UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN SEPS 2022-002 PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO DE SEGMENTO 3"

Trabajo de titulación previo a la obtención del título en Magíster en computación con mención en seguridad informática

Línea de investigación: Desarrollo, aplicación de software y cyber security (seguridad cibernética)

AUTOR:

DONY ANDERSON REINA LÓPEZ

DIRECTOR:

FABIÁN GEOVANNY CUZME RODRÍGUEZ

Ibarra – Ecuador 2025

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0401665732		
APELLIDOS Y NOMBRES:	DONY ANDERSON REINA LÓPEZ		
DIRECCIÓN:	TULCÁN, AV. SAN FRANCISCO Y R. DARÍO		
EMAIL:	dareinal1@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0980342368

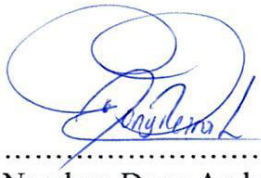
DATOS DE LA OBRA	
TÍTULO:	CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN SEPS 2022-002 PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO DE SEGMENTO 3
AUTOR (ES):	DONY ANDERSON REINA LÓPEZ
FECHA:	27/10/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA:	Magíster en computación con mención en seguridad informática
ASESOR /DIRECTOR:	JORGE CARAGUAY PROCEL / FABIÁN GEOVANNY CUZME RODRÍGUEZ

2. CONSTANCIAS

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

Ibarra, a los 28 días del mes de octubre de 2025.

EL AUTOR:



.....
Nombre: Dony Anderson Reina López

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 28 de octubre de 2025

Msc. Fabián Geovanny Cuzme Rodríguez

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f). . . . . .

Msc. Fabián Geovanny Cuzme Rodríguez

C.C: 1311527012

AGRADECIMIENTO

Agradezco infinitamente a Dios, por haberme permitido luchar contra todo obstáculo para alcanzar un objetivo más en mi vida profesional, y también a mis profesores y tutor por compartir sus conocimientos que han sido fundamentales en el desarrollo del presente trabajo de titulación.

Dony Anderson Reina López

DEDICATORIA

Dedico este trabajo de investigación a mis padres, quienes siempre han estado al pendiente de mi trayectoria profesional, motivándome a superarme cada día más y recordarme que con fe todo es posible; también dedico este logro a mi esposa e hijas quienes me impulsan a dar siempre mi mayor esfuerzo y hacer las cosas con amor, lo que ha marcado en mí una inspiración para soñar siempre en alto.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de investigación se enfoca en el cumplimiento normativo del Anexo 1 de la resolución SEPS 2022-002 respecto a la seguridad de la información con aplicación en cooperativas de ahorro y crédito de segmento 3. Esta normativa establece requisitos que deben cumplir las instituciones del sector económico popular y solidario, pero no existe una base sólida que garantice una correcta implementación de controles de seguridad, por lo cual, se ha recopilado información relevante de artículos científicos, libros, normas internacionales, buenas prácticas de seguridad de la información y otras investigaciones con la finalidad de establecer lineamientos válidos para el diseño de un framework que abarca, políticas, procedimientos, metodologías y herramientas de seguridad de la información, alineado a los controles de seguridad establecidos en la normativa utilizando la metodología MAGERIT v3 orientada a la gestión de riesgos tecnológicos, de igual manera se apoya en marcos de referencia de la familia ISO/IEC 27000 e ITIL v4. Finalmente se utiliza la metodología Mehari para evaluar la efectividad de la implementación de los controles de seguridad, identificando los riesgos asociados a cada control de seguridad y el nivel de impacto, comparando con la situación actual de la cooperativa manteniendo el criterio de mejora continua.

Palabras claves: Seguridad de la información, MAGERIT v3, gestión de riesgo, controles de seguridad de la información.

ABSTRACT

This research work focuses on regulatory compliance with Annex 1 of SEPS resolution 2022-002 regarding information security applicable to segment 3 savings and credit cooperatives. This regulation establishes requirements that institutions in the popular and solidarity economic sector must meet, but there is no solid basis to guarantee a correct implementation of security controls, therefore, relevant information has been collected from scientific articles, books, international standards, good information security practices and other research in order to establish valid guidelines for the design of a framework that covers policies, procedures, methodologies and information security tools, aligned with the security controls established in the regulations using the MAGERIT v3 methodology aimed at technological risk management, in the same way it is based on reference frameworks of the ISO / IEC 27000 family and ITIL v4. Finally, the Mehari methodology is used to evaluate the effectiveness of the implementation of security controls, identifying the risks associated with each security control and the level of impact, comparing them with the cooperative's current situation while maintaining the criterion of continuous improvement.

Keywords: Information security, MAGERIT v3, risk management, information security controls.

CAPITULO I

EL PROBLEMA

1.1. Problema de investigación

La Superintendencia de Economía Popular y Solidaria (SEPS), es el organismo técnico de supervisión y control de las entidades del sector Financiero Popular y Solidario, y de las organizaciones de la Economía Popular y Solidaria del Ecuador que, promueve su sostenibilidad y correcto funcionamiento para proteger a sus socios. (SEPS, 2023)

En tema de Seguridad de la Información hasta mayo de 2022, no existía una normativa que controle o regule la implementación de controles de seguridad, pero dentro de las auditorías que realiza el ente regulador existían hallazgos que simplemente se basaban en normativas internacionales o por recomendaciones de buenas prácticas de seguridad de la información. Lo cual no garantizaba que las cooperativas de ahorro y crédito cumplan conscientemente con salvaguardar la información que operan.

Además, dentro de las auditorías, la SEPS no contaba con personal calificado en temas de seguridad de la información, más bien se iban alimentando poco a poco del conocimiento adquirido por instituciones que libremente consideraban sensato la implementación de medidas de seguridad tanto físicas, electrónicas y de ciberseguridad. Y en base a estas experiencias formulaban los hallazgos para otras instituciones en crecimiento.

Para suplir esta problemática, la SEPS en obediencia a su misión el 03 de mayo de 2022 emite la Norma SEPS 2022-002, que tiene como objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades bajo su supervisión deben definir e implementar para el resguardo y protección de su activo

de información, preservando su confidencialidad, disponibilidad e integridad. (SEPS, 2022)

La SEPS ha subdividido a las entidades que supervisa en base a su tamaño según los segmentos de jerarquías ya establecidas para las cooperativas de ahorro y crédito, en tres regímenes: (SEPS, 2022)

- Régimen General: a las cooperativas de ahorro y crédito de segmento 1 y 2; a las asociaciones mutualistas de ahorro y crédito para la vivienda y a la CONAFIPS;
- Régimen Especial: a las cooperativas de ahorro y crédito del segmento 3; y,
- Régimen simplificado: a las cooperativas de ahorro y crédito de los segmentos 4 y 5.

La estructura de esta normativa está bien distribuida, estableciendo claramente los requisitos obligatorios para cada régimen. Sin embargo, hay aspectos que se generalizan demasiado y no se proporciona una explicación precisa sobre cómo dar cumplimiento a la mayoría de los controles fijados en el Anexo I, dejando a criterio propio del responsable de seguridad de la información la definición de lineamientos específicos para cumplir con dichos requisitos. Además, diversas entidades del sector enfrentan limitaciones en la aplicación efectiva de estos lineamientos debido a la falta de madurez en sus procesos tecnológicos, escasa cultura de seguridad, ausencia de controles documentados y carencia de recursos especializados.

Es necesario realizar un estudio de diferentes normas relacionadas a ciberseguridad o seguridad de la información, apoyando al desarrollo de un documento guía para cumplir la normativa de la SEPS, garantizando que los controles establecidos

se encuentren implementados correctamente, para ser evaluados y determinar su efectividad.

1.2. Interrogantes de la investigación

¿Cuáles son los lineamientos de la norma SEPS 2022-002 y que normas, framework y herramientas de seguridad de la información se relacionan a estos?

¿Cómo dar un cumplimiento sistemático y correcto a la Norma SEPS 2022-002 en base a normativas reconocidas?

¿Cómo evaluar la efectividad de los controles de seguridad implementados?

1.3. Objetivos de la investigación

1.2.1. Objetivo general

Evaluar controles de seguridad de acuerdo con normativas y herramientas establecidas en un framework para el cumplimiento de la normativa de Seguridad de la Información SEPS 2022-002, a partir del enfoque cualitativo aplicada en una Cooperativa de Ahorro y Crédito de Segmento 3

1.2.2 Objetivos específicos

- Analizar los lineamientos de la normativa de Seguridad SEPS 2022-002, a través de un estudio documental para extraer las bondades que se relacionan con los controles de seguridad.
- Diseñar un framework para la implementación y cumplimiento de la normativa de Seguridad SEPS 2022-002 en base a la metodología MAGERIT v3.
- Evaluar los resultados preliminares de los controles de seguridad implementados en una Cooperativa de Ahorro y Crédito de Segmento 3 mediante la metodología Mehari.

1.3. Justificación

Considerando los Objetivos de Desarrollo Sostenible de las Naciones Unidas, en su numeral **16.10** "Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales" (Naciones Unidas Ecuador, 2021), se considera que el cumplimiento a esta normativa ayuda a garantizar el acceso a la información pública y su buen tratamiento, enfocados en la Ley Orgánica de Datos Personales. En la Figura 1 se muestra el objetivo de desarrollo sostenible número 16 cuya iniciativa es promover sociedades pacíficas e incluyentes en todos los niveles.

Figura 1. Objetivo 16 de las Naciones Unidas

Fuente: (Naciones Unidas Ecuador, 2021)

La Constitución de la República del Ecuador, en su artículo 66, numeral 19 expone: "*Se reconoce y Garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre la información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley*". (Asamblea Nacional Constituyente de la República del Ecuador, 2008), que en concordancia la Normativa SEPS 2022-002 menciona controles de seguridad de la información con la finalidad de resguardar y

proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad.

Antes de la normativa SEPS 2022-002 no existía un marco regulatorio para las entidades financieras del sector económico popular y solidario respecto a la gestión de seguridad de información, por lo que las instituciones de este sector no aplicaban de manera adecuada lineamientos de seguridad de la información, a pesar de que este tipo de instituciones por su naturaleza deben implementar por lo menos controles mínimos de seguridad, los cuales por general incluían dentro de la gestión de TI.

La Normativa SEPS 2022-002 determina tiempos máximos para su cumplimiento en base a la segmentación en la que se encuentre la institución financiera, este trabajo de grado considera su caso de estudio para una cooperativa de ahorro y crédito de segmento 3, por lo cual, su tiempo de cumplimiento máximo es de tres años a partir de la fecha de publicación de la normativa o a partir de su cambio de segmentación para los casos que amerite.

El margen de tiempo establecido por la SEPS para la implementación de controles de seguridad es amplio, lo que permite que las entidades financieras del segmento 3 puedan cumplir con los requerimientos de seguridad descritos.

El uso de un Framework que permita orientar el proceso de implementación de controles de seguridad establecidos por la SEPS garantiza que su cumplimiento de manera eficiente y eficaz a través de una metodología comprobada y evaluada.

Este proyecto se adapta a la línea de investigación de Desarrollo, aplicación de software y cyber security (seguridad cibernética), debido a que realiza análisis y aplicación de lineamientos de una normativa de seguridad de la información.

CAPITULO II
MARCO REFERENCIAL

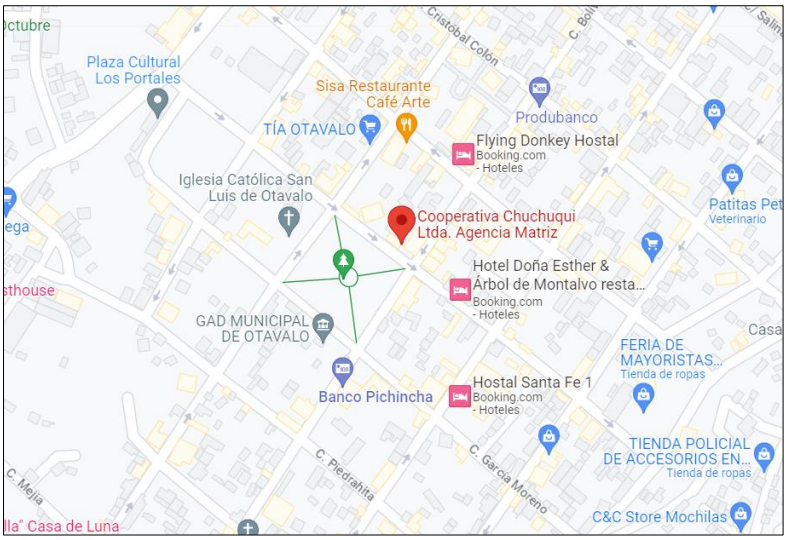
2.1. Antecedentes

En el sector financiero, las cooperativas de Ahorro y crédito se encuentran bajo la supervisión de la Superintendencia de Economía Popular y Solidaria (SEPS), la cual para el cumplimiento de sus funciones podrá expedir todos los actos y contratos que fueren necesarios. Así mismo podrá expedir las normas en materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales que expida la junta de política y Regulación Financiera. (Asamblea Nacional del Ecuador, 2014)

Antes de expedir la Norma SEPS 2022-002, no existía ninguna otra dedicada netamente a la Seguridad de la Información, solo se mencionaba lineamientos puntuales dentro de otros temas, como por ejemplo en la Norma de Administración del Riesgo Operativo SEPS-IGT-IR-IGJ-2018-0279 se hace mención de la importancia de realizar capacitaciones respecto al uso adecuado de la tecnología y seguridad e la información así como la gestión de seguridad de la información para proveedores, pero no engloba un tema general sobre todo lo que implica la seguridad de la información.

La Cooperativa de Ahorro y Crédito de Segmento 3 ubicada en la ciudad de Otavalo como se muestra en la figura 2, es una cooperativa creada para participar en la solución de problemas sociales y económicos de los asociados, brinda servicios financieros y no financieros de calidad, adaptados a las necesidades del sector.

Figura 2. Ubicación de la cooperativa de Ahorro y Crédito Chuchuqui Ltda.



