESENNIA DEL PILAR CARDENAS COBO

Lic. Jesennia Cárdenas Cobo, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
JORGE LUIS ZAMBRANO MARTINEZ

Ing. Jorge Zambrano Martínez, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por DORIS MICHELLE SOLANO CHICO, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
SANG GUUN YOO .

Ing. SANG GUUN YOO, PhD.

Santa Elena, 15 de diciembre de 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **DORIS MICHELLE SOLANO CHICO**

DECLARO QUE:

El trabajo de Titulación, Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria (SEPS), previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 15 de diciembre de 2024

EL AUTOR

Firmado electrónicamente por:
DORIS MICHELLE
SOLANO CHICO

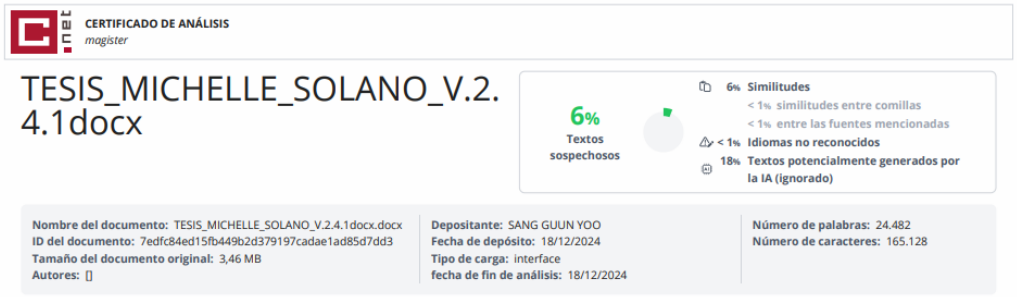
DORIS MICHELLE SOLANO CHICO

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria (SEPS), presentado por el estudiante, DORIS MICHELLE SOLANO CHICO fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 6%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

TESIS_MICHELLE_SOLANO_V.2.4.1docx

6% Textos sospechosos

6% Similitudes
< 1% similitudes entre comillas
< 1% entre las fuentes mencionadas
< 1% Idiomas no reconocidos
18% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TESIS_MICHELLE_SOLANO_V.2.4.1docx.docx
ID del documento: 7edfc84ed15fb449b2d379197cadae1ad85d7dd3
Tamaño del documento original: 3,46 MB
Autores: []

Depositante: SANG GUUN YOO
Fecha de depósito: 18/12/2024
Tipo de carga: interface
fecha de fin de análisis: 18/12/2024

Número de palabras: 24.482
Número de caracteres: 165.128

TUTOR

Firmado electrónicamente por:
SANG GUUN YOO .

Ing. SANG GUUN YOO, PhD.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **DORIS MICHELLE SOLANO CHICO**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de la propuesta metodológica y tecnológica avanzada con fines de difusión pública, además apruebo la reproducción de esta propuesta metodológica y tecnológica avanzada dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 15 de diciembre de 2024

EL AUTOR

Firmado electrónicamente por:
DORIS MICHELLE SOLANO CHICO

DORIS MICHELLE SOLANO CHICO

AGRADECIMIENTO

Este trabajo es un reflejo del esfuerzo y la dedicación invertidos en el avance del conocimiento en mi área de estudio y profesional. A mi familia, y de manera especial a mis padres, Doris y Geovanny, les agradezco por confiar siempre en mí, así como a mi novio cuya dedicación y apoyo han sido un pilar fundamental en este proceso.

Agradezco a la Universidad Estatal Península de Santa Elena por ofrecer este programa de postgrado en Ciberseguridad, a mis docentes y tutor de tesis quienes compartieron su tiempo y experiencia a mi desarrollo académico.

Doris Michelle, Solano Chico

DEDICATORIA

El presente trabajo se lo dedico a Dios por ser mi guía y fortaleza.

A todas las personas que contribuyeron a lo largo del proceso de este posgrado, especialmente a mi familia, por su apoyo incondicional en cada meta alcanzada. Extiendo mi gratitud a mi novio, por su respaldo y motivación en esta etapa tan importante.

Doris Michelle, Solano Chico

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto titulado “Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria (SEPS)” tiene como propósito analizar los posibles riesgos informáticos que afectan a esta entidad financiera y proponer una metodología de gestión en conformidad con la normativa de la SEPS. Para reconocer y evaluar los riesgos vinculados a cada uno de los activos, se utilizó un método que fusiona la metodología de MAGERIT con la norma ISO 27005. A través del estudio realizado con la herramienta PILAR, se reveló que los activos fundamentales de la cooperativa se encuentran con distintos grados de riesgo. En este proyecto, se destaca lo importante y esencial que es implementar un plan de mitigación acorde a las normativas emitidas por la SEPS, que incluya medidas de seguridad, formación del personal y procedimientos formales. Este grupo de medidas potenciará la seguridad de la información y asegurará el cumplimiento de las regulaciones.

Palabras claves: Gestión de Riesgos, Seguridad Informática, COAC.

ABSTRACT

The purpose of this project entitled “Analysis of IT Risks at Cooperativa de Ahorro y Crédito Metrópolis LTDA, under the regulatory compliance of the Superintendencia de Economía Popular y Solidaria (SEPS)” is to analyze the possible IT risks affecting this financial institution and to propose a management methodology in compliance with SEPS regulations. In order to recognize and evaluate the risks linked to each of the assets, a method that merges the MAGERIT methodology with the ISO 27005 standard was used. Through the study carried out with the PILAR tool, it was revealed that the cooperative's key assets have different degrees of risk. This project highlights how important and essential it is to implement a mitigation plan in accordance with the regulations issued by SEPS, including security measures, staff training and formal procedures. This set of measures will enhance information security and ensure compliance with regulations.

Keywords: Risk Management, Information Security, COAC.

INTRODUCCIÓN

La Cooperativa de Ahorro y Crédito Metrópolis LTDA. (COAC Metrópolis), es una entidad financiera en Ecuador que resalta por su compromiso, servicio a la comunidad y su constante labor durante más de 17 años. Desde su fundación en el año 2006 en el cantón Quinsaloma de la provincia de Los Ríos, ha vivido un notable desarrollo, estableciéndose como una cooperativa con más de ocho mil socios (*Cooperativa de Ahorro y Credito Metropolis LTDA.*, 2024).

En un mundo cada vez más digital donde la protección de la información es una prioridad esencial, surgen retos para las cooperativas, particularmente. Históricamente, tanto COAC Metrópolis como otras entidades financieras han tratado la administración de riesgos desde un enfoque financiero. No obstante, el progreso tecnológico ha originado retos novedosos, tales como el hurto de datos, la pérdida de información o la manipulación de bases de datos (Abril et al., 2013). Esto ha generado que la Superintendencia de Economía Popular y Solidaria (SEPS) emita normativas más estrictas, para que las instituciones financieras se preparen mejor y puedan hacer frente a estos posibles eventos.

Las regulaciones de la SEPS se aplican de acuerdo con la segmentación, en el caso de la COAC Metrópolis fue notificada como segmento 3 mediante oficio N.º SEPS-SGD-IGS2023-16268-OF el 01 de junio de 2023 por parte de la SEPS, la cooperativa reconoce la necesidad de fortalecer su protección frente a los riesgos informáticos, en cumplimiento con las normativas establecidas.

El objetivo principal de este proyecto es examinar los peligros informáticos a los que se enfrenta la COAC Metrópolis, con el propósito principal de robustecer la seguridad de la información delicada. Por medio de este, se intentará reconocer los riesgos más significativos y sugerir un método para reducirlos en conformidad con las regulaciones de la SEPS, asegurando de esta manera la protección de los datos y el cumplimiento de las normativas. El procedimiento de desarrollo se fundamenta en un enfoque híbrido que incorpora ISO 27005 y MAGERIT, las cuales posibilitan una evaluación más integral.

Planteamiento del problema

Con una sólida trayectoria de 18 años en el país La Cooperativa de Ahorro y Crédito Metrópolis LTDA, ha sobresalido por su dedicación a la comunidad y por los servicios financieros de alta calidad que brinda a sus más de ocho mil socios. En un ambiente corporativo cada vez más digital surgen retos para las cooperativas de ahorro y crédito, como la COAC Metrópolis, enfrentando desafíos significativos en la protección de la información sensible y el cumplimiento de las normativas establecidas por la Superintendencia de Economía Popular y Solidaria (SEPS).

En el Ecuador la SEPS es la entidad encargada de regular y controlar las cooperativas. La SEPS en junio del 2023 catalogó a la COAC Metrópolis, como segmento 3, por lo cual la entidad debe cumplir los requerimientos de la RESOLUCIÓN NO. SEPS-IGS- IGT-IGJ-INGINT-INTICINSESF-INR-DNSI 2022-002 - "Norma de control respecto a la seguridad de la información en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria".

Los riesgos de la ciberseguridad, como las amenazas de malware, los ataques de phishing y los fallos de seguridad, aumentan a la par que nuestra creciente dependencia de las tecnologías de la información. Con el fin de proteger la disponibilidad, confidencialidad e integridad de la información de sus socios, la COAC Metrópolis debe gestionar con éxito estas cuestiones. Sin embargo, sus intentos de identificar, evaluar y mitigar con precisión las vulnerabilidades de su infraestructura informática pueden verse obstaculizados por la ausencia de un proceso de gestión de riesgos informáticos.

Por lo tanto, surge la interrogante sobre cómo diseñar e implementar una metodología con enfoque integral de gestión de riesgos informáticos en la Cooperativa Metrópolis LTDA, alineado con las normativas de la SEPS, que permita fortalecer la protección de la información sensible y garantizar el cumplimiento normativo de manera efectiva.

Formulación

¿Cuáles son los riesgos informáticos a los que se enfrenta la Cooperativa de Ahorro y Crédito Metrópolis LTDA en cuanto a la protección de la información sensible, considerando las normativas de la Superintendencia de Economía Popular y Solidaria (SEPS)?

Sistematización

1. ¿Cuáles son los riesgos informáticos más significativos que afectan la protección de la información en la Cooperativa de Ahorro y Crédito Metrópolis LTDA?
2. ¿A qué desafíos se enfrenta la cooperativa al tratar de manejar eficientemente los riesgos informáticos identificados?
3. ¿Cuál es la metodología recomendada para mitigar los riesgos informáticos identificados en la Cooperativa Metrópolis LTDA.?

Delimitación

- ✓ El análisis se enfocará en la identificación y evaluación de riesgos informáticos específicos para la Cooperativa de Ahorro y Crédito Metrópolis LTDA.
- ✓ Se considerarán las normativas establecidas por la Superintendencia de Economía Popular y Solidaria (SEPS) como marco normativo principal para el análisis de riesgos.
- ✓ La investigación se centrará en proponer metodologías para evaluar riesgos y políticas adecuadas para mitigar los riesgos informáticos identificados, en línea con las necesidades y requisitos de la cooperativa.

Justificación

Tras 18 años de trayectoria ofreciendo sus servicios como entidad financiera en el Ecuador y con más de 7,000 socios hasta el año 2023. La Cooperativa de Ahorro y Crédito Metrópolis LTDA, con su oficina Matriz en la provincia de Los Ríos, cantón Quinsaloma se enfrenta a los retos de un entorno cada vez más digitalizado y con más amenazas de ciberseguridad, principalmente con retos relacionados a proteger los activos digitales y garantizar la integridad de cada uno de los socios.

Al utilizar medidas de ciberseguridad la COAC Metrópolis no solo cumple con la necesidad de salvaguardar los datos sensibles de sus socios, que incluyen información financiera y personal, sino también a la importancia de cumplir con las estrictas regulaciones en materia de protección de datos y seguridad de la información establecidas por la Superintendencia de Economía Popular y Solidaria (SEPS).

También es importante resaltar que, dado que la cooperativa depende en gran medida de sus sistemas y plataformas digitales para llevar cada una de sus actividades financieras,

la interrupción causada por cualquier tipo de ciberataque podría tener graves repercusiones, tanto en términos financieros como en la confianza de los socios. Al poner en marcha estrategias de ciberseguridad, no solo se busca prevenir ataques, sino también aumentar la resistencia de la cooperativa ante cualquier inconveniente, error humano y ataque. Con ello, se busca proteger los recursos digitales, cumplimos con las normas, mantenemos la confianza de los asociados y garantizamos que la empresa siga funcionando sin contratiempos.

Hipótesis

La implementación de una metodología de gestión de riesgos informáticos en la Cooperativa Metrópolis LTDA tendría como resultado una mejora significativa en la protección de la información sensible y el cumplimiento normativo establecido por la SEPS.

Objetivo General

Analizar los peligros tecnológicos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA y sugerir un método acorde a las regulaciones de la Superintendencia de Economía Popular y Solidaria (SEPS) para robustecer la salvaguarda de la información delicada.

Objetivos específicos

1. Identificar los riesgos e impactos más significativos que podrían comprometer la seguridad de la información en la Cooperativa de Ahorro y Crédito Metrópolis LTDA.
2. Evaluar y analizar los desafíos a los que se enfrenta la Cooperativa de Ahorro y Crédito Metrópolis LTDA en la gestión de los riesgos informáticos y la integridad de los datos.
3. Determinar la metodología adecuada para mitigar los riesgos informáticos identificados en la Cooperativa Metrópolis LTDA, de acuerdo con las normativas establecidas por la Superintendencia de Economía Popular y Solidaria (SEPS).

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

1.1. Revisión de literatura

1.1.1. Comparación entre las metodologías

Para tener una visión de la compatibilidad de las metodologías y su aporte en la gestión de riesgos en tecnología de la información, en la siguiente tabla se muestran la comparación de cada una de ellas:

Tabla 1 Comparación entre metodologías

Metodología	Referencia	Descripción	Fases	Ventajas
MAGERIT	(Magerit, 2012)	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Esta metodología ayuda a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.	1: Identificación y valoración de activos 2: Identificación y valoración de amenazas 3: Salvaguardas 4: Impacto residual 5: Riesgo residual	• Ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC) • Caracterización del valor que representan los activos para la Organización, así como de las dependencias entre los diferentes activos. • Relaciones entre las amenazas a las que los activos están sujetos.
NIST SP 800-30	(NIST, 2012)	Marco de gestión de riesgos creado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos.	Esto incluye cuatro pasos: (i) Preparación para la evaluación; (ii) Ejecutar la evaluación; (iii) comunicar los resultados de la evaluación; y (iv)	• Proporciona u ofrece una guía detallada para detectar vulnerabilidades y amenazas específicas en sistemas y redes.

			mantener o preservar la evaluación.	
ISO 27005		Estándar internacional para la gestión de riesgos de seguridad de la información. Presenta un sistema de gestión del riesgo de seguridad de la información con énfasis en tecnología de la información.	1: Identificar los activos de información. 2: Evaluar los riesgos. 3: Seleccionar controles adecuados. 4: Implementar los controles seleccionados. 5: Monitorear y revisar continuamente el sistema de gestión de riesgos.	• Estándar internacional reconocido • Compatible con otros estándares ISO
OCTAVE	(Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, 1999)	Operationally Critical Threat, Asset, and Vulnerability Evaluation.	Fase 1: Crear requisitos de seguridad para toda la empresa Fase 2: Identificar vulnerabilidades de la infraestructura Fase 3: Determinar la estrategia de gestión de riesgos de seguridad	• Se centra en la identificación de vulnerabilidades en la infraestructura informática de una organización. • Define los componentes esenciales de una evaluación sistemática de los riesgos de seguridad de la información.

1.1.2. Revisión bibliográfica de metodologías aplicadas en el área financiera

La selección de los artículos analizados en el presente trabajo se basa en un enfoque metódico, enfocando la aplicabilidad de la investigación en los objetivos planteados. Los criterios para seleccionar estos trabajos son los siguientes: Primero la relevancia temática, porque se seleccionaron artículos que abordan directamente la gestión de riesgos de seguridad de la información, específicamente dentro del contexto de metodologías reconocidas como MAGERIT, NIST SP 800-30, ISO 27005 y OCTAVE. Segundo el año de publicación, considerando la naturaleza cambiante en el ámbito de la ciberseguridad y la administración de riesgos, se seleccionaron artículos que se han publicado entre 2019 y 2024, para garantizar así incorporar las investigaciones más recientes, pertinentes y actualizadas. En tercer lugar, el método comparativo, el número escogido facilita una comparación efectiva entre las distintas metodologías sin que el análisis se convierta en redundante. Seguidamente, se muestra la tabla que detalla los artículos:

Tabla 2 Revisión bibliográfica

ID ART.	**TÍTULO**	**AÑO**	**METODOLOGÍA**			
			MAGERIT	NIST SP 800-30	ISO 27005	OCTAVE
Art. 01	CYBER RISK MANAGEMENT AND ISO 27005 APPLIED IN ORGANIZATIONS: A SYSTEMATIC LITERATURE REVIEW (Cerqueira Junior & Arima, 2023)	2023			**X**	

Art. 02	Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector" (A. P. Putra & Soewito, 2023)	2023		**X**		
Art. 03	Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency (Al Fikri et al., 2019)	2019			**X**	
Art. 04	An analysis of methods for assessing information security risks of financial institutions (Belyaev et al., 2021)	2021		**X**	**X**	
Art. 05	Intrusion Detection System in Financial Institutions (Christos Blekos, 2022)	2022			**X**	**X**
Art. 06	Bangladesh Bank Money Heist: A Concern of Cybersecurity System of Bangladesh Bank and Way Forward (Md Alamgir Hossain et al., 2022)	2022			**X**	
Art. 07	Prototype to Mitigate the Risks, Vulnerabilities and Threats of Information to Ensure Data Integrity (Toapanta et al., 2022)	2022	**X**			
Art. 08	A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches (X. M. Liu, 2021)	2021		**X**		
Art. 09	The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector (Kitsios et al., 2023)	2023		**X**	**X**	
Art. 10	PROPOSED OCTAVE-SMALL BASED SECURITY FRAMEWORK FOR MOBILE BANKING AMONG COMMERCIAL BANKS IN DEMOCRATIC REPUBLIC OF CONGO (Marjorie & Kamotho, 2020)	2020				**X**

Art. 11	Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review (Ali et al., 2024)	2024				**X**

En la siguiente tabla se describen artículos que utilizan las metodólogas de riesgos estudiadas

Tabla 3 Análisis de los artículos revisados

ID ART. → Art. 01
Objetivo del Estudio
Este estudio tiene como objetivo identificar las motivaciones y objetivos para la adopción de la norma ISO 27005 en organizaciones en sistemas productivos.
Resumen
Los resultados sugieren que las organizaciones buscan adoptar la norma ISO 27005 con el objetivo de mejorar los procesos relacionados con la gestión de riesgos, evaluación de riesgos, mejorar la gestión de la seguridad de la información y cumplir con las leyes, reglamentos y partes interesadas.
Análisis de Resultados
El análisis de los resultados de este estudio permite observar que las organizaciones prefieren al adoptar la norma para resolver cuestiones relacionadas con los procesos de gestión y evaluación de riesgos en seguridad de la información.
ID ART. → Art. 02
Objetivo del Estudio
Evaluar riesgos de seguridad de información en un sistema ERP de seguros usando ISO 27005:2018 y NIST SP 800-30 rev.1.
Resumen

Este estudio propone una metodología integrada de gestión de riesgos de seguridad de la información, combinando ISO 27005:2018 y NIST SP 800-30 rev.1. Se aplica a un sistema ERP en el sector de seguros, abarcando contexto, evaluación y tratamiento de riesgos, con controles basados en ISO 27002:2022.
Análisis de Resultados
Se identificaron 142 riesgos: 2 altos, 30 moderados, 97 bajos y 13 muy bajos. 110 fueron aceptables y 32 inaceptables. Se propusieron controles organizacionales, de personal, físicos y tecnológicos. Se recomienda un equipo de seguridad y un registro de riesgos. La integración de marcos demostró ser eficaz para una gestión de riesgos más completa.
ID ART. → Art. 03
Objetivo del Estudio
Proporcionar una explicación detallada sobre cómo implementar la técnica combinada de evaluación de riesgos de seguridad de la información utilizando ISO 27005 y NIST SP 800-30 revisión 1.
Resumen
Este artículo destaca ya que analiza un método combinado de valoración de riesgos de seguridad informática que emplea tanto las normas ISO 27005 y NIST SP 800-30 rev 1. Aplica este método en un análisis de caso enfocado a una entidad con fines de lucro, ofreciendo etapas exhaustivas del proceso.
Análisis de Resultados
Se puede utilizar las técnicas combinada tanto en organizaciones e instituciones con y sin fines de lucro, con una explicación paso a paso del proceso de evaluación de riesgos en cada una de sus etapas. El artículo demuestra cómo implementar esta técnica en la práctica.
ID ART. → Art. 04
Objetivo del Estudio

Analizar y comparar las metodologías existentes para la evaluación de riesgos de seguridad de la información en instituciones financieras, destacando sus características, ventajas y desventajas.
Resumen
El proyecto revisa diversas metodologías de evaluación de riesgos de seguridad de la información, el documento enfatiza que la norma ISO/IEC 27005 contiene una metodología detallada de evaluación de riesgos y suele utilizarse para formarse una idea general de la organización del proceso de gestión de riesgos para la seguridad de la información. El procedimiento de evaluación de riesgos para la seguridad de la información se consagra a la Guía de Evaluación de Riesgos NIST 800-303. A diferencia de la norma ISO/IEC 27005, el documento NIST 800-30 sólo tiene carácter consultivo y contiene una descripción más detallada de los procedimientos de evaluación de riesgos, así como recomendaciones prácticas.
Análisis de Resultados
En el artículo el autor señala que las entidades financieras optan por la certificación ISO para obtener un reconocimiento mundial. En el marco de la evaluación de los riesgos para la seguridad de la información, se evalúa el valor de los activos, se identifican las amenazas y vulnerabilidades actuales, se analizan los medios de protección y se evalúan las consecuencias de la materialización de los riesgos.
ID ART. → Art. 05
Objetivo del Estudio
Evaluar la situación actual de la ciberseguridad en el sector financiero y analizar la efectividad de los sistemas de detección de intrusiones (IDS) en la protección de los activos de las instituciones financieras, cumpliendo con las regulaciones europeas.
Resumen
El artículo destaca al hacer referencia y emplear diversas metodologías de administración de riesgos, entre las que se incluyen ISO 27005 y OCTAVE. En relación con la ISO 27005 indica que la determinación del riesgo puede realizarse de manera cuantitativa, cualitativa o ambas.

La tesis trata los retos de ciberseguridad en el ámbito financiero, resaltando la aplicación de sistemas de detección de intrusiones (IDS) para salvaguardar los bienes esenciales. Además, en relación con OCTAVE, indica que fomenta un enfoque autónomo en la administración de riesgos, dado que puede ajustarse a las necesidades y riesgos específicos de una organización. La determinación del riesgo se fundamenta en valores probabilísticos y valores de consecuencia.
Análisis de Resultados
La gestión de riesgos de seguridad de la información basada en la norma 27005 consta de subprocesos, uno de ellos es establecer el contexto que se refiere a la especificación de la evaluación y aceptación de los criterios de riesgo, alcance y límites para la evaluación de riesgos, seguido de la identificación del riesgo que incluye la identificación de activos, amenazas, controles, vulnerabilidades e impacto. Se utilizan metodologías de gestión de riesgos como ISO 27005 y OCTAVE para estructurar y evaluar los riesgos de manera efectiva. Hay cuatro opciones de tratamiento del riesgo: modificación del riesgo, retención del riesgo, evitación del riesgo y distribución del riesgo. Los resultados muestras que tanto los sistemas de detección de intrusiones que se basan en host como los basados en red son eficientes en el reconocimiento y reducción de ataques cibernéticos habituales en las entidades financieras.
ID ART. → Art. 06
Objetivo del Estudio
El objetivo de este artículo es identificar las áreas vulnerables en la infraestructura de ciberseguridad existente del Banco de Bangladesh y proponer intervenciones para abordar diferentes escenarios de riesgo en el sistema de ciberseguridad del banco, especialmente a la luz del reciente robo de dinero en 2016.
Resumen
El artículo se centra en analizar el ataque cibernético que ocurrió en el Banco de Bangladesh en 2016, el cual es considerado uno de los robos de dinero más grandes de la historia. El estudio realiza un análisis de los interesados y las legislaciones pertinentes, destacando la necesidad de

fortalecer el marco legislativo. Analiza las debilidades del sistema de ciberseguridad del banco y propone recomendaciones para mejorar la seguridad. La gestión de riesgos para la seguridad de la información debe considerarse una parte esencial de todas las actividades, debe ser una parte integral de una gestión de riesgos. El autor enfatiza que la ISO 27005, es un enfoque sistemático que se ocupa de la gestión de riesgos de seguridad de la información de una organización en su conjunto o de cualquier parte diferenciada de la organización.
Análisis de Resultados
Los resultados del análisis de riesgos cualitativo realizado muestra varias áreas críticas de vulnerabilidad en la infraestructura de ciberseguridad del Banco de Bangladesh lo que provocaron que ocurra dicho ataque. Se reconocieron y otorgaron prioridad a los riesgos habituales, y se sugirieron sugerencias para atenuar los impactos negativos de los ataques cibernéticos. Se destacó la importancia de una colaboración efectiva entre los interesados y la necesidad de actualizar y fortalecer las legislaciones existentes.
ID ART. → Art. 07
Objetivo del Estudio
Diseñar un prototipo de seguridad aplicado a la gestión empresarial para mitigar riesgos, vulnerabilidades y amenazas a la información, garantizando la integridad de los datos.
Resumen
El artículo aborda los problemas de seguridad de la información en instituciones públicas y privadas, proponiendo un prototipo de seguridad que utiliza varias metodologías de gestión de riesgos. Este prototipo está diseñado para identificar, evaluar y mitigar riesgos, vulnerabilidades y amenazas en sistemas de información. Para lo cual se aplicó un modelo de seguridad basado en la metodología MAGERIT para adaptar el prototipo de mitigación. Esto facilitó que el sistema identificara las vulnerabilidades, amenazas y riesgos que pudieran surgir en los sistemas de información, para tener seguridad en los datos.

Análisis de Resultados
El análisis de riesgos cualitativo y cuantitativo realizado reveló varias áreas críticas de vulnerabilidad en la infraestructura de ciberseguridad. Se desarrolló un modelo conceptual y un prototipo de seguridad. Primera fase: Aquí encontramos los activos que posee la organización y las bases de datos donde se almacenarán los datos. Segunda fase: Se identifican las vulnerabilidades y amenazas que dan lugar a que se generen riesgos en los sistemas de información. Tercera fase: Si existen riesgos, deben ser analizados y categorizados por niveles (leve, bajo, normal, alto y crítico), con el fin de implementar estrategias de mitigación de riesgos priorizando los riesgos que requieren atención urgente. Cuarta fase: Finalmente, el prototipo indica que se debe generar un plan de acción para llevar a cabo las estrategias de mitigación. Una vez implementado el plan de acción, éste debe ser monitoreado, para verificar que se esté llevando a cabo correctamente, evitando la pérdida de información.
ID ART. → Art. 08
Objetivo del Estudio
Analizar las brechas de datos en las redes de mensajería financiera, como SWIFT, y proponer un enfoque basado en la gestión de riesgos para mejorar la ciberseguridad en el sector bancario internacional.
Resumen
El autor analiza diversas vías para que los bancos adopten nuevas mentalidades en materia de ciberseguridad e incorporen mecanismos de gobernanza a sus procesos de gestión de riesgos en lo que respecta al control de la seguridad, la retención de datos y la supervisión continua. Se sugiere un método fundamentado en la administración de riesgos, incorporando el marco de administración de riesgos del NIST, con el objetivo de robustecer la seguridad en las redes de comunicación financiera.
Análisis de Resultados

El estudio de los sucesos en el sistema SWIFT revela que las lagunas de seguridad se originan por malas prácticas de seguridad y la ausencia de implementación de normas sólidas. La incorporación del NIST RMF a los sistemas de seguridad de SWIFT puede ofrecer un avance notable en la defensa frente a ataques sofisticados y persistentes (APT). En el contexto de la gestión de riesgos (NIST RMF), se utilizó la metodología NIST SP 800-30 para valorar y potenciar la seguridad informática en las entidades financieras.
ID ART. → Art. 09
Objetivo del Estudio
El autor investiga una institución internacional de servicios de consultoría de TI que es responsable de la implementación de proyectos y de inserción de asistencia empresarial a gran escala. Demuestra el marco de gestión de riesgos y la estructura administrativa de las situaciones apropiadas para que sus procedimientos sean adecuados y también alineados con los lineamientos fundados por la norma ISO 27001.
Resumen
A través de un estudio de caso de una consultora internacional, se analiza el marco de gestión de riesgos y la estructura administrativa necesaria para lograr el cumplimiento con la norma ISO 27001. El artículo menciona tanto la norma ISO 27005 como la NIST SP 800-30 en el contexto de la gestión de riesgos en la seguridad de la información. Sobre la norma ISO 27005 se menciona como un estándar que puede utilizarse para la gestión de riesgos en seguridad de la información dentro del contexto de la norma ISO 27001. También se señalan que las normas ISO 27005 puede combinarse con otras herramientas de ciberseguridad NIST SP 800-30 con lo que se buscar crear un mejorar la capacidad de evaluación de riesgos.
Análisis de Resultados
En esta investigación el articulo resalta que se pueden complementar la ISO 27005 con la NIST SP 800-30 con el objetivo de obtener enfoque más completo para la gestión y evaluación de riesgos en el ámbito de la seguridad de la información. Mientras que la ISO 27005 se enfoca en

proporcionar directrices para la gestión de riesgos dentro del contexto de la ISO 27001, la NIST SP 800-30 ofrece un enfoque detallado para la evaluación de riesgos, lo cual es útil para identificar y mitigar riesgos específicos en sistemas de información.