Fuente: Google maps, 2024

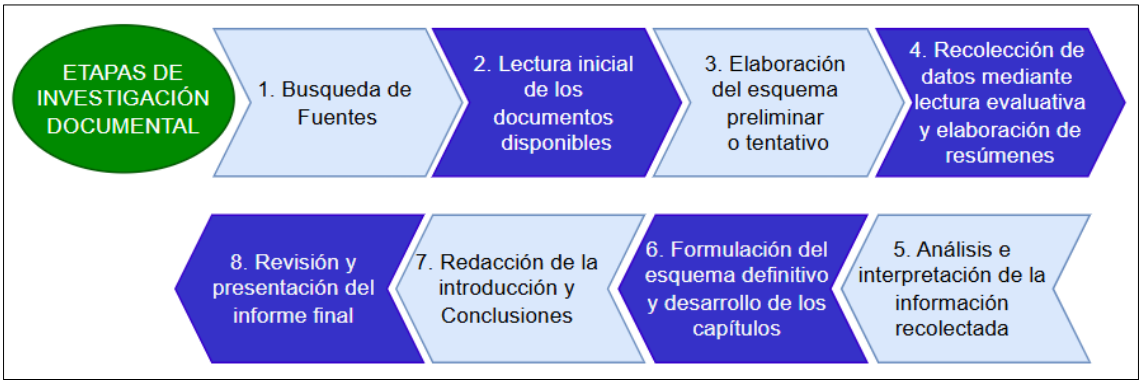
Fue creada en la Parroquia Eugenio Espejo, Cantón Otavalo, en el año de 1985, adquiere su personería jurídica el 02 de septiembre de 1986 con Acuerdo Ministerial No 86-141-DC Reg # 5259 DGC. La idea nació por un grupo de pequeños artesanos, panaderos, comerciantes indígenas del sector. (COAC CHUCHUQUI LTDA., 2023)

En base al crecimiento de la institución, en al año 2014, se ve la necesidad de crear el departamento de Tecnología, y a finales del año 2022 se nombra al primer Oficial de Seguridad de la Información, quien estará al frente de dar cumplimiento a los requerimientos de la SEPS, tomando en cuenta que hasta a partir de este punto, nunca existió ningún estudio, documentación o auditoría en seguridad informática.

2.2. Investigación documental

Según (Arias, 2016) la investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, lo que quiere decir que son obtenidos y registrados de fuentes documentales, realizadas por otros investigadores ya sean impresas, audiovisuales o digitales. En la figura 3 se muestra un esquema de las etapas sugeridas por Arias para una investigación documental.

Figura 3. Etapas para una investigación documental



Fuente: (Arias, 2016)

La investigación documental puede hacer uso de estudios de medición de variables independientes a partir de datos secundarios. Esto quiere decir que se puede emplear documentos de cifras o datos numéricos que han sido obtenidos o procesados con anterioridad por cualquier tipo de institución ya sea pública, privada o gubernamental. (Arias, 2016)

A partir de estos datos secundarios se puede elaborar un análisis significativo para la investigación ya que se considera las conclusiones representadas por el comportamiento o estado actual de las diferentes variables de estudio como demográficas, sociales o económicas.

Para gestionar de manera adecuada la documentación de la investigación se hace uso de la herramienta en línea “Parsifal”, que está diseñada para ayudar a los investigadores a realizar revisiones sistemáticas de la literatura en el contexto de la ingeniería de software. (Parsifal, 2021)

La herramienta antes mencionada permite identificar, analizar e interpretar información disponible en documentos de estudios relacionados con preguntas de investigación específicas a través de una planificación en ella establecida.

2.2.1. Búsqueda de Fuentes

Para la búsqueda de fuentes, se recopiló información de Artículos científicos, trabajos de titulación, libros que se encuentren dentro de los últimos 5 años, pero también se consideró información de normativas relevantes a la Seguridad de la Información y Gestión de Riesgos en sus últimas publicaciones.

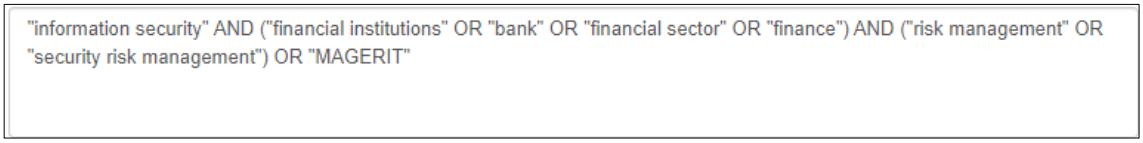
Las herramientas de búsqueda que se utilizó son: Google scholar, Servicio Ecuatoriano de Normalización (INEN), SCOPUS, IEEE y Science@Direct, de las cuales las tres últimas fueron gestionadas en la herramienta de Parsifal obteniendo los resultados que se indican en la figura 4.

Figura 4. Resumen de estudios importados a Parsifal

Fuente: Parsifal

Para la obtención de los artículos o documentos de investigación mostrados en Parsifal se hace uso de lo que se denomina criterio de búsqueda compartido, que se refiere a combinar dos o más criterios para nos arroje un resultado más específico. En este caso se emplea una combinación como cadena de búsqueda mediante operadores booleanos (AND, OR) como se muestra en la figura 5.

Figura 5. Cadena de búsqueda



Fuente: Parsifal

Parsifal, así como también las librerías que se emplean en dicha herramienta se caracterizan por trabajar en idioma inglés, lo cual en base a los resultados de búsqueda se pudo observar que no existen mucha documentación relacionada a la metodología MAGERIT, ya que esta es más empleada en zonas hispanohablantes. Por lo tanto, es necesario considerar otras librerías como Google Scholar e INEN para la búsqueda de estudios relacionados, obteniendo en total los resultados que se muestran en la tabla 1.

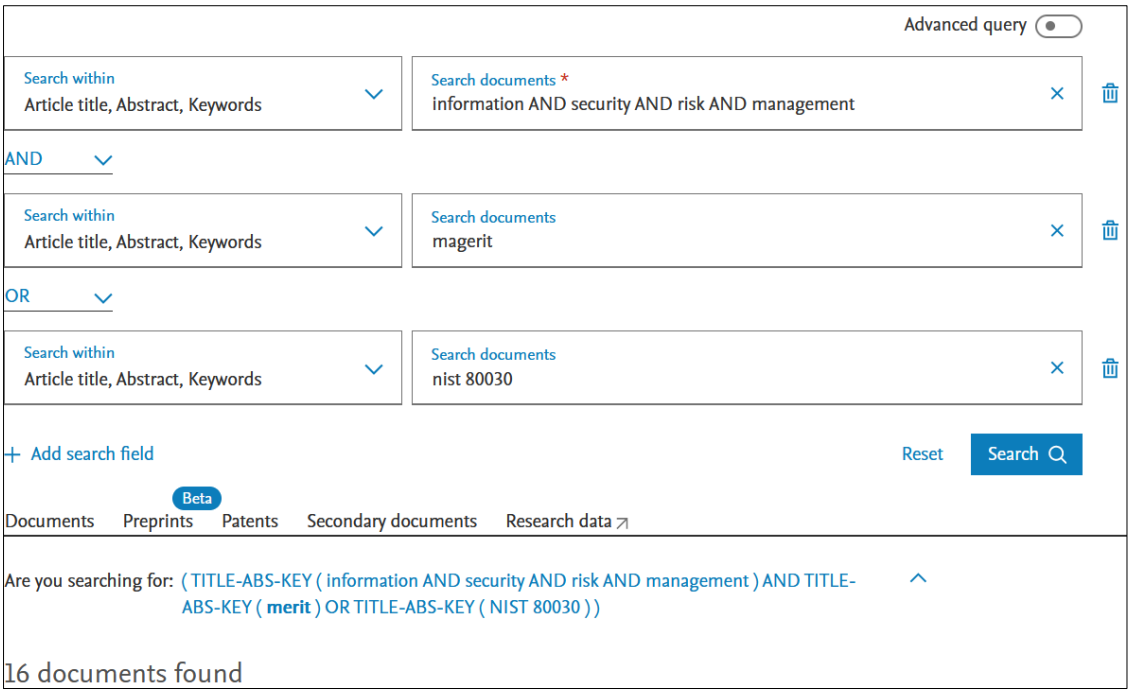
Tabla 1. Resultados de búsqueda de fuentes.

CRITERIO DE BUSQUEDA	HERRAMIENTA DE BUSQUEDA	TOTAL DE RESULTADOS
Seguridad de la información, Instituciones financieras, MAGERIT, Gestión de Seguridad de la Información, Gestión de Riesgos de la Seguridad de la Información, clasificación de la información, Arquitectura Segura, Procesos Agregadores de valor, Gestión de Configuración, Normas ISO 27000	Google Scholar	962
	Servicio Ecuatoriano de Normalización (INEN)	64
	SCOPUS	81
	Science@Direct	70
	IEEE Digital Library	26
TOTAL		1203

*Fuente: (Google Scholar), (INEN), (SCOPUS), (*Science@Direct), (IEEE Digital Library)

En la figura 6, se muestra un ejemplo de la herramienta de búsqueda SCOPUS donde nos permite el uso de conectores para realizar la búsqueda combinada, de donde se obtiene la expresión de búsqueda booleana avanzada.

Figura 6. Ejemplo de búsqueda combinada en SCOPUS



Fuente: SCOPUS

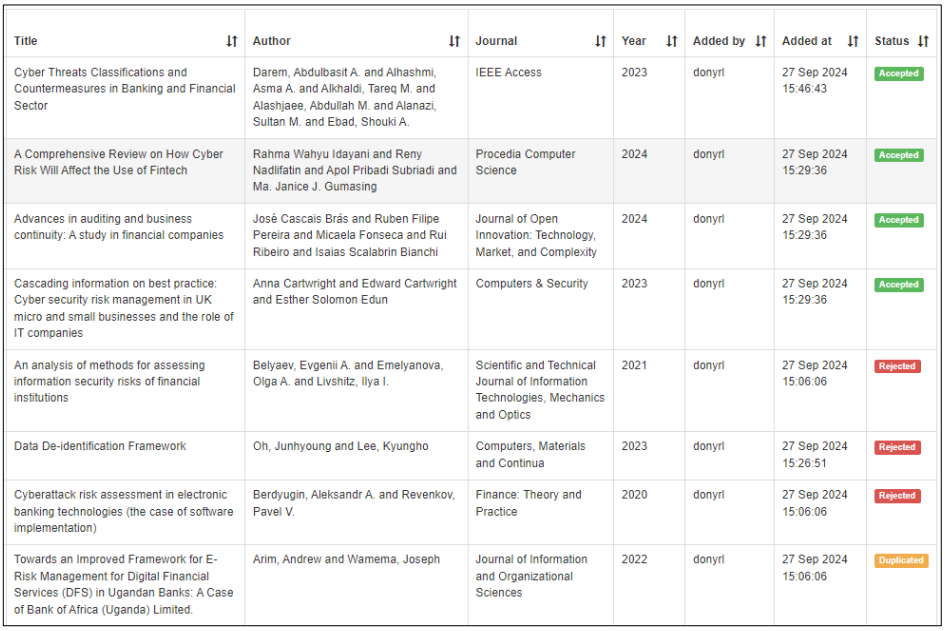
Cabe mencionar que estos indicadores mostrados forman parte de la investigación inicial del proyecto, ya que en el transcurso de su desarrollo pueden surgir necesidades investigativas adicionales, que requieran una gestión documental adicional.

2.2.2. Lectura Inicial

En esta etapa en base a la cantidad de resultados obtenidos en la búsqueda se realiza una lectura rápida enfocándose en el título y resumen de la documentación, utilizando la herramienta Parsifal que permite cargar la base de documentos encontrados en las librerías de búsqueda y nos genera una tabla con la información más relevante de cada uno.

Con los estudios importados Parsifal permite ir descartando aquellos que no se encuentran directamente relacionados al trabajo de investigación o ir aceptando los que si pueden contener información de interés y de igual manera etiquetar aquellos que se encuentran duplicados como se observa en la figura 7.

Figura 7. Ejemplo de selección de estudios en Parsifal



Title	Author	Journal	Year	Added by	Added at	Status
Cyber Threats Classifications and Countermeasures in Banking and Financial Sector	Darem, Abdulbasit A. and Alhashmi, Asma A. and Alkhaldi, Tareq M. and Alashjaee, Abdullah M. and Alanazi, Sultan M. and Ebad, Shouki A.	IEEE Access	2023	donyrl	27 Sep 2024 15:46:43	Accepted
A Comprehensive Review on How Cyber Risk Will Affect the Use of Fintech	Rahma Wahyu Idayani and Reny Nadlifatin and Apol Pribadi Subriadi and Ma. Janice J. Gumasing	Procedia Computer Science	2024	donyrl	27 Sep 2024 15:29:36	Accepted
Advances in auditing and business continuity: A study in financial companies	José Cascais Brás and Ruben Filipe Pereira and Micaela Fonseca and Rui Ribeiro and Isaias Scalabrin Bianchi	Journal of Open Innovation: Technology, Market, and Complexity	2024	donyrl	27 Sep 2024 15:29:36	Accepted
Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies	Anna Cartwright and Edward Cartwright and Esther Solomon Edun	Computers & Security	2023	donyrl	27 Sep 2024 15:29:36	Accepted
An analysis of methods for assessing information security risks of financial institutions	Belyaev, Evgenii A. and Emelyanova, Olga A. and Livshitz, Ilya I.	Scientific and Technical Journal of Information Technologies, Mechanics and Optics	2021	donyrl	27 Sep 2024 15:06:06	Rejected
Data De-identification Framework	Oh, Junhyoung and Lee, Kyungho	Computers, Materials and Continua	2023	donyrl	27 Sep 2024 15:26:51	Rejected
Cyberattack risk assessment in electronic banking technologies (the case of software implementation)	Berdyugin, Aleksandr A. and Revenkov, Pavel V.	Finance: Theory and Practice	2020	donyrl	27 Sep 2024 15:06:06	Rejected
Towards an Improved Framework for E-Risk Management for Digital Financial Services (DFS) in Ugandan Banks: A Case of Bank of Africa (Uganda) Limited.	Arim, Andrew and Wamema, Joseph	Journal of Information and Organizational Sciences	2022	donyrl	27 Sep 2024 15:06:06	Duplicated

Fuente: Parsifal

Una vez reducido el número de documentos se procede a realizar una lectura un poco más detallada, enfocándose en el contenido de los documentos, títulos y subtítulos que nos pueden dar una perspectiva más detallada de la calidad de la información. En base a esto se presenta en la tabla 2 el resultado del análisis de la documentación.

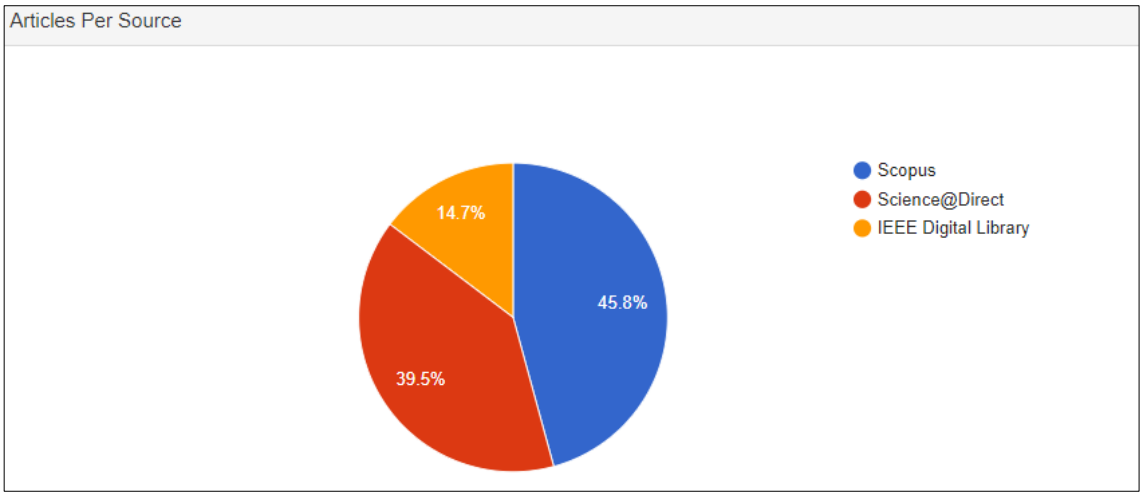
Tabla 2. Selección de documentos

Herramienta de Búsqueda	**Resultados Iniciales**	**Resultados después de lectura rápida**	**Resultados después de lectura detallada**
Google Scholar	962	20	4
INEN	64	6	5
SCOPUS	81	11	2
Science@Direct	70	7	1
IEEE Digital Library	26	6	2
TOTAL	1203	50	14

*Fuente: (Google Scholar), (INEN), (SCOPUS), (*Science@Direct), (IEEE Digital Library)

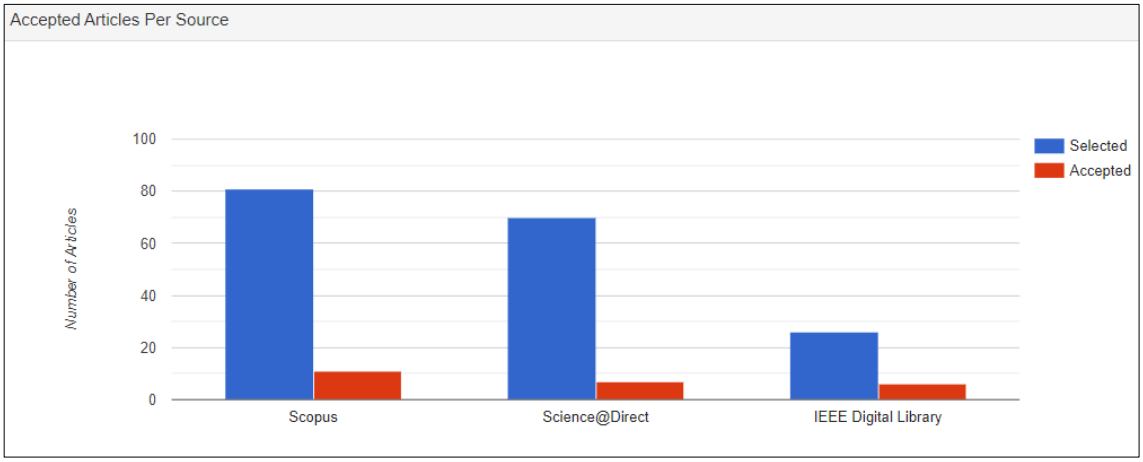
Parsifal permite al final de realizar toda la revisión sistemática de la documentación obtener gráficas y un informe resumen de los resultados obtenidos el cual se puede apreciar de mejor manera en el Anexo I. A través de esta herramienta se ha importado los estudios encontrados en 3 librerías digitales como se observa en la figura 8 de las cuales se ha seleccionado solo los estudios de interés como se observa en la figura 9.

Figura 8. Estudios importados en Parsifal



Fuente: Parsifal

Figura 9. Resultado de selección de estudios en Parsifal



Fuente: Parsifal

En el Anexo II se presenta una tabla con los detalles de la documentación que fue seleccionada después del proceso de selección a través de lectura rápida y lectura

detallada en la cual consta: un código del documento o artículo, título, autor y un pequeño resumen de la información relevante.

2.2.3. Elaboración de Esquema Preliminar

En esta etapa, se establece a que tema o control de seguridad está aportando cada documento seleccionado, para ello se establece una matriz que contiene los controles de seguridad extraídos del Anexo 1 de la normativa SEPS 2022-002 y los documentos seleccionados.

Este esquema se puede observar en la tabla x del Anexo III de este documento en el cual se hace un match entre la documentación identificada por su código y temas o controles de seguridad determinados en la normativa SEPS 2022-002.

2.2.4. Recolección de datos mediante lectura evaluativa y resúmenes

La lectura evaluativa para la recolección de datos es un punto relevante en el análisis de información que ayuda a obtener una comprensión clara y contextualizada de los documentos seleccionados previamente. Esta lectura implica una evaluación detallada de los contenidos que para este caso deben estar relacionados con alguno de los controles descritos en la normativa SEPS 2022-002, evaluando su relevancia, precisión y calidad.

Según (López & Fernandez, 2022), la lectura evaluativa no solo facilita la identificación de patrones y tendencias en los datos, sino que también asegura que los datos recogidos sean fiables y válidos para la investigación en cuestión. La lectura evaluativa facilita a los investigadores extraer información relevante de una variedad de fuentes documentales, garantizando que se mantenga la integridad y la relación con el

tema de investigación durante la recolección de datos, como se lo realizó en la tabla del Anexo I donde después de seleccionar el documento se extrae una breve descripción o resumen resultado de esta lectura evaluativa.

2.2.5. Análisis e interpretación de la información recolectada

El análisis e interpretación de la información recolectada es la última etapa de la investigación documental, y por ende la más importante ya que determina la validez y la aplicabilidad de la información. (García, 2021), menciona que el análisis de datos involucra descomponer la información en componentes más manejables y estudiarla en busca de patrones, tendencias y relaciones relevantes.

Esta etapa requiere un estudio riguroso y el uso de herramientas o técnicas evaluativas adecuadas para asegurar que los descubrimientos reflejen con certeza la realidad investigada. Por otro lado, la interpretación busca relacionar los resultados en concordancia con el problema de investigación, proporcionando un entendimiento más claro de su significado y relevancia.

2.3. Marco teórico

2.3.1. Seguridad de la Información

La seguridad de la información hace referencia a la protección de los activos de la organización contra la interrupción de las operaciones institucionales, posibles modificaciones de datos confidenciales o privados, así como su divulgación. Dicha protección se la describe como el mantenimiento de la confidencialidad, integridad y disponibilidad (conocida como triada de seguridad de la información) de los activos, las operaciones y la información de la institución. (Vacca, 2020)

La gestión de la seguridad de la información en las instituciones financieras ha tomado una gran demanda y a su vez su responsabilidad también ha aumentado, tanto por las exigencias del ente de control como la misma necesidad de las instituciones de proteger las grandes inversiones que gastan en sus presupuestos de TI, todo con la finalidad de garantizar a sus socios o clientes una correcta gestión de riesgos y mitigación de intrusiones por terceros. Este incremento en presupuestos se deriva de la innovación o migración de las tecnologías y su infraestructura en Cloud Computing.

Dentro del ambiente de administración de la seguridad de la información es de suma importancia la intervención y colaboración de todos los departamentos o unidades que se desenvuelven en los procesos agregadores de valor de la institución, que en sector financiero los que más se destacan son la captación de dinero y la colocación de créditos.

2.3.2. Clasificación de la Información

El principal objetivo de la clasificación de la información es "garantizar que los datos o activos de información reciban un nivel adecuado de seguridad de acuerdo con su nivel de importancia para cada institución". Además, la clasificación de la información también es un punto de partida muy importante para el desarrollo del análisis de riesgos que siempre debe realizarse como parte fundamental del SGSI.

La información identificada como un activo debe clasificarse de acuerdo con su valor y criticidad para la organización, y protegerse en consecuencia. Normalmente, un esquema de clasificación utiliza categorías en un modelo jerárquico, donde cada categoría está asociada con procedimientos sobre cómo manejar la información y qué mecanismos de protección requiere. (Bergström & Åhlfeldt, 2014)

Es recomendable que las instituciones no usen o generen demasiadas categorías de clasificación de la información, ya que al crear un esquema complejo hace que el proceso de clasificación se vuelva más difícil y tedioso para usar, una institución común puede tener tres o un máximo de cinco categorías. El esquema de clasificación de información probablemente más conocido proviene del ejército de los EE. UU. e incluye los tres niveles: ultrasecreto, secreto y sin clasificar. En un entorno institucional la categorización que podemos usar puede ser: restringido o confidencial, privado y público.

2.3.3. Gestión de Riesgos de Seguridad de la Información

El proceso de gestión del riesgo de la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque periódico suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos de impacto alto se valoren de manera correcta. (Ministerio de Telecomunicaciones, 2020)

Según (Ministerio de Telecomunicaciones, 2020) las actividades que se debe considerar para la gestión del riesgo de la seguridad de la información son:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Figura 10. Pasos del proceso de gestión de riesgos

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	**1** *Consideraciones Generales - Levantamiento de información inicial* **2** *Establecer criterios básicos para la Gestión del Riesgo* **3** *Definir alcance y límites de la Gestión del Riesgo* **4** *Establecer una organización para la operación del SGRSI*
Valoración del Riesgo	**5** *Identificar Activos de Información* **6** *Identificar las amenazas y las vulnerabilidades* **7** *Identificar los controles existentes* **8** *Identificar consecuencias* **9** *Valorar las consecuencias* **10** *Valorar los incidentes* **11** *Determinar el nivel de estimación del riesgo* **12** *Evaluar el riesgo*
Tratamiento del Riesgo	**13** *Seleccionar controles*
Aceptación del Riesgo	**14** *Aceptar el riesgo*
Comunicación del Riesgo	**15** *Comunicar el riesgo*
Monitoreo y Revisión del Riesgo	**16** *Monitorear y revisar los riesgos*

Fuente: (Ministerio de Telecomunicaciones, 2020)

Cada institución para la planificación de la gestión de riesgos de la seguridad de la información debe determinar un alcance y sus objetivos de gestión, ya que dependiendo de su giro de negocio y sus procesos agregadores de valor van a tener enfoques diferentes y así mismo se debe establecer criterios básicos, como tipo de evaluación de riesgos, tipos de impactos, niveles aceptables de riesgo, etc.

2.3.4. Control de Accesos Físicos y Tecnológicos

Según (Caldas Urduy, 2020) el control de acceso involucra los siguientes conceptos, con el fin de poderlos distinguir y más importante aún, tenerlos en cuenta para el momento de aplicarlo:

- Identificación: lo que se presenta para demostrar la identidad.
- Autenticación: como se comprueba la identidad.

- Autorización: que se debe hacer después.

Para mantener un buen control de accesos en una institución se deben determinar áreas seguras, donde se encuentre localizada la información crítica para la organización, y esta a su vez deben estar protegidas por un perímetro de seguridad, que impida el acceso no autorizado a aquellas personas a las cuales no se brinde los permisos correspondientes para acceder a esta área, y esta información crítica deberá estar localizada en un lugar que no sea de constante paso de distintos usuarios, sino por el contrario, deberá estar aislada en un sitio donde no sea tan recurrente el paso de personas. (Caldas Urduy, 2020)

Parece que el control está dejando de ser territorio exclusivo de los proveedores de sistemas de acceso electrónicos: están ganando protagonismo rápidamente las empresas tecnológicas internacionales, capaces de dibujar un nuevo horizonte para la seguridad y revolucionar el paradigma clásico. Las ciudades y los edificios inteligentes presentan grandes oportunidades y muchos apuntan a un rápido crecimiento del mercado del control de acceso moderno gracias a la facilidad de implementación y la sofisticación de las tecnologías actuales, que aportan numerosas ventajas en los entornos inteligentes. (Axis comunications, 2021)

Las nuevas e innovadoras metodologías de la ciberdelincuencia están obligando a las instituciones a poner más atención a todas las vulnerabilidades de seguridad de la información, por lo cual dentro del proceso de gestión de riesgos se debe considerar el tema de los Controles de accesos, los cuales también han ido creciendo tecnológicamente incursionando dentro del IoT, manteniendo una base de datos de todos los registros, que periten dar un seguimiento a posibles incumplimientos a las políticas de seguridad o fugas de información.

2.3.5. Procesos agregadores de Valor

Según (Paltín León , 2022) los procesos conocidos como “agregadores de valor” son clave para el cliente, siendo el conjunto de actividades que dan sustento a la misión, visión, planes y objetivos institucionales; y de apoyo o que proporcionan productos o servicios a los procesos gobernantes. La cadena de valor constituye un modelo de aplicación que permite visualizar las actividades y funciones entrelazadas que se ejecutan de manera interna en la institución. En el entorno financiero los procesos agregadores de valor más comunes son: colocación de créditos, captación de inversiones y ahorro a la vista.

2.3.6. Plan de Contingencia Informática y Continuidad de Negocio

Según (Nuñez Santamaría, 2022) un plan de contingencia permite identificar los riesgos (de origen natural o humano) a sistemas o recursos informáticos, para mantener la continuidad del negocio de la organización recuperando la totalidad de su funcionalidad en el menor tiempo posible, proteger la información es primordial, para garantizar su integridad, confidencialidad y disponibilidad.

La ISO / IEC 24762: 2008 proporciona directrices sobre la provisión de servicios de recuperación de desastres de tecnología de la información y las comunicaciones (DR de TIC) como parte de la gestión de la continuidad del negocio, aplicable a proveedores de servicios de DR de TIC internos y subcontratados de instalaciones físicas y servicios. Esta norma internacional especifica:

- Los requisitos para implementar, operar, monitorear y mantener los servicios e instalaciones de recuperación de desastres de TIC.