ID ART. → Art. 10

Objetivo del Estudio

Este trabajo propone implementar una metodología de seguridad basado en OCTAVE-S para los servicios digitales de la banca móvil entre los bancos comerciales en la República Democrática del Congo (RDC). Para ello se identificó la información crítica de la entidad, las amenazas a los activos esenciales de los sistemas de información, las vulnerabilidades de la infraestructura y los riesgos, y proponiendo estrategias de protección y mitigación.

Resumen

Este artículo aborda las brechas de seguridad en los marcos de seguridad de la banca móvil, especialmente en economías en desarrollo como la RDC. Utilizando la metodología OCTAVE-S, el autor creó un marco de seguridad que se adapta a las necesidades de los bancos comerciales en la RDC. Se justifica que el uso de OCTAVE-S es debido a su aplicabilidad en entidades con recursos limitados en seguridad de la información.

Análisis de Resultados

En los resultados detallan la metodología de seguridad adaptado a la banca móvil en la RDC, basado en la metodología OCTAVE-S. Esta metodología permite a los bancos identificar y evaluar de manera efectiva los riesgos de los sistemas de información, así como desarrollar estrategias de mitigación convenientes.

Metodologías mencionadas:

- **OCTAVE-S:** Esta metodología es principal en el artículo para evaluar y gestionar los riesgos de seguridad en la banca móvil en la RDC. Su aplicación se enfoca principalmente en la protección de la confidencialidad, integridad y disponibilidad de los activos críticos de información.

ID ART. → Art. 11
Objetivo del Estudio
En ese artículo se evaluaron varios métodos de riesgo de seguridad de la información en el contexto de la computación en la nube, destacando su aplicabilidad y adaptabilidad de algunas metodologías vigentes.
Resumen
Como objetivo del trabajo se destaca el análisis de las amenazas y los riesgos de seguridad en la computación en la nube, utilizando esquemas de clasificación reconocidos, como la triada de CIA (Confidencialidad, Integridad, y Disponibilidad), en este contexto se realizó una comparación de metodologías de evaluación de riesgos como NIST SP 800-30, ISO 27005, CRAMM, CORAS, OCTAVE Allegro y COBIT 5, los resultados del trabajo indican que OCTAVE Allegro como la que más destaca en sus beneficios de aplicación para el almacenamiento en la nube.
Análisis de Resultados
Los resultados del estudio demuestran que OCTAVE Allegro se destaca por su aplicabilidad y facilidad de implementación en entornos dinámicos como es el almacenamiento en la nube.

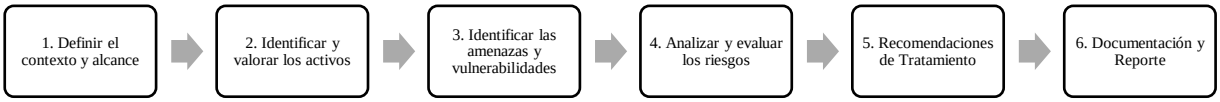
Para concluir, el presente trabajo recomienda realizar un análisis de gestión de riesgos en el área de sistemas de la COAC Metrópolis LTDA., utilizando características de la norma ISO 27005 y otras bondades de la metodología MAGERIT. La propuesta de fusionarlas se fundamenta en que ISO 27005 ofrece una estructura clara reconocida a nivel internacional para identificar y manejar riesgos en la seguridad de la información, mientras que MAGERIT ofrece un análisis más exhaustivo de los activos, amenazas y vulnerabilidades dentro del ambiente informático de la cooperativa, donde permite también aplicar durante el desarrollo del análisis la herramienta PILAR, esta fusión genera una herramienta útil y adaptable, acorde con las exigencias de la Superintendencia de Economía Popular y Solidaria (SEPS), que puede adaptarse a las particularidades de cualquier entidad, independientemente de su magnitud, reforzando significativamente la seguridad de la misma información.

1.2. Fases de la metodología que integra ISO 27005 y MAGERIT

La metodología propuesta integra los principios normativos de ISO 27005 y las herramientas de MAGERIT, mediante el cual se crea una fusión que maximiza sus fortalezas respectivas. Por un lado, ISO 27005 aporta un marco estructurado y reconocido internacionalmente para la gestión de riesgos. Por otro lado, MAGERIT proporciona una metodología detallada para la identificación y análisis de riesgos, complementada con herramientas específicas como PILAR para identificar los activos, amenazas y salvaguardas, lo que facilita la personalización y aplicación práctica del análisis de riesgos en la cooperativa.

Mientras ISO 27005 establece las bases para definir el alcance, evaluar los riesgos y tomar decisiones estratégicas, MAGERIT enriquece el proceso con técnicas avanzadas de valoración y categorización, asegurando una evaluación detallada y accionable. A continuación, se detalla la metodología propuesta:

Figura 1 Fases de la metodología del proyecto



Esta metodología híbrida combina la estructura y enfoque normativo de ISO 27005 con las herramientas prácticas y detalladas de MAGERIT.

1.2.1. Fase 1.- Definir el contexto y alcance

Como se establece en la norma ISO 27005 primero se debe establecer el contexto, este paso se trata de establecer los objetivos y criterios para la gestión de riesgos de seguridad de la información.

1.2.2. Fase 2.- Identificar y valorar los activos

Para identificar los riesgos, este proyecto trabaja con un enfoque basado en activos, por ello se identifica los activos relevantes para la Cooperativa Metrópolis, asignándoles un valor basado en su importancia para los procesos de negocio y la confidencialidad, integridad y disponibilidad de la información.

1.2.3. Fase 3.- Identificar las amenazas y vulnerabilidades

En esta fase se considera diferentes escenarios y responde preguntas del tipo "¿qué pasaría sí?" para identificar las amenazas y riesgos a los que están expuestos los activos de la cooperativa.

1.2.4. Fase 4.- Analizar y evaluar los riesgos

En esta fase se realiza una evaluación detallada de los riesgos mediante la combinación de la probabilidad de ocurrencia de las amenazas y su impacto sobre los activos críticos. Para ello, se emplean matrices de riesgo y herramientas especializadas como PILAR, que permiten cuantificar los riesgos de forma precisa y estructurada, asegurando una visualización clara de las prioridades y áreas de atención.

1.2.5. Fase 5.- Recomendaciones de Tratamiento

Proporciona sugerencias de medidas de mitigación o tratamiento de los riesgos identificados, alineadas con las mejores prácticas de seguridad y las necesidades de la organización.

1.2.6. Fase 6.- Documentación y Reporte

Registra todo el proceso de análisis, desde la identificación hasta la evaluación de riesgos, y genera un informe comprensible para la toma de decisiones estratégicas.

1.3. Desarrollo teórico y conceptual

1.3.1. Antecedentes

(Barragán, 2019) considera que las instituciones financieras tienen la responsabilidad con la sociedad, sobre todo porque la comunidad ha depositado su confianza en estas instituciones para guardar sus recursos económicos provenientes de sus trabajos, ahorros, etc. Por lo cual indica la importancia de aplicar medidas para resguardar de forma confiable la información. La parte tecnológica no puede quedar aislada, por lo que es necesario que las entidades incorporen dentro de sus análisis de riesgos, los mecanismos necesarios para mitigar y controlar los riesgos pertinentes a la tecnología. Concluye en la necesidad de que las entidades financieras consideren dentro de su análisis de riesgos, al riesgo informático.

(Maldonado, 2013) resalta que, desde sus inicios, los sistemas informáticos se han visto involucrados en diferentes riesgos por no poseer seguridades ya sea en los recursos

humanos, técnicos, de infraestructura, organizativos entre otros. Para evitar los efectos de la inseguridad se debe implementar un análisis y gestión de riesgos informáticos que permita ayudar a la realización de los objetivos de la organización.

(Abril et al., 2013) consideran que, en la actualidad, uno de los factores más importantes que se debe tener en cuenta en todo tipo de organizaciones es la seguridad de la información, puesto que los incidentes relacionados con ésta comprometen los activos de las empresas y las ponen en riesgo.

En (Santos-Olmo et al., 2024) consideran que la sociedad de la información depende cada vez más de los sistemas de evaluación y gestión de riesgos como medios para proteger adecuadamente sus activos de información clave. La disponibilidad de estos sistemas es hoy vital para la protección y evolución de las empresas. Sin embargo, varios factores han llevado a una creciente necesidad de enfoques de análisis de riesgos más precisos.

El concepto de gestión de la seguridad surgió como solución en un intento de mejorar la seguridad de la información de las empresas. Las vulnerabilidades cibernéticas plantean riesgos corporativos significativos, como interrupción de negocios, violación de la privacidad y pérdidas financieras (Cremer et al., 2022).

Por lo cual se considera importante crear un enfoque basado en la correcta gestión de riesgos, ya que la gestión de riesgos es un proceso esencial en cualquier modelo de gestión empresarial, y todas las actividades esenciales de una entidad implican riesgos, por tanto, una evaluación de riesgos eficaz ayuda a la alta dirección de una organización a tomar decisiones óptimas y evitar pérdidas. Por ello, es necesario seleccionar e implementar salvaguardas con el fin de conocer, prevenir, impedir, reducir o controlar los riesgos identificados (Shameli-Sendi, 2020).

De acuerdo con lo señalado, la COAC Metrópolis por considerarse una entidad financiera presenta la necesidad de realizar un análisis de riesgos para minimizar así consecuencias no deseadas.

1.3.2. ISO 27005

Por su impacto en los negocios, ISO 27005, norma internacional que maneja el proceso de Gestión de Riesgos de Seguridad de la Información (ISRM), es el documento que fue desarrollado y publicado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) para apoyar a las organizaciones de todo el

mundo a gestionar los riesgos cibernéticos. La primera versión de esta norma se publicó en 2008 y su última versión en 2022 (Cerqueira Junior & Arima, 2023).

La norma ISO 27005 sirve de guía exhaustiva para gestionar los riesgos de seguridad de la información. Esta norma se aplica a todas las organizaciones, tales como empresas comerciales, agencias gubernamentales y organizaciones sin ánimo de lucro que tengan la intención de gestionar los riesgos que pueden comprometer la seguridad de la información de la organización (I. M. M. Putra & Mutijarsa, 2021).

El marco proporcionado por la norma ISO 27005 es versátil y aplicable a diversas estructuras organizativas (Flores & Perugachi, 2023). Tanto si se trata de una corporación con ánimo de lucro como de un organismo gubernamental o una entidad sin ánimo de lucro, cualquier organización que pretenda hacer frente a posibles amenazas para su seguridad de la información puede beneficiarse de esta norma.

1.3.3. MAGERIT

El Consejo Superior de Administración Electrónica desarrolló MAGERIT. Esta iniciativa surgió del progresivo reconocimiento de que tanto la administración pública como la sociedad en general dependen cada vez más de las tecnologías de la información para cumplir sus objetivos en sus actividades diarias (Ferruzola Gómez et al., 2019).

La metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) proporciona un marco de gestión estructurado para el análisis y la gestión de riesgos de sistemas de información, alineándose con la norma ISO 27005. Su característica distintiva es la modelización de activos y sus dependencias, lo que permite calcular valores de degradación mediante impactos. La metodología abarca identificación de activos, valoración de amenazas, cálculo de riesgos y establecimiento de salvaguardas para mitigar riesgos residuales, combinando análisis cualitativos y cuantitativos para una gestión integral y personalizada (*Comparison between MONARC and Different Risk Management Methods*, n.d.).

El objetivo central de Magerit está vinculado a la adopción generalizada de las tecnologías de la información. Aunque esta integración tecnológica ofrece numerosas ventajas a los usuarios, también introduce riesgos potenciales. Estos riesgos hacen necesaria la aplicación de medidas de seguridad para generar confianza en los sistemas.

La metodología es especialmente valiosa para las personas y organizaciones que manejan información digital y utilizan sistemas informáticos para el tratamiento de datos. Proporciona un marco para identificar, evaluar y mitigar los riesgos asociados al uso de las tecnologías de la información.

Magerit pretende lograr un equilibrio entre el aprovechamiento de las ventajas de las TI y la minimización de los riesgos asociados. De este modo, contribuye a crear un entorno digital más seguro y fiable tanto para el sector público como para el privado.

Comprender los riesgos potenciales a los que se enfrentan los distintos componentes operativos es un requisito previo crucial para una gestión eficaz. Este conocimiento constituye la base para aplicar estrategias adecuadas de mitigación de riesgos y tomar decisiones con conocimiento de causa.

1.3.4. Objetivos de Magerit

Magerit persigue los siguientes objetivos (Amutio et al., 2012):

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

1.3.5. Herramienta PILAR

"Procedimiento Informático Lógico para el Análisis de Riesgos", PILAR, es un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) ((CCN), 2019) cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Se actualizan periódicamente y existen diversas variantes. Creado por el Centro Nacional de Inteligencia (María Fernanda Molina-Miranda, 2017).

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para tratar el riesgo se proponen: salvaguardas o

contramedidas, normas y procedimientos de seguridad. Esta herramienta soporta las fases del método MAGERIT (María Fernanda Molina-Miranda, 2017):

- Caracterización de los activos: identificación, clasificación, dependencias y valoración.
- Caracterización de las amenazas.
- Evaluación de las salvaguardas

Evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de porqué se da cierto impacto o riesgo.

PILAR puede interpretar los niveles de madurez, bien como madurez o como el estado de la implementación de las salvaguardas. Es decir, se presenta un texto u otro junto a los niveles L0 a L5.

Tabla 4 Niveles de madurez

Nivel	Madurez	Estado
L0	inexistente	inexistente
L1	inicial / ad hoc	iniciado
L2	reproducible, pero intuitivo	parcialmente realizado
L3	proceso definido	en funcionamiento
L4	gestionado y medible	monitorizado
L5	optimizado	mejora continua

FUENTE: PILAR

1.3.6. Inventario de activos

En el contexto de una organización, un activo representa cualquier elemento que tenga valor o sirva a un propósito útil para las operaciones y la continuidad del negocio de la entidad (Dave et al., 2023). Dada su importancia, los activos requieren protección para garantizar el buen funcionamiento de la organización y salvaguardar la conservación de sus operaciones.

Los activos de información, en particular, abarcan una amplia gama de elementos. Es crucial disponer de definiciones claras y conceptuales de estos activos para llevar a cabo un análisis y una evaluación de riesgos precisos (Ferruzola Gómez et al., 2019).

El proceso de identificación y evaluación de activos debe ser un esfuerzo de colaboración. Requiere la aportación de un equipo diverso compuesto por personas implicadas en varios procesos y subprocesos dentro del ámbito del modelo de gestión de riesgos.

Particularmente importante es la inclusión de los propietarios de activos clave en este grupo multidisciplinar.

Un propietario de activos se define como un individuo que tiene la responsabilidad de supervisar el mantenimiento, la utilización y la seguridad de activos específicos. Este papel suele estar sancionado por la dirección de la organización.

La participación de los propietarios de los activos y de otras partes interesadas en el proceso de identificación y evaluación garantiza una comprensión exhaustiva del valor de los activos y de los riesgos potenciales, permitiendo así estrategias de gestión de riesgos más eficaces.

1.3.7. Seguridad de la información

El objetivo de la seguridad de la información es garantizar la continuidad de la actividad empresarial y minimizar los daños a la empresa limitando el impacto de los incidentes de seguridad (Von Solms & Van Niekerk, 2013).

1.3.8. Importancia de la seguridad de la información en las organizaciones

En lo que respecta a la seguridad de la información, se busca salvaguardar la confidencialidad, integridad y disponibilidad de los datos mediante la implementación de procedimientos de gestión de riesgos, asegurando así que la información esté protegida contra accesos no autorizados, divulgaciones, alteraciones, destrucciones e interrupciones (AL-Dosari & Fetais, 2023). La gestión de riesgos implica la identificación, evaluación y control de las amenazas a los activos digitales de las organizaciones, incluyendo información, redes y sistemas. La evaluación de riesgos, parte esencial de este proceso, consiste en identificar peligros, vulnerabilidades y vectores de amenazas, así como en evaluar el impacto y la probabilidad de los riesgos identificados, proporcionando una base para la toma de decisiones en la mitigación de riesgos.

Las amenazas adversas se definen como peligros que surgen de personas u organizaciones que buscan explotar la dependencia de los sistemas de información y los recursos de información. Estas personas pueden ser externas o internas. Las amenazas accidentales provienen de acciones equivocadas realizadas por usuarios individuales o administradores por la falta de cultura de seguridad de la información en la institución.

1.3.9. Desarrollo de una cultura de seguridad de la información

El desarrollo de una cultura organizativa puede servir de referencia para determinar cómo se desarrolla una cultura de la seguridad de la información. Una cultura organizativa se desarrolla cuando los ejecutivos y la dirección desarrollan una visión y una estrategia para la organización. La visión y la estrategia a menudo se plasman en políticas y procedimientos organizativos (da Veiga & Martins, 2017). El comportamiento de los empleados se hará evidente guiado por la visión, la estrategia y las políticas. Con el tiempo surge una cultura organizativa que engloba la visión y la estrategia, así como las experiencias de los empleados a la hora de aplicarlas. Un componente de cultura de seguridad de la información se desarrolla en una institución del mismo modo que la cultura organizativa.

1.3.10. Superintendencia de Economía Popular y Solidaria (SEPS)

La SEPS es una entidad del Estado ecuatoriano que tiene como misión regular, controlar y supervisar a las entidades del sector de la economía popular y solidaria. Entre sus funciones se encuentran (seps.gob.ec, 2024):

- Controlar el cumplimiento de la normativa legal y reglamentaria del sector.
- Promover el desarrollo del sector de la economía popular y solidaria.
- Brindar asistencia técnica y capacitación a las entidades del sector.

1.3.11. Desafíos y particularidades de la seguridad de la información en las cooperativas

La transformación digital del sector de cooperativismo es un reto que ha tomado la Superintendencia de Economía Popular y Solidaria (SEPS) menciona Cristian Aguirre, Director Nacional de Seguridad de la Información de la SEPS el 18 de enero del 2023 a la Revista IT de Ecuador, dice que como entidad de control busca el fortalecimiento y correcto funcionamiento de las entidades bajo su ámbito, generado varios mecanismos para que las entidades trabajen en beneficio de sus socios, al ofertar servicios financieros de calidad en términos de su acceso y uso. Para el sector es fundamental robustecer sus procesos digitales y es así que el 52 % de las entidades considera que sus servicios financieros digitales ya han alcanzado su nivel de madurez y una cobertura en 210 cantones del país, de los 221 (IT, n.d.).

Por otra parte, la Superintendencia de Economía Popular y Solidaria (SEPS), reconociendo la importancia de que los productos financieros y los procesos desarrollados y ejecutados por las entidades bajo su supervisión generen confianza, ha establecido la Norma de Control sobre seguridad de la información. Esta normativa no solo busca que las cooperativas implementen controles de seguridad, sino que también fomenten una cultura de seguridad de la información y protección de sus activos. En este sentido, la Norma establece que las cooperativas clasificadas en los segmentos 4 y 5 deben contar con un responsable de seguridad de la información y ciberseguridad; aquellas en el segmento 3 deben tener un oficial de seguridad de la información; mientras que las entidades en los segmentos 1 y 2 deben contar con una dirección de seguridad de la información (Hernández, 2022). El propósito de esta disposición es que dicho personal brinde apoyo, impulse y fortalezca los procesos en las entidades, implementando medidas de control, evaluación, capacitación, entre otras, y que la seguridad de la información sea un aspecto transversal en la asesoría sobre temas de seguridad de la información, ciberseguridad y protección de datos.

1.3.12. Amenazas Cibernéticas

Las entidades financieras, como la COAC Metrópolis LTDA., debido a la información sensible que se maneja son un objetivo atrayente para los ciberdelincuentes, las amenazas más comunes a los que se podría enfrentar la entidad incluyen (Safonova et al., 2020):

- Ataques de *malware*; Los ataques de malware, como el *ransomware*, pueden infectar los sistemas informáticos y encriptar sus datos, impidiendo el acceso a la información (Alsulami et al., 2017).
- Ataques de *phishing;* Los ataques de *phishing* intentan engañar a los usuarios para que revelen sus datos personales o financieros (Patil & Dhage, 2019).
- Ataques de denegación de servicio (DoS); Los ataques DoS (C. Liu et al., 2023) pueden atacar a los servidores con tráfico falso, lo que puede impedir que los usuarios legítimos accedan a los servicios (Wylde et al., 2022).

1.3.13. Norma de control respecto a la seguridad de la información en las entidades del sector financiero, popular y solidario bajo control de la Superintendencia de Economía Popular y Solidaria

La norma tiene por objetivo regular los niveles mínimos para la administración de seguridad de la información que las entidades deben implementar con la finalidad de resguardar y proteger los activos de información. Para efectos de la norma se aplican por regímenes, en el caso de la COAC Metrópolis por ser segmento 3 se cataloga como Régimen especial (Hernández, 2022).

En el art 14 de esta norma se indica que el régimen especial de seguridad de la información lo conforman:

a. El Consejo de Administración y El Gerente General o Representante Legal
b. El Comité de Seguridad de la Información (CSI) y El Oficial de Seguridad de la Información (OSI)

Por su parte el CSI de la COAC Metrópolis de acuerdo con la norma deberá conformarse por los siguientes miembros:

a. El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente
b. El Gerente General o Representante Legal
c. El OSI, quien actuará como secretario del Comité
d. El responsable del área de tecnología o su delegado
e. Un delegado de Auditoría Interna.

Además, en el art. 18 se enfatizan los requisitos obligatoritos que debe cumplir la COAC Metrópolis, los cuales se detallan a continuación:

a. Asignación de recursos humanos, técnicos y financieros para seguridad de la información;
b. Plan de Gestión de Riesgos de Seguridad de la Información;
c. Plan de Concienciación y Formación para Seguridad de la Información;
d. Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
e. Clasificación e identificación de tipos de información críticos o sensibles con criterios de integridad confidencialidad y disponibilidad

f. Identificación de activos de información, tomando en cuenta que contendrá;
    1. Personas y procesos agregadores de valor y/o catalogados como sensibles o críticos;
    2. Unidades de las entidades y empresas intervinientes en los procesos;
    3. Infraestructura tecnología;
    4. Ubicaciones físicas y puntos de atención, oficina matriz, sucursales, agencias, puntos móviles, corresponsales solidarios
    5. Relaciones con personas naturales y/o jurídicas que pudieren acceder a información crítica o sensible.

En el art. 20 de esta normativa se detallan las responsabilidades en la gestión de seguridad de la información, la COAC Metrópolis debe cumplir con lo descrito a continuación;

- Consejo de Administración o Directorio:
    a. Aprobar la asignación de los recursos humanos, técnicos y financieros que sean necesarios;
    b. Aprobar los planes de concienciación y formación concernientes a seguridad de la información
    c. Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información
- Comité de Seguridad de la Información (CSI), deberá proponer al consejo de administración:
    a. La asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información
    b. Las políticas, procedimientos, roles y responsabilidades para la gestión de seguridad de la información
    c. Los Planes de Concienciación y Formación concernientes a seguridad de la información
    d. El Plan de Gestión de Riesgos de seguridad de la información

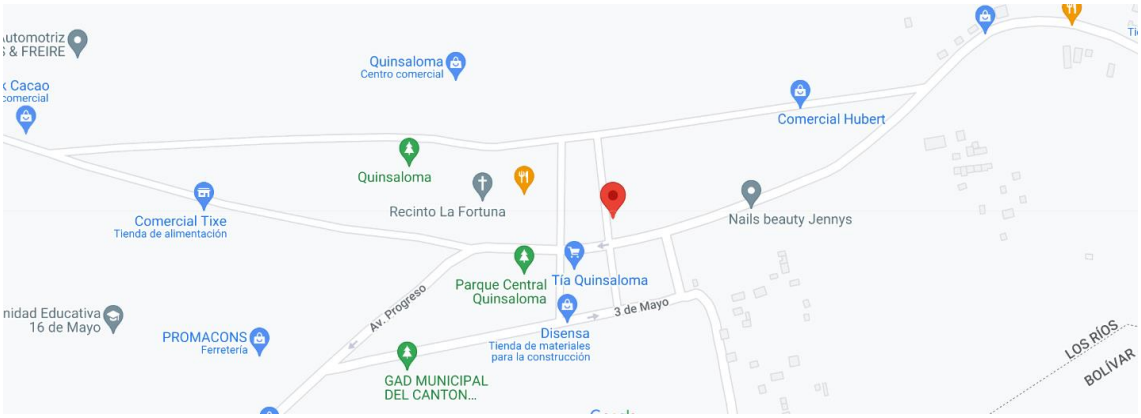
Para la gestión de riesgo la SEPS indica en la norma que se debe incluir los criterios básicos señalados por la ISO/IEC 27000, se refiere a la Norma Técnica emitida por el Servicio Ecuatoriano de Normalización, INEN, NTE INEN-ISO/IEC 27000 Cuarta edición 2016-1 1 TECNOLOGÍAS DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN – DESCRIPCION GENERAL Y VOCABULARIO (ISO/IEC 27000:2016, IDT)

CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

Para llevar a cabo el desarrollo del proyecto, se realizó un proceso de recolección de datos en la oficina matriz de la Cooperativa Metrópolis, ubicada en el Cantón Quinsaloma, provincia de Los Ríos. Esta oficina se encuentra en la Avenida Progreso, vía Moraspungo.

Figura 2 Localización de COAC METRÓPOLIS



FUENTE: GOOGLE MAPS

2.2. Diseño y alcance de la investigación

La implementación de este trabajo implica el uso de investigación exploratoria y descriptiva. Este proceso de investigación permitió crear una base sólida para el desarrollo del proyecto. La primera se utiliza para identificar las diferentes herramientas y técnicas necesarias para ejecutar las fases del desarrollo del proyecto, esto incluye la revisión de proyectos relacionados con seguridad de la información en diversas instituciones, así como la recopilación de información sobre los activos de información, se llevó a cabo una revisión de artículos científicos en revistas indexadas y de sitios web especializados en seguridad de la información que contienen trabajos relevantes sobre análisis de riesgos.

En cuanto a la investigación descriptiva, se llevó a cabo una evaluación de la metodología propuesta para determinar su efectividad, esta evaluación permitirá identificar mejoras en el área de TI. A través de esta evaluación, también se puede destacar características importantes para mitigar los riesgos, como su usabilidad, lo que proporciona información valiosa para su optimización y aplicación efectiva en el contexto del proyecto.

2.3. Identificación de los Activos

Se realizaron reuniones en la identificación de los activos, estas reuniones incluyeron delegados de cada uno de los departamentos clave de la cooperativa tales como la Gerencia, Finanzas, Riesgos, TIC y el Área Jurídica, con la finalidad de efectuar la identificación de activos. Gracias a este método fue posible la identificación de los activos esenciales para el funcionamiento seguro de la cooperativa, ya que se llevó a cabo un estudio detallado de los procesos y recursos empleados, garantizando que se escogieran aquellos componentes de mayor relevancia en la protección de la información y la continuidad de las operaciones. La lista de activos está compuesta software, hardware, servicios y personal, los cuales se encuentra agrupados según su importancia y función en la cooperativa.

2.4. Alcance del Análisis de riesgo

Para la definición de los activos más críticos de la cooperativa, fue necesario implementar y utilizar una metodología integral que incluyó *focus groups*, se realizaron encuestas al personal de áreas claves. El análisis de riesgo se centró en los activos esenciales que sirven como pilares para la continuidad operativa del departamento de informática de la COAC Metrópolis.

La encuesta que se realizó fue diseñada para obtener la información clave sobre la criticidad y riesgos relacionados a cada una de las áreas críticas y activos esenciales (Ver Anexo 2), gracias a esto se pudo priorizar los recursos de áreas como TICs, Gerencia, Finanzas, Riesgos y Legal, los cuales poseen un papel prioritario en la protección de los datos, mantenimientos activos y la continuidad operativa, esta información permitió establecer el alcance del análisis de riesgos, concentrando esfuerzos sobre la Confidencialidad, Integridad y Disponibilidad de aquellos activos cuya criticidad se basaba en su impacto en todas las actividades de institución financiera.

2.5. Tipo y métodos de investigación

Método analítico

Se dividieron cada uno de los activos de información en sus componentes esenciales mediante la utilización del Método Analítico, esto se hizo para comprender su valor, vulnerabilidades y riesgos asociados, este enfoque analítico ayuda a identificar la

prioridad de cada recurso y que acciones de protección se deben aplicar en función de la importancia y sensibilidad de cada activo.