- Las capacidades que deben poseer los proveedores de servicios de recuperación de desastres de TIC subcontratados y las prácticas que deben seguir, a fin de proporcionar entornos operativos básicos seguros y facilitar los esfuerzos de recuperación de las organizaciones.
- Guía para la selección del sitio de recuperación.
- Guía para que los proveedores de servicios de DR de TIC mejoren continuamente sus servicios de DR de TIC" (Nuñez Santamaría, 2022)

2.3.7. Vulnerabilidades Informáticas

Según (CRESPO OROZCO, 2022), son fallos o debilidades de un sistema informático. Se trata de agujeros que puede ser producido por un error de configuración, o por una persona malintencionada para comprometer su seguridad. Dichos fallos pueden comprometer a los principios de la seguridad (confidencialidad, integridad y disponibilidad).

Las vulnerabilidades están ligadas a las amenazas, ya que, si no existe una gestión de vulnerabilidades, tendremos la probabilidad de que las amenazas se desenvuelvan en los sistemas informáticos, por lo que podríamos decir que las vulnerabilidades son la puerta de ingreso para los incidentes informáticos.

2.3.8. NIST 800-30

La metodología NIST 800-30 se enfoca en la clasificación de la información en diversas categorías, determinadas por su nivel de riesgo aplicando estándares para garantizar que la gestión de la información sea adecuada a cada nivel. Esta metodología fue fundada para evaluar los riesgos de seguridad de la información especialmente en

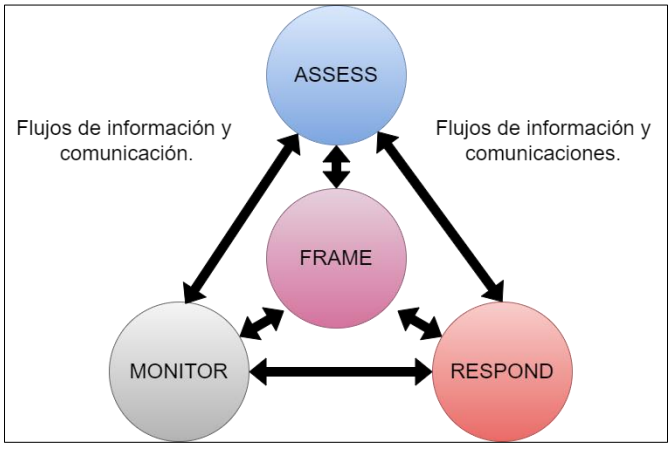
sistemas TI (Tecnología de la Información) con el objetivo de apoyar a las organizaciones con todo lo relacionado al uso de Tecnología. (ISOTools, 2021)

Los objetivos principales en los que se fundamenta la metodología NIST SP800-30 son: (ISOTools, 2021)

- Seguridad de los sistemas de información que se encargan de almacenar, procesar y transmitir información.
- Gestión de Riesgos.
- Mejorar la administración de Riesgos a partir del resultado del análisis.
- Sostener las habilidades y procesos fundamentales de la organización para alcanzar su misión.
- Ser una función esencial en la administración de TI.

El proceso de gestión de riesgos que establece la NIST 800-30 incluye: 1) enmarcar el riesgo; 2) evaluación del riesgo; 3) responder al riesgo; y 4) seguimiento del riesgo. A continuación, se presenta de manera gráfica los cuatro pasos fundamentales del proceso de gestión de riesgos, así mismo, se visualiza los flujos de información y comunicaciones esenciales para asegurar que el proceso funcione de manera óptima.

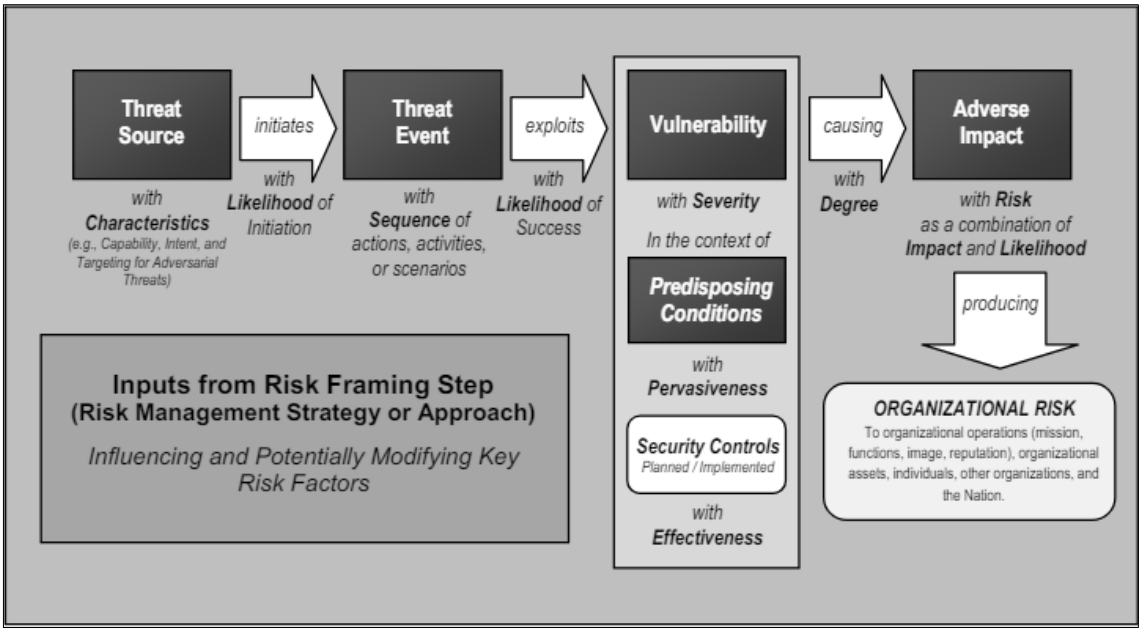
Figura 11. Evaluación de riesgos dentro del proceso de gestión de riesgos.



Fuente: NIST 800-30

El modelo de Riesgo debe definir los factores que van a ser evaluados, éstos son características que utilizan para determinar los niveles de riesgo. Los factores de riesgo más típicos que se utilizan incluyen: amenaza, vulnerabilidad, impacto, probabilidad y condición predisponente. Para ello es necesario que antes de realizar una evaluación de riesgo la organización documente bien estas definiciones. (National Institute of Standars and Technology (NIST), 2012)

Figura 12. Modelo de riesgo NIST 800-30



Fuente: NIST 800-30

En la imagen 6, se observa el modelo de riesgo de la NIST 800-30 que incluye los factores de riesgo claves que ésta utiliza para su evaluación. El modelo inicia evaluando una amenaza, con sus respectivas características, la cual tiene una probabilidad inicial que puede desencadenar una secuencia de eventos o escenarios para explotar una vulnerabilidad.

Esta vulnerabilidad puede tener una gravedad amplia o puede tener condiciones que hacer que la vulnerabilidad no sea tan fácil de cruzar, como es la implementación de

algún tipo de control de seguridad y esto determinará el impacto que esta amenaza puede tener en base a la probabilidad con la se puede producir, dando como resultado el Riesgo Organizacional.

2.3.9. MAGERIT v.3

MAGERIT v3.0 es una metodología desarrollada en el Centro Criptológico Nacional (CCN) de España como respuesta a que la Administración Pública (y en general toda organización y sociedad) dependen de forma creciente tecnologías de la información para alcanzar sus objetivos. El creciente uso de tecnologías de información y comunicaciones (TIC) promete beneficios indiscutibles para las organizaciones; pero de igual forma da lugar a ciertos riesgos que deben gestionarse con la implementación de medidas de seguridad que garanticen confianza en los usuarios de los servicios. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Esta metodología proporciona una guía estructurada para evaluar y gestionar los riesgos relacionados con la seguridad de la información que puede aplicarse para cualquier organización. Esta metodología se basa en la Norma ISO/IEC 27005, pero brinda un enfoque más detallado de los principios y procesos para gestionar los riesgos de la seguridad de la información.

La metodología de MAGERIT se acopla al marco de trabajo de la ISO 31000 a la sección 4.4 (“Implementación de la gestión de los Riesgos”), determinando el proceso más adecuado para la gestión del riesgo permitiendo que cada organización tome decisiones tomando en cuenta los riesgos procedentes del uso de tecnologías de la información. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

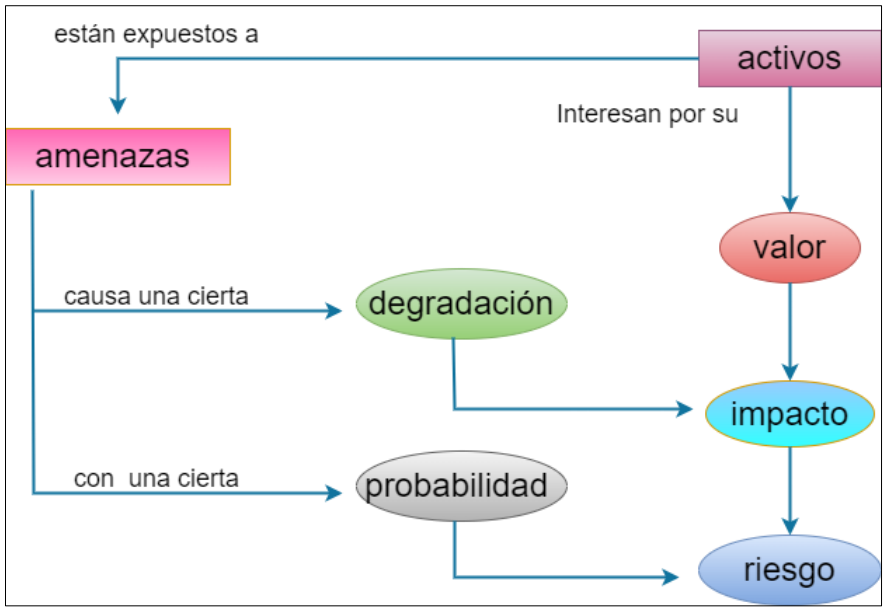
Figura 13. Marco de trabajo para la gestión de riesgos

Fuente: ISO 31000: 2018

El método de análisis de Riesgo que determina MAGERIT v3.0 en su primer libro consta de 5 pasos: (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

- Determinar los activos relevantes para la organización describiendo su importancia y su valor, considerando el daño que ocasionaría su degradación.
- Determinar todas las amenazas a las que están expuestos aquellos activos.
- Determinar las salvaguardas correspondientes y su eficacia frente al riesgo.
- Estimar el impacto, al considerar los daños que se podrían ocasionar en el activo en caso de que la amenaza se materialice.
- Estimar el riesgo, entendido como la ponderación del impacto junto con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Figura 14. Elementos de la metodología MAGERIT v3



Fuente: MAGERIT v3.0 Libro 1

2.3.10. MEHARI

Mehari es una metodología que se caracteriza por presentar dos tipos de gestión de riesgo: directa e individual y global. El objetivo en los dos tipos de gestión es evaluar qué nivel de seguridad tiene una organización.

La diferencia se encuentra en la profundidad de la evaluación, siendo el tipo de gestión global menos preciso que el tipo de gestión directa e individual que garantiza un nivel superior de fiabilidad. En la tabla 3 se presenta las ventajas y desventajas de cada tipo de gestión: (Grupo ESG Innova, 2021)

Tabla 3. Tipos de gestión de riesgo según Mehari

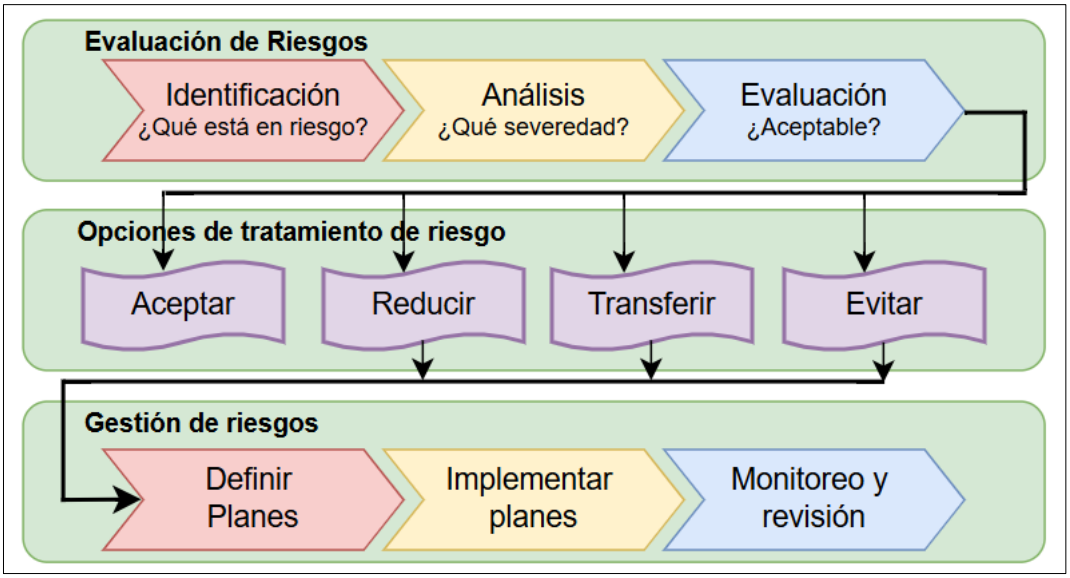
	Gestión directa e individual	**Gestión global**
Ventajas	Identificación y análisis de todas las posibles situaciones de riesgo. Evaluación más exacta del nivel de riesgo para cada posible situación de riesgo. Evaluación más exacta del efecto de las medidas de seguridad	Presentación simple de riesgos. Los conceptos son fáciles de entender. Facilita la comunicación de los riesgos.

	establecidas en el nivel de riesgo para cada posible situación de riesgo.	Facilita la conexión de los riesgos con las medidas de seguridad a implementar.
Desventajas	Requiere determinar un modelo completo que presente todos los riesgos. Requiere que cada situación de riesgo se evalúe en toda su complejidad	Posiblemente podría ignorar situaciones de riesgo con nivel alto. Complica la evaluación del nivel de gravedad de los riesgos de forma exacta. Infravaloración en el tratamiento del riesgo.

Fuente: CLUSIF 2010

Mehari adopta el enfoque de la gestión de riesgo descrito en la norma ISO/IEC 27005, como se detalla en la Figura 15.

Figura 15. Fases en la gestión de riesgos



Fuente: CLUSIF 2010

3.3. Marco legal

En primera instancia se menciona a la 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 (SEPS 2022-002) la cual es el principal enfoque de este trabajo de grado, adicional a esto es una normativa de carácter obligatorio que toda institución financiera bajo supervisión de la SEPS debe cumplir en el lapso de tiempo establecido.

Código Orgánico Monetario Y Financiero, está encargado de regular los sistemas monetarios y financieros, y es quien da la faculta a la SEPS para la emisión de normativas que fuesen necesarios con la finalidad de velar por la estabilidad y correcto funcionamiento de las instituciones bajo su supervisión.