Método inductivo

Gracias al método inductivo se logró en este proceso deducir los principios generales y la implementación de acciones preventivas para dar respuestas ante posibles incidentes. El uso del Método Inductivo en la seguridad de la información permite la observación sistemática de incidentes de seguridad previos en la cooperativa, con el objetivo de identificar las causas y las repercusiones que estas han tenido.

2.6. Población y muestra

En este presente proyecto, la población objetivo se encuentra conformada por cada uno de los trabajadores de la COAC Metrópolis LTDA los mismo que se encuentran directamente involucrados en los procesos de los activos seleccionados como esenciales dentro del contexto del análisis de riesgos.

Esta muestra se compone de empleados de pertenecientes a las áreas estratégicas de la cooperativa, como Gerencia, Tecnologías de la Información (TICs), finanzas, legal y el administrador de Riesgos. Esto asegura que el análisis de riesgos se lleve a cabo con el punto de vista correcto y con un enfoque completo en la seguridad de la información y la administración de riesgos.

2.7. Técnicas e instrumentos de recolección de datos

Con el objetivo de obtener una comprensión más completa, contextualizada y precisa de las prácticas y conocimiento en seguridad cibernética entre los colaboradores de la COAC Metrópolis LTDA. En este trabajo se propone implementar una metodología de desarrollo de análisis de riesgo híbrida que contemplen la necesidad de obtener y combinar técnicas cuantitativas y cualitativas con el objetivo de identificar tendencias generales y patrones útiles para obtener un entorno seguro y que, al mismo tiempo, ayude a explorar los contextos que influyen en estas tendencias al estado actual de la COAC.

2.8. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

Los instrumentos de investigación permiten recabar información clave sobre el tema de estudio. En este caso, se busca identificar y evaluar la percepción de las áreas críticas

respecto a la importancia, riesgos y necesidades de protección de los activos esenciales de COAC Metrópolis LTDA. Esta información será fundamental para cumplir con los objetivos de la investigación y respaldar el caso de estudio. Para ello, se aplica una encuesta que asegure la formalidad y relevancia del proceso de investigación.

Para la validación y confiabilidad de estos instrumentos, fue necesario buscar a un experto y/o especialista en temas referentes auditorias informáticas en cooperativas de ahorro crédito; quién los revisó, analizó, validó y aprobó (Ver Anexo 1).

De acuerdo con la valoración realizada por el Msc. Fernando Guzman Flores, consultor de tecnología y seguridad de la información, se obtuvieron las siguientes calificaciones de acuerdo con los criterios establecidos por el investigador; obteniendo como resultado un promedio final de 4 para la encuesta de 8 preguntas; lo cual significa que los instrumentos de investigación son válidos para este proceso investigativo.

Tabla 5 Validación de la encuesta

Indicadores	**Criterios o aspectos para considerar**	**Total**	**Promedio**
SUFICIENCIA	El instrumento está alineado con el objetivo de la investigación.	4	4
CLARIDAD	Las preguntas formuladas responden a la finalidad del estudio.	4	
COHERENCIA	Las preguntas guardan coherencia con el objetivo de la investigación.	4	
RELEVANCIA	La redacción de las preguntas es clara y está bien argumentada.	4	

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

3.1. Aplicación de Magerit con la herramienta PILAR

3.1.1. Identificación de activos

En esta sección se detallan los activos identificados en la Cooperativa Metrópolis. Para mayor identificación los activos se han clasificado en seis categorías, las cuales se especifican en el siguiente diagrama.

Figura 3 Categorías de activos

La identificación de activos se realizó con las personas del departamento de sistemas de la cooperativa que está conformado por dos colaboradores y la administradora de riesgos de la cooperativa. La administradora de riesgos forma parte del CAIR (Consejo de Administración Integral de Riesgos) quienes son los responsables de evaluar los procesos de todas las áreas de la cooperativa en materia de riesgos. A continuación, se describe el motivo por el cual se seleccionaron estas categorías de activos para el análisis de riesgos:

1. **Servicios:** Los activos de servicio como internet y el almacenamiento en la nube son claves para la administración de la información de la Cooperativa.
2. **Activos de Hardware:** En esta categoría se concentran activos como computadora o los servidores y centros de datos considerados como esenciales porque es donde se concentran la información financiera y de sus clientes.
3. **Activos de Software:** Esta categoría es importante para la gestión de la información que maneja la cooperativa. Entre los activos más significativos se encuentra el Core financiero junto con la aplicación web y móvil para clientes. Estos activos resultan fundamentales para la administración financiera y la prestación de servicios al cliente.
4. **Activos de Información:** Se consideran activos de esta categoría a la base de datos de clientes, documentos de políticas y procedimientos, debido a su alta sensibilidad y relevancia para el funcionamiento de la cooperativa.

5. **Personal:** Los colaboradores con acceso a información sensible y los administradores de sistemas representan activos cruciales, por cuanto gestionan y protegen la infraestructura tecnológica y los datos críticos de la cooperativa, es por ello que forman parte importante de este análisis de riesgo.
6. **Activos Físicos:** Los bienes materiales, tales como el edificio principal y el cuarto de servidores fueron seleccionados porque son esenciales para la gestión de los recursos y mantener la confidencialidad e integridad de la información con las seguridades físicas que se requieren por la entidad de control SEPS.

Identificar los activos es una tarea importante porque cada activo contribuye de manera positiva al desarrollo diario de las operaciones financieras de la Cooperativa Metrópolis. Para lo cual se realizó una reunión en la oficina matriz ubicada en el cantón Quinsaloma donde participaron las dos personas que son encargadas del departamento de sistemas y la administradora de riesgos, la reunión dio como resultado la identificación y valoración de los siguientes activos que fueron detallados de acuerdo a las categorías establecidas.

Los activos identificados fueron ingresados a la herramienta PILAR por cuanto el análisis de riesgos se realizó aplicando los parámetros de evaluación de la Metodología MAGERIT.

Figura 4 Activos de la COAC METROPOLIS

3.1.2. Valoración de activos

En la valoración de activos se asignó un valor de relación a la importancia para la operatividad de la cooperativa. Esta valoración se realizó en seis aspectos como la Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A), Trazabilidad (T) y Dependencia (DP). A continuación, se proporciona una descripción detallada de cada activo por categoría:

[S] Servicios

Figura 5 Valoración de los activos de la categoría [S] Servicios

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
[S] Servicios						
[S.1] Conexión a Internet	[A]	[M+]	[A]	[A+]	[A]	[A]
[S.2] Servicios en la Nube	[A-]	[M]	[A+]	[A]	[M]	[A]
[S.3] Servicios de Respaldo y Recuperación	[M+]	[A+]	[A+]	[A+]	[A]	[A]
[S.4] Soporte Técnico y Mantenimiento	[M-]	[B]	[B+]	[B+]	[B+]	[B]
[S.5] Servicios de Telefonía (fija y móvil)	[M-]	[B+]	[M]	[B+]	[M-]	[B+]
[S.6] Servicios de Correo Electrónico Corporativo	[M+]	[A]	[A+]	[A]	[M]	[A]

Resultados de valoración en categoría [S] Servicios:

[S.1] Conexión a Internet: La disponibilidad se valora como alta (A), debido a la importancia de este servicio para el funcionamiento diario de la cooperativa, puesto que se necesita este servicio para mantener una comunicación a las dos agencias con el servidor de aplicaciones donde se encuentra alojado el Core Financiero. También para realizar transacción de servicios no financieros en ventanilla de caja. Sin embargo, la integridad se califica como media-alta (M+), debido a posibles riesgos de manipulación de datos durante la transmisión.

[S.2] Servicios en la Nube: Este activo tiene una disponibilidad moderada (A-), lo cual refleja la dependencia de la infraestructura proporcionada por terceros. Aunque la confidencialidad se valora como alta (A+), la dependencia sigue siendo un punto crítico para considerar.

[S.3] Servicios de Respaldo y Recuperación: En estos servicios la disponibilidad y la integridad son valoradas como medias y altas (M+ y A+, respectivamente), debido al destacado rol de este servicio en el Plan de recuperación de desastres tecnológicos que también es considerado dentro de la normativa de la SEPS.

[S.4] Soporte Técnico y Mantenimiento: En este activo se valora como disponibilidad media (M-) y una confidencialidad baja (B+), lo cual indica que existe la necesidad de mejorar la estabilidad y la seguridad de estos servicios.

[S.5] Servicios de Telefonía (fija y móvil): El resultado de este activo tiene una disponibilidad media (M-) y una integridad baja (B+). Esta valoración es por cuanto la cooperativa no mantiene una comunicación telefónica conectada a las agencias. Es decir, únicamente se utiliza para comunicación interna en el edificio matriz ubicado en Quinsaloma. Para comunicare con las agencias se utiliza celulares móviles de propiedad de la cooperativa.

[S.6] Correo Electrónico Corporativo: Este activo es muy valioso porque es el medio de comunicación entre los colaboradores, proveedores externos o socios. La confidencialidad se valora como alta (A+), debido a los riesgos de interceptación y acceso no autorizado, mientras que la disponibilidad también es moderada (M+). La valoración tiene esos resultados porque los colaboradores de la cooperativa se comunican para entregar documentos a socios, proveedores o hacer negociaciones con otras entidades mediante este medio formalizado como normativa interna de la cooperativa. Por ello es muy valioso conservar la confidencialidad en el correo electrónico instruccional. Los colaboradores no pueden abrir sus correos institucionales en computadoras externas de la cooperativa.

[AH] Activos de Hardware

Figura 6 Valoración de los activos de la categoría [AH] Activos de Hardware

[AH] Activos de Hardware						
[AH.1] Servidores y Centros de Datos	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[AH.2] Equipos de Red	[A]	[A]	[A]	[A]	[A]	[A]
[AH.3] Computadoras de Escritorio y Laptops	[A]	[A-]	[M]	[M]	[M]	[M]
[AH.4] Sistemas de Alimentación Ininterrumpida	[M]	[B]	[B+]	[B+]	[B+]	[B+]
[AH.5] Impresoras y Escáneres	[B]	[B]	[B]	[B]	[B]	[B]

Resultados de valoración en categoría [AH] Activos de Hardware:

[AH.1] Servidores y Centros de Datos: Este activo también es esencial para la cooperativa Metrópolis. El resultado define una alta disponibilidad (A+), ya que son esenciales para la continuidad del negocio. La confidencialidad y la integridad también son altas, reflejando la necesidad de proteger este activo.

[AH.2] Equipos de Red: Los resultados reflejan que los equipos de red se categorizan como alta (A) en los seis aspectos, debido a la importancia de estos equipos para mantener toda la infraestructura de red operativa en todas las áreas de la cooperativa.

[AH.3] Computadoras de Escritorio y Laptops: Este activo tiene una integridad alta-baja (A-) y una confidencialidad media (M). Esto indica que se requieren mejoras en la protección de datos, porque se ha identificado que los colaboradores utilizan dispositivos de almacenamiento externo propios para transferir archivos como actas o informes.

[AH.4] Sistemas de Alimentación Ininterrumpida: El resultado de la valoración de este activo presente como resultado la Disponibilidad Media (M) puesto que son primordiales para mantener el funcionamiento de los servidores y computadoras, es decir la disponibilidad de este activo evita pérdidas de datos en caso de fallas eléctricas o cortes de energía.

[AH.5] Impresoras y Escáneres: El resultado de este activo es de menor impacto en la continuidad operativa, ya que la cooperativa puede trabajar sin estos dispositivos por un tiempo sin comprometer la operación principal.

[AS] Activos de Software

Resultados de valoración en categoría [AS] Activos de Software:

Figura 7 Valoración de los activos de la categoría [AS] Activos de Software

[AS] Activos de Software						
[AS.1] Sistema Core Financiero	[A+]	[A+]	[A+]	[A+]	[A]	[A+]
[AS.3] Sistemas de Seguridad y Autenticación	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[AS.2] Aplicacion web y movil para clientes	[A+]	[A+]	[A+]	[A+]	[A]	[A+]

[AS.1] Sistema Core Financiero: La función de este activo es realizar todas las operaciones de la cooperativa, es el software que permite el registro diario de las transacciones financieras. En los resultados se detalla que la disponibilidad tiene valoración Alta (A+) por cuanto cualquier interrupción puede afectar la capacidad de realizar transacciones financieras a los socios de la cooperativa. De igual manera la integridad, confidencialidad y autenticidad son aspectos considerados como altos debido a la información sensible que administra. El Core financiero es contratado por una empresa externa, es decir los responsables del departamento de sistemas no gestionan el código fuente, sin embargo, cualquier actualización debe ser autorizado por el jefe de sistemas.

[AS.3] Sistemas de Seguridad y Autenticación: Los resultados de este activo tienen valoración alta, debido a que la integridad de estos sistemas garantiza que la autenticación no sea alterada evitando vulnerabilidades de seguridad. Con ello se enfatiza que es necesaria la confidencialidad para evitar fugas de información crítica y por su parte la autenticidad permite que solo los usuarios con permisos accedan a la información requerida.

[AS.2] Aplicación web y móvil para clientes: Este activo fue desarrollado con la intención de mejorar el servicio para que los socios tengan disponible sus cuentas en cualquier horario del día. Por eso, se considera que caso de falla causaría malestar en los socios de la cooperativa, para este trabajo el resultado de la valoración es alta, también la disponibilidad es considerada como fundamental puesto que la falta de acceso podría afectar la confianza del cliente, mediante este medio realizan transferencias internas e interbancarias en cualquier hora y lugar, además es importante la autenticidad para garantizar que únicamente los usuarios con las credenciales registradas en la base de datos de la cooperativa puedan acceder a realizar las transferencias y con ello evitar fraudes.

[AI] Activos de Información

Resultados de valoración en categoría [AI] Activos de Información:

Figura 8 Valoración de los activos de la categoría [AI] Activos de Información

[AI] Activos de información						
[AI.1] Base de Datos	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[AI.2] Registros de Transacciones Financieras	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[AI.3] Documentos de Políticas y Procedimientos	[M]	[M]	[M]	[M]	[M]	[M]
[AI.5] Informes Financieros y Auditorías	[M+]	[A-]	[A-]	[M]	[M]	[M]

[AI.1] Base de Datos: En la base de datos se almacena todos los datos críticos de la cooperativa. La valoración en los seis aspectos es A+, es decir en todos los aspectos la base de datos es considerada como valiosa debido a la naturaleza sensible de la información almacenada como los registros financieros y registros contables.

[AI.2] Registros de Transacciones Financieras: La integridad de estos registros es crucial para garantizar que las transacciones no sean alteradas sin autorización, debido a que la pérdida o modificación de estos registros podría tener graves consecuencias financieras y legales. En este caso la trazabilidad es un factor importante debido a que se debe llevar

un registro de cada transacción para auditar que las operaciones financieras se estén almacenando de forma correcta.

[AI.3] Documentos de Políticas y Procedimientos: Este activo es importante para asegurar el cumplimiento de los procedimientos internos establecidos por el Consejo de Administración y el Consejo de Vigilancia de la Cooperativa Metrópolis, el activo fue valorado como medio en los 6 aspectos puesto que esos documentos deben ser accesibles para los empleados pero asegurando que no se realicen modificaciones sin autorización por ello es importante mantener un historial de actualizaciones y garantizar que las políticas aplicadas sean las correctas.

[AI.5] Informes Financieros y Auditorías: este activo es importante para el cumplimiento normativo ante el organismo de control, para lo cual existe auditoría externa quienes realizan su trabajo de forma mensual. Es por ello que se considera importante conservar su integridad para siempre mantener la situación financiera real de la entidad.

[P] Personal

Resultados de valoración en categoría [P] Personal:

Figura 9 Valoración de los activos de la categoría [P] Personal

[P] Personal						
[P.1] Empleados con Acceso a Información Sensible	[A]	[A+]	[A+]	[A]	[M]	[A]
[P.2] Administradores de Sistemas	[A+]	[A+]	[A+]	[A+]	[M]	[A-]
[P.3] Personal de Atención al Cliente	[M-]	[M]	[M-]	[M-]	[M-]	[M-]
[P.4] Directivos y Gerentes	[A]	[A]	[A]	[A]	[M]	[M]
[P.5] Desarrolladores / Programadores	[A-]	[A-]	[A-]	[M+]	[M+]	[M+]
[P.6] Proveedores Externos	[A]	[A]	[A-]	[M+]	[M+]	[M+]

[P.1] Empleados con Acceso a Información Sensible: Los colaboradores tienen asignadas sus opciones de acuerdo a las actividades del cargo que desempeñan, se tiene mayor control en aquellos que manejan información sensible hola porque deben tener control de sus credenciales asignadas.

[P.2] Administradores de Sistemas: los colaboradores que administran el sistema tienen una valoración alta porque la se debe conservar la integridad en todas las acciones que ellos realicen en la información que manejan de la cooperativa.

[P.3] Personal de Atención al Cliente: el personal que atiende a los socios es la cara de la cooperativa ante la población por ello es activo fue valorado en categoría media.

[P.4] Directivos y Gerentes: alta gerencia es importante que mantenga su integridad para tomar decisiones esas técnicas que permitan el progreso de la cooperativa.

[P.5] Desarrolladores / Programadores: la disponibilidad de los desarrolladores es importante para el mantenimiento del software, en este caso para realizar un cambio en el código fuente del Core Financiero los encargados del departamento de sistemas de la cooperativa se comunican con el proveedor externo para dar acceso y autorizar los cambios solicitados por la cooperativa. Por ello es importante la integridad en el desarrollo para evitar vulnerabilidades y errores de código.

[P.6] Proveedores Externos: este activo también es importante puesto que los proveedores manejan información sensible por ello la importancia que las acciones sean realizadas de manera íntegra y que los proveedores cumplan con las políticas de confidencialidad.

[AF] Activos Físicos

Resultados de valoración en categoría [AF] Activos Físicos:

Figura 10 Valoración de los activos de la categoría [AF] Activos Físicos

[AF] Activos Físicos						
[AF.1] Edificio Principal	[M+]	[M+]	[M+]	[M+]	[M+]	[M+]
[AF.2] Salas de Servidores	[A]	[M+]	[A+]	[A+]	[M+]	[A]
[AF.4] Generadores Eléctricos	[A-]	[M]	[B]	[B]	[B]	[B]
[AF.5] Cableado de Datos	[A]	[A-]	[A]	[A]	[A]	[A]

[AF.1] Edificio Principal: el resultado de esta activo en la disponibilidad y la integridad del edificio principal se han valorado en [M+]. Aunque no es el activo más crítico, mantener su infraestructura en buen estado asegura la continuidad de las operaciones. La trazabilidad y autenticidad también han sido valoradas en [M+], exponiendo la necesidad de mantener el edificio seguro y en buen estado para el personal colaborador y los socios de la cooperativa.

[AF.2] Salas de Servidores: el espacio físico donde se encuentra el servidor de datos y donde se almacenan y procesan información tiene una valoración alta, con valoraciones [A] y [A+] en disponibilidad, integridad, autenticidad y trazabilidad, se subraya la importancia de mantener un entorno seguro y controlado para los equipos. En la Cooperativa Metrópolis las dos personas encargadas del departamento de sistemas son quienes ingresan al cuarto de servidores y deben llenar una bitácora de ingreso, el control de acceso es por medio de un biométrico y posteriormente ingresar una clave única del colaborador responsable.

[AF.4] Generadores Eléctricos: en la oficina matriz de la Cooperativa Metrópolis se posee un generador que abastece todo el sistema eléctrico del edificio, se valoraron con un enfoque de disponibilidad en [A-], lo que indica su relevancia para asegurar la continuidad del suministro eléctrico en caso de fallos. Sin embargo, la valoración de la integridad y trazabilidad en [B] sugiere que, aunque son importantes, no son críticos para cada aspecto las operaciones de negocio, pero son necesarios para minimizar las interrupciones en la operatividad.

[AF.5] Cableado de Datos: en la oficina matriz se mantiene en buen estado todo el cableado de datos. Porque se considera fundamental para garantizar la conectividad y transferencia de datos en todo momento, asegurando de esta forma que las operaciones de negocios se mantengan continuas y también la integridad de las comunicaciones en las operaciones de la cooperativa.

3.1.3. Valoración de amenazas

La notificación y valoración de amenazas se realizó siguiendo la metodología de MAGERIT, a continuación, se detalla la amenaza identificada por cada activo:

[S] Servicios

[S.1] Conexión a Internet

Figura 11 Valoración de amenazas del activo [S.1]

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS								
[S] Servicios								
[S.1] Conexión a Internet			50%	100%	100%	100%	100%	
[I.9] Interrupción de otros servicios o suministros esenciales		1	50%					
[E.1] Errores de los usuarios		1	10%	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%			
[E.15] Alteración de la información		1		10%				
[E.18] Destrucción de la información		1	10%					
[E.19] Fugas de información		1			10%			
[E.24] Caída del sistema por agotamiento de recursos		10	50%					
[A.5] Suplantación de la identidad		1		100%	100%	100%		
[A.6] Abuso de privilegios de acceso		1	1%	10%	10%	100%		
[A.7] Uso no previsto		1	1%	10%	10%			
[A.11] Acceso no autorizado		1		10%	50%	100%		
[A.13] Repudio (negación de actuaciones)		5					100%	
[A.15] Modificación de la información		10		50%				
[A.18] Destrucción de la información		1	50%					
[A.19] Revelación de información		1			50%			
[A.24] Denegación de servicio		10	50%					

En los resultados se detalla que la disponibilidad de la conexión a internet tiene una valoración del 50% lo cual enfatiza en proteger a la infraestructura de red contra amenazas como la negación de servicio A.24 y la caída del sistema por agotamiento de recursos E.24. Estas amenazas también tienen una frecuencia elevada de 10, es decir que son consideradas críticas e impactan directamente a la disponibilidad de servicio de internet.

[S.2] Servicios en la Nube:

Figura 12 Valoración de amenazas del activo [S.2]

[S.2] Servicios en la Nube				100%	100%	100%	100%	100%
[I.9] Interrupción de otros servicios o suministros esenciales			1	50%				
[E.15] Alteración de la información			1		10%			
[E.18] Destrucción de la información			1	10%				
[E.19] Fugas de información			1			10%		
[A.5] Suplantación de la identidad			0,2		100%	100%	100%	
[A.13] Repudio (negación de actuaciones)			1					100%
[A.15] Modificación de la información			1		50%			
[A.18] Destrucción de la información			1	50%				
[A.19] Revelación de información			5			50%		
[A.24] Denegación de servicio			1	50%				
[A.28] Indisponibilidad del personal			0,5	10%				
[A.29] Extorsión			0,9	10%	10%	50%		
[A.30] Ingeniería social (picaresca)			1	10%	10%	50%		
[SR.1] Lock-in			1	10%				
[SR.2] Loss of governance			10	100%	100%	100%		
[SR.7] Isolation failure			1	50%	50%	50%		
[SR.9] Management interface compromise			0,5	100%				
[SR.11] Insecure or ineffective deletion of data			0,5			100%		
[SR.14] Compromise of service engine			0,1	100%	100%	100%		
[SR.19] Subpoena and e-discovery			1	10%		10%		
[SR.20] Risk from changing of jurisdiction			1	50%		50%		
[SR.21] Data protection risks			1			50%		
[SR.31] Accountability and data ownership			1	10%				
[SR.32] User identity federation			0,5	10%				
[SR.35] User privacy and secondary usage of data			1			50%		
[SR.38] Incidence analysis and forensics support			0,5	1%	1%	1%		
[SR.53] Insecure interfaces and APIs			0,1	50%	50%	50%		
[X.2] Phishing			1			100%		

Este activo fue valorado como importante para la operación de la entidad, en todos los aspectos las amenazas se mantienen al 100% tales como la suplantación de identidad, fuga de información y denegación de servicio son considerados riesgos críticos, la cooperativa hasta el momento no ha presentado ningún evento de este tipo, sin embargo, mantiene debidamente legalizados los contratos con proveedores y respaldados con acuerdos de confidencialidad que permiten de esa manera también evitar las extorsión en caso de que se presente alguna de estas amenazas.

[S.3] Servicios de Respaldo y Recuperación

Figura 13 Valoración de amenazas del activo [S.3]

[S.3] Servicios de Respaldo y Recuperación				50%	100%	100%	100%	100%
[I.9] Interrupción de otros servicios o suministros esenciales			1	50%				
[E.1] Errores de los usuarios			1	10%	10%	10%		
[E.2] Errores del administrador del sistema / de la seguridad			1	20%	20%	20%		
[E.15] Alteración de la información			1		10%			
[E.18] Destrucción de la información			1	10%				
[E.19] Fugas de información			1			10%		
[E.24] Caída del sistema por agotamiento de recursos			10	50%				
[A.5] Suplantación de la identidad			1		100%	100%	100%	
[A.6] Abuso de privilegios de acceso			1	1%	10%	10%	100%	
[A.7] Uso no previsto			1	1%	10%	10%		
[A.11] Acceso no autorizado			1		10%	50%	100%	
[A.13] Repudio (negación de actuaciones)			5					100%
[A.15] Modificación de la información			10		50%			
[A.18] Destrucción de la información			1	50%				
[A.19] Revelación de información			1			50%		
[A.24] Denegación de servicio			10	50%				

La valoración de amenazas de este activo incluye la denegación de servicio (A.24) y la caída del sistema por agotamiento de recursos (E.24), esas amenazas podrían presentar un impacto del 50% en disponibilidad, lo cual en caso de presentarse afectaría la recuperación de datos en situaciones críticas. De igual manera, la suplantación de identidad (A.5) tiene un impacto del 100% en la confidencialidad, integridad, y

autenticidad, y la revelación de información (A.19) y la destrucción de la información (A.18) también representan riesgos considerables.

[S.4] Soporte técnico y mantenimiento

Figura 14 Valoración de amenazas del activo [S.4]

[S.4] Soporte Técnico y Mantenimiento		50%	100%	100%	100%	100%	
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%					
[E.1] Errores de los usuarios	1	10%	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			
[E.15] Alteración de la información	1		10%				
[E.18] Destrucción de la información	1	10%					
[E.19] Fugas de información	1			10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%					
[A.5] Suplantación de la identidad	1		100%	100%	100%		
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	100%		
[A.7] Uso no previsto	1	1%	10%	10%			
[A.11] Acceso no autorizado	1		10%	50%	100%		
[A.13] Repudio (negación de actuaciones)	5					100%	
[A.15] Modificación de la información	10		50%				
[A.18] Destrucción de la información	1	50%					
[A.19] Revelación de información	5			50%			
[A.24] Denegación de servicio	10	50%					
[A.28] Indisponibilidad del personal	0,5	10%					
[A.29] Extorsión	0,9	10%	10%	50%			
[A.30] Ingeniería social (picaresca)	1	10%	10%	50%			

En este activo las amenazas más críticas incluyen la denegación de servicio (A.24) y la caída del sistema por agotamiento de recursos (E.24), ambas con un impacto del 50% en la disponibilidad del soporte y mantenimiento.

[S.5] Servicio de Telefonía (fija y móvil)

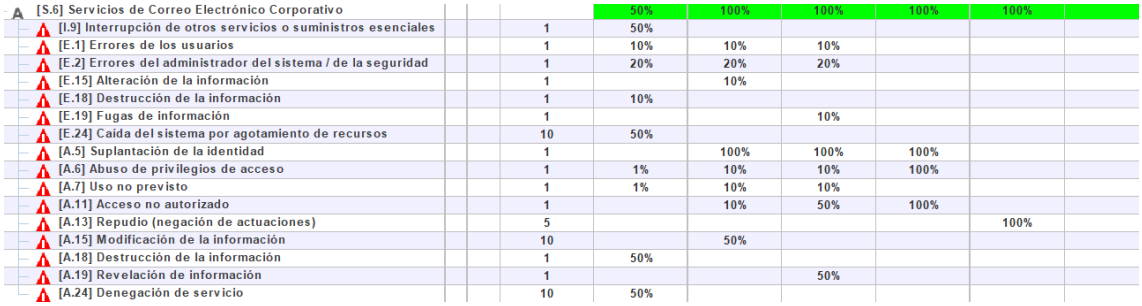
Figura 15 Valoración de amenazas del activo [S.5]

[S.5] Servicios de Telefonía (fija y móvil)		50%	100%	100%	100%	100%	
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%					
[E.15] Alteración de la información	1		10%				
[E.18] Destrucción de la información	1	10%					
[E.19] Fugas de información	1			10%			
[A.5] Suplantación de la identidad	0,2		100%	100%	100%		
[A.13] Repudio (negación de actuaciones)	1					100%	
[A.15] Modificación de la información	1		50%				
[A.18] Destrucción de la información	1	50%					
[A.19] Revelación de información	1			50%			
[A.24] Denegación de servicio	1	50%					

Resultados de este activo muestran que la confidencialidad (C) e integridad (I) tienen amenazas como la suplantación de identidad (A.5) y fugas de información (E.19), ambas con un impacto del 100%, es decir que representan riesgos significativos, ya que la suplantación podría permitir el acceso no autorizado a comunicaciones internas de la cooperativa.