Resolución SEPS-IGT-IR-IGJ-2018-021 emitida en julio 2018, hace referencia a las medidas mínimas de seguridad física, considerando que esta se encuentra inmersa dentro de seguridad de la información, además de tener estrictamente que cumplir con estos lineamientos según lo establecido en el Anexo I de la normativa SEPS 2022-002.

Resolución No. SEPS-IGT-IR-IGJ-2018-0279 emitida en noviembre de 2018, habla sobre la administración del riesgo operativo, en la cual también se hace una pequeña referencia sobre lineamientos de seguridad de la información.

Resolución No. SEPS-IGT-IGS-INFMR-INGINT-IGJ-2020-0153, norma sobre los principios y lineamientos de educación financiera, donde se considera a la seguridad de la información como un tema importante de educación financiera, además de que uno de los controles del Anexo I de la normativa SEPS 2022-002 menciona un plan de capacitación sobre seguridad de la información.

CAPITULO III
MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

El estudio de la normativa SEPS 2022-002 se desarrolla en el ambiente de la Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda., ubicada en la ciudad de Otavalo perteneciente a la provincia de Imbabura. Esta cooperativa se encuentra en el segmento 3, según la distribución financiera de la SEPS, por lo tanto, se acoge a lo estipulado para el Régimen Especial de la normativa.

3.2. Enfoque y tipo de investigación

El análisis de la normativa SEPS 2022-002 tendrá un enfoque cualitativo, considerando que la cooperativa Chuchuqui Ltda., al momento de realizar la planificación de trabajo no cuenta con políticas, procesos, procedimientos y metodologías establecidos en base a normas de seguridad que se pueda documentar. El proyecto inicia sin elementos de seguridad de la información que puedan ser valorados por lo que se enfoca en visualizar las mejoras de los aspectos cualitativos que se describen en su desarrollo.

El tipo de investigación es de tipo documental, realizando primeramente una búsqueda de documentación relacionada a cada control de seguridad de la información descrito en el Anexo I de la normativa SEPS 2022-002, para luego llevar a cabo un análisis de la misma y extraer lineamientos que permitan cumplir con la normativa.

3.3. Procedimiento de investigación

La investigación se enfoca al análisis de la normativa SEPS 2022-002, luego se extrae datos de la revisión sistemática de literatura obtenidos del estudio de artículos científicos, framework de seguridad de la información, y normativas internacionales que

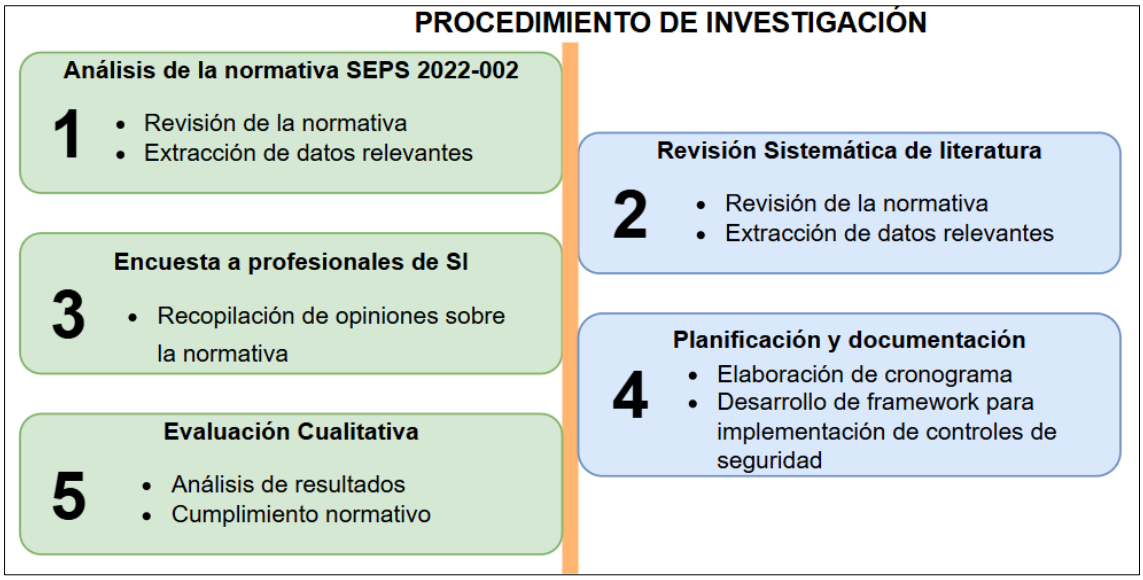
se relacionen al cumplimiento de los lineamientos de seguridad establecidos por la Superintendencia de Economía Popular y Solidaria.

También se realiza una encuesta dirigida a profesionales de seguridad de la información del sector financiero con el objetivo de analizar las diversas opiniones de dichos profesionales sobre aspectos específicos de la normativa de seguridad que rige al sector financiero popular y solidario.

Se realizará un cronograma de planificación en base a los controles de seguridad de la información descritos en la normativa SEPS 2022-002, considerando la documentación recolectada sobre cada uno de estos, para ser analizados y construir un framework de implementación de cada control, apoyado en la metodología MAGERIT v3.

Una vez establecida la documentación necesaria para cumplimiento de dicha normativa se evaluará los resultados obtenidos de forma cualitativa. En la figura16 se muestra un esquema del procedimiento de investigación.

Figura 16. Procedimiento de investigación



Fuente: Autor

3.4. Consideraciones bioéticas

Este trabajo de grado beneficiará a todas las instituciones financieras que se encuentren en segmento 3, pero de manera principal a la Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda., de la cual el Comité de Seguridad de la Información y el Consejo Administrativo tiene el pleno conocimiento de las exigencias de la Superintendencia de Economía Popular y Solidaria para el cumplimiento de la misma y los tiempos que se han establecido para su desarrollo, por lo cual se establece una reunión de trabajo conjunto para determinar los lineamientos para su ejecución y los niveles de divulgación de información.

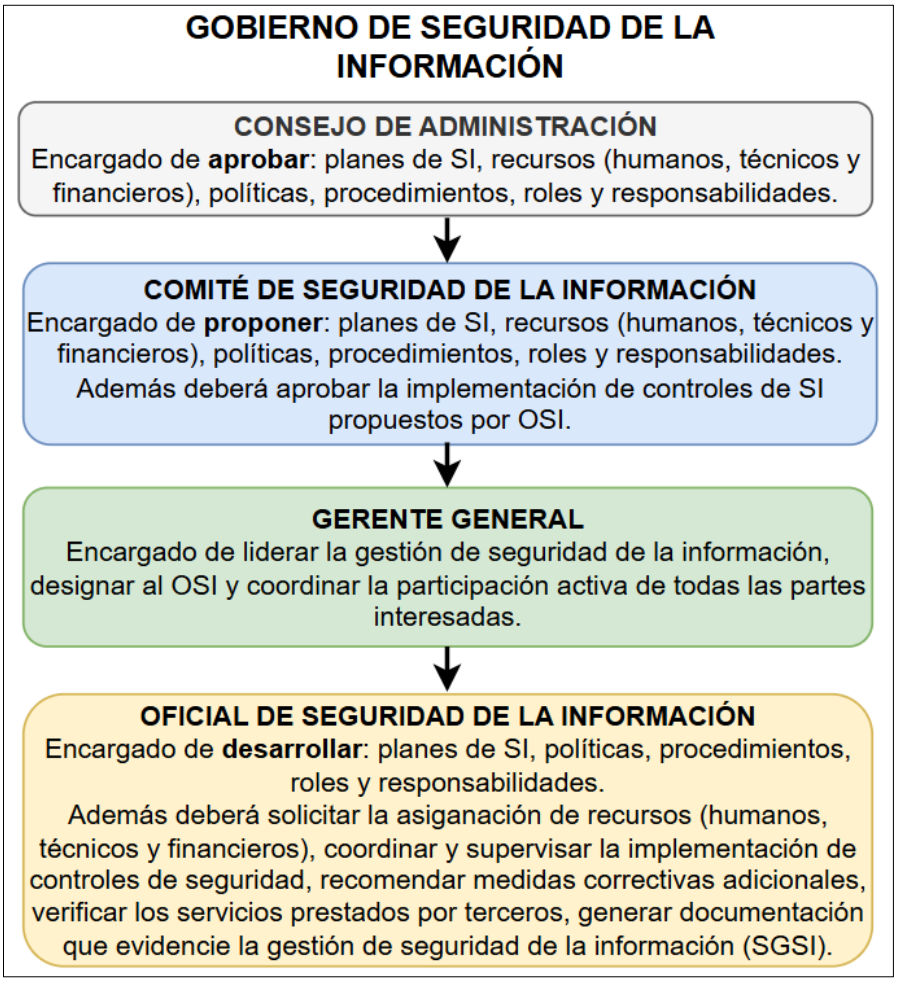
El desarrollo de este proyecto de investigación se pone en consideración en reunión del Comité de Seguridad de la Información (CSI) de la cooperativa, con la finalidad de obtener su consentimiento para su desarrollo y evaluación. La resolución del Comité queda plasmada en el acta N° CSI-002 con fecha 22 de junio de 2023. La designación de los miembros de dicho Comité se encuentra alineada a la normativa SEPS 2022-002 y están debidamente formalizados con los siguientes miembros:

- El Presidente del Comité de Administración Integral de Riesgos. - a quien se le asigna la distinción de Presidente del CSI.
- Gerente General. – no se le asigna ninguna distinción, pero tiene voz y voto en las decisiones del CSI.
- Oficial de Seguridad de la Información (OSI). – se le asigna la distinción de secretario del CSI, quien debe llevar a cabo a redacción de las actas del Comité y su debida custodia.
- El responsable del área de tecnología o su delegado. - no se le asigna ninguna distinción, pero tiene voz y voto en las decisiones del CSI.

- Un delegado de Auditoría Interna. - no se le asigna ninguna distinción, pero tiene voz y voto en las decisiones del CSI. A partir de la publicación de la resolución SEPS-IGT-IGS-INR-INGINT-INSESF-2023-008, en la que se obliga a las instituciones de segmento 3 contar con un Auditor Informático, quien por sus conocimientos será quien pasa a ser miembro del CSI.

La estructura de gobierno de seguridad de la información y sus principales funciones se la describen en la figura 17.

Figura 17. Gobierno de Seguridad de la Información.



Fuente: SEPS 2022-002

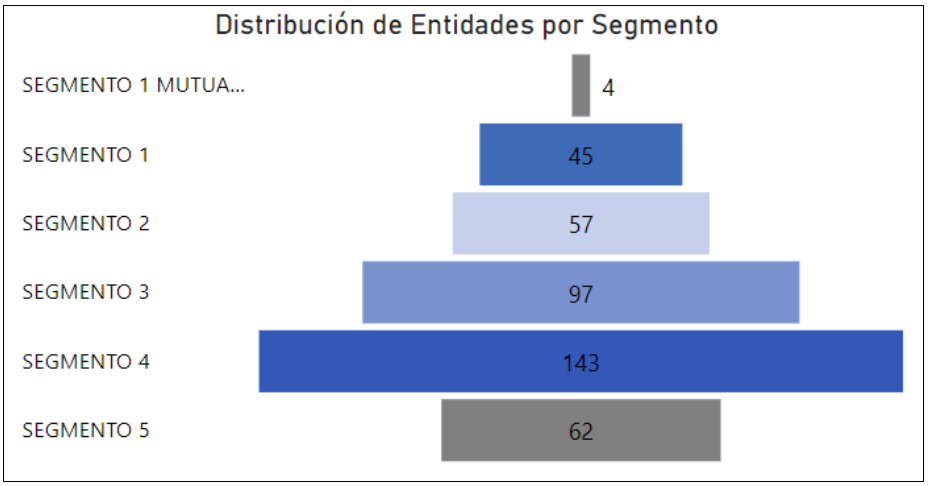
CAPITULO IV
RESULTADOS Y DISCUSIÓN

Este capítulo tiene como objetivo desarrollar un framework de cumplimiento de la normativa SEPS 2022-002, iniciando con el análisis de los resultados obtenidos de la encuesta realizada a profesionales de Seguridad de la Información del SFPS adoptada como herramienta de la investigación documental a pesar de que es más comúnmente utilizada en las investigaciones de campo, pero se ha visto la necesidad de contar con la opinión de profesionales que se encuentran dentro de la misma segmentación financiera y en base a esto analizar las mejores opciones para establecer una guía para cumplir cada uno de los controles establecidos en el Anexo I de dicha normativa.

3.1. Encuesta dirigida a profesionales de Seguridad de la Información

Para la encuesta se ha considerado un cálculo de la muestra en base a los datos de la SEPS, sobre la cantidad de entidades financieras que se encuentran en el segmento 3, como se observa en la figura 18, con fecha de corte enero 2024 existen 97 instituciones a nivel nacional en esa distribución, por lo cual se utilizará este número como variante de población total.

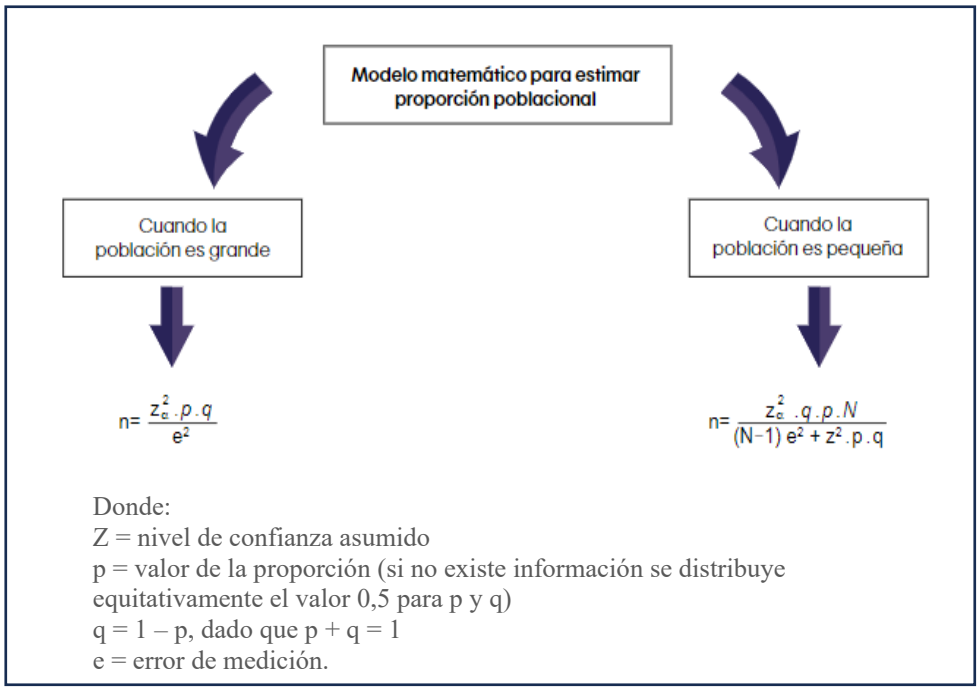
Figura 18. Distribución de entidades por segmento.



Fuente: SEPS 2024

Según (Mucha Hospinal, Chamorro Mejía, Oseda Lazo, & Alania Contreras, 2021) existen dos modelos matemáticos para estimar proporción poblacional, la una es cuando la población es grande y la otra cuando la población es pequeña, como se muestra en la figura 19.

Figura 19. Modelos para estimar proporción poblacional



Fuente: Mucha Hospinal, Chamorro Mejía, Oseda Lazo, & Alania Contreras, 2021

En base a la imagen anterior podemos establecer el valor de la muestra requerida para este estudio, para ello se considera un nivel de confianza (Z) del 95%, un valor de proporción tanto para p y para q de 0,5 y un error de medición de 5%. Estos valores se los toma en base a las recomendaciones establecidas en varios casos de estudio.

Entonces el resultado obtenido para la muestra es de 46,99 lo que quiere decir que por lo menos se debe recolectar la opinión de 47 personas para una buena estimación de los resultados de la encuesta.

La encuesta se encuentra respaldada por la validación de un instrumento de evaluación pidiendo el apoyo de un profesional con trayectoria en el ámbito de seguridad de la información, este documento se presenta en el Anexo III.

3.1.1. Análisis e interpretación

La encuesta consta de un total de 15 preguntas de las cuales 5 son preguntas generales para identificar a que sector social se está realizando la encuesta y 10 son directamente relacionadas con el trabajo de estudio, los resultados obtenidos se muestran de completamente en el Anexo IV. Sin embargo, se presenta un resumen con los aspectos más relevantes:

- El 81,2% de los profesionales de seguridad declaran tener un alto conocimiento de la SEPS 2022-002, pero vemos que existe un porcentaje que aún no tiene una claridad total sobre cómo dar cumplimiento a la normativa, por lo que se considera que el framework será de mucha ayuda, no solo para aquellos que tienen debilidad de conocimiento sino también para aquellos que piensan tener certeza, para poder tener una guía con la que se puede comparar el trabajo ya implementado.
- En cuanto a enfoques de investigación para proyectos de seguridad, predomina la investigación documental (37,5%) y la cualitativa (27,1%), lo que sugiere preferencia por marcos y buenas prácticas ya comprobadas con resultados reales, complementadas con levantamiento de contexto organizacional.
- Sobre la claridad de los requisitos de la SEPS 2022-002, las respuestas con mayor porcentaje son: “de acuerdo” (45,8%) e “indiferente” (39,6%), con

una fracción menor en desacuerdo. Adicionalmente, cuando se pregunta si se considera que la normativa está bien definida y no necesita mejoras, el 89,6% responde “No”, lo que da a comprender que los profesionales creen que la normativa tiene oportunidades de mejora. Las justificaciones indican que se debe reforzar el tema de mejora continua, mejorar la explicación o descripción de controles y alineación a la realidad institucional de segmento 3.

- Respecto al cumplimiento se visualiza que solo el 22,9% considera que su implementación de la normativa es suficiente como para cubrir lo que se determina en la normativa. Entre las limitaciones que se describe que existen para lograr el cumplimiento es la falta de apoyo de alta gerencia y recursos limitados, es ahí donde el framework presenta su mayor fortaleza que es la optimización de recursos.
- En metodologías, predomina la familia ISO/IEC 27000 (62,5%), seguida por MAGERIT v3 y, en menor medida, NIST 800-30, COBIT 5 e ITIL. Si bien es cierto las normas ISO/IEC 27000 no son consideradas una metodología, se las consideró dentro de la encuesta para demostrar que existe una confusión de términos, por lo cual, la metodología que en verdad tiene mayor aceptación es MAGERIT v3.

3.2.Framework para el cumplimiento de la normativa SEPS 2022-002

El Framework de Cumplimiento ha sido elaborado específicamente para las cooperativas de ahorro y crédito del segmento 3, con el propósito de ofrecer un recurso práctico para la implementación de los controles de seguridad correspondientes a la segmentación establecidos en el Anexo 1 de la normativa SEPS 2022-002. Para cada

control de seguridad se proporciona la información necesaria para el cumplimiento de los requisitos establecidos, así como para los casos que aplique se presenta sugerencias para la generación de documentos y herramientas de que faciliten su cumplimiento.

Además, este framework se estructura para proporcionar una comprensión clara y práctica de cada uno de los controles, permitiendo a las entidades financieras del segmento 3 realizar una evaluación de su situación actual en términos de seguridad y establecer medidas correctivas y preventivas de acuerdo con lo establecido en la normativa SEPS 2022-002.

El framework es un recurso educativo para las cooperativas de ahorro y crédito del segmento 3, pero también se considera un mecanismo para fortalecer la cultura de seguridad de la información que brinde estabilidad y confianza en el sector financiero popular y solidario. La implementación efectiva de los controles descritos contribuirá a la protección integral de los datos y activos financieros, alineándose con mejores prácticas de seguridad y exigencias regulatorias establecidas por la SEPS.

Para su desarrollo se considera los lineamientos descritos principalmente en la metodología Magerit v3, pero también se rescatan aspectos de otros recursos de buenas prácticas relevantes como COBIT 2019, ITIL v4, y de la familia ISO 27000.

Su implementación en base al tiempo establecido por la SEPS para segmento 3 es de tres años, pero con la guía del framework se estima reducir ese tiempo a tan solo un año, para ello se ha elaborado un cronograma anual, el cual se detalla en el Anexo V. Adicionalmente se establece una matriz como guía de implementación resumida de los controles de seguridad la cual se presenta en el Anexo VI.

3.2.1. Políticas

Según la norma ISO/IEC 27001:2022 la política de seguridad de la información debe ser establecida por la alta dirección y debe por lo menos:

- Estar orientada a la misión y visión de la organización.
- Incluir objetivos de seguridad de la información o establecer un marco de referencia para la formulación de objetivos de seguridad de la información.
- Comprometer el cumplimiento de los requisitos aplicables a la seguridad de la información.
- Comprometer a la institución a la mejora continua del SGSI.
- Su información debe estar disponible, documentada y formalizada.
- Socializar a todos los funcionarios de la institución.
- Estar disponible para las partes interesadas pero protegida por el principio de no divulgación.

Existen varios métodos para la socialización interna de la Política de Seguridad de la Información que las instituciones pueden implementar, entre los cuales se menciona los siguientes:

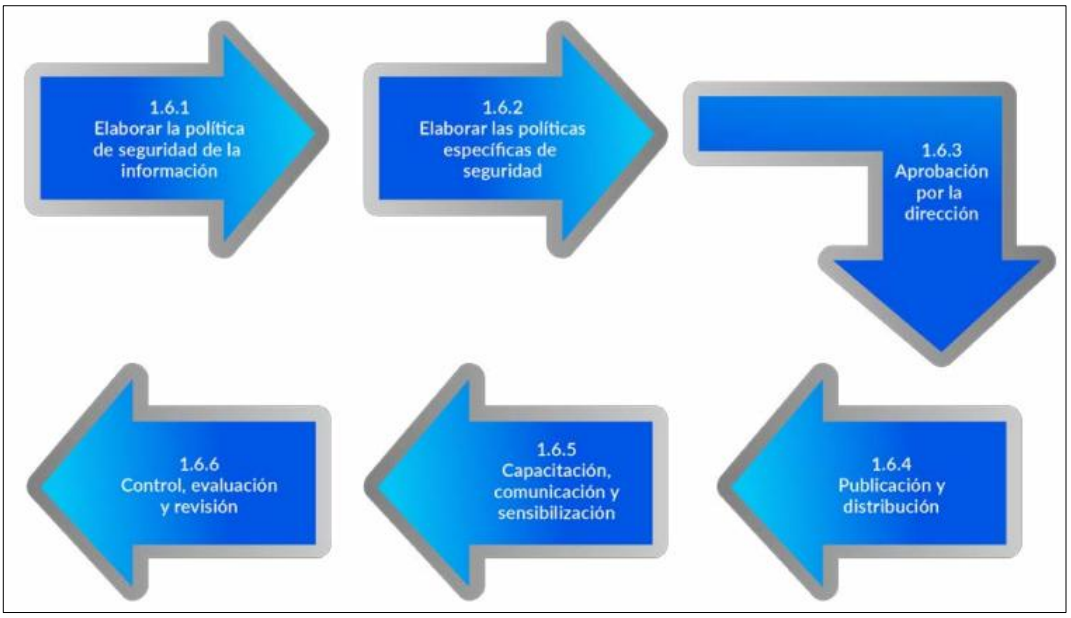
- Charlas dentro del procedo de inducción a los nuevos funcionarios.
- Envío de correo electrónico y publicación en alguna carpeta compartida.
- Entrega de la documentación de forma personal.
- Publicación en cartelera informativa.
- Publicación en la página de intranet institucional.

Los métodos antes mencionados pueden ser utilizados de forma individual o combinada para el fortalecimiento del programa de sensibilización. Además, se debe

garantizar la comprensión de todos los colaboradores, para lo cual se debe medir el conocimiento mediante evaluaciones periódicas generando registros de los resultados obtenidos.

En base a las directrices mencionadas anteriormente (CERTIPROF , 2022) ha establecido un esquema de las etapas que debe cumplir la política de seguridad de la información como se muestra en la Figura 20.

Figura 20. Etapas de la Política de Seguridad de la Información



Fuente: CERTIPROF 2022

Para la elaboración de las políticas se debe tomar en cuenta que éstas pueden ser de tres tipos: permisivas, mandatarias y prohibitivas, por ejemplo:

- Permisivas. - Los funcionarios pueden solicitar al jefe de tecnología la generación de respaldos de la información relevante para sus funciones.
- Mandatarias. - La cooperativa debe designar a un Oficial de Seguridad de la Información con conocimientos competentes y brindar los recursos necesarios para el cumplimiento de sus funciones.

- Prohibitivas. – Está prohibido copiar información en dispositivos USB personales, para evitar la fuga de información.

3.2.1.1. Política General de Seguridad de la Información

El propósito de la política General de seguridad de la información es definir o establecer directrices, reglas y principios básicos para la gestión de la seguridad de la información. Su finalidad es garantizar la continuidad de la seguridad de la información, dando cumplimiento a la normativa vigente con estrategias aplicables e implementando un conjunto de medidas adecuadas para la gestión de riesgos de la seguridad de la información. (Subsecretaria de Desarrollo Regional y Administrativo del Gobierno de Chile, 2023)

La política General debe contener por lo mínimo lo siguiente:

- Objetivos de la política
- Alcance
- Documentos de referencia
- Definiciones
- Roles y Responsabilidades
- Directrices para la aplicación de la política
- Evaluación del cumplimiento
- Revisión de la política
- Vulneración de las políticas de Seguridad de la Información, y
- Excepciones

En base a lo descrito en el Anexo VII se presenta un modelo de política general que puede adaptarse a cualquier institución de segmento 3.

La política general debe identificar las necesidades de seguridad de la información en el contexto de la realidad institucional, también debe considerar la cultura, los problemas y las preocupaciones de la institución por lo que debe estar alineada a los objetivos estratégicos de la organización. (INEN, 2022)

La política general debe incluir a la alta Gerencia y el compromiso que debe tener para apoyar al cumplimiento de los requisitos de seguridad de la información. Como lo estable la normativa SEPS 2022-002, el gerente general es quien debe liderar la gestión de seguridad de la información asegurando la participación de todas las partes interesadas.

La política general debe tener una redacción de fácil comprensión, ya que debe ser comunicada a todas las partes interesadas que también puede incluir a externos como clientes, proveedores, contratistas o el ente regulador (SEPS). (INEN, 2022)

3.2.1.2. Política de Clasificación de la información

El propósito de esta política es identificar, categorizar y garantizar la protección de la información según el nivel de sensibilidad y criticidad basado en los principios de confidencialidad, integridad y disponibilidad.

Según Andersson, 2023, la clasificación de la información se basa en el valor de la información contenida en los activos, para lo cual se debe establecer una lista de activos clasificados indicando su importancia y valor en función de su criticidad para la institución, las clasificaciones más comunes de los activos son:

- Activos de información: bases de datos, documentos digitales, buzón de correos electrónicos, informes impresos, licitudes de fondos, pagares, historial crediticio, entre otros.

- Activos tecnológicos: equipos de usuarios finales, teléfonos fijos o móviles, firewall, servidores, equipos de comunicación, entre otros.
- Activos de software: Antivirus, licencias, desarrollos internos, aplicaciones, sistemas operativos, entre otros.
- Activos de servicios: internet, almacenamiento en la nube, energía eléctrica, plataforma de recaudación, mensajería masiva, consultas de registro civil, consultas de buró de crédito, entre otros.
- Activos físicos: Edificios, Data Center, bóveda, caja fuerte, oficinas, entre otros.
- Activos humanos: Empleados, personal bajo contrato de servicios profesionales, consultores, auditores, proveedores con acceso privilegiado, entre otros.

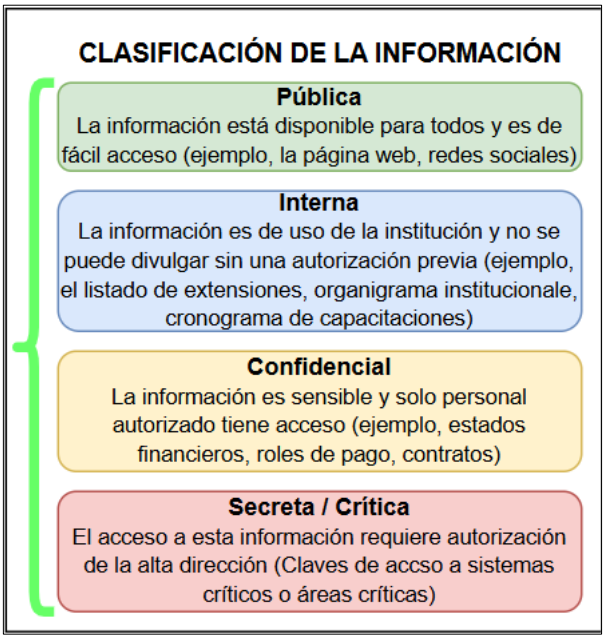
Lo anterior descrito es lo más común dentro de las organizaciones, pero en base a la necesidad se puede incluir otras clasificaciones más específicas como son: Activos electrónicos, activos eléctricos, activos de imagen corporativa, activos de transporte, activos de virtualización, activos de respaldo y continuidad, activos de voz IP, entre otros.