[S.6] Servicios de Correo Electrónico Corporativo]

Figura 16 Valoración de amenazas del activo [S.6]



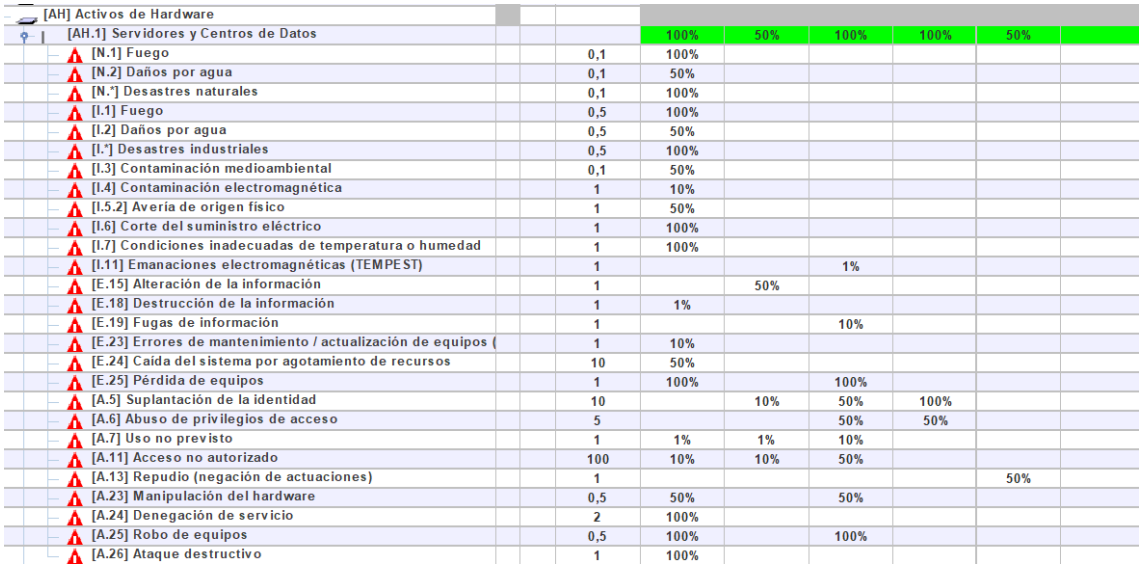
[S.6] Servicios de Correo Electrónico Corporativo		50%	100%	100%	100%	100%	
[I.9] Interrupción de otros servicios o suministros esenciales	1	50%					
[E.1] Errores de los usuarios	1	10%	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			
[E.15] Alteración de la información	1		10%				
[E.18] Destrucción de la información	1	10%					
[E.19] Fugas de información	1			10%			
[E.24] Caída del sistema por agotamiento de recursos	10	50%					
[A.5] Suplantación de la identidad	1		100%	100%	100%		
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	100%		
[A.7] Uso no previsto	1	1%	10%	10%			
[A.11] Acceso no autorizado	1		10%	50%	100%		
[A.13] Repudio (negación de actuaciones)	5					100%	
[A.15] Modificación de la información	10		50%				
[A.18] Destrucción de la información	1	50%					
[A.19] Revelación de información	1			50%			
[A.24] Denegación de servicio	10	50%					

Por su parte la valoración de amenazas del activo muestra que la disponibilidad tiene un valor del 50%, lo cual indica vulnerabilidad frente a interrupciones en el servicio. Entre las amenazas más significativas incluyen la denegación de servicio (A.24) y la caída del sistema por agotamiento de recursos (E.24), ambas con un impacto del 50% en la disponibilidad, lo que podría afectar la comunicación interna y externa, en cuanto a la confidencialidad y autenticidad, la suplantación de identidad (A.5) se calcula con un impacto crítico del 100%, Lo que indica que en caso de presentarse puede permitir accesos indebidos y comprometer la seguridad del correo electrónico.

[AH] Activos de Hardware

[AH.1] Servicios y Centro de Datos

Figura 17 Valoración de amenazas del activo [AH.1]



[AH] Activos de Hardware							
[AH.1] Servidores y Centros de Datos			100%	50%	100%	100%	50%
[N.1] Fuego	0,1		100%				
[N.2] Daños por agua	0,1		50%				
[N.*] Desastres naturales	0,1		100%				
[I.1] Fuego	0,5		100%				
[I.2] Daños por agua	0,5		50%				
[I.*] Desastres industriales	0,5		100%				
[I.3] Contaminación medioambiental	0,1		50%				
[I.4] Contaminación electromagnética	1		10%				
[I.5.2] Avería de origen físico	1		50%				
[I.6] Corte del suministro eléctrico	1		100%				
[I.7] Condiciones inadecuadas de temperatura o humedad	1		100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)	1				1%		
[E.15] Alteración de la información	1			50%			
[E.18] Destrucción de la información	1		1%				
[E.19] Fugas de información	1				10%		
[E.23] Errores de mantenimiento / actualización de equipos (	1		10%				
[E.24] Caída del sistema por agotamiento de recursos	10		50%				
[E.25] Pérdida de equipos	1		100%		100%		
[A.5] Suplantación de la identidad	10			10%	50%	100%	
[A.6] Abuso de privilegios de acceso	5				50%	50%	
[A.7] Uso no previsto	1		1%	1%	10%		
[A.11] Acceso no autorizado	100		10%	10%	50%		
[A.13] Repudio (negación de actuaciones)	1						50%
[A.23] Manipulación del hardware	0,5		50%		50%		
[A.24] Denegación de servicio	2		100%				
[A.25] Robo de equipos	0,5		100%		100%		
[A.26] Ataque destructivo	1		100%				

El centro de datos es considerado como un área restringida dentro de la cooperativa, en este activo se analizan varias amenazas críticas que afectan la disponibilidad, integridad, confidencialidad, y autenticidad de los activos de hardware. Entre las amenazas más significativas incluyen fuego (N.1), desastres naturales (N.2), y daños por agua (N.2), todas con un impacto del 100% en la disponibilidad, lo cual muestra la necesidad de contar con sistemas de protección como sensores de humo y planes de contingencia para desastres naturales, por otra parte la suplantación de identidad (A.5) y el robo de equipos (A.25) presentan un impacto crítico del 100% en la confidencialidad y autenticidad, subrayando la importancia de implementar controles de acceso físico y medidas de seguridad adicionales. Sin embargo, en la visita al sitio se ha identificado que la cooperativa Metrópolis ha considerado estas amenazas y sí tiene aplicado controles en la seguridad física con acceso biométrico al centro de datos y también sensores de movimiento y detectores de humo.

[AH.2] Equipos de Red

Figura 18 Valoración de amenazas del activo [AH.2]

A	[AH.2] Equipos de Red			100%	10%	50%			
	[N.1] Fuego		0,1	100%					
	[N.2] Daños por agua		0,1	50%					
	[N.*] Desastres naturales		0,1	100%					
	[I.1] Fuego		0,5	100%					
	[I.2] Daños por agua		0,5	50%					
	[I.*] Desastres industriales		0,5	100%					
	[I.3] Contaminación medioambiental		0,1	50%					
	[I.4] Contaminación electromagnética		1	10%					
	[I.5.2] Avería de origen físico		1	50%					
	[I.6] Corte del suministro eléctrico		1	100%					
	[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%					
	[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%			
	[E.23] Errores de mantenimiento / actualización de equipos (		1	10%					
	[E.24] Caída del sistema por agotamiento de recursos		10	50%					
	[E.25] Pérdida de equipos		1	20%		50%			
	[A.7] Uso no previsto		1	10%		10%			
	[A.11] Acceso no autorizado		1	10%	10%	50%			
	[A.23] Manipulación del hardware		0,5	100%		50%			
	[A.24] Denegación de servicio		2	100%					
	[A.25] Robo de equipos		0,5	20%		50%			
	[A.26] Ataque destructivo		1	100%					

En la Cooperativa Metrópolis tienen 2 switch, entre las amenazas que se identifican en los resultados incluyen fuego (N.1), desastres naturales (N.2), y corte del suministro eléctrico (I.6), todas con un impacto del 100% en la disponibilidad. Otras amenazas relevantes son los errores de mantenimiento (E.23) y caída del sistema por agotamiento de recursos (E.24), ambas con un impacto significativo en la integridad y disponibilidad. En la oficina matriz por ser un edificio construido en el 2022 si destaca con las medidas de protección física, sistemas de respaldo eléctrico y planes de recuperación ante desastres.

[AH.3] Computadoras de Escritorio y Laptops

Figura 19 Valoración de amenazas del activo [AH.3]

[AH.3] Computadoras de Escritorio y Laptops				100%	10%	50%			
[N.1] Fuego			0,1	100%					
[N.2] Daños por agua			0,1	50%					
[N.*] Desastres naturales			0,1	100%					
[I.1] Fuego			0,5	100%					
[I.2] Daños por agua			0,5	50%					
[I.*] Desastres industriales			0,5	100%					
[I.3] Contaminación medioambiental			0,1	50%					
[I.4] Contaminación electromagnética			1	10%					
[I.5.2] Avería de origen físico			1	50%					
[I.6] Corte del suministro eléctrico			1	100%					
[I.7] Condiciones inadecuadas de temperatura o humedad			1	100%					
[I.11] Emanaciones electromagnéticas (TEMPEST)			1			1%			
[E.23] Errores de mantenimiento / actualización de equipos (			1	10%					
[E.24] Caída del sistema por agotamiento de recursos			10	50%					
[E.25] Pérdida de equipos			5	5%		10%			
[A.7] Uso no previsto			1	10%	1%	10%			
[A.11] Acceso no autorizado			1	10%	10%	50%			
[A.23] Manipulación del hardware			0,5	50%		50%			
[A.24] Denegación de servicio			2	100%					
[A.25] Robo de equipos			5	5%		10%			
[A.26] Ataque destructivo			1	100%					

Los dispositivos informáticos de uso diario cómo son las computadoras y laptops son necesarias para realizar las operaciones diarias, es por eso que en los resultados tiene disponibilidad (100%), lo que indica que es necesario mantener estos equipos operativos en todo momento para asegurar la continuidad de las operaciones y atención al cliente. Las amenazas más significativas incluyen fuego (N.1), desastres naturales (N.2), y corte del suministro eléctrico (I.6), todas con un impacto del 100% en la disponibilidad. Otras amenazas que destacan son los errores de mantenimiento (E.23) y caída del sistema por agotamiento de recursos (E.24), que afectan la integridad y la disponibilidad de estos activos.

[AH.4] Sistemas de Alimentación Ininterrumpida

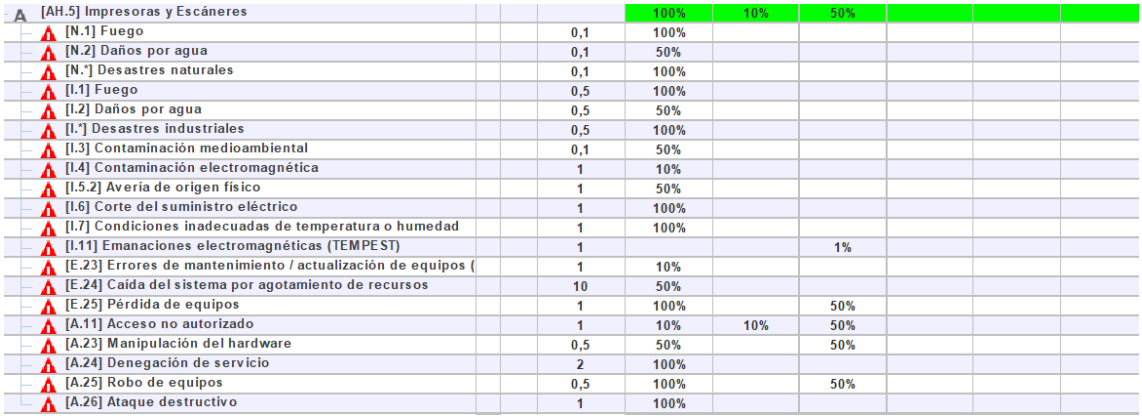
Figura 20 Valoración de amenazas del activo [AH.4]

[AH.4] Sistemas de Alimentación Ininterrumpida				100%	0	0			
[N.1] Fuego			0,1	100%					
[N.2] Daños por agua			0,1	50%					
[N.*] Desastres naturales			0,1	100%					
[I.1] Fuego			0,5	100%					
[I.2] Daños por agua			0,5	50%					
[I.*] Desastres industriales			0,5	100%					
[I.3] Contaminación medioambiental			0,1	50%					
[E.23] Errores de mantenimiento / actualización de equipos (			1	10%					
[A.7] Uso no previsto			1	50%					
[A.23] Manipulación del hardware			1	50%					
[A.25] Robo de equipos			0,5	100%					
[A.26] Ataque destructivo			1	100%					

Sobre el sistema de alimentación interrumpida UPS, tiene un valor del 100% puesto que permite mantener el suministro eléctrico durante los cortes de energía además de proteger a los equipos. En los resultados se detallan que las principales amenazas incluyen fuego (N.1), desastres naturales (N.*) y daños por agua (N.2), todas con un impacto del 100% en la disponibilidad.

[AH.5] Impresoras y Escáneres

Figura 21 Valoración de amenazas del activo [AH.5]



[AH.5] Impresoras y Escáneres				100%	10%	50%			
[N.1] Fuego			0,1	100%					
[N.2] Daños por agua			0,1	50%					
[N.*] Desastres naturales			0,1	100%					
[I.1] Fuego			0,5	100%					
[I.2] Daños por agua			0,5	50%					
[I.*] Desastres industriales			0,5	100%					
[I.3] Contaminación medioambiental			0,1	50%					
[I.4] Contaminación electromagnética			1	10%					
[I.5.2] Avería de origen físico			1	50%					
[I.6] Corte del suministro eléctrico			1	100%					
[I.7] Condiciones inadecuadas de temperatura o humedad			1	100%					
[I.11] Emanaciones electromagnéticas (TEMPEST)			1			1%			
[E.23] Errores de mantenimiento / actualización de equipos (			1	10%					
[E.24] Caída del sistema por agotamiento de recursos			10	50%					
[E.25] Pérdida de equipos			1	100%		50%			
[A.11] Acceso no autorizado			1	10%	10%	50%			
[A.23] Manipulación del hardware			0,5	50%		50%			
[A.24] Denegación de servicio			2	100%					
[A.25] Robo de equipos			0,5	100%		50%			
[A.26] Ataque destructivo			1	100%					

Este activo tiene una valoración entre el 50% y el 100% puesto que son necesarios para las operaciones y actividades de los colaboradores, pero en caso de presentarse una amenaza no afecta directamente a las transacciones financieras de la institución, el resultado muestra que las amenazas más significativas se encuentran fuego (N.1), desastres naturales (N.2), todas con un impacto del 100% en la disponibilidad. También se identifican errores de mantenimiento (E.23) y caída del sistema por agotamiento de recursos (E.24), que afectan la integridad y disponibilidad de estos equipos, lo que hace esencial implementar planes de mantenimiento regulares y una correcta gestión de recursos para garantizar su operatividad continua.

[AS] Activos de Software

[AS.1] Sistema Core Financiero

Figura 22 Valoración de amenazas del activo [AS.1]

[AS] Activos de Software										
[AS.1] Sistema Core Financiero				100%	100%	100%	100%	100%	100%	
[I.5.1] Avería de origen lógico			1	50%						
[I.9] Interrupción de otros servicios o suministros esenciales			1	50%						
[E.8] Difusión de software dañino			1	10%	10%	10%				
[E.15] Alteración de la información			1		10%					
[E.18] Destrucción de la información			1	10%						
[E.19] Fugas de información			1			10%				
[E.20] Vulnerabilidades de los programas (software)			1	1%	20%	20%				
[E.21] Errores de mantenimiento / actualización de programas (software)			10	1%	10%	50%				
[A.5] Suplantación de la identidad			0,2		100%	100%	100%			
[A.8] Difusión de software dañino			1	100%	100%	100%				
[A.13] Repudio (negación de actuaciones)			1					100%		
[A.15] Modificación de la información			1		50%					
[A.18] Destrucción de la información			1	50%						
[A.19] Revelación de información			1			50%				
[A.22] Manipulación de programas			1	50%	100%	100%				
[A.24] Denegación de servicio			1	50%						
[PR.g1] 1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender			10							20%
[PR.g2] 2. Tratar datos inadecuados y excesivos para la finalidad del tratamiento			10							50%
[PR.g3] 3. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos			10							50%
[PR.g4] 4. Tratar datos personales con una finalidad distinta para la cual fueron recabados			10							90%
[PR.g5] 5. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización			5							50%
[PR.g6] 6. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente			10							50%
[PR.g7] 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado			10							90%
[PR.g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados			10							100%
[PR.g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma			10							100%
[PR.g10] 10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas			10							90%
[PR.g11] 11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento			10							90%
[PR.g12] 12. No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad			5							50%
[PR.g13] 13. No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable			5							50%
[PR.g24] 24. Información no actualizada o incorrecta (pe. registros duplicados con informaciones contradictorias o con campos de datos incorrectos)			10							50%
[PR.2g] Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.			10							50%
[PR.2m] Accesos no autorizados a datos personales (modificación)			10							30%
[PR.2n] Accesos no autorizados a datos personales (lectura)			10							80%

El activo del Core Financiero él nos resultados detallados se muestra una alta criticidad en la disponibilidad (100%), integridad (100%), confidencialidad (100%), y trazabilidad (100%), este análisis enfatiza la importancia de mantener el sistema operativo sin interrupciones para el funcionamiento de la cooperativa y realizar el registro de operaciones financieras y contables.

Entre las amenazas más significativas se encuentran errores de origen lógico (I.5.1) con un impacto del 50% en la disponibilidad. Además, suplantación de la identidad (A.5) y vulnerabilidades en los programas (software) (E.20) presentan un riesgo crítico del 100% en confidencialidad y autenticidad.

[AS.3] Sistema de Seguridad y Autenticación

Figura 23 Valoración de amenazas del activo [AS.3]

activo	co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[AS.3] Sistemas de Seguridad y Autenticación			100%	100%	100%	100%		
[I.5.1] Avería de origen lógico		1	50%					
[I.8] Fallo de servicios de comunicaciones		1	50%					
[E.2] Errores del administrador del sistema / de la seguridad		1	20%	20%	20%			
[E.8] Difusión de software dañino		1	10%	10%	10%			
[E.9] Errores de [re-]encaminamiento		1			10%			
[E.10] Errores de secuencia		1		10%				
[E.15] Alteración de la información		1		50%				
[E.18] Destrucción de la información		1	1%					
[E.19] Fugas de información		1			10%			
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	10%	50%			
[E.24] Caída del sistema por agotamiento de recursos		1	50%					
[E.28] Indisponibilidad del personal		1	10%					
[A.5] Suplantación de la identidad		10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso		10	1%	10%	50%	50%		
[A.7] Uso no previsto		1	10%	10%	10%			
[A.8] Difusión de software dañino		1	100%	100%	100%			
[A.9] [Re-]encaminamiento de mensajes		1			10%			
[A.10] Alteración de secuencia		1		10%				
[A.11] Acceso no autorizado		100		10%	50%	100%		
[A.12] Análisis de tráfico		1			2%			
[A.14] Interceptación de información (escucha)		1			10%			
[A.15] Modificación de la información		1		50%				
[A.18] Destrucción de la información		1	50%					
[A.19] Revelación de información		10			50%			
[A.22] Manipulación de programas		1	50%	100%	100%			
[A.24] Denegación de servicio		10	50%					
[A.28] Indisponibilidad del personal		0,5	20%					
[A.29] Extorsión		0,9	1%	100%	100%			
[A.30] Ingeniería social (picaresca)		0,5	1%	100%	100%			
[X.1] Ransomware		2	100%					

Los resultados de la valoración de amenaza de este activo muestran una alta criticidad en todos los aspectos fundamentales: disponibilidad (100%), integridad (100%), confidencialidad (100%), y autenticidad (100%), además sugiere que las amenazas más significativas incluyen suplantación de identidad (A.5), que impacta la confidencialidad, autenticidad e integridad con un valor del 100%. Además, errores del administrador del sistema (E.2) y errores de mantenimiento o actualización (E.21) presentan riesgos en la integridad y disponibilidad, con impactos de hasta el 50%.

[AS.2] Aplicación web y móvil para clientes

Figura 24 Valoración de amenazas del activo [AS.2]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[AS.2] Aplicacion web y movil para clientes				100%	100%	100%	100%		
[I.5.1] Avería de origen lógico			1	50%					
[E.8] Difusión de software dañino			1	10%	10%	10%			
[E.15] Alteración de la información			1		50%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[E.20] Vulnerabilidades de los programas (software)			1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programas (software)			10	1%	10%	50%			
[E.28] Indisponibilidad del personal			1	10%					
[A.5] Suplantación de la identidad			10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso			5			50%	50%		
[A.8] Difusión de software dañino			1	100%	100%	100%			
[A.11] Acceso no autorizado			100		10%	50%			
[A.15] Modificación de la información			1		50%				
[A.18] Destrucción de la información			1	10%					
[A.19] Revelación de información			10			50%			
[A.22] Manipulación de programas			1	50%	100%	100%			
[A.28] Indisponibilidad del personal			0,5	50%					
[A.29] Extorsión			0,9	50%	100%	100%			
[A.30] Ingeniería social (picaresca)			1	50%	100%	100%			
[X.2] Phishing			1			50%			

La cooperativa tiene los servicios digitales que permiten al socio acceder a sus cuentas en cualquier momento y lugar, el resultado de esta valoración indica que este activo es crítico para la cooperativa, por ello se muestra que tiene en disponibilidad (100%), integridad (100%), confidencialidad (100%), y autenticidad (100%), esto representa la importancia de mantener la operatividad y seguridad de esta aplicación. Las amenazas más significativas incluyen la suplantación de identidad (A.5), con un impacto crítico en confidencialidad, integridad, autenticidad y trazabilidad. También se destaca el riesgo de phishing (X.2), que impacta la confidencialidad, enfatizando la importancia de educar a los usuarios y aplicar filtros de seguridad.

[AI] Activos de información

[AI.1] Base de Datos

Figura 25 Valoración de amenazas del activo [AI.1]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[AI] Activos de información									
[AI.1] Base de Datos				100%	100%	100%	100%	50%	
[E.4] Errores de configuración			1		1%				
[E.15] Alteración de la información			1		10%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[E.28] Indisponibilidad del personal			1	30%					
[A.4] Manipulación de los ficheros de configuración			10	10%	10%	10%			
[A.5] Suplantación de la identidad			10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso			10	1%	10%	50%			
[A.11] Acceso no autorizado			100		10%	50%			
[A.13] Repudio (negación de actuaciones)			1					50%	
[A.15] Modificación de la información			1		50%				
[A.18] Destrucción de la información			1	10%					
[A.19] Revelación de información			10			50%			
[A.28] Indisponibilidad del personal			0,5	50%					
[A.29] Extorsión			0,9	50%	100%	100%			
[A.30] Ingeniería social (picaresca)			0,5	50%	100%	100%			
[X.1] Ransomware			2	100%					
[X.2] Phishing			1			50%			

Los resultados de este activo demuestran que la base de datos presenta valores elevados en términos de disponibilidad (100%), integridad (100%), confidencialidad (100%), y autenticidad (100%), esto significa que es un activo esencial en la institución. Las amenazas más significativas incluyen la suplantación de identidad (A.5), que tiene un impacto crítico en confidencialidad, integridad, autenticidad y trazabilidad. Otras amenazas que podrían presentarse son la extorsión (A.29) y el ransomware (X.1) dónde se detalla un alto riesgo tanto para la disponibilidad como para la confidencialidad de los datos, con impactos del 100% en caso de presentarse esta amenaza, Por otra parte, la fuga de información (E.19) y revelación de información (A.19) también son amenazas significativas, comprometiendo la confidencialidad con impactos considerables.

[AI.2] Registro de transacciones Financieras

Figura 26 Valoración de amenazas del activo [AI.2]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[AI.2] Registros de Transacciones Financieras				100%	10%	50%	100%	50%	
[E.15] Alteración de la información			1		1%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[A.5] Suplantación de la identidad			10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso			10	1%	10%	50%			
[A.11] Acceso no autorizado			100		10%	50%			
[A.13] Repudio (negación de actuaciones)			1					50%	
[X.1] Ransomware			2	100%					

El registro de las transacciones financieras es muy importante mantener la integridad y confidencialidad de cada registro diario es por esto que en los resultados se muestra que también es considerado como crítico. Entre las amenazas más significativas está el ransomware (X.1), con un impacto del 100% en la disponibilidad, la suplantación de identidad (A.5) también representa una amenaza significativa con impactos en la confidencialidad, autenticidad e integridad de los registros. Las amenazas relacionadas con el acceso no autorizado (A.11) y el abuso de privilegios de acceso (A.6) presentan riesgos que podrían comprometer tanto la integridad como la confidencialidad de los datos financieros. Aunque en la institución aún no se han registrado este tipo de eventos se sugiere la necesidad de revisar y limitar el acceso a los registros según el rol de cada usuario.

[AI.3] Documentos de Políticas y Procedimientos

Figura 27 Valoración de amenazas del activo [AI.3]

activo			co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[AI.3] Documentos de Políticas y Procedimientos					100%	10%	50%	100%	50%	
[E.15] Alteración de la información				1		1%				
[E.18] Destrucción de la información				1	1%					
[E.19] Fugas de información				1			10%			
[A.5] Suplantación de la identidad				10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso				10	1%	10%	50%			
[A.11] Acceso no autorizado				100		10%	50%			
[A.13] Repudio (negación de actuaciones)				1					50%	
[X.1] Ransomware				2	100%					

Los documentos de políticas y procedimientos que detallan las operaciones que se deben cumplir diariamente en cada área de la cooperativa para dar cumplimiento al organismo de control y también control interno de la institución es considerado un activo importante, sin embargo, en su valoración de amenazas presenta la suplantación de identidad (A.5) y el acceso no autorizado (A.11) que impactarían la confidencialidad, autenticidad e integridad de los documentos. Abuso de privilegios de acceso (A.6) también representa un riesgo importante para la confidencialidad y autenticidad de la información. Por otra parte, también puede ocurrir amenazas como la alteración (E.15) y la destrucción de la información (E.18) afectan la integridad de los documentos y resaltan la importancia de medidas de auditoría y control para evitar modificaciones o eliminaciones no autorizadas.

[AI.5] Informes Financieros y Auditorías

Figura 28 Valoración de amenazas del activo [AI.5]

activo			co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[AI.5] Informes Financieros y Auditorías					100%	10%	50%	100%	50%	
[E.15] Alteración de la información				1		1%				
[E.18] Destrucción de la información				1	1%					
[E.19] Fugas de información				1			10%			
[A.5] Suplantación de la identidad				10		10%	50%	100%		
[A.6] Abuso de privilegios de acceso				10	1%	10%	50%			
[A.11] Acceso no autorizado				100		10%	50%			
[A.13] Repudio (negación de actuaciones)				1					50%	
[X.1] Ransomware				2	100%					

Los informes financieros y auditorías son documentación valiosa que reflejan la realidad de la institución donde firman profesionales que auditan de forma mensual y anual a la cooperativa. Sin embargo, está activo en su valoración es también presentan amenazas que pueden ocurrir tales como el ransomware (X.1), con un impacto crítico en la disponibilidad, la suplantación de identidad (A.5) y el acceso no autorizado (A.11) representan grandes riesgos para la confidencialidad, autenticidad e integridad de estos documentos, indicando la importancia de implementar controles fuertes de autenticación y limitar los accesos a las personas autorizadas. Por otro lado, amenazas como la alteración de la información (E.15) afectan la integridad de los informes, por ello es

importante conservar estos documentos originales con las firmas de los profesionales responsables.

[P] Personal

[P.1] Empleados con Acceso a Información Sensible

Figura 29 Valoración de amenazas del activo [P.1]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[P] Personal									
[P.1] Empleados con Acceso a Información Sensible				50%	100%	100%			
[E.15] Alteración de la información			1		10%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[E.28] Indisponibilidad del personal			1	5%					
[A.15] Modificación de la información			1		50%				
[A.18] Destrucción de la información			1	10%					
[A.19] Revelación de información			10			50%			
[A.28] Indisponibilidad del personal			0,5	20%					
[A.29] Extorsión			0,9	50%	100%	100%			
[A.30] Ingeniería social (picaresca)			1	50%	100%	100%			

Sobre el personal la valoración de los colaboradores con acceso a información sensible también presenta algunas amenazas entre ellas se encuentran la extorsión (A.29) y la ingeniería social (A.30), ambas con un impacto crítico en la confidencialidad, autenticidad y disponibilidad porque estos colaboradores tienen acceso y credenciales a la información financiera de la institución. Es por esto que la fuga de información (E.19) y la revelación de información (A.19) también presentan un riesgo significativo para la confidencialidad.

[P.2] Administradores de Sistemas

Figura 30 Valoración de amenazas del activo [P.2]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[P.2] Administradores de Sistemas				50%	100%	100%			
[E.15] Alteración de la información			1		10%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[E.28] Indisponibilidad del personal			1	10%					
[A.15] Modificación de la información			1		50%				
[A.18] Destrucción de la información			1	10%					
[A.19] Revelación de información			10			50%			
[A.28] Indisponibilidad del personal			0,5	20%					
[A.29] Extorsión			0,9	50%	100%	100%			
[A.30] Ingeniería social (picaresca)			0,5	50%	100%	100%			

Pasión de los administradores de sistemas presentan algunos resultados que detallan amenazas que podrían presentarse tales como la extorsión (A.29) y la ingeniería social (A.30), ambas con un impacto crítico en confidencialidad, autenticidad, y disponibilidad, la fuga de información (E.19) y la revelación de información (A.19) representan riesgos

importantes para la confidencialidad. De igual manera puede ocurrir, la alteración (E.15) y modificación de la información (A.15) afectan la integridad.