La clasificación ayuda a la organización a evaluar la criticidad de su información para que pueda elegir medidas de seguridad adecuadas para que no reciba poca protección. La valoración de la información se realiza considerando las consecuencias que una protección insuficiente de la información podría causar para la organización. (MSB – Myndigheten för samhällsskydd och beredskap, 2024)

Dentro de la gestión de riesgo operativo de las instituciones financieras, la clasificación de la información es un factor muy importante, que permite valorar de

manera más objetiva el impacto que puede tener en la institución la pérdida o divulgación de la información en base al tipo de clasificación presentada en la figura 21.

Figura 21. Clasificación de la información



Fuente: Propia

3.2.1.3. Política de Gestión de riesgos de seguridad de la información

El propósito es establecer los lineamientos para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos relacionados con la seguridad de la información, con el fin de proteger la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información de la Cooperativa de Ahorro y Crédito, asegurando el cumplimiento de la Norma SEPS-2022-002 y los principios del Sistema de Gestión de Seguridad de la Información (SGSI) institucional.

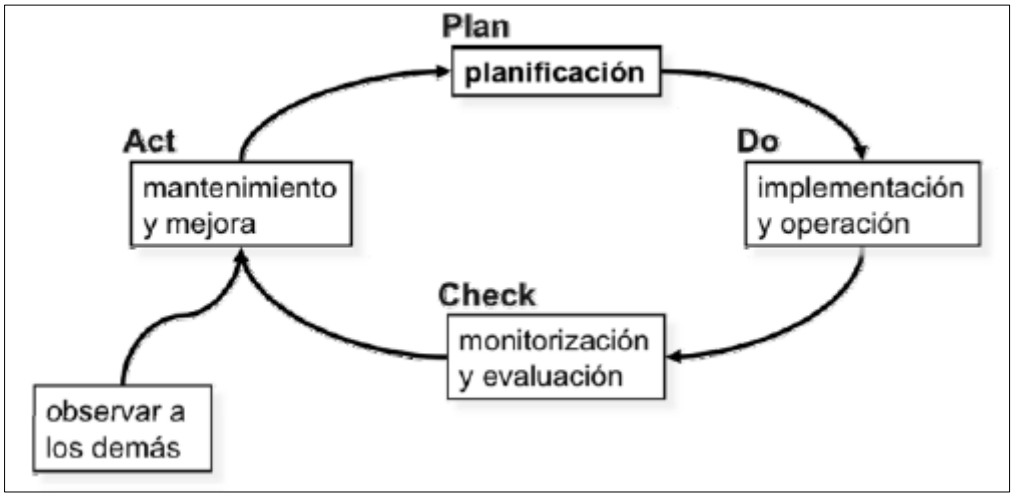
La Gestión de riesgos de seguridad de la información de acuerdo a la clasificación determinada en el punto anterior se enfoca en brindar los lineamientos para proteger la información confidencial y sensible, para ello se considera la metodología de MAGERIT v3.

El objetivo de la gestión de riesgos según MAGERIT v3 es brindar a los sistemas o redes de información la capacidad de resistir accidentes o acciones malintencionadas que afecten a los principios de seguridad (disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad).

Entonces lo que MAGERIT propone es que se realice un análisis de los riesgos que permita determinar cómo es (cual es el riesgo y como se genera), cuánto vale (en base a la afectación que tiene a los principios de seguridad) y cómo protegido está (que salvaguardas se tiene implementado) un activo de información.

Para una gestión eficiente de riesgos, es importante que se involucre a todos los actores de la institución, ya que el personal en su operación diaria es quien se enfrenta a las incidencias por lo cual su aporte en el monitoreo general es relevante para tener una eficiencia para alcanzar objetivos propuestos. Con este fin se establece cuatro etapas cíclicas de la gestión de riesgos de la información que se muestra en la figura 22.

Figura 22. Clasificación de la información



Fuente: MAGERIT v3

Dentro de la planificación el tema de concienciación y formación es clave para prevenir problemas o poder reaccionar de manera eficiente cuando se produzcan. Se

necesita una colaboración activa de los empleados, sobre todo cuando existe una resistencia ante el cumplimiento de medidas de seguridad, por lo que la cultura de seguridad se encarga de recalcar la responsabilidad de cada propietario, encargado, custodio o generador de información.

Lieamientos:

- La gestión de riesgos deberá realizarse de manera sistemática y documentada, de acuerdo con la metodología adoptada por la Cooperativa (basada en MAGERIT v3 o metodologías equivalentes).
- Todo activo de información deberá ser identificado, clasificado y valorado para determinar su importancia y los riesgos asociados.
- Los riesgos tecnológicos y de seguridad de la información serán analizados considerando la probabilidad de ocurrencia y el impacto potencial sobre los procesos institucionales.
- Los planes de tratamiento de riesgos deberán definirse priorizando los niveles de riesgo no aceptables, estableciendo controles adecuados para su mitigación.
- Se mantendrá un registro actualizado de riesgos, con responsables asignados, controles asociados y seguimiento de su evolución.
- Los niveles de riesgo residual deberán ser aprobados por la Alta Dirección, garantizando su aceptación documentada.
- La Oficialía de Seguridad de la Información (OSI) será responsable de coordinar la gestión integral de riesgos y de presentar informes periódicos al Comité de Seguridad de la Información (CSI) y a la Gerencia General.

- La política se complementará con los procedimientos específicos de gestión de riesgos y deberá revisarse al menos una vez al año o cuando existan cambios significativos en el entorno tecnológico o regulatorio.

3.2.1.4. Política de Control de accesos físicos y tecnológicos

Según (Zamora Pomaquiza, 2023) el control de accesos físicos y tecnológicos tiene como objetivo establecer medidas de protección para prevenir el acceso no autorizado a la información sensible o crítica como base de datos, servidores, redes. Las medias de seguridad física pueden incluir sistemas de alarmas, sistemas de CCTV, puertas blindadas, controles de acceso biométrico, entre otros.

Dentro de las instituciones financieras se debe determinar políticas y procedimientos específicas tanto para el ingreso a de las instalaciones, permanencia y salida, las cuales deben contemplar tanto para funcionarios, directivos, visitantes, socios, clientes, proveedores y personal de limpieza y seguridad.

Las entidades financieras están supervisadas en tema de seguridad física por el COSP (Control de Organizaciones de Seguridad Privada) que es un organismo técnico de la Policía Nacional, encargada de realizar inspecciones y emite permisos de operación. Si una institución financiera no obtiene el certificado de seguridad del COSP, en base a la normativa de la SEPS deberá someterse al cierre total de sus operaciones. Para ello los controles involucran desde contar con distintos manuales (Recursos humanos, reglamento interno, manual general de procesos, seguridad de la información, Salud y Seguridad Ocupacional, Auditoría, etc.), y certificaciones de instalación de los sistemas de seguridad en general (Alarmas, contra incendios, CCTV, puertas blindadas y vidrios blindados).

En base a esto se detalla algunos lineamientos para cumplir con las políticas y procedimientos de accesos físicos y tecnológicos, los cuales también se basan en la norma de la SEPS-IGT-IR-IGJ-2018-021 respecto al control de Seguridad Física y Electrónica.

Para el ingreso se debe considerar políticas sobre la responsabilidad de los guardias de seguridad antes de la apertura, como es revisar el perímetro exterior para garantizar que ha existido forcejeo, manipulación de las cerraduras o riesgos externos. Se debe asegurar que se giga el protocolo de ingreso establecido por la institución, por lo general los requisitos de ingreso son:

- Asegurar el perímetro exterior, vigilando que no exista personas sospechosas.
- Cumplir con el mínimo de funcionarios para el ingreso.
- Verificar que se encuentren el custodio de llaves y custodio de claves de acceso.
- Cumplir con el horario establecido para el ingreso.
- El delegado de llaves debe abrir todas las cerraduras incluyendo candados y cerraduras de ventanas y lanford que se encuentren en la oficina.
- El delegado de claves debe realizar la desactivación del sistema de alarmas y debe esperar la llamada de confirmación de apertura de la Consola de monitoreo de la empresa encargada del servicio de seguridad privada.
- Determinar un máximo de dos aperturas parciales (una para ingreso de personal operativo y otra para ingreso de personal administrativo)
- El momento de ingreso realizar una revisión de bolsos a los funcionarios.
- Verificar que los funcionarios cumplan con el código de vestimenta y porten su credencial institucional.

- Entre otros.

Para la estadía en las instalaciones de la cooperativa se debe establecer medias de seguridad con la que deben cumplir tanto personal interno como externo, dentro de las medidas más comunes para instituciones financieras están:

- Mantener celulares o cualquier dispositivo electrónico fuera de las áreas críticas y restringidas.
- Hacer uso del uniforme y credenciales en todo momento.
- Mantener los escritorios limpios, ordenados y sin objetos o documentos de valor mientras no se encuentren en uso por el funcionario encargado.
- No permitir el ingreso de personas no autorizadas tales como invitados, familiares y amigos a las instalaciones sin previa autorización.
- Mantener señalética informativa y de prevención de riesgos en todas las instalaciones, así como también contar con mapa de rutas de evacuación.
- No brindar número de contacto telefónico de autoridades o empleados de la cooperativa sin previa autorización.
- Todo proveedor debe contar con una autorización para ingreso que detalle el listado del personal y las acciones que van a realizar, y deberán pasar por un proceso de revisión y registro.
- Toda área crítica o restringida debe contar con un formato de registro físico que detalle la persona que está ingresando, el detalle de la actividad, la hora de ingreso y salida y observaciones.
- Entre otros.

Para el cierre parcial, salida del personal, socios y clientes, y cierre total de las instalaciones debe ser autorizado por el jefe operativo o jefe de agencia, y entre las políticas más comunes de cierre se encuentran:

- El guardia debe realizar el cierre de la puerta principal y mantendrá la custodia de la llave hasta que salga el último socio o cliente.
- No se permite el ingreso de más socios después del cierre parcial, a no ser que cuente con la autorización del oficial de seguridad.
- Los empleados deben apagar sus equipos y guardar sus materiales, documentos y objetos de valor bajo llave.
- Antes de la salida los empleados deben pasar por la revisión de bolsos.
- El guardia debe garantizar que todas las áreas críticas y restringidas estén aseguradas, para la salida de todos los funcionarios y proceder a la activación de la alarma.
- El delegado de llaves debe garantizar que todas las cerraduras y candados externos estén asegurados.

Adicional a las directrices de ingreso, permanencia y salida de las instalaciones se debe establecer políticas y procedimientos para las áreas críticas o restringidas, sobre todo el acceso al Data Center y área de valores. Estas áreas deben contar con una partición independiente en el sistema de alarmas para llevar un mejor control.

Respecto al área de valor es recomendable establecer sistemas de exclusa, para lo cual dentro de la distribución estructural deberá contar con una puerta de ingreso principal al área de valores (puerta blindada tipo A) y posterior a esta deben existir dos puertas de seguridad más una para ingreso al área de cajas y otra para acceso al área de bóveda o pre-bóveda.

El sistema de CCTV debe garantizar una resolución de imagen óptima, dentro de la norma no se establece específicamente la calidad de imagen, pero la resolución mínima aceptada por los delegados del COSP es de 2Mpx, sin embargo, se debe considerar lo más adecuado en base a la criticidad de las áreas, por ejemplo, las áreas críticas como la zona de valores (interna y externa) se recomienda manejar una resolución de 8Mpx y para el resto de las áreas sería recomendable una resolución de 4Mpx. En todas las áreas de atención al público y áreas críticas se debe garantizar que no existan puntos ciegos.

Los sistemas de alarma tanto de intrusión como de detección de incendios deben estar enlazadas por cualquier medio a centrales de monitoreo ya se al servicio integrado de seguridad ECU 911 o a empresas de seguridad privada. Se debe garantizar que todos los elementos del sistema de alarmas estén operativos en todo momento para ello se debe llevar un cronograma de mantenimientos preventivos y pruebas de simulacro.

3.2.1.5. Política de Gestión de Incidentes

Para poder establecer la política de gestión de incidentes hay que dejar claro la diferenciación con la gestión de riesgos, ya que esto forma parte de la limitación de su alcance.

La gestión de riesgos se enfoca en identificar, evaluar y tratar posibles riesgos antes de que ocurran incidentes, para ello se elabora matrices de riesgos, escenarios y se planifica simulaciones para verificar la eficacia, mientras que la gestión de incidentes se encarga de responder, minimizar daños y recuperar la operación después de que un incidente se encuentra en curso o ya sucedió.

En base a lo mencionado, su alcance se delimita a la detección, respuesta, mitigación de daños y recuperación ante incidentes de todos los sistemas, procesos, personal, terceros y proveedores con acceso privilegiado a los activos de información de la institución.

Según ITIL v4 un incidente es una interrupción no planificada de un servicio o una reducción de la calidad del servicio. La gestión eficaz de los incidentes tiene un buen impacto en la satisfacción del cliente, socios y usuarios.

Se debe registrar cada incidente y gestionar garantizando su solución en un tiempo adecuado que cumpla las expectativas planteadas. Se debe realizar una priorización de los incidentes en base a una clasificación por su criticidad según el impacto institucional. Es recomendable contar con una herramienta que permita el registro de los incidentes y su seguimiento para generar una base de conocimiento. Esta herramienta también debe permitir registrar cambios, problemas, errores conocidos, solución brindada y otros elementos que alimenten la base de conocimientos lo que permite brindar una recuperación más rápida y eficiente.