[P.3] Personal de Atención al Cliente

Figura 31 Valoración de amenazas del activo [P.3]

activo	co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[P.3] Personal de Atención al Cliente			50%	50%	50%			
[E.15] Alteración de la información		1		10%				
[E.18] Destrucción de la información		1	1%					
[E.19] Fugas de información		1			10%			
[E.28] Indisponibilidad del personal		1	30%					
[A.15] Modificación de la información		1		50%				
[A.18] Destrucción de la información		1	10%					
[A.19] Revelación de información		10			50%			
[A.28] Indisponibilidad del personal		0,5	50%					
[A.29] Extorsión		0,9	20%	10%	50%			
[A.30] Ingeniería social (picaresca)		0,5	20%	20%	20%			

Los colaboradores que se encuentran en el área de atención al cliente también presentan amenazas más significativas incluyen la ingeniería social (A.30) y la extorsión (A.29), con un impacto considerable en la confidencialidad, integridad, y autenticidad. Se considera también otra amenaza la indisponibilidad del personal (E.28) lo que representaría un impacto del 30%. De igual manera se considera que la amenaza de la fuga de información (E.19) y la revelación de información (A.19) afectan la confidencialidad de los datos, indicando la importancia de aplicar políticas de seguridad rigurosas y monitoreo constante para evitar divulgaciones no autorizadas.

[P.4] Directivos y Gerentes

Figura 32 Valoración de amenazas del activo [P.4]

activo	co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[P.4] Directivos y Gerentes			50%	100%	100%			
[E.15] Alteración de la información		1		10%				
[E.18] Destrucción de la información		1	1%					
[E.19] Fugas de información		1			10%			
[E.28] Indisponibilidad del personal		1	10%					
[A.15] Modificación de la información		1		50%				
[A.18] Destrucción de la información		1	10%					
[A.19] Revelación de información		10			50%			
[A.28] Indisponibilidad del personal		0,5	20%					
[A.29] Extorsión		0,9	50%	100%	100%			
[A.30] Ingeniería social (picaresca)		0,5	50%	100%	100%			

En el caso de la alta gerencia tales como los directivos y gerentes de la cooperativa fueron analizado y valorado las amenazas de este activo en donde los resultados incluyen la extorsión (A.29) y la ingeniería social (A.30), ambas representan un impacto crítico en la confidencialidad, integridad, y autenticidad. Además, la fuga de información (E.19) y la revelación de información (A.19) presentan un alto riesgo para la confidencialidad. La indisponibilidad del personal (E.28) también presenta un riesgo importante para la

disponibilidad (50%), lo cual resalta la necesidad de contar con planes de continuidad que permitan sustituir o cubrir funciones críticas en caso de ausencia.

[P.5] Desarrolladores / Programadores

Figura 33 Valoración de amenazas del activo [P.5]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[P.5] Desarrolladores / Programadores				20%	100%	100%			
[E.15] Alteración de la información			1		10%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[E.28] Indisponibilidad del personal			1	10%					
[A.15] Modificación de la información			1		50%				
[A.18] Destrucción de la información			1	10%					
[A.19] Revelación de información			10			50%			
[A.28] Indisponibilidad del personal			0,5	20%					
[A.29] Extorsión			0,9	1%	100%	100%			
[A.30] Ingeniería social (picaresca)			0,5	1%	100%	100%			

En los resultados del análisis de amenazas de Desarrolladores/Programadores se muestra una alta criticidad en la integridad (100%), confidencialidad (100%), y autenticidad (100%) de la información que gestionan, subrayando su rol crucial en la seguridad y operatividad de los sistemas de la cooperativa. Las amenazas más significativas incluyen la extorsión (A.29) y la ingeniería social (A.30), con impactos críticos en la confidencialidad, integridad, y autenticidad, es por ello que cada contrato está debidamente legalizado con el acuerdo de confidencialidad para mitigar estas amenazas, porque la fuga de información (E.19) y la revelación de información (A.19) también representan un riesgo considerable para la confidencialidad.

[P.6] Proveedores Externos

Figura 34 Valoración de amenazas del activo [P.6]

activo		co...	frecu...	[D]	[I]	[C]	[A]	[T]	[DP]
[P.6] Proveedores Externos				10%	50%	50%			
[E.15] Alteración de la información			1		10%				
[E.18] Destrucción de la información			1	1%					
[E.19] Fugas de información			1			10%			
[A.15] Modificación de la información			1		50%				
[A.18] Destrucción de la información			1	10%					
[A.19] Revelación de información			1			50%			
[A.28] Indisponibilidad del personal			0,5	10%					
[A.29] Extorsión			0,9	10%	10%	50%			
[A.30] Ingeniería social (picaresca)			0,5	10%	10%	50%			

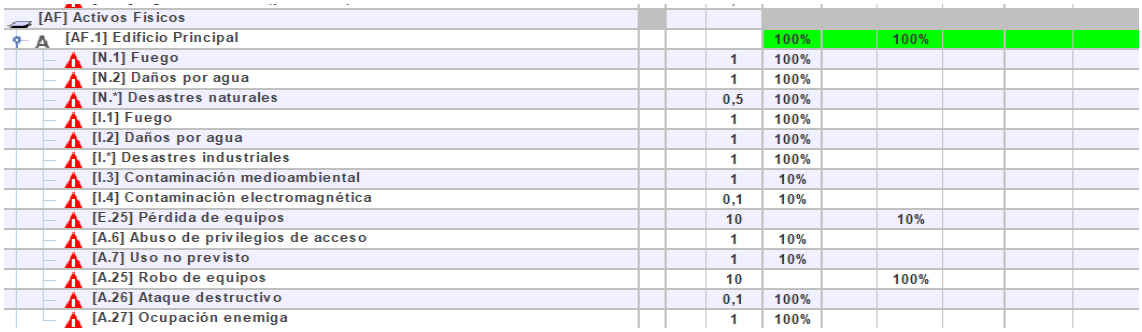
Los proveedores de externos también fueron analizados porque procesan información sensible de la institución tal es el caso que la valoración de amenazas presenta en sus resultados que la fuga de información (E.19) y la revelación de información (A.19) representan riesgos importantes para la confidencialidad. Además, la alteración (E.15) y la modificación no autorizada de la información (A.15) pueden comprometer la integridad de los datos. De igual manera la indisponibilidad del personal (A.28) presenta riesgos

para la capacidad de los proveedores de cumplir sus obligaciones, afectando la disponibilidad, aunque en menor medida.

[AF] Activos Fijos

[AF.1] Edificio Principal

Figura 35 Valoración de amenazas del activo [AF.1]

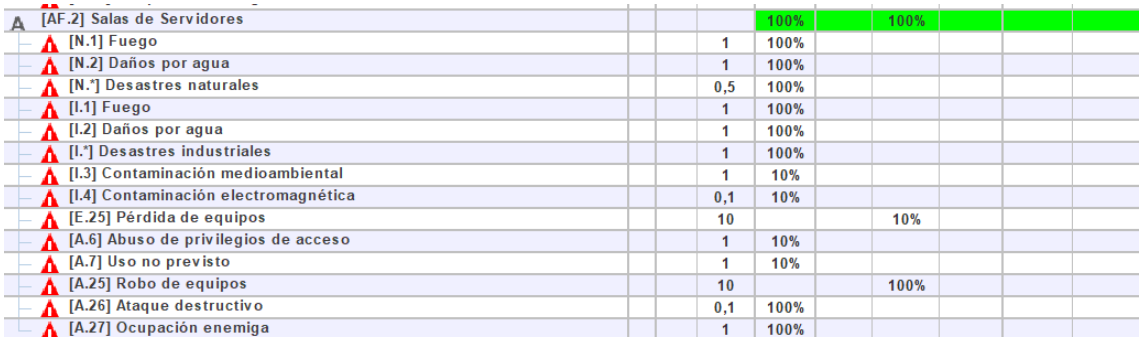


[AF] Activos Físicos						
[AF.1] Edificio Principal			100%		100%	
[N.1] Fuego		1	100%			
[N.2] Daños por agua		1	100%			
[N.*] Desastres naturales		0,5	100%			
[I.1] Fuego		1	100%			
[I.2] Daños por agua		1	100%			
[I.*] Desastres industriales		1	100%			
[I.3] Contaminación medioambiental		1	10%			
[I.4] Contaminación electromagnética		0,1	10%			
[E.25] Pérdida de equipos		10			10%	
[A.6] Abuso de privilegios de acceso		1	10%			
[A.7] Uso no previsto		1	10%			
[A.25] Robo de equipos		10			100%	
[A.26] Ataque destructivo		0,1	100%			
[A.27] Ocupación enemiga		1	100%			

Dentro de los activos fijos, el edificio de la oficina matriz ubicada en la provincia de Los Ríos en el cantón Quinsaloma fue revisado para identificar y valorar las amenazas a las que está expuesta, las principales amenazas identificadas incluyen fuego (N.1), daños por agua (N.2) y desastres naturales (N.7), todos con un impacto del 100% en la disponibilidad e integridad del edificio. Desastres industriales (I.2), ataques destructivos (A.26), y ocupación enemiga (A.27) también representan amenazas críticas con un impacto del 100% en la disponibilidad y seguridad del edificio.

[AF.2] Sala de servidores

Figura 36 Valoración de amenazas del activo [AF.2]



[AF.2] Salas de Servidores			100%		100%	
[N.1] Fuego		1	100%			
[N.2] Daños por agua		1	100%			
[N.*] Desastres naturales		0,5	100%			
[I.1] Fuego		1	100%			
[I.2] Daños por agua		1	100%			
[I.*] Desastres industriales		1	100%			
[I.3] Contaminación medioambiental		1	10%			
[I.4] Contaminación electromagnética		0,1	10%			
[E.25] Pérdida de equipos		10			10%	
[A.6] Abuso de privilegios de acceso		1	10%			
[A.7] Uso no previsto		1	10%			
[A.25] Robo de equipos		10			100%	
[A.26] Ataque destructivo		0,1	100%			
[A.27] Ocupación enemiga		1	100%			

El espacio físico donde se encuentran los servidores están protegidos por controles de acceso sin embargo durante la valoración de las amenazas también existen algunos que podrían afectar este espacio como se muestra en la imagen donde se incluyen fuego (N.1), daños por agua (N.2), y desastres naturales (N.7), todas con un impacto crítico del 100%

en la disponibilidad e integridad de los servidores, subrayando la necesidad de contar con sistemas de protección contra incendios, inundaciones y desastres, así como un plan de recuperación ante desastres. Es por ello que siempre se destaca la importancia de las medidas de seguridad física robustas, incluyendo el control de acceso, vigilancia 24/7, y planes de contingencia para proteger estos activos críticos. La cooperativa ha demostrado contar con todas las medidas de seguridad de este espacio físico.

[AF.4] Generadores Eléctricos

Figura 37 Valoración de amenazas del activo [AF.4]

[AF.4] Generadores Eléctricos				100%					
[N.1] Fuego			0,1	100%					
[N.2] Daños por agua			0,1	50%					
[N.*] Desastres naturales			0,1	100%					
[I.1] Fuego			0,5	100%					
[I.2] Daños por agua			0,5	50%					
[I.*] Desastres industriales			0,5	100%					
[I.3] Contaminación medioambiental			0,1	50%					
[I.9] Interrupción de otros servicios o suministros esenciales			1	1%					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)			1	10%					
[A.7] Uso no previsto			1	50%					
[A.23] Manipulación del hardware			1	50%					
[A.25] Robo de equipos			0,5	100%					
[A.26] Ataque destructivo			1	100%					

Los generadores de eléctricos son indispensables cuando existen cortes de energía, en momentos de crisis energética estos cumplen un papel fundamental sin embargo durante el análisis se identificaron las principales amenazas que son fuego (N.1), desastres naturales (N.7), y ataques destructivos (A.26), todas con un impacto del 100%. También se identifican amenazas como errores de mantenimiento (E.23) que podrían afectar funcionamiento de los generadores.

[AF.5] Cableado de Datos

Figura 38 Valoración de amenazas del activo [AF.5]

[AF.5] Cableado de Datos				100%	10%	50%			
[N.1] Fuego			0,1	100%					
[N.2] Daños por agua			0,1	50%					
[N.*] Desastres naturales			0,1	100%					
[I.1] Fuego			0,5	100%					
[I.2] Daños por agua			0,5	50%					
[I.*] Desastres industriales			0,5	100%					
[I.3] Contaminación medioambiental			0,1	50%					
[I.4] Contaminación electromagnética			0,5	10%					
[I.11] Emanaciones electromagnéticas (TEMPEST)			1			1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)			1	10%					
[A.7] Uso no previsto			1	50%	1%	1%			
[A.11] Acceso no autorizado			1		10%	50%			
[A.23] Manipulación del hardware			1	50%		50%			
[A.25] Robo de equipos			0,8	100%					
[A.26] Ataque destructivo			1	100%					

El cableado de datos también fue analizado por qué son un activo importante para la comunicación de red en la institución, en el análisis se enlistan algunas amenazas entre ellas se encuentran fuego (N.1), desastres naturales (N.*) y desastres industriales (I.*), todas con un impacto del 100% en la disponibilidad. De igual manera otra amenaza importante son las emanaciones electromagnéticas (I.11) que, aunque con menor impacto, podrían afectar la confidencialidad de la información.

3.1.4. Evaluación del impacto potencial sobre los activos

En esta sección se va a analizar el impacto potencial de los activos para lo cual se ha realizado una evaluación qué permitió identificar los activos de la cooperativa Metrópolis, entre ellos se ha determinado distintos niveles de impacto cumpliendo lo establecido en la metodología MAGERIT con el uso de la herramienta PILAR. Esta evaluación tiene como objetivo identificar las consecuencias que podrían suscitarse sobre los activos críticos de la cooperativa, considerando tanto la información como los procesos asociados a cada uno de ellos.

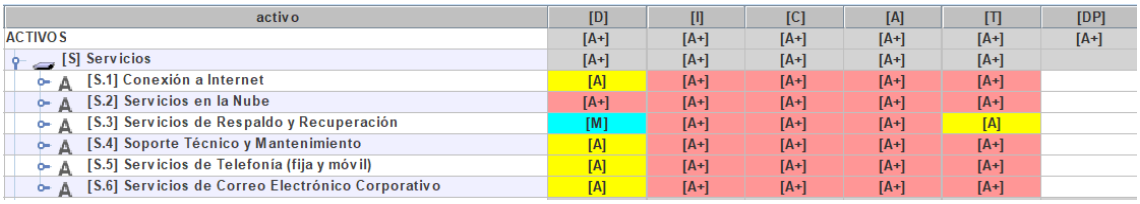
En la fase de Evaluación del Impacto Potencial sobre los activos de la Cooperativa de Ahorro y Crédito, se han determinado distintos niveles de impacto siguiendo la metodología MAGERIT utilizando la herramienta PILAR. La evaluación tiene como objetivo identificar las posibles consecuencias de incidentes sobre los activos críticos de la cooperativa, considerando tanto la información como los procesos asociados. Los niveles de impacto potencial definidos permiten establecer la prioridad de las medidas de seguridad a implementar y optimizar la gestión de riesgos.

A continuación, se describen los niveles de impacto identificados:

Figura 39 Niveles de impacto

[S] Servicios

Figura 40 Valoración del impacto de los activos en la [S]

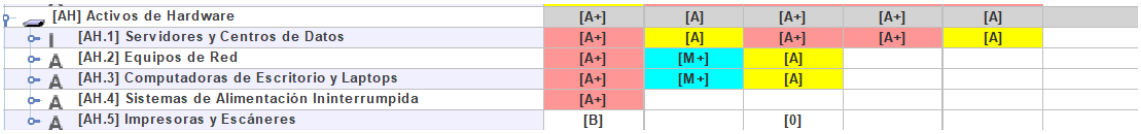


activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[S] Servicios	[A+]	[A+]	[A+]	[A+]	[A+]	
[S.1] Conexión a Internet	[A]	[A+]	[A+]	[A+]	[A+]	
[S.2] Servicios en la Nube	[A+]	[A+]	[A+]	[A+]	[A+]	
[S.3] Servicios de Respaldo y Recuperación	[M]	[A+]	[A+]	[A+]	[A]	
[S.4] Soporte Técnico y Mantenimiento	[A]	[A+]	[A+]	[A+]	[A+]	
[S.5] Servicios de Telefonía (fija y móvil)	[A]	[A+]	[A+]	[A+]	[A+]	
[S.6] Servicios de Correo Electrónico Corporativo	[A]	[A+]	[A+]	[A+]	[A+]	

Los servicios que tiene contratada la cooperativa para mantener sus actividades diarias y respaldos de la información son importantes, para lo cual se realizó una valoración del impacto. El resultado indica que los activos relacionados con los servicios críticos, como la Conexión a Internet, Servicios en la Nube, y el Correo Electrónico Corporativo, presentan niveles de impacto A+ en la mayoría de las dimensiones evaluadas.

[AH] Activos de Hardware

Figura 41 Valoración del impacto de los activos en la [AH]

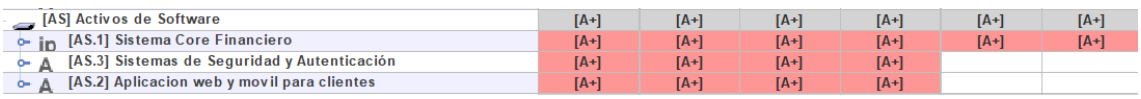


[AH] Activos de Hardware	[A+]	[A]	[A+]	[A+]	[A]
[AH.1] Servidores y Centros de Datos	[A+]	[A]	[A+]	[A+]	[A]
[AH.2] Equipos de Red	[A+]	[M+]	[A]		
[AH.3] Computadoras de Escritorio y Laptops	[A+]	[M+]	[A]		
[AH.4] Sistemas de Alimentación Ininterrumpida	[A+]				
[AH.5] Impresoras y Escáneres	[B]		[0]		

El análisis y valoración del impacto de los activos de hardware de la cooperativa indica que los Servidores y Centros de Datos, Equipos de Red y Sistemas de Alimentación Ininterrumpida son activos fundamentales para la infraestructura tecnológica de la cooperativa, con un impacto evaluado en A+ en la mayoría de las dimensiones. Además, las Computadoras de Escritorio y Laptops presentan un impacto M+ en integridad.

[AS] Activos de Software

Figura 42 Valoración del impacto de los activos en la [AS]



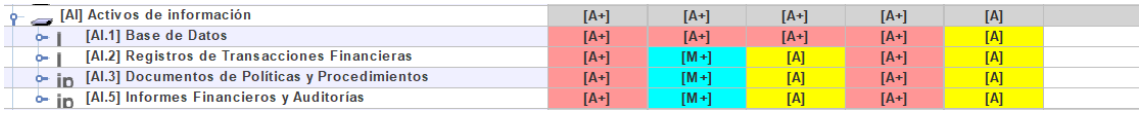
[AS] Activos de Software	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[AS.1] Sistema Core Financiero	[A+]	[A+]	[A+]	[A+]	[A+]	[A+]
[AS.3] Sistemas de Seguridad y Autenticación	[A+]	[A+]	[A+]	[A+]		
[AS.2] Aplicacion web y movil para clientes	[A+]	[A+]	[A+]	[A+]		

Por otra parte, también se realizó la valoración del impacto de los activos de software y como se muestra en la imagen el resultado demuestra que los sistemas Core Financiero, de Seguridad y Autenticación, y la Aplicación Web y Móvil para clientes presentan un impacto A+ en todas las dimensiones evaluadas. Estos sistemas son cruciales para el

funcionamiento diario de la cooperativa y para la satisfacción de los clientes, ya que manejan información sensible y soportan procesos esenciales.

[AI] Activos de Información

Figura 43 Valoración del impacto de los activos en la [AI]

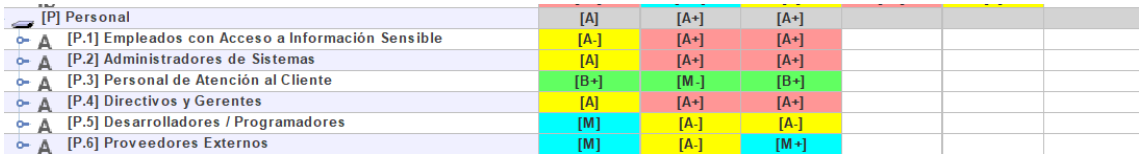


[AI] Activos de información	[A+]	[A+]	[A+]	[A+]	[A]
[AI.1] Base de Datos	[A+]	[A+]	[A+]	[A+]	[A]
[AI.2] Registros de Transacciones Financieras	[A+]	[M+]	[A]	[A+]	[A]
[AI.3] Documentos de Políticas y Procedimientos	[A+]	[M+]	[A]	[A+]	[A]
[AI.5] Informes Financieros y Auditorías	[A+]	[M+]	[A]	[A+]	[A]

Los activos de información, como la Base de Datos, Registros de Transacciones Financieras, Documentos de Políticas y Procedimientos, e Informes Financieros y Auditorías, presentan niveles de impacto A+ en su mayoría, especialmente en confidencialidad e integridad.

[P] Personal

Figura 44 Valoración del impacto de los activos en la [P]

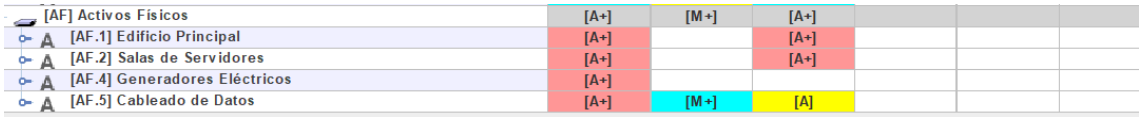


[P] Personal	[A]	[A+]	[A+]		
[P.1] Empleados con Acceso a Información Sensible	[A-]	[A+]	[A+]		
[P.2] Administradores de Sistemas	[A]	[A+]	[A+]		
[P.3] Personal de Atención al Cliente	[B+]	[M-]	[B+]		
[P.4] Directivos y Gerentes	[A]	[A+]	[A+]		
[P.5] Desarrolladores / Programadores	[M]	[A-]	[A-]		
[P.6] Proveedores Externos	[M]	[A-]	[M+]		

En el en el análisis y valoración del impacto de los cargos críticos los resultados demuestran que los colaboradores con acceso a información sensible y los administradores de sistemas presentan niveles de impacto A+ en varias dimensiones, destacando la importancia de controles estrictos de acceso y capacitación en seguridad. Es decir que también el personal de atención al cliente y los desarrolladores tienen un nivel M o B+, lo cual indica que su rol, aunque importante, no tiene un impacto crítico en todas las dimensiones, pero se requiere monitoreo para evitar posibles riesgos derivados del uso indebido de privilegios.

[AF] Activos Físicos

Figura 45 Valoración del impacto de los activos en la [AF]



[AF] Activos Físicos	[A+]	[M+]	[A+]		
[AF.1] Edificio Principal	[A+]		[A+]		
[AF.2] Salas de Servidores	[A+]		[A+]		
[AF.4] Generadores Eléctricos	[A+]				
[AF.5] Cableado de Datos	[A+]	[M+]	[A]		

Los activos físicos, como el Edificio Principal, Salas de Servidores, Generadores Eléctricos y Cableado de Datos también presentan niveles de impacto A+ en la mayoría de las dimensiones.

3.1.5. Evaluación del nivel de riesgo asociado

A continuación, se presentan los resultados de la Evaluación del nivel de riesgo asociado a los activos de la Cooperativa Metrópolis, utilizando la herramienta Pilar. La evaluación se basa en la categorización de los niveles de criticidad de 0 a 9, que va desde "despreciable" hasta "catástrofe", con el fin de identificar los activos más vulnerables, con un coloreado para realzar la visibilidad:

Figura 46 Niveles de criticidad

[S] Servicios

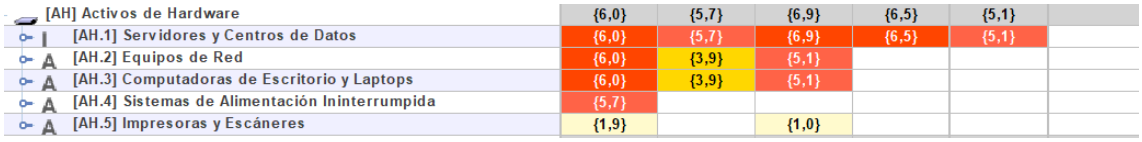
Figura 47 Evaluación del nivel de riesgo de los activos de la categoría [S]

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{6,5}	{6,5}	{6,9}	{7,4}	{6,3}	{6,5}
[S] Servicios	{6,5}	{6,5}	{6,5}	{5,7}	{6,3}	
[S.1] Conexión a Internet	{6,0}	{6,0}	{5,7}	{5,7}	{6,3}	
[S.2] Servicios en la Nube	{6,5}	{6,5}	{6,5}	{5,0}	{5,7}	
[S.3] Servicios de Respaldo y Recuperación	{4,2}	{6,0}	{5,7}	{5,7}	{5,7}	
[S.4] Soporte Técnico y Mantenimiento	{6,0}	{6,0}	{5,7}	{5,7}	{6,3}	
[S.5] Servicios de Telefonía (fija y móvil)	{5,1}	{5,1}	{5,1}	{5,0}	{5,7}	
[S.6] Servicios de Correo Electrónico Corporativo	{6,0}	{6,0}	{5,7}	{5,7}	{6,3}	

Los resultados de la evaluación del nivel de riesgos de los activos de la categoría servicios muestran que los servicios de conexión a Internet y los servicios en la nube presentan un nivel de riesgo muy crítico, con una puntuación de {6.5}. De igual manera, los servicios de respaldo y recuperación, soporte técnico y servicios de telefonía (fija y móvil) también muestran niveles de riesgo elevados, con valores entre {5.7} y {6.0}.

[AH] Activos de Hardware

Figura 48 Evaluación del nivel de riesgo de los activos de la categoría [AH]

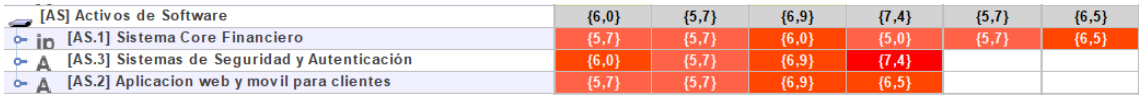


[AH] Activos de Hardware	{6,0}	{5,7}	{6,9}	{6,5}	{5,1}	
[AH.1] Servidores y Centros de Datos	{6,0}	{5,7}	{6,9}	{6,5}	{5,1}	
[AH.2] Equipos de Red	{6,0}	{3,9}	{5,1}			
[AH.3] Computadoras de Escritorio y Laptops	{6,0}	{3,9}	{5,1}			
[AH.4] Sistemas de Alimentación Ininterrumpida	{5,7}					
[AH.5] Impresoras y Escáneres	{1,9}		{1,0}			

En cuanto a los activos de hardware, los servidores y centros de datos, así como los equipos de red, se encuentran en un nivel de riesgo muy crítico ({6.9}). Las computadoras de escritorio y laptops presentan un nivel de riesgo crítico ({5.1}).

[AS] Activos de Software

Figura 49 Evaluación del nivel de riesgo de los activos de la categoría [AS]

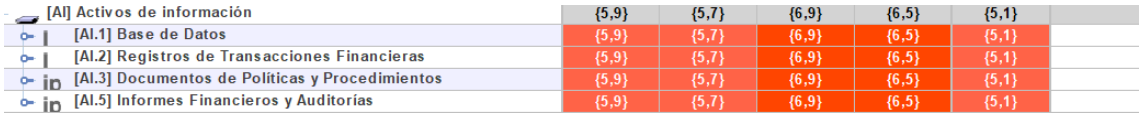


[AS] Activos de Software	{6,0}	{5,7}	{6,9}	{7,4}	{5,7}	{6,5}
[AS.1] Sistema Core Financiero	{5,7}	{5,7}	{6,0}	{5,0}	{5,7}	{6,5}
[AS.3] Sistemas de Seguridad y Autenticación	{6,0}	{5,7}	{6,9}	{7,4}		
[AS.2] Aplicacion web y movil para clientes	{5,7}	{5,7}	{6,9}	{6,5}		

Además, en una evaluación el nivel de riesgo de los de software como es el Core financiero y los sistemas de seguridad y autenticación, presentan un nivel de riesgo muy crítico ({6.9} y {6.0}, respectivamente), esto sugiere que cualquier compromiso en estos sistemas podría tener un impacto severo en la estabilidad financiera y la seguridad de la información de la cooperativa. La aplicación web y móvil para clientes también presenta un riesgo crítico ({5.7}).

[AI] Activos de Información

Figura 50 Evaluación del nivel de riesgo de los activos de la categoría [AI]

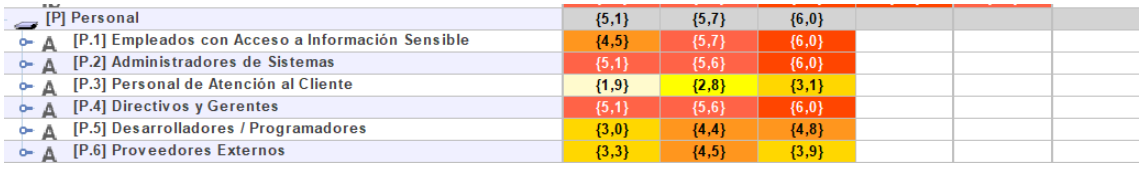


[AI] Activos de información	{5,9}	{5,7}	{6,9}	{6,5}	{5,1}	
[AI.1] Base de Datos	{5,9}	{5,7}	{6,9}	{6,5}	{5,1}	
[AI.2] Registros de Transacciones Financieras	{5,9}	{5,7}	{6,9}	{6,5}	{5,1}	
[AI.3] Documentos de Políticas y Procedimientos	{5,9}	{5,7}	{6,9}	{6,5}	{5,1}	
[AI.5] Informes Financieros y Auditorías	{5,9}	{5,7}	{6,9}	{6,5}	{5,1}	

En lo que respecta a los activos de información, la base de datos y los registros de transacciones financieras tienen niveles de riesgo muy críticos ({6.9} y {6.0}). Los documentos de políticas y procedimientos.

[P] Personal

Figura 51 Evaluación del nivel de riesgo de los activos de la categoría [P]

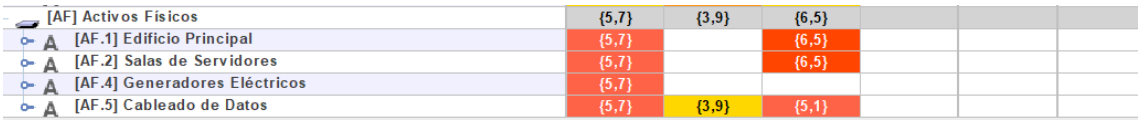


[P] Personal	{5,1}	{5,7}	{6,0}			
[P.1] Empleados con Acceso a Información Sensible	{4,5}	{5,7}	{6,0}			
[P.2] Administradores de Sistemas	{5,1}	{5,6}	{6,0}			
[P.3] Personal de Atención al Cliente	{1,9}	{2,8}	{3,1}			
[P.4] Directivos y Gerentes	{5,1}	{5,6}	{6,0}			
[P.5] Desarrolladores / Programadores	{3,0}	{4,4}	{4,8}			
[P.6] Proveedores Externos	{3,3}	{4,5}	{3,9}			

El personal de atención al cliente se evalúa con un nivel de riesgo alto ({3.1}), lo cual refleja la posibilidad de errores humanos que podrían comprometer la seguridad de la información. Por otro lado, los administradores de sistemas presentan un riesgo muy crítico ({6.0}), siendo fundamental su capacitación continua en ciberseguridad. Los directivos, gerentes y desarrolladores también presentan riesgos significativos, con valores de {4.8}.

[AF] Activos Físicos

Figura 52 Evaluación del nivel de riesgo de los activos de la categoría [AF]



[AF] Activos Físicos	{5,7}	{3,9}	{6,5}			
[AF.1] Edificio Principal	{5,7}		{6,5}			
[AF.2] Salas de Servidores	{5,7}		{6,5}			
[AF.4] Generadores Eléctricos	{5,7}					
[AF.5] Cableado de Datos	{5,7}	{3,9}	{5,1}			

Finalmente, los activos físicos, como el edificio principal y las salas de servidores, presentan niveles de riesgo crítico y muy crítico ({5.7} y {6.5}, respectivamente). Los generadores eléctricos y el cableado de datos también presentan un riesgo crítico ({5.1}), lo que subraya la necesidad de implementar mecanismos de protección adicionales para asegurar la continuidad del servicio en caso de incidentes físicos.

3.1.6. Análisis de Salvaguardas

De acuerdo con el análisis realizado se ha identificado salvaguardas que permiten mejorar la protección ante posibles riesgos. En tal virtud, se evalúan distintas salvaguardas, clasificadas por su nivel de nivel actual ("current") y el nivel objetivo ("target"). Se han considerado las salvaguardas más importantes que se consideran necesitas aplicar en el presente análisis de riesgos de la Cooperativa Metrópolis.

Tabla 6 Aspecto que trata la salvaguarda

G	Para Gestión
T	Para Técnico
F	Para Seguridad Física
P	Para Gestión del Personal

FUENTE: PILAR

A continuación, te detallo las salvaguardas más relevantes, basándome en los valores de "nivel actual" que están en los niveles críticos (L4 o superior), donde es prioritario tomar medidas:

Figura 53 Matriz de salvaguardas

aspecto	tdp	recomendación		nivel	salvaguarda	...	...	...	current	target	...	PILAR
					SALVAGUARDAS				_-L4	_-L5	...	L2-L5
G	EL	8			[IA] Identificación y autenticación				_-L4	_-L4	...	L2-L4
T	EL	7			[AC] Control de acceso lógico				L3	L5	...	L2-L4
G	PR	8			[D] Protección de la Información				L3	L5	...	L2-L5
G	EL	8			[K] Protección de claves criptográficas [SC-12]				L2	L3	...	L2-L5
G	PR	5			[S] Protección de los Servicios				L3	L4	...	L2-L3
G	PR	5			[SW] Protección de las Aplicaciones Informáticas (SW)				L3	L4	...	L2-L3
G	PR	5			[HW] Protección de los Equipos Informáticos (HW)				L3	L4	...	L2-L3
G	PR	9			[COM] Protección de las Comunicaciones				L3	L3	...	L2-L5
G	PR				[M] Protección de los Soportes de Información				L2	L4	...	n.a.
G	PR	5			[AUX] Elementos Auxiliares				L4	L4	...	L2-L3
F	EL	5			[PPE] Protección física de los equipos				L4	L5	...	L3
F	PR	5			[L] Protección de las Instalaciones				L4	L5	...	L2-L3
P	PR	5			[P] Gestión del Personal				L2	L3	...	L2-L3
G	CR	5			[IM] Gestión de incidentes				L2	L3	...	L2-L3
T	PR	7			[tools] Herramientas de seguridad				L4	L5	...	L2-L4
G	CR	3			[V] Gestión de vulnerabilidades				L3	L3	...	L2-L3
T	MN	4			[A] Registro y auditoría				L2	L4	...	L2-L3
G	RC	3			[BC] Continuidad del negocio				L2	L4	...	L2-L3
G	AD	4			[G] Organización				L2	L3	...	L2-L3
G	AD	5			[E] Relaciones Externas				L2	L3	...	L2-L3
G	AD	5			[NEW] Adquisición / desarrollo				L3	L4	...	L2-L3
G	PR	7			[PDS] Servicios potencialmente peligrosos				L3	L4	...	L2-L4
G	PR				[IP] Sistema de protección de frontera lógica				L4	L5	...	n.a.
F	EL				[PPS] Protección del perímetro físico				L4	L5	...	n.a.
G	EL	2			[TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]				L1	L2	...	L2

Entre las salvaguardas que más destacan están:

Tabla 7 Salvaguardas con mayor criticidad

Salvaguarda:	**Nivel actual:**	**Nivel objetivo:**	**Recomendación ..**	**Observación:**
Identificación y autenticación	L4	L5	8	Este control es fundamental para asegurar que solo usuarios autorizados accedan a los sistemas. Se necesita fortalecer esta área para alcanzar el nivel objetivo.
Control de acceso lógico	L4	L5	7	Es crucial mejorar la gestión de acceso para proteger la información de accesos no autorizados.
Protección de la Información	L3	L5	7	Este aspecto requiere especial atención para asegurar la confidencialidad e integridad de la información sensible.
Protección de claves criptográficas	L2	L5	8	La protección de claves es un pilar de la seguridad. Mejorar su manejo y almacenamiento es crítico para fortalecer la infraestructura de seguridad.

Gestión de incidentes	L4	L5	7	Contar con una respuesta efectiva ante incidentes es crucial. Aumentar la capacidad de respuesta ante incidentes ayudará a reducir riesgos.
Protección de los Servicios (Servicios Informáticos SW)	L3	L5	5	Proteger los servicios informáticos es clave para mantener la continuidad operativa y evitar interrupciones de servicios esenciales.
Gestión de vulnerabilidades	L4	L5	7	La identificación y mitigación de vulnerabilidades son esenciales para reducir los riesgos a tiempo. Se recomienda mejorar en este aspecto.
Continuidad del negocio	L3	L5	6	La preparación ante interrupciones es vital para garantizar la continuidad de operaciones. Se debe optimizar la estrategia de continuidad.

Las áreas con mayor prioridad de mejora incluyen la identificación y autenticación, control de acceso lógico, y gestión de vulnerabilidades. En todas estas salvaguardas es esencial alcanzar o superar el nivel objetivo para reducir los riesgos y mejorar la seguridad general del sistema.

Cada salvaguarda está clasificada de acuerdo con el tipo de protección, la clasificación se detalla en la siguiente tabla:

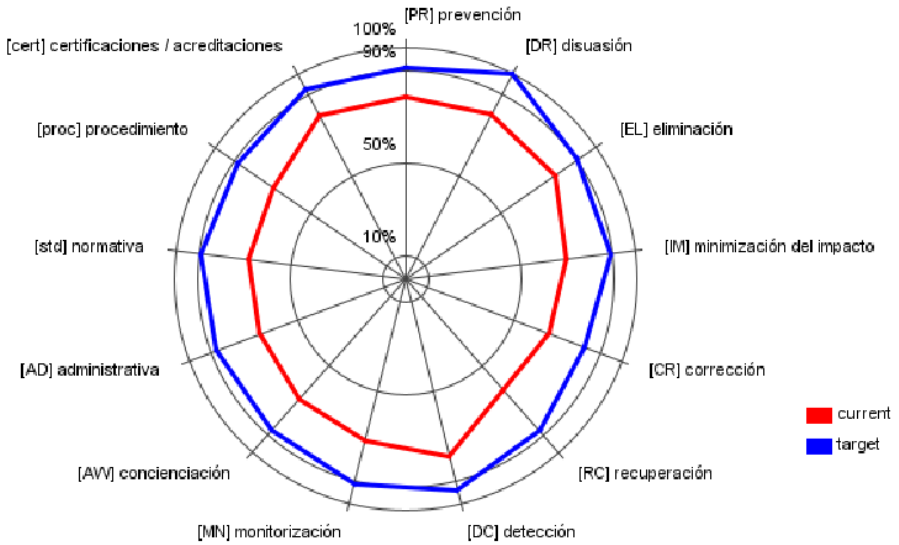
Tabla 8 Tipo de protección de salvaguardas

PR	prevención
DR	disuasión
EL	eliminación
IM	minimización del impacto
CR	corrección
RC	recuperación
AD	administrativa
AW	concienciación
DC	detección
MN	monitorización
std	Norma
proc	Procedimiento
cert	Certificación o acreditación

FUENTE: PILAR

A continuación, se muestra un gráfico radar con los resultados del Tipo de protección:

Figura 54 Grafico radar de Tipos de protección



Este gráfico de radar muestra una comparación entre los niveles actuales de seguridad (en rojo) y los niveles objetivo (en azul) en varias categorías de control. A continuación, detallo un análisis de los puntos clave:

Tabla 9 Análisis de resultados según el tipo de protección

Tipo de protección	**Observación**
Prevención (PR)	Hay una brecha significativa entre el nivel actual y el objetivo. Es prioritario mejorar la capacidad de prevención para evitar incidentes de seguridad.
Disuasión (DR) y Eliminación (EL)	Ambas áreas también muestran un desfase notable. La disuasión es crucial para reducir la probabilidad de ataques, y la eliminación asegura que se mitiguen amenazas conocidas. Se recomienda fortalecer las políticas y controles en estas áreas.
Minimización del Impacto (IM)	Aunque la brecha es menor, aún hay margen de mejora para reducir el impacto en caso de que ocurra un incidente de seguridad.
Corrección (CR) y Recuperación (RC)	Estas dos áreas están mejor cubiertas, pero aún no alcanzan el nivel objetivo. Se sugiere optimizar los planes de contingencia y recuperación para asegurar una respuesta rápida y efectiva ante incidentes.
Detección (DC) y Monitorización (MN)	Estas áreas están relativamente cercanas al objetivo, lo que indica que existen controles de detección y monitorización efectivos, aunque con espacio para mejoras para alcanzar el nivel deseado.

Concienciación (AW) y Normativa (std)	Hay una discrepancia importante entre el nivel actual y el objetivo. Es esencial reforzar la capacitación y concienciación de los empleados, así como mejorar la normativa interna para alinearse con mejores prácticas.
Administrativa (AD) y Procedimiento (proc)	Existen brechas considerables en estos controles. Se debe trabajar en mejorar las políticas y procedimientos administrativos para alcanzar un nivel de seguridad adecuado.
Certificaciones / Acreditaciones (cert)	Esta es otra área con una diferencia notoria. Obtener certificaciones puede fortalecer la postura de seguridad y demostrar conformidad con normas y estándares de la industria.

El análisis revela que, en general, hay deficiencias en varias áreas clave, en particular en prevención, disuasión, eliminación, normativa y concienciación. Para acercarse al nivel objetivo, es recomendable implementar medidas adicionales en estas áreas, así como en certificaciones y procedimientos administrativos. Esto ayudará a crear una infraestructura de seguridad más sólida y resiliente.

IMPACTO

Los siguientes gráficos fueron generados en la herramienta PILAR, el impacto acumulado en distintos activos claves, comparando el nivel potencial (rojo), el actual (azul), y el objetivo (verde). A continuación, el análisis detallado por cada activo:

Servicios [S]

Figura 55 Impacto acumulado de los activos en categoría Servicios [S]

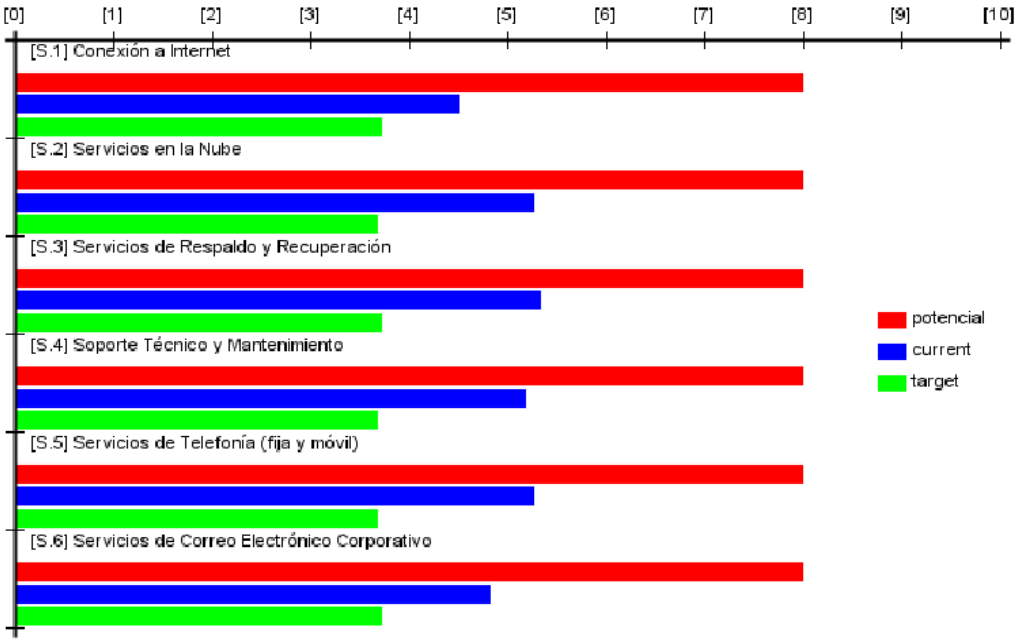


Tabla 10 Análisis del impacto acumulado de los activos en categoría Servicios [S]

Activo	**Análisis**
Conexión a Internet (S.1)	El impacto potencial es máximo, indicando que cualquier vulnerabilidad en la conexión a Internet podría ser crítico. Se recomienda reducir el impacto actual hasta alcanzar el objetivo.
Servicios en la Nube (S.2)	Los servicios en la nube tienen un impacto significativo. Se debe trabajar para reducir el riesgo actual hacia el objetivo para asegurar una mayor protección de datos y continuidad en la nube.
Servicios de Respaldo y Recuperación (S.3)	Dado el alto impacto potencial, es esencial reducir el riesgo actual, asegurando que los planes de respaldo y recuperación sean sólidos y efectivos.
Soporte Técnico y Mantenimiento (S.4)	El soporte técnico y mantenimiento tiene un impacto potencial considerable. Reducir su nivel actual mejorará la resiliencia operativa.
Servicios de Telefonía (fija y móvil) (S.5)	Las telecomunicaciones son críticas. Reducir el impacto en este servicio ayudará a evitar interrupciones en la comunicación interna y externa.
Servicios de Correo Electrónico Corporativo (S.6)	El correo electrónico es vital y presenta un alto impacto potencial. Es necesario bajar el impacto actual para minimizar riesgos de seguridad y disponibilidad.

En todos los activos se observa que el impacto potencial es elevado, lo que implica que cualquier vulnerabilidad podría tener consecuencias significativas. Actualmente, el nivel actual está en niveles moderados, pero lejos de los objetivos (verde). Para mitigar riesgos, es recomendable implementar controles más estrictos y revisar los procedimientos en cada uno de estos activos para acercarse a los niveles de impacto objetivo y garantizar una mayor seguridad y continuidad operativa.

Figura 56 Impacto acumulado de los activos en categoría Activos de Hardware [AH]

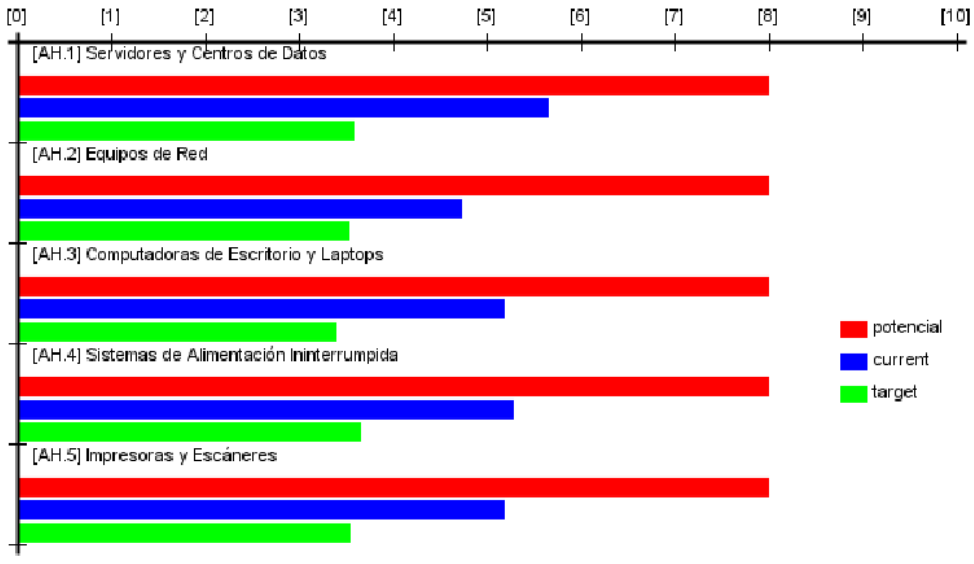


Tabla 11 Análisis del Impacto acumulado de los activos en categoría Activos de Hardware [AH]

Activo	**Análisis**
Servidores y Centros de Datos (AH.1)	Los servidores y centros de datos son críticos, con el máximo impacto potencial. Se requiere una reducción significativa del riesgo actual para proteger estos activos clave.
Equipos de Red (AH.2)	La infraestructura de red es esencial para la conectividad. Es importante reducir el impacto actual para asegurar la continuidad y la integridad de las comunicaciones.
Computadoras de Escritorio y Laptops (AH.3)	Las computadoras de los empleados son vulnerables y tienen un impacto considerable. Se recomienda fortalecer las medidas de seguridad para reducir el riesgo actual.
Sistemas de Alimentación Ininterrumpida (AH.4)	Los sistemas de respaldo de energía son cruciales para la continuidad operativa. Reducir el impacto actual es necesario para evitar interrupciones ante fallas de energía.
Impresoras y Escáneres (AH.5)	Aunque su impacto es menor comparado con otros activos, aún representan un riesgo. Se recomienda mejorar las prácticas de seguridad para reducir su impacto actual.

Se observa que todos los activos tienen un impacto potencial alto o muy alto. Los niveles actuales están en un rango moderado, pero aún están lejos de los objetivos. Para mitigar riesgos, es fundamental implementar controles adicionales en los Servidores y Centros de Datos, así como en los Sistemas de Alimentación Ininterrumpida y Equipos de Red. Esto ayudará a alcanzar los niveles de impacto objetivo, garantizando una mayor seguridad y resiliencia operativa en los activos críticos.

Figura 57 Impacto acumulado de los activos en categoría Activos de Software [AS]

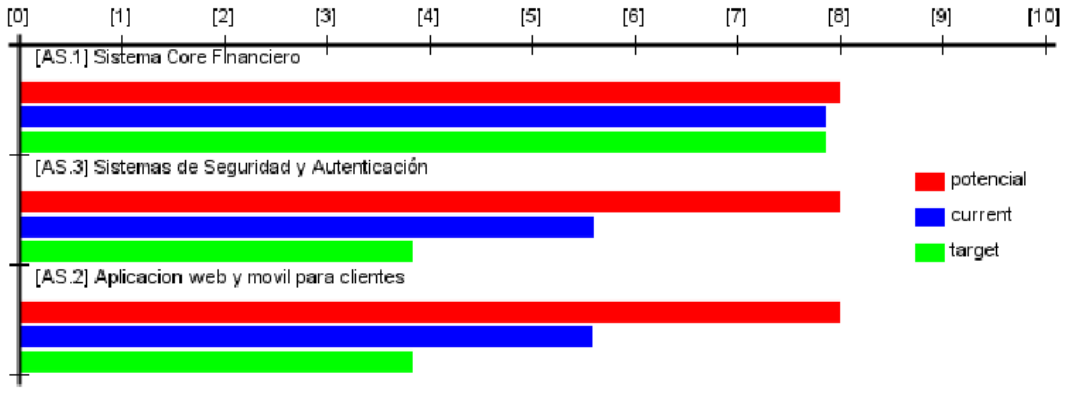


Tabla 12 Análisis del Impacto acumulado de los activos en categoría Activos de Software [AS]

Activo	**Análisis**
Sistema Core Financiero (AS.1)	Este es uno de los sistemas más críticos debido a su función en las operaciones financieras. Aunque el impacto actual se ha reducido en comparación con el potencial, aún está muy por encima del objetivo. Se recomienda implementar controles adicionales para reducir el riesgo en este sistema.
Aplicación Web y Móvil para Clientes (AS.2)	La aplicación web y móvil tiene un impacto considerable, especialmente porque interactúa con clientes y puede ser vulnerable a ataques externos. Es necesario trabajar en medidas adicionales para acercarse al nivel objetivo y asegurar una experiencia segura para los usuarios.
Sistemas de Seguridad y Autenticación (AS.3)	Este sistema es fundamental para proteger la infraestructura y los datos de acceso. El nivel actual es moderado, pero aún se requiere reducirlo significativamente para cumplir con el objetivo y mejorar la postura de seguridad general.

Todos los sistemas aquí analizados presentan un impacto potencial alto o muy alto, destacando especialmente el Sistema Core Financiero y la Aplicación Web y Móvil para Clientes. Los niveles actuales están en un rango más controlado, pero aún se encuentran lejos de los objetivos. Para minimizar riesgos, es fundamental fortalecer las medidas de seguridad, especialmente en el Sistema Core Financiero, que es el más crítico en términos de impacto. Esto contribuirá a mejorar la resiliencia y a reducir vulnerabilidades en los sistemas clave de la organización.

Figura 58 Impacto acumulado de los activos en categoría Activos de Información [AI]

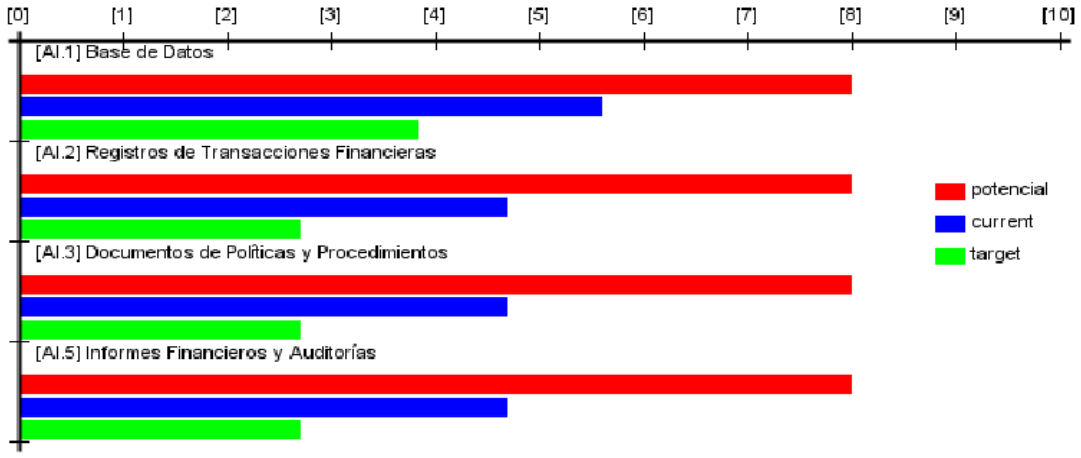


Tabla 13Análisis del Impacto acumulado de los activos en categoría Activos de Información [AI]

Activo	**Análisis**
Base de Datos (AI.1)	Las bases de datos son activos críticos debido a la gran cantidad de información almacenada. Es necesario reducir el impacto actual para proteger adecuadamente estos datos y acercarse al nivel objetivo.
Registros de Transacciones Financieras (AI.2)	Los registros financieros son de alto riesgo debido a su sensibilidad. Se requiere mejorar las medidas de protección para reducir el impacto actual y alinearse con el nivel objetivo, minimizando riesgos de fraude o manipulación de datos.
Documentos de Políticas y Procedimientos (AI.3)	La documentación de políticas es importante para la gobernanza y cumplimiento. Reducir el impacto actual es esencial para garantizar que las políticas y procedimientos sean seguros y accesibles solo para personal autorizado.
Informes Financieros y Auditorías (AI.5)	Los informes financieros y auditorías son fundamentales para la transparencia y regulación. Es prioritario disminuir el riesgo actual y proteger estos documentos para evitar pérdidas o manipulaciones.

El impacto potencial es alto o muy alto para todos los activos de información, lo que subraya la necesidad de robustecer las medidas de seguridad. Los niveles actuales son moderados, pero aún están por encima de los objetivos. Para reducir riesgos, es crucial implementar controles adicionales en las Bases de Datos y Registros de Transacciones Financieras, que presentan el impacto más crítico. Esto ayudará a proteger la información sensible y asegurar la integridad de los datos en la organización.

Figura 59 Impacto acumulado de los activos en categoría Personal [P]

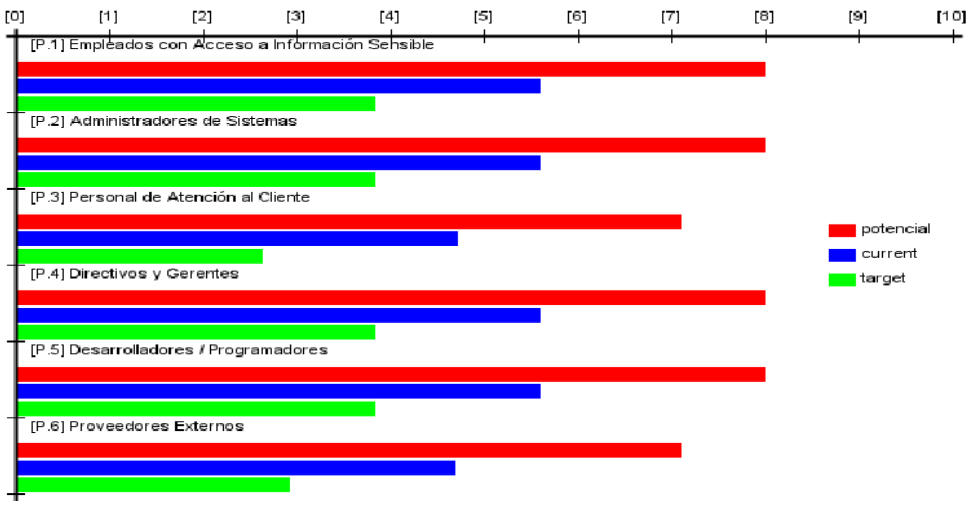


Tabla 14 Análisis del Impacto acumulado de los activos en categoría Personal [P]

Activo	**Análisis**
Empleados con Acceso a Información Sensible (P.1)	Estos empleados tienen un impacto potencial crítico, dado su acceso a datos sensibles. Es fundamental implementar controles adicionales para reducir el impacto actual y asegurar la protección de esta información.
Administradores de Sistemas (P.2)	Los administradores de sistemas son clave para la seguridad de la infraestructura. Reducir el impacto actual es esencial para evitar riesgos derivados de posibles errores o accesos indebidos.
Personal de Atención al Cliente (P.3)	Este grupo tiene un impacto menor en comparación con otros, pero aún es importante reducirlo un poco más para alcanzar el objetivo, minimizando el riesgo en interacciones directas con los clientes.
Directivos y Gerentes (P.4)	Los directivos y gerentes tienen acceso a información estratégica. Es crucial implementar controles de seguridad adicionales para proteger la información a la que acceden.
Desarrolladores / Programadores (P.5)	Los desarrolladores tienen un impacto potencial alto debido a su rol en la creación y mantenimiento de sistemas. Reducir su nivel de impacto actual ayudará a asegurar que el código y los sistemas se mantengan seguros.
Proveedores Externos (P.6)	Los proveedores externos pueden representar un riesgo considerable si no están debidamente gestionados. Alcanzar el nivel objetivo ayudará a minimizar el riesgo de accesos no autorizados o vulnerabilidades introducidas a través de terceros.

Los grupos con impacto potencial más alto son los Empleados con Acceso a Información Sensible, Administradores de Sistemas y Desarrolladores/Programadores, debido a su acceso a información crítica y su rol en la infraestructura de TI. Aunque los niveles actuales han sido mitigados en cierta medida, aún es necesario implementar controles adicionales para alcanzar los objetivos. En particular, se deben enfocar esfuerzos en fortalecer los controles de acceso y realizar capacitación en seguridad.

Figura 60 Impacto acumulado de los activos en categoría Activos Físicos [AF]

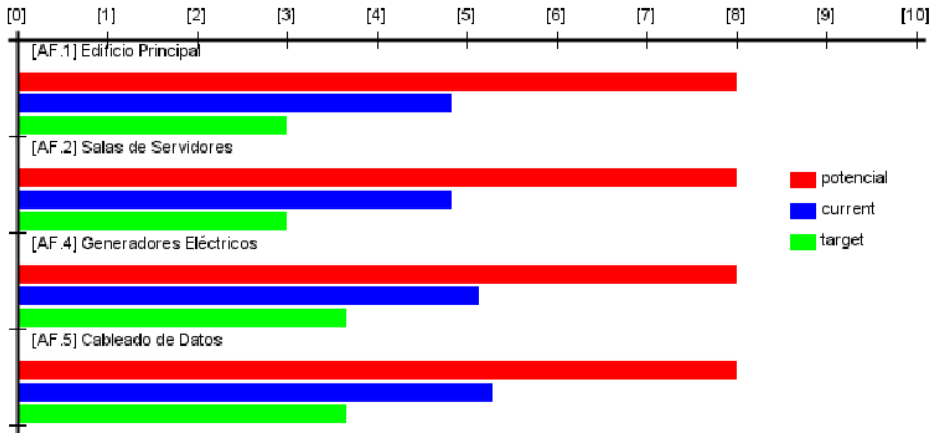


Tabla 15 Análisis del Impacto acumulado de los activos en categoría Activos Físicos [AF]

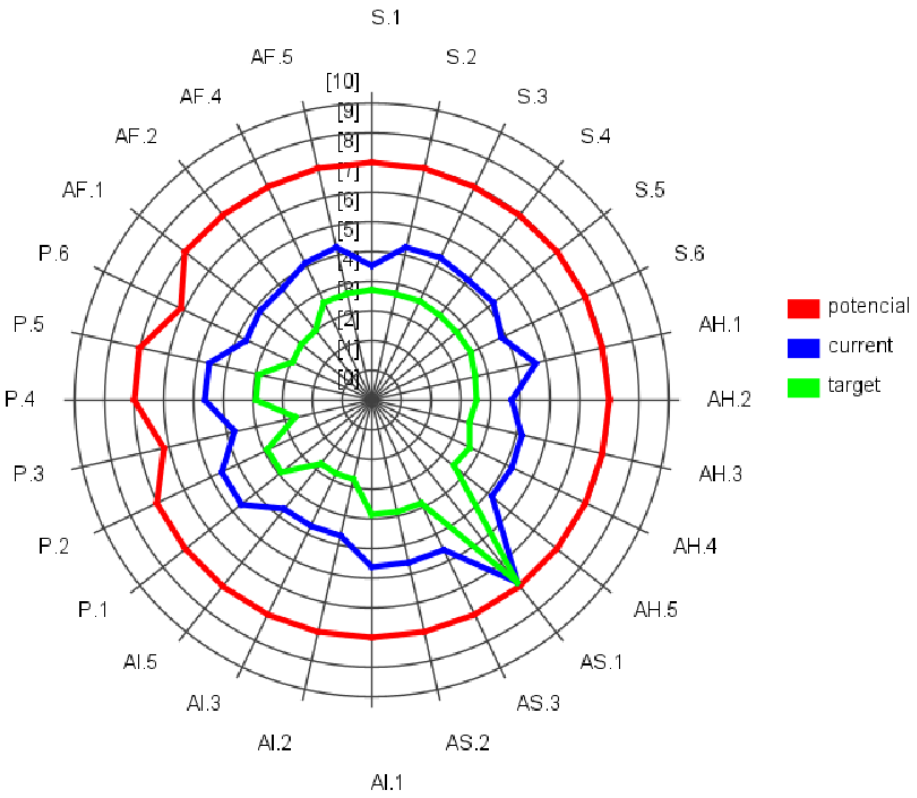
Activo	**Análisis**
Edificio Principal (AF.1)	El edificio principal es fundamental para la infraestructura física de la organización. A pesar de la reducción del impacto actual, sigue siendo alto. Se recomienda mejorar las medidas de seguridad física y protección de instalaciones para acercarse al nivel objetivo.
Salas de Servidores (AF.2)	Las salas de servidores son activos críticos debido a la concentración de infraestructura tecnológica. Se deben implementar controles adicionales de seguridad y condiciones ambientales para reducir el riesgo.
Generadores Eléctricos (AF.4)	Los generadores eléctricos son vitales para la continuidad operativa durante interrupciones de energía. La reducción del impacto actual es crucial para garantizar un suministro eléctrico estable y sin interrupciones.
Cableado de Datos (AF.5)	El cableado de datos es fundamental para la conectividad de red interna. Fortalecer las medidas de protección y ordenamiento del cableado ayudará a reducir el impacto y asegurar la continuidad de la comunicación.

Todos los activos físicos analizados presentan un impacto potencial alto o muy alto, destacando especialmente el Edificio Principal y las Salas de Servidores. Los niveles actuales han sido mitigados parcialmente, pero aún se encuentran por encima de los objetivos. Para reducir riesgos, es necesario implementar controles adicionales de seguridad física, protección contra incendios, control ambiental y medidas de continuidad eléctrica, especialmente en el Edificio Principal, Salas de Servidores, y Generadores Eléctricos. Esto contribuirá a la protección de la infraestructura física crítica y garantizará la resiliencia operativa de la organización.

3.1.7. Resumen del impacto

Este gráfico de radar muestra el impacto acumulado en diversas categorías de activos, incluyendo Sistemas (S), Activos Físicos (AF), Activos Humanos (P), Activos de Información (AI), Activos Hardware (AH), y Aplicaciones y Servicios (AS). Cada línea representa el impacto potencial (rojo), actual (azul) y objetivo (verde) en cada una de estas categorías. A continuación, el análisis de los puntos clave:

Figura 61 Gráfico radar del impacto



Impacto Potencial (Rojo):

La línea roja muestra que el impacto potencial es muy alto en casi todas las categorías de activos, alcanzando niveles cercanos al 9 o 10 en varias áreas, como:

Edificio Principal (AF.1), Salas de Servidores (AF.2), y Generadores Eléctricos (AF.4).

Sistema Core Financiero (AS.1) y Servicios en la Nube (S.2).

Empleados con Acceso a Información Sensible (P.1) y Administradores de Sistemas (P.2).

Este alto nivel de riesgo potencial indica que cualquier vulnerabilidad en estos activos podría tener un impacto severo en la organización.

Impacto Actual (Azul):

La línea azul muestra una reducción en el impacto respecto al potencial, pero aún se encuentra en niveles altos en muchos activos, especialmente en:

Edificio Principal (AF.1), Salas de Servidores (AF.2), y Generadores Eléctricos (AF.4), que mantienen un impacto actual significativo.

Sistema Core Financiero (AS.1) y Sistemas de Seguridad y Autenticación (AS.3).

Existe aún la posibilidad de mejorar las medidas de reducción de riesgo y complementar las que ya se encuentras implementadas con el fin de acercarse a los niveles objetivos.

Impacto Objetivo (Verde):

Esta línea verde representa los niveles de impacto a los que se tiene como objetivo llegar, estos mismo son considerablemente más bajos en todas las categorías. Indicando el objetivo claro de querer reducir los riesgos, con el enfoque en proteger y mantener la integridad tanto física, sistemática y personal de los activos.

Se sugiere en el análisis que a pesar de que se ha realizado esfuerzos para reducir los riesgos actuales, siempre es necesario realizar mejoras adicionales y actualización en las medidas de seguridad para alcanzar y mantener los niveles de impacto objetivo.

RIESGO

Este gráfico de radar presenta el peligro en tres grados de análisis: potencial (rojo), actual (azul) y objetivo (verde).

Figura 62 Riesgo acumulado de los activos en categoría Servicios [S]

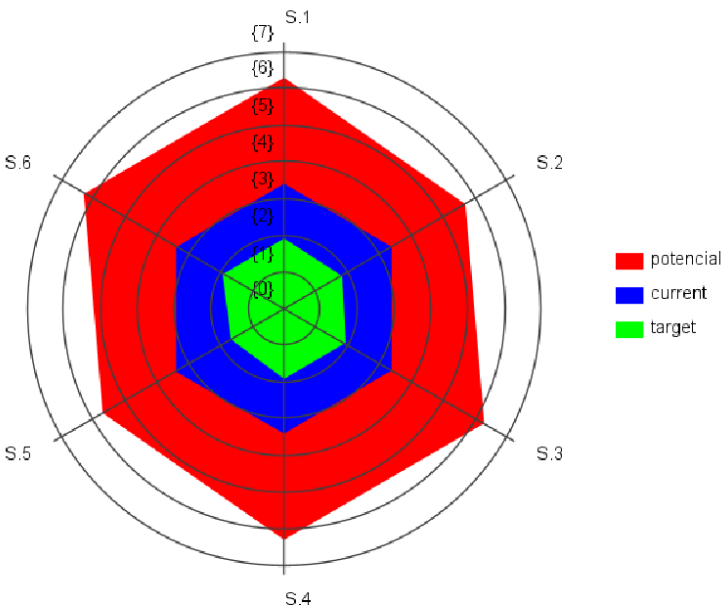


Tabla 16 Análisis del Riesgo acumulado de los activos en categoría Servicios [S]

Riesgo	**Análisis**
Potencial (Rojo):	Al observar la capa roja, esta muestra que el riesgo potencial es alto para todos los sistemas (S.1 a S.6) y se puede evidenciar que alcanza niveles cercanos a 7 en la escala, indicando que al ocurrir cualquier vulnerabilidad o fallo en estos sistemas se generaría un impacto considerable en la organización y más si no se aplican acciones al respecto para mitigar las consecuencias.
Actual (Azul):	Se puede observar el riesgo actual en la capa azul y este ha sido reducido en comparación con el riesgo potencial, pero sigue siendo moderado por lo que se sitúa entre los niveles 3 y 5 en la mayoría de los sistemas, estando por aun lejos de los niveles objetivos siendo necesario aun implementar mejoras para evitar impacto de las vulnerabilidades existentes.
Objetivo (Verde):	La capa verde representa el riesgo objetivo, el cual es notablemente inferior, ubicándose entre los niveles 1 y 2. Demostrando el claro objetivo que tiene la cooperativa de mitigar las vulnerabilidades y tener sistemas fuertes y seguros.

Figura 63 Riesgo acumulado de los activos en categoría Activos de Hardware [AH]

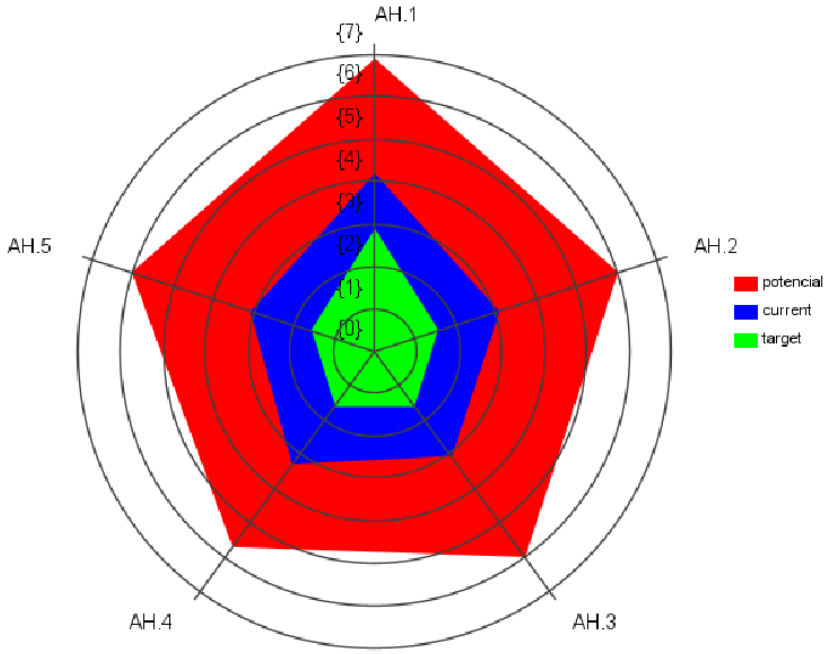


Tabla 17 Análisis del Riesgo acumulado de los activos en categoría Activos de Hardware [AH]

Riesgo	**Análisis**
Potencial (Rojo):	- Esta capa muestra el alto riesgo potencial en todos los activos de hardware, los cuales en su mayoría alcanzan niveles entre 6 y 7 siendo puntos importantes para el análisis. - Esto nos indica que son activos críticos para la cooperativa teniendo un impacto grande en caso de que tengan algún falla o vulnerabilidad.
Actual (Azul):	- Esta capa simboliza el riesgo presente, que ha disminuido respecto al potencial, situándose en niveles moderados (de 3 a 5). - A pesar de que se ha reducido parte del riesgo, aún persiste una brecha significativa respecto al objetivo, lo que indica que existen áreas de mejora para disminuir aún más este riesgo.
Objetivo (Verde):	- La capa verde del riesgo objetivo es significativamente menor, situándose en niveles entre 1 y 2 para todos los activos, reflejando objetivo de minimizar el riesgo en los activos críticos.

El análisis ayudo a destacar la importancia de seguir trabajando en implementar medidas de mantenimiento, protección física y modernización, que ayuden en la mitigación de los riesgos para estos activos de hardware y asegurar la continuidad del negocio en todas su áreas.

Figura 64 Riesgo acumulado de los activos en categoría Activos de Software [AS]

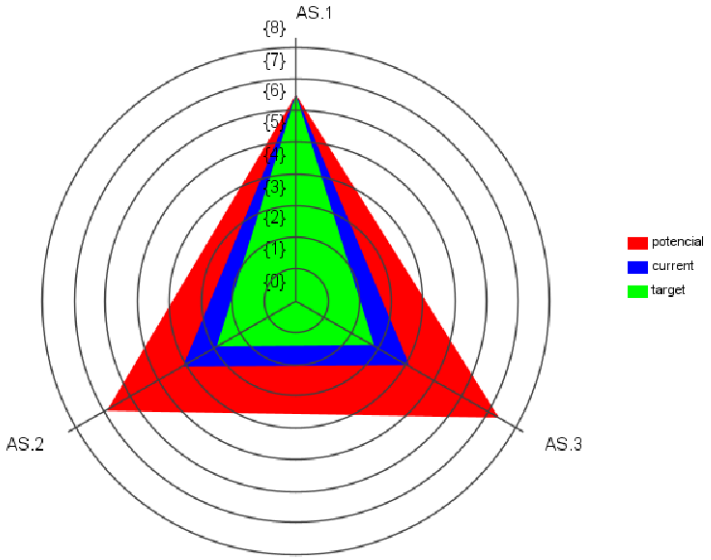


Tabla 18 Análisis del Riesgo acumulado de los activos en categoría Activos de Software [AS]

Riesgo	**Análisis**
Potencial (Rojo):	- Para las tres aplicaciones o servicios el riesgo es algo ya que alcanzan niveles cercanos a 8. Indicando que sin controles las áreas son vulnerables representar un riesgo importante para la organización.
Actual (Azul):	- En la capa azul muestra una reducción en el riesgo en comparación con el nivel potencial, manteniéndose entre los niveles 3 y 5, indicando que no son suficientes todas las medidas de seguridad y se deben implementar más para alcanzar los objetivos.
Objetivo (Verde):	- El nivel objetivo es bajo ya que es aproximadamente 1 o 2 para todas las aplicaciones y servicios. Aunque los niveles son buenos se recomienda aplicar más medidas para minimizar al máximo el riesgo en estas aplicaciones críticas.

Figura 65 Riesgo acumulado de los activos en categoría Activos de Información [AI]

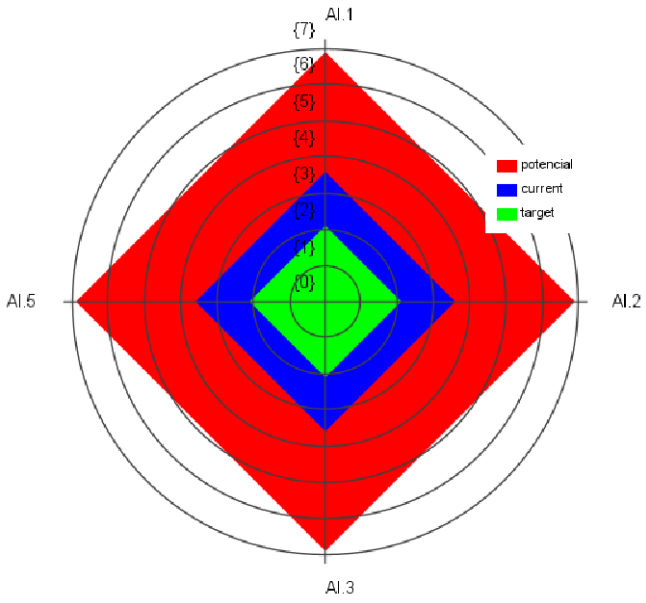


Tabla 19 Análisis del Riesgo acumulado de los activos en categoría Activos de Información [AI]

Riesgo	**Análisis**
Potencial (Rojo):	- El riesgo potencial es alto en todos los activos de información, alcanzando niveles cercanos a 7. Esto indica que, sin medidas de mitigación, estos activos podrían representar un riesgo

	significativo para la organización debido a su importancia y la sensibilidad de la información contenida.
Actual (Azul):	- El riesgo actual se ha reducido en comparación con el potencial, ubicándose en un rango de 3 a 5. Esto sugiere que ya se han implementado ciertas medidas de control y seguridad que han disminuido el riesgo. Sin embargo, todavía existe una brecha entre el nivel actual y el objetivo, lo que implica áreas de mejora.
Objetivo (Verde):	- El riesgo objetivo es bajo, en un rango de 1 a 2 para todos los activos de información. Esto representa el nivel deseado de seguridad y control para estos activos críticos, con el fin de minimizar posibles impactos negativos en la organización.

Figura 66 Riesgo acumulado de los activos en categoría Personal [P]

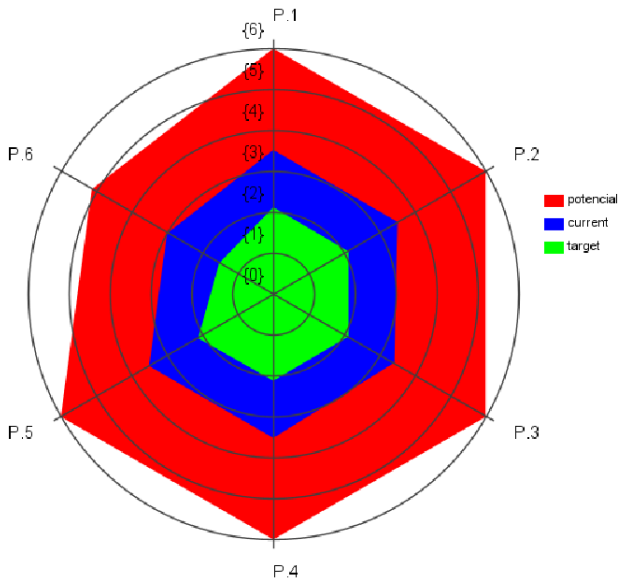


Tabla 20 Análisis del Riesgo acumulado de los activos en categoría Personal [P]

Riesgo	**Análisis**
Potencial (Rojo):	- El riesgo potencial es alto para todos los perfiles, alcanzando niveles cercanos a 6 en cada caso. Esto indica que, sin controles adecuados, estos perfiles pueden representar un riesgo significativo para la organización, probablemente debido al acceso a información crítica o a la capacidad de influir en sistemas importantes.

Actual (Azul):	- La capa azul muestra una reducción considerable en el riesgo en comparación con el potencial, situándose entre 2 y 4 para la mayoría de los perfiles. Esto sugiere que se han implementado algunas medidas de control y seguridad para mitigar el riesgo. Sin embargo, aún queda una brecha respecto al nivel objetivo, lo que implica oportunidades de mejora.
Objetivo (Verde):	- El nivel de riesgo objetivo es bajo, en un rango de 1 a 2 para todos los perfiles. Esto refleja el objetivo de la organización de mantener un riesgo mínimo en cuanto a la exposición y acciones de estos perfiles, protegiendo de manera efectiva contra accesos no autorizados o errores críticos.

Figura 67 Riesgo acumulado de los activos en categoría Activos Físicos [AF]

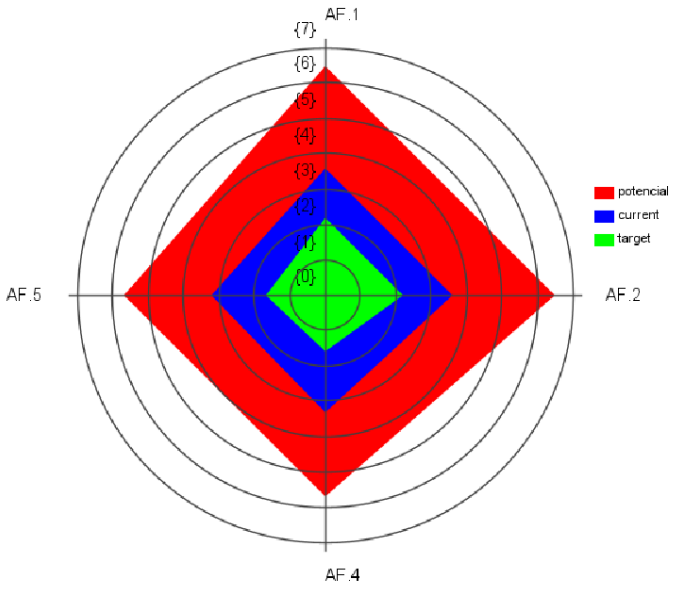


Tabla 21 Análisis del Riesgo acumulado de los activos en categoría Activos Físicos [AF]

Riesgo	**Análisis**
Potencial (Rojo):	- La capa roja revela un alto nivel de riesgo potencial en todos los activos físicos, alcanzando valores cercanos a 7. Esto sugiere que, si no se implementan controles adecuados, estos activos representan un riesgo significativo para la organización, posiblemente debido a su papel en la infraestructura física y operativa.

Actual (Azul):	- El riesgo actual ha sido reducido en comparación con el potencial, situándose entre los niveles 3 y 4 en la mayoría de los casos. Esto indica que ya se han implementado medidas para mitigar el riesgo, aunque aún se está por encima del nivel objetivo, lo que implica que hay margen para mejorar la seguridad y el control.
Objetivo (Verde):	- El nivel de riesgo objetivo es bajo, alrededor de 1 o 2 en todos los activos. Este es el nivel deseado de riesgo que la organización se ha propuesto alcanzar, probablemente para asegurar la continuidad de la infraestructura física y reducir la exposición a posibles amenazas o fallas.

3.2. Metodología de mitigación

La normativa *IGT-IGJ-INGINT-INTIC- INSESF-INR-DNSI 2022-002*, emitida por la SEPS busca establecer los niveles o estándares mínimos para la administración de seguridad de la información en las entidades del sector popular y solidario.

Para que la Cooperativa cumpla las regulaciones de la SEPS y con ello mitigar los riesgos informáticos identificados, se propone la siguiente metodología:

1. Aplicar el enfoque MAGERIT: Se recomienda continuar utilizando MAGERIT para gestionar los riesgos, adaptándose a las regulaciones descritas en la norma para el régimen especial. Esto implica priorizar los activos esenciales y enfocarse principalmente en aquellos que impactan más la actividades y procesos de la cooperativa.
2. Plan de Continuidad: Elaborar un plan de continuidad y recuperación ante desastres, que permitan calcular el tiempo de respuesta ante incidentes y verificar con ello la eficacia de los respaldos realizados de forma diaria.
3. Capacitación específica para el personal: Capacitar al personal en medidas de seguridad informática adecuadas para el régimen especial.
4. Ciclo de mejora continua: Establecer un ciclo de mejora continua con revisiones trimestrales de controles de seguridad y la identificación de nuevas vulnerabilidades.

CONCLUSIONES

En conclusión, el análisis de riesgos informáticos realizado en la Cooperativa de Ahorro y Crédito Metrópolis LTDA ayudó a identificar el impacto de los principales riesgos a la seguridad de la información, en donde se destacan las vulnerabilidades de los servicios esenciales. Según los resultados obtenidos estos activos presentan niveles de riesgo con niveles variados, convirtiéndose en puntos vulnerables de la cooperativa y propenso amenazas. En este mismo análisis también se han evaluado los desafíos que enfrenta la cooperativa en la supervisión, manejo y gestión de estos riesgos, encontrando que la capacidad de respuesta y los conocimientos del personal deben ser fortalecidas de manera urgente ya sea en capacitaciones y en fortalecimiento de las herramientas de trabajo.

En cuanto a la metodología para mitigar los riesgos identificados, es importante resaltar que se debe priorizar las normativas de implementación de medidas de seguridad, la capacitación constante del personal, la formalización de normativas y los procesos que garanticen una administración integral de la seguridad de la información determinadas por la Superintendencia de Economía Popular y Solidaria (SEPS).

RECOMENDACIONES

En base a las conclusiones y con la prioridad de alcanzar los objetivos propuestos. A continuación, se realizan las siguientes recomendaciones:

Es necesario potenciar la protección de los activos esenciales: es importante establecer más controles de seguridad en los servicios esenciales en base a las regulaciones de la SEPS.

Formación permanente del personal: es necesario implementar de manera continua programas de capacitación en temas de ciberseguridad para prevenir fallos humanos y mejorar la reacción ante incidente, estas capacitaciones deben cumplir con los requerimientos y regulaciones solicitadas por la SEPS.

Mejorar la administración de riesgos: es importante resaltar que se deben de mejorar e invertir constantemente en los procesos de monitoreo, vigilancia y detección de vulnerabilidades. Al adquirir instrumentos modernos que faciliten la detección y reacción ante posibles amenazas la cooperativa asegura que las funciones operativas puedan seguir.

Formalización de regulaciones y procesos: Se considera importante siempre finalizar la oficialización de las regulaciones y certificaciones de seguridad, en base a lo pedido por la SEPS y así garantizar la creación de un buen historial de cumplimiento de normas de seguridad.

Elaborar estrategias de reacción y recuperación: Es recomendables de manera constante establecer y evaluar los planes de recuperación y respuesta ante catástrofes e incidentes, que garanticen la continuidad del negocio.

REFERENCIAS

(CCN), M. de D.-C. C. N. (2019). *Pilar methodology for risk management*. https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar

Abril, A., Jarol, P., & John, B. (2013). Risk Analysis in Security of Information. *Risk Analysis in Security of Information*, *1*.

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics (Switzerland)*, *12*(17). https://doi.org/10.3390/electronics12173629

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluations (OCTAVE(SM)) Framework, Version 1.0. Carnegie Mellon Software Engineering Institute,. June*, 1–72. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473

Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2024.2329985

Alsulami, B., Srinivasan, A., Dong, H., & Mancoridis, S. (2017). Lightweight behavioral malware detection for windows platforms. *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, 75–81. https://doi.org/10.1109/MALWARE.2017.8323959

Amutio, M., Candau, J., & Mañas, J. (2012). MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. *Ministerio de Hacienda y Administraciones Publicas*, *3*, 127. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Barragán, C. G. B. (2019). Análisis de Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 en la ciudad de Ambato utilizando COBIT 5. *Universidad Técnica de Ambato*. https://repositorio.uta.edu.ec/bitstream/123456789/29843/1/Tesis_t1584msi.pdf

Belyaev, E. A., Emelyanova, O. A., & Livshitz, I. I. (2021). An analysis of methods for assessing information security risks of financial institutions. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, *21*(3). https://doi.org/10.17586/2226-1494-2021-21-3-437-441

Cerqueira Junior, A. S., & Arima, C. H. (2023). Cyber Risk Management and Iso 27005 Applied in Organizations: a Systematic Literature Review. *Revista Foco*, *16*(02), e1188. https://doi.org/10.54751/revistafoco.v16n2-215

Christos Blekos. (2022). Intrusion Detection System in Financial Institutions. *International Hellenic University*, *February*.

Comparison between MONARC and different Risk Management Methods. (n.d.). https://www.monarc.lu/publications/comparison-between-monarc-and-different-risk-management-methods/

Cooperativa de Ahorro y Credito Metropolis LTDA. (2024). https://coacmetropolis.fin.ec/

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security*, *70*, 72–94. https://doi.org/10.1016/j.cose.2017.05.002

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The New Frontier of Cybersecurity: Emerging Threats and Innovations. *2023 29th International Conference on Telecommunications (ICT)*, 1–6. https://doi.org/10.1109/ICT60153.2023.10374044

Ferruzola Gómez, E., Duchimaza S., J., Ramos Holguín, J., & Alejandro Lindao, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la

metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1). https://doi.org/10.26423/rctu.v6i1.429

Flores, D. A., & Perugachi, R. (2023). *A GDPR-compliant Risk Management Approach based on Threat Modelling and ISO 27005*. *April 2019*. http://arxiv.org/abs/2306.04783

Hernández, S. (2022). Seps-Igs-Igt-Igj-Igdo-Intgint-Intic-Insesf-Inr-Dnsi-2022-002. In *Superintendencia de Economía Popular y Solidaria* (pp. 1–26). https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

IT, R. (n.d.). *SFPS: Robustecer la digitalización y seguridad de la información para el 2023*. 2023. https://itahora.com/2023/01/18/sfps-robustecer-la-digitalizacion-y-seguridad-de-la-informacion-para-el-2023/

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, *15*(7). https://doi.org/10.3390/su15075828

Liu, C., Du, D., Zhang, C., Peng, C., & Fei, M. (2023). Observability Analysis of Networked Control Systems Under DoS Attacks. *IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society*, 1–6. https://doi.org/10.1109/IECON51785.2023.10312197

Liu, X. M. (2021). A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches. *The Coastal Business Journal*, *18*(1). http://usat.lookproxy.com/scholarly-journals/risk-based-approach-cybersecurity-case-study/docview/2666603718/se-2?accountid=37610%0Ahttps://media.proquest.com/media/hms/PFT/1/Sk8zM?_a=ChgyMDIyMTExNjAzNDc0NzY5Njo5NDk3ODgSBTY0OTc2GgpPTkVfU0VBUkNIIg4xODEuNjc

Magerit, M. de H. y F. P. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Ministerio de Hacienda y Administraciones Publicas*, *2006*. http://administracionelectronica.gob.es/

Maldonado, D. (2013). GESTIÓN DE RIESGOS INFORMÁTICOS PARA LA

PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN EN LA COOPERATIVA DE AHORRO Y CREDITO CAMPESINA COOPAC. *UNIANDES*. http://dspace.uniandes.edu.ec/handle/123456789/4522

María Fernanda Molina-Miranda. (2017). Análisis De Riesgos De Centro De Datos Basado En La Herramienta Pilar De Magerit. *Espiral*, *1*(11).

Marjorie, O. P., & Kamotho, C. (2020). PROPOSED OCTAVE-SMALL BASED SECURITY FRAMEWORK FOR MOBILE BANKING AMONG COMMERCIAL BANKS IN DEMOCRATIC REPUBLIC OF CONGO. *Global Scientific*, *8*(7).

Md Alamgir Hossain, Md Deen Amin Sarker, Md Sakhawat Hossain, Mohammad Atiqur Rahman Shaon, Md Shahin Hossain, & Md Mehedi Hasan Rayhan. (2022). *Bangladesh Bank Money Heist: A Concern of Cybersecurity System of Semester theme: Operational Risk Management in Projects*.

NIST. (2012). NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. *NIST Guide for Conducting Risk Assessments*, *September*, 95.

Patil, S., & Dhage, S. (2019). A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 588–593. https://doi.org/10.1109/ICACCS.2019.8728356

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *IJACSA) International Journal of Advanced Computer Science and Applications*, *14*(4), 1–9. www.ijacsa.thesai.org

Putra, I. M. M., & Mutijarsa, K. (2021). Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005. *3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021*, 14–19. https://doi.org/10.1109/EIConCIT50028.2021.9431865

Safonova, O. M., Lontsikh, N. P., Golovina, E. Y., Elshin, V. V., & Koniuchov, V. Y. (2020). Methodology for creating, implementing and system effectiveness evaluation of the business processes' information security system. *Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and*

Information Security, Information Technologies", IT and QM and IS 2020, 127–131. https://doi.org/10.1109/ITQMIS51053.2020.9322855

Santos-Olmo, A., Sánchez, L. E., Rosado, D. G., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2024). Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals. *Frontiers of Computer Science*, *18*(3). https://doi.org/10.1007/s11704-023-1582-6

seps.gob.ec. (2024). *SEPS Superintendency of Popular and Solidarity Economy*. https://www.seps.gob.ec/base-legal/

Shameli-Sendi, A. (2020). An efficient security data-driven approach for implementing risk assessment. *Journal of Information Security and Applications*, *54*, 102593. https://doi.org/10.1016/j.jisa.2020.102593

Toapanta, S. M. T., Durango, R. H. D. P., Gallegos, L. E. M., Díaz, E. Z. G., Quintana, Y. J. M., Jimenez, J. N. M., Arellano, M. R. M., & Trejo, J. A. O. (2022). Prototype to Mitigate the Risks, Vulnerabilities and Threats of Information to Ensure Data Integrity. *Advances in Science, Technology and Engineering Systems Journal*, *7*(6). https://doi.org/10.25046/aj070614

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*. https://doi.org/10.1016/j.cose.2013.04.004

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2). https://doi.org/10.1007/s42979-022-01020-4

ANEXOS

Anexo 1.- Valoración de encuesta

	UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
	MAESTRÍA EN CIBERSEGURIDAD **INSTITUTO DE POSTGRADO**
	HOJA DE REGISTRO PARA VALIDACIÓN DE EXPERTOS
	NOMBRE: DORIS MICHELLE SOLANO CHICO
	Correo: doris.solanochico9759@upse.edu.ec

Instrumento: Formato de encuesta para expertos en ciberseguridad

Sobre el instrumento: Este documento permite evaluar con expertos la encuesta que tiene el objetivo de identificar y evaluar la percepción de las áreas clave sobre la criticidad, riesgos y necesidades de protección de los activos esenciales de COAC Metrópolis LTDA.

Tema de Trabajo de Titulación: Análisis de Riesgos Informáticos en la Cooperativa de Ahorro y Crédito Metrópolis LTDA, bajo el cumplimiento normativo de la Superintendencia de Economía Popular y Solidaria (SEPS).

Sobre la validación: Para analizar se detallan los indicadores y criterios de evaluación.

Indicadores	Criterios o aspectos para considerar
SUFICIENCIA	El instrumento está alineado con el objetivo de la investigación.
CLARIDAD	Las preguntas formuladas responden a la finalidad del estudio.
COHERENCIA	Las preguntas guardan coherencia con el objetivo de la investigación.
RELEVANCIA	La redacción de las preguntas es clara y está bien argumentada.

Al realizar la evaluación marque con una "X" la casilla correspondiente a un número del uno (1) al cuatro (4), según la siguiente escala.

Expresión cual	Calificación
Alto Nivel	4
Moderado Nivel	3
Bajo Nivel	2
No cumple con el contenido	1

El cuestionario incluye 8 preguntas, todas con respuestas de selección múltiple. Además de evaluar cada pregunta, se pide a los participantes que proporcionen comentarios para mejorar la claridad y precisión del formulario, buscando hacerlo más efectivo.

Página **1** de **5**

CUESTIONARIO DE PREGUNTAS:

Pregunta 1.-		
¿Qué tan crucial es la participación de la alta dirección en la gestión de riesgos informáticos en una institución financiera?		Es fundamental
		Es importante, pero no esencial
		Puede delegarse completamente al equipo de TI
		No es necesario
Pregunta 2.-		
¿Cuál es el principal desafío para asegurar la confidencialidad de los datos?		Acceso no autorizado a datos sensibles
		Falta de políticas claras de acceso y control de datos
		Falta de herramientas de monitoreo de seguridad
		Capacitación insuficiente sobre manejo de información confidencial
Pregunta 3.-		
¿Qué aspecto considera más crítico para mantener la integridad de la información?		Prevención de errores en la manipulación de datos
		Procesos de auditoría y verificación de datos
		Controles insuficientes en la modificación de datos
		Falta de procedimientos estandarizados para actualización de datos
Pregunta 4.-		
¿Cuál considera el mayor riesgo para la disponibilidad de los sistemas y datos?		Fallas en la infraestructura de tecnología
		Ausencia de planes de respaldo y recuperación ante desastres
		Ataques cibernéticos que afecten la operatividad
		Limitaciones de recursos para garantizar disponibilidad continua
Pregunta 5.-		
¿Qué considera el mayor riesgo al manejar datos financieros?		Fuga de información confidencial
		Errores en el registro y consolidación de datos financieros
		Vulnerabilidad ante auditorías por falta de integridad de datos
		Pérdida de datos sensibles por fallos en almacenamiento

Pregunta 6.-		
¿Cuál es el principal reto de TIC para asegurar la infraestructura operativa?		Mantenimiento constante de la infraestructura de red y servidores
		Control de acceso y autenticación en todos los sistemas
		Implementación de políticas de seguridad efectivas
		Respuesta rápida ante incidentes y recuperación
Pregunta 7.-		
¿Qué considera prioritario para asegurar el cumplimiento normativo?		Revisión y actualización continua de contratos
		Políticas claras para el manejo de información legal y confidencial
		Coordinación con las áreas para asegurar cumplimiento
		Capacitación sobre regulaciones de SEPS y políticas internas
Pregunta 8.-		
En términos generales, ¿qué aspectos considera fundamentales para proteger los activos esenciales de COAC Metrópolis LTDA?		Implementación de mejores prácticas de ciberseguridad
		Mejor coordinación entre áreas para reducir riesgos
		Capacitación constante sobre manejo de riesgos y regulaciones
		Mayor inversión en infraestructura tecnológica y seguridad de la información

RUBRICA: INSTRUMENTO DE ENCUESTA PARA EXPERTOS EN CIBERSEGRUDAD.																	
CRITERIOS		SUFICIENCIA				CLARIDAD				COHERENCIA				RELEVANCIA				OBSERVACION
Nº	PREGUNTAS	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
1	¿Qué tan crucial es la participación de la alta dirección en la gestión de riesgos informáticos en una institución financiera?				X				X				X				X	
2	¿Cuál es el principal desafío para asegurar la confidencialidad de los datos?				X				X				X				X	
3	¿Qué aspecto considera más crítico para mantener la integridad de la información?				X				X				X				X	
4	¿Cuál considera el mayor riesgo para la disponibilidad de los sistemas y datos?				X				X				X				X	
5	¿Qué considera el mayor riesgo al manejar datos financieros?				X				X				X				X	
6	¿Cuál es el principal reto de TIC para asegurar la infraestructura operativa?				X				X				X				X	
7	¿Qué considera prioritario para asegurar el cumplimiento normativo?				X				X				X				X	
8	En términos generales, ¿qué aspectos considera fundamentales para proteger los activos esenciales de COAC Metrópolis LTDA?				X				X				X				X	

DATOS DEL EVALUADOR:

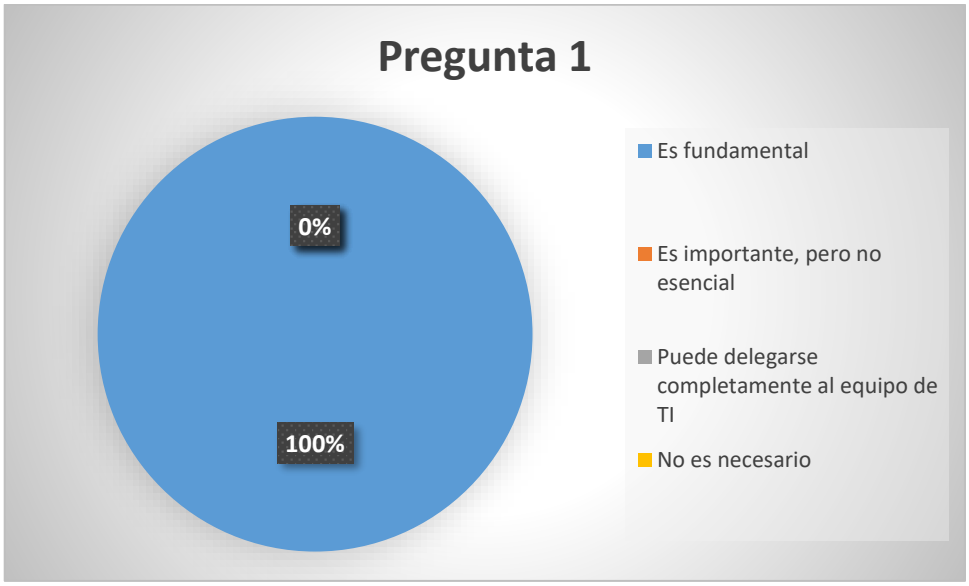
Nombres/Apellidos:	FERNANDO GEOVANNY GUZMAN FLORES
Ultima titulación académica:	MASTER EN INGENIERIA DEL SOFTWARE Y SISTEMAS INFORMÁTICOS
Institución de adscripción:	UNIVERSIDAD INTERNACIONAL DE LA RIOJA
Cargo:	CONSULTOR DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN
Teléfono celular (opcional):	
Dirección de correo:	ferguztech@juanfersoft.com
Firma:	

Anexo 2.- Resultado de encuesta

Pregunta 1.-

¿Qué tan crucial es la participación de la alta dirección en la gestión de riesgos informáticos en una institución financiera?

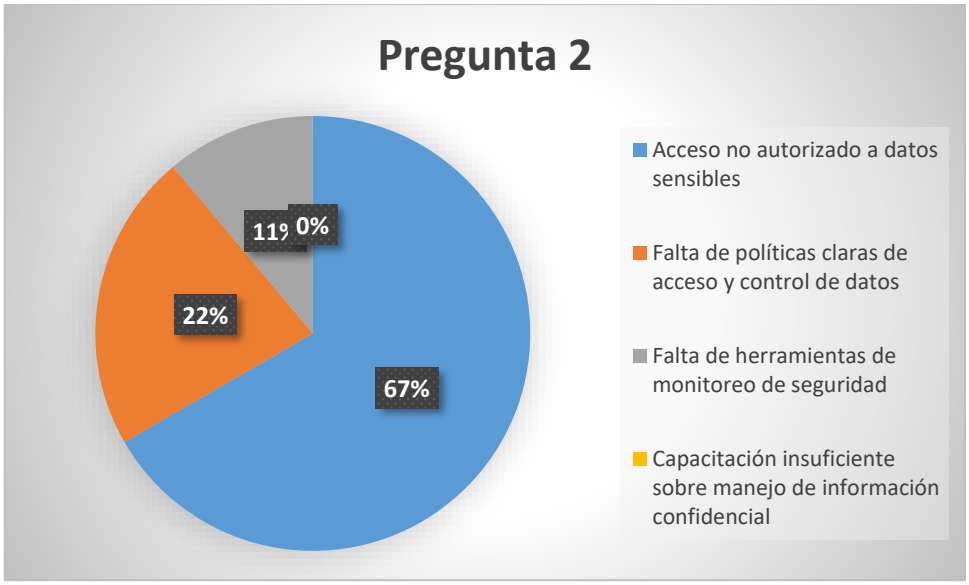
Respuesta	Cantidad
Es fundamental	**9**
Es importante, pero no esencial	**0**
Puede delegarse completamente al equipo de TI	**0**
No es necesario	**0**



Pregunta 2.-

¿Cuál es el principal desafío para asegurar la confidencialidad de los datos?

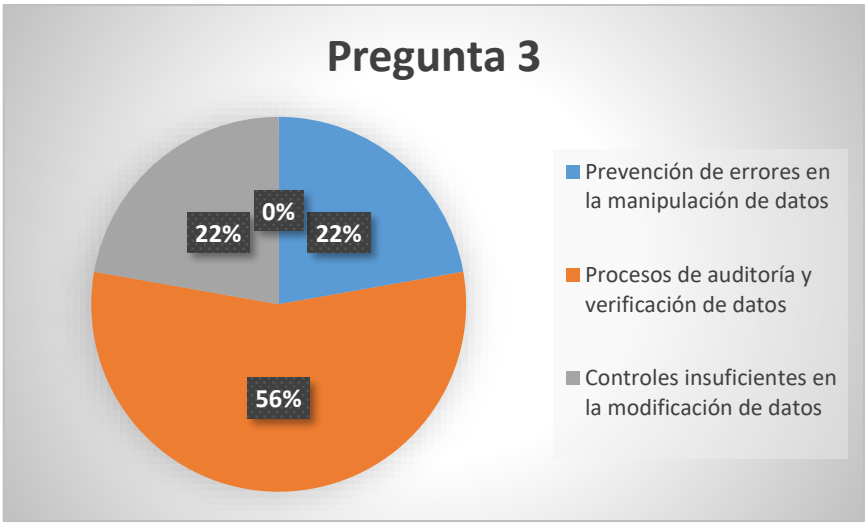
Respuesta	Cantidad
Acceso no autorizado a datos sensibles	**6**
Falta de políticas claras de acceso y control de datos	**2**
Falta de herramientas de monitoreo de seguridad	**1**
Capacitación insuficiente sobre manejo de información confidencial	**0**



Pregunta 3.-

¿Qué aspecto considera más crítico para mantener la integridad de la información?

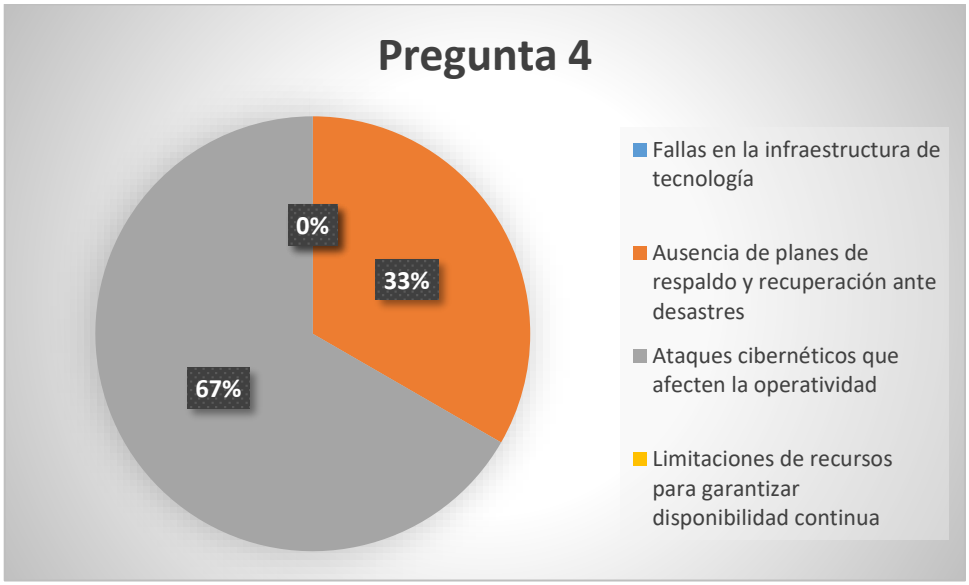
Respuesta	**Cantidad**
Prevención de errores en la manipulación de datos	**2**
Procesos de auditoría y verificación de datos	**5**
Controles insuficientes en la modificación de datos	**2**
Falta de procedimientos estandarizados para actualización de datos	**0**



Pregunta 4.-

¿Cuál considera el mayor riesgo para la disponibilidad de los sistemas y datos?

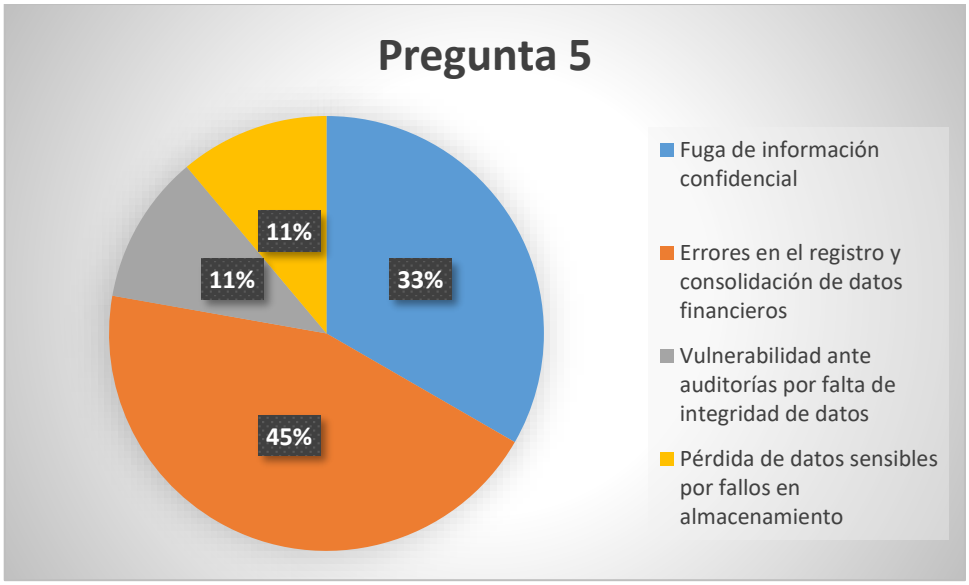
Respuesta	**Cantidad**
Fallas en la infraestructura de tecnología	**0**
Ausencia de planes de respaldo y recuperación ante desastres	**3**
Ataques cibernéticos que afecten la operatividad	**6**
Limitaciones de recursos para garantizar disponibilidad continua	**0**



Pregunta 5.-

¿Qué considera el mayor riesgo al manejar datos financieros?

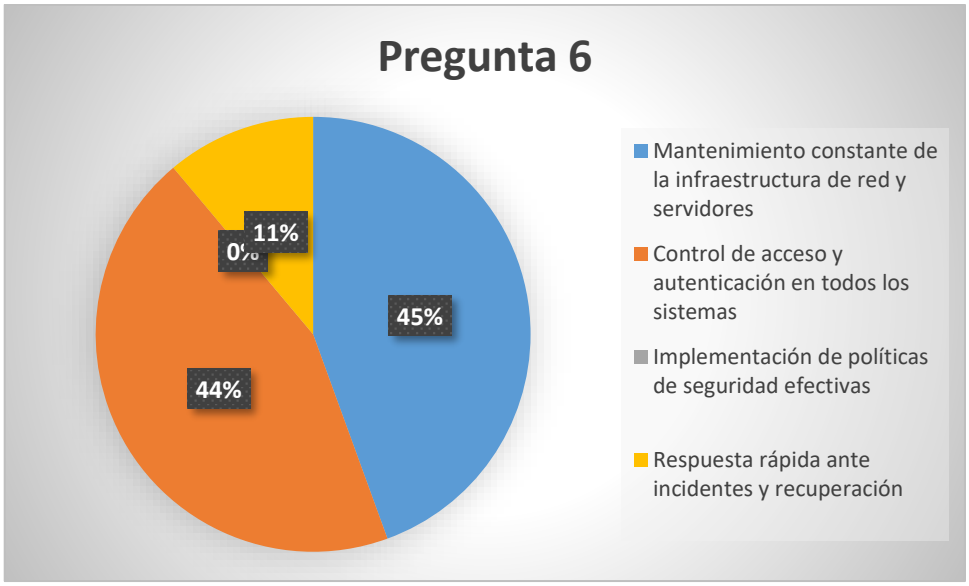
Respuesta	**Cantidad**
Fuga de información confidencial	**3**
Errores en el registro y consolidación de datos financieros	**4**
Vulnerabilidad ante auditorías por falta de integridad de datos	**1**
Pérdida de datos sensibles por fallos en almacenamiento	**1**



Pregunta 6.-

¿Cuál es el principal reto de TIC para asegurar la infraestructura operativa?

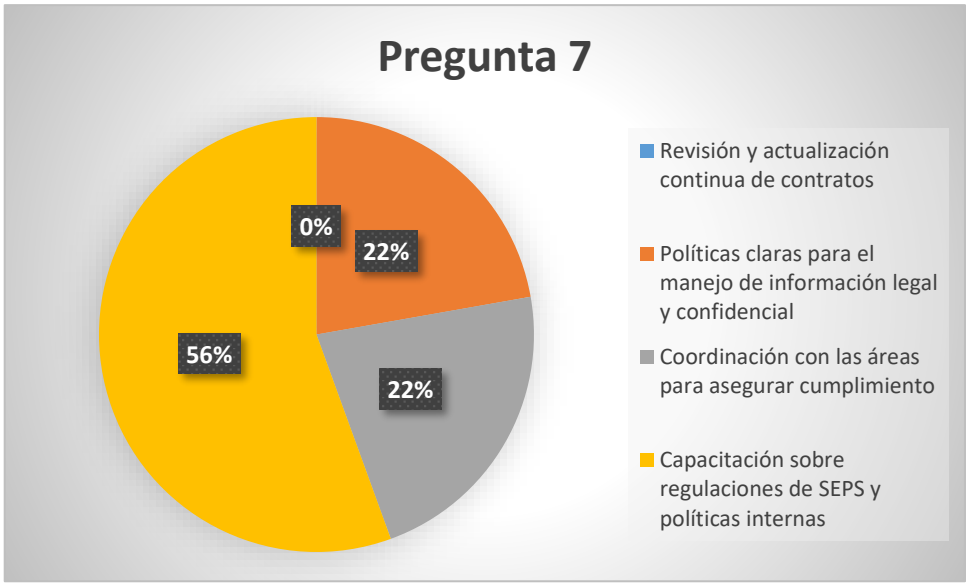
Respuesta	**Cantidad**
Mantenimiento constante de la infraestructura de red y servidores	**4**
Control de acceso y autenticación en todos los sistemas	**4**
Implementación de políticas de seguridad efectivas	**0**
Respuesta rápida ante incidentes y recuperación	**1**



Pregunta 7.-

¿Qué considera prioritario para asegurar el cumplimiento normativo?

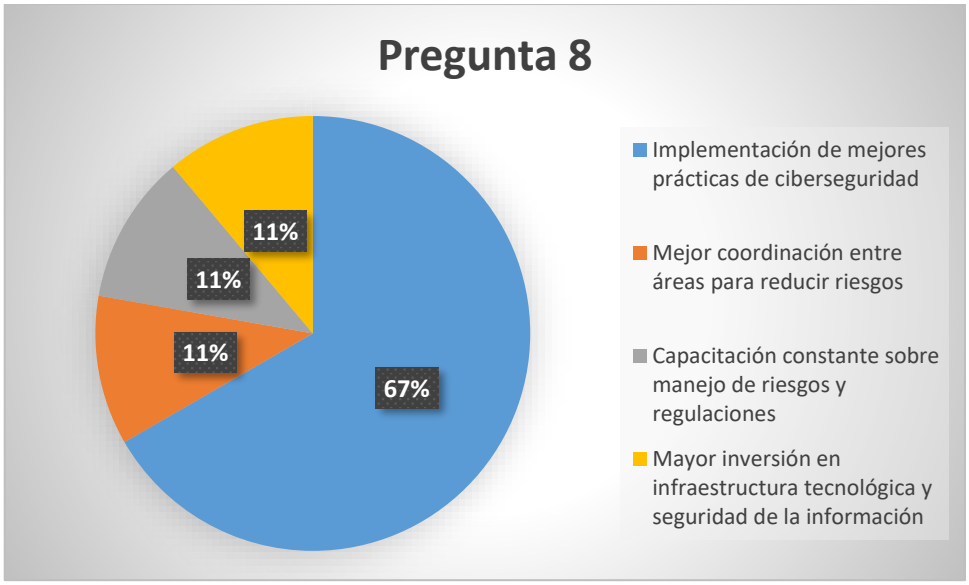
Respuesta	**Cantidad**
Revisión y actualización continua de contratos	**0**
Políticas claras para el manejo de información legal y confidencial	**2**
Coordinación con las áreas para asegurar cumplimiento	**2**
Capacitación sobre regulaciones de SEPS y políticas internas	**5**



Pregunta 8.-

En términos generales, ¿qué aspectos considera fundamentales para proteger los activos esenciales de COAC Metrópolis LTDA?

Respuesta	**Cantidad**
Implementación de mejores prácticas de ciberseguridad	**6**
Mejor coordinación entre áreas para reducir riesgos	**1**
Capacitación constante sobre manejo de riesgos y regulaciones	**1**
Mayor inversión en infraestructura tecnológica y seguridad de la información	**1**


Pregunta 8
11%
11%
11%
67%
Implementación de mejores prácticas de ciberseguridad
Mejor coordinación entre áreas para reducir riesgos
Capacitación constante sobre manejo de riesgos y regulaciones
Mayor inversión en infraestructura tecnológica y seguridad de la información