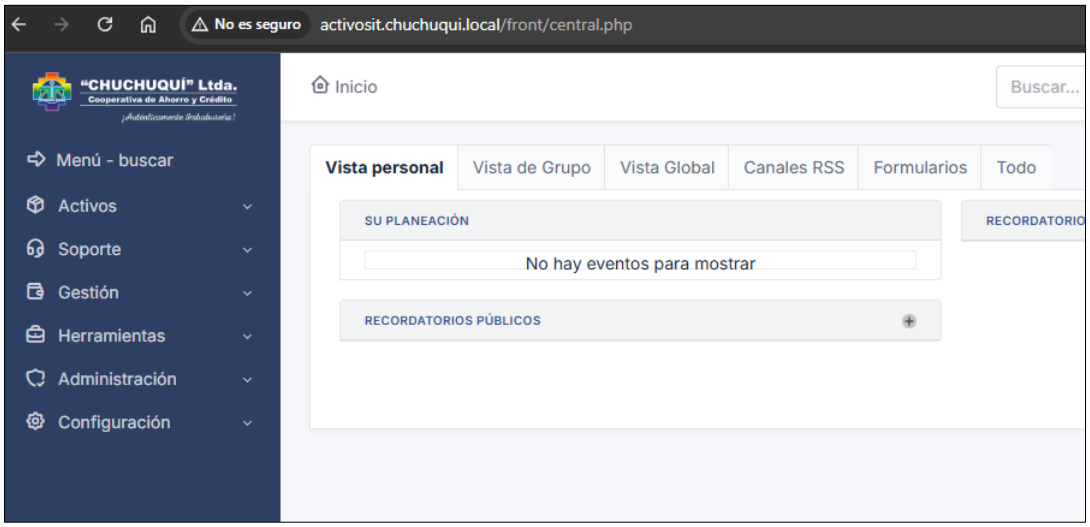
Lineamientos:

- Todo incidente se resolverá dentro de los tiempos establecidos en SLA vigentes.
- Los incidentes de seguridad de la información serán gestionados bajo liderazgo del OSI.
- Los incidentes recurrentes o de riesgo alto deberán escalarse como Problemas para análisis de causa raíz.
- Todo incidente deberá documentarse en la base de conocimientos con su solución.

- Los incidentes atendidos por proveedores deberán registrarse con número de caso y trazabilidad en el ticket.

Una herramienta muy común para la gestión de incidentes es GLPI (Gestionnaire Libre de Parc Informatique) que es open source que permite también gestionar servicios de Tecnología de la información, es de uso común debido a que es gratuita, cumple con lineamientos de buenas prácticas de ITIL y es personalizable como se observa en la figura 23.

Figura 23. Personalización de GLPI



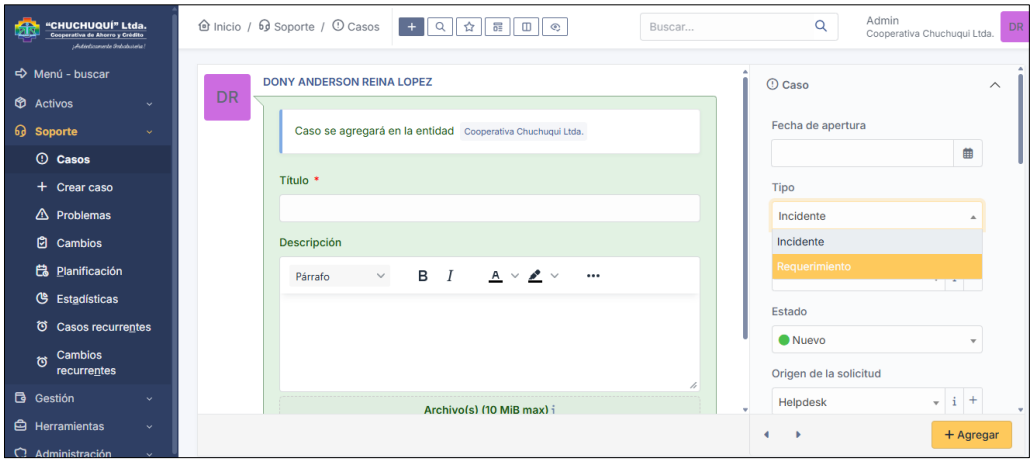
Fuente: Propia

Dentro de las principales funcionalidades de GLPI se encuentran:

- Inventario de activos (hardware, software, licencias, dispositivos de red, periféricos, entre otros).
- Gestión de ticket de soporte (incidentes, problemas, requerimientos)
- Gestión de cambios y proyectos.
- Base de conocimientos para documentar soluciones a incidentes.
- Generación de Reportes e indicadores

En este caso lo que nos compete es la gestión de incidentes que se encuentra en el módulo de soporte que cuenta con casos, problemas, cambios, planificación, estadísticas, casos y cambios recurrentes, como se observa en la figura 24.

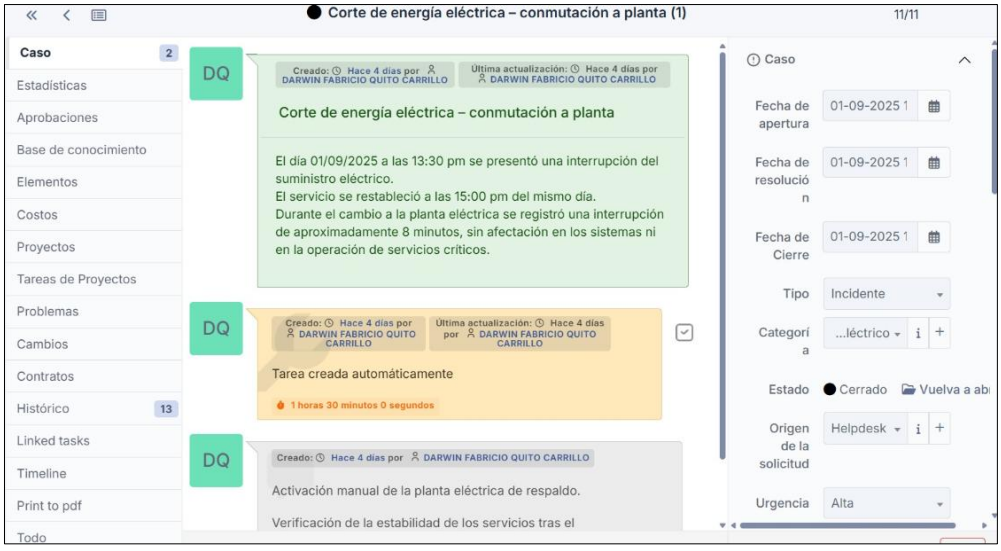
Figura 24. Módulo de soporte de GLPI



Fuente: Propia

A continuación, en la figura 25, se presenta un ejemplo de registro de un incidente donde se especifica el detalle del incidente, la fecha de apertura, fecha de resolución, fecha de cierre, tipo, categoría, estado.

Figura 25. Módulo de soporte de GLPI



Fuente: Propia

Los incidentes deben categorizarse y clasificarse de acuerdo a su nivel de impacto, para ello se propone que se lo realice bajos los siguientes criterios:

Categoría del incidente.

- Alto: El incidente de seguridad tiene impacto sobre activos de información críticos e influyen directamente en la continuidad de los servicios de la cooperativa. En este grupo también se considera aquellos incidentes que afectan a la imagen institucional, involucren aspectos legales o al cumplimiento normativo.
- Medio: El incidente de seguridad genera un impacto moderado en los activos de información, que influye directamente a un servicio, proceso o actividad en específico.
- Bajo: El incidente de seguridad tiene un impacto menor o insignificante sobre los activos de información, sin afectar a los servicios de la institución.

Clasificación del incidente (depende de la perspectiva de cada institución, y esta clasificación

- Problema de credenciales de acceso.
- Virus malware.
- Manipulación de logs.
- Phishing.
- Cambios no autorizados.
- Filtración de datos.
- Violación de seguridad física.
- Incumplimiento de políticas de seguridad.
- Entre otros que se considere para la institución.

3.2.1.6. Política de Gestión de software

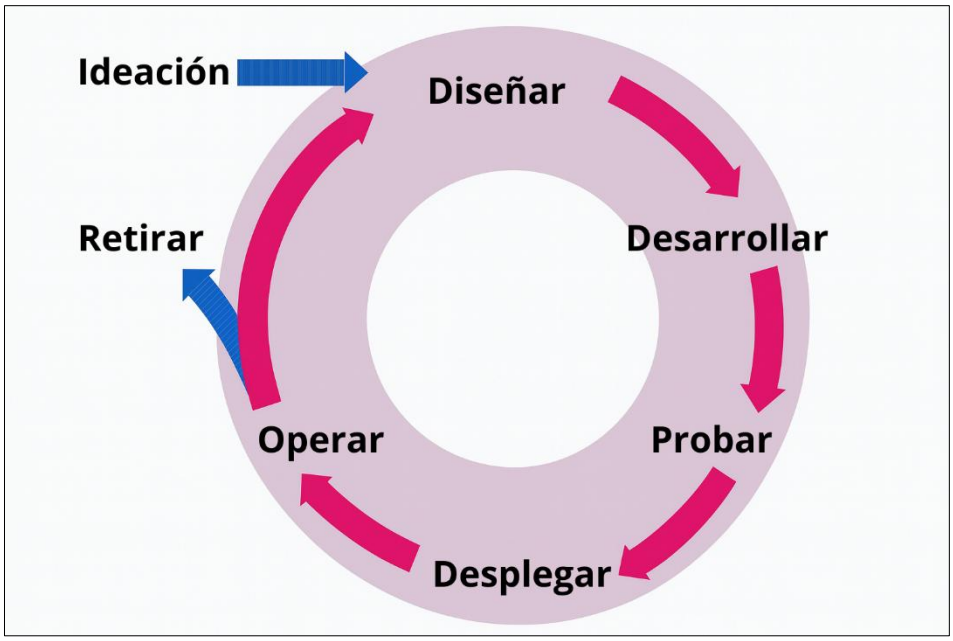
Esta política proporciona medidas de seguridad en el proceso de adquisición, desarrollo, instalación, actualización o eliminación de software que sea gestionado por o para la Cooperativa con la finalidad de reducir el riesgo a la exposición a amenazas de seguridad. Para ello se recomienda que la institución cumpla lo siguiente:

- Todo software incluyendo sistemas operativos y aplicaciones, requieren una gestión continua y oportuna.
- Asignar a una persona o departamento la responsabilidad de la gestión de software documentado formalmente.
- Es responsabilidad del jefe de tecnología verificar que la instalación de software se realice con programas y licencias oficiales para garantizar que estén libres de malware.
- Es responsabilidad del jefe de tecnología aplicar los parches de seguridad de manera correcta a los sistemas operativos, así como exigir que también se cumpla en las aplicaciones de terceros.
- Para la adquisición del software se debe establecer dentro de los términos contractuales soporte futuro y la vida útil estimada del aplicativo. Es importante obtener la garantía de los fabricantes para el seguimiento de actualizaciones con la finalidad de mitigar cualquier vulnerabilidad de seguridad.
- Hacer uso de instalaciones que permitan una administración centralidad para restringir el uso de privilegios administrativos individuales.

- Se prohíbe el uso de software que comprometa la seguridad de la infraestructura de la Cooperativa, como la instalación de programas crackeados.
- Se prohíbe el uso de software que genere inconvenientes operativos a nivel general que puedan saturar la infraestructura y que exija recursos excesivos.
- El software que no cuente con una licencia oficial debe desinstalarse de inmediato.
- Todo equipo de usuario final debe contar con un antivirus con licencia y base de datos actualizada.

Según ITIL v4 la gestión de software abarca actividades en todo el ciclo de vida del software: diseño, prueba, operación y mejora continua de aplicaciones de software. En la figura 26 se muestra el ciclo de vida del software establecido por ITIL

Figura 26. Ciclo de vida del software



Fuente: ITIL v4

En base al ciclo de vida ITIL menciona que la gestión de software debe abarcar las siguientes actividades (AXELOS, 2019):

- Diseño de soluciones.
- Desarrollo de software.
- Pruebas de software (se debe incluir pruebas de seguridad de la información).
- Gestión de repositorios o bibliotecas de código para mantener la integridad.
- Creación de paquetes en caso de aplicar, para un despliegue y actualización eficiente.
- Control de versiones.

3.2.1.7. Política de Gestión de infraestructura tecnológica

La gestión de infraestructura es un tema de prioridad para el cumplimiento de la normativa de Riesgo Operativo SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116, específicamente lo dispuesto en el Art. 14, numeral 7 cuyo objetivo es "*garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las entidades y la Corporación, deben contar con políticas y procedimientos de gestión de la infraestructura*".

En base a lo mencionado anteriormente, se describe los siguientes lineamientos a cumplir:

Mantenimiento preventivo y correctivo

La cooperativa debe contar con el soporte de los proveedores calificados de tecnología de información para cumplir con un cronograma de mantenimientos de forma periódica, además dentro del *manual* de tecnología de la información y

comunicación (Manual TIC) de debe establecer políticas de mantenimientos programados a los equipos de cómputo institucional, tanto en su parte física (hardware) y su parte lógica (software). Los mantenimientos deben ser registrados en la herramienta GLPI, para constatación y presentación de reportes.

Actualización y renovación de equipos de cómputo

La actualización y renovación se hará de conformidad con el análisis de la capacidad y rendimiento de los recursos tecnológicos como lo establece la normativa de la SEPS. Este análisis debe ser comunicado al comité de tecnología con una frecuencia semestral, donde se debe establecer límites y alertas de al menos: almacenamiento, memoria, procesador, ancho de banda. El comité deberá considerar si en base al análisis presentado es necesario realizar una actualización o renovación de equipos, sus resoluciones deben quedar plasmadas en las actas del comité y comunicadas a Gerencia General para poder tomar acción.

El análisis de capacidad y rendimiento también aplica para la actualización y la renovación de servidores, estos equipos están regidos por el ciclo de vida y funcionalidad. Se debe considerar que estos equipos tienen un rol fundamental en los servicios de la Cooperativa, y de ser necesario se puede solicitar la opinión del proveedor que mediante informes técnicos debidamente sustentados recomienden la actualización.

Mantenimiento de servidores

El mantenimiento de estos equipos se debe realizar por personal calificado, preferiblemente con el proveedor directo la marca o quien haya brindado su garantía y deberá ejecutarse en base a un cronograma planificado fuera del horario laboral para no afectar la atención al cliente y operaciones normales de La Cooperativa.

Data Center

Los racks, gabinetes de telecomunicaciones, equipos de red y cableado estructurado, se renovarán de acuerdo con las necesidades de ampliación, actualización y cambios tecnológicos; la actualización estará sometida a análisis del Comité TIC quien realizará la valoración necesaria, además se puede solicitar el apoyo de proveedores de tecnología de la información. También se debe plantear una valoración de sus componentes principales:

a) Aire acondicionado para el Data Center.

El equipo de aire acondicionado se encarga de mantener la temperatura ambiente adecuada la cual se recomienda se encuentre entre 20 ºC y 24 ºC, este rango de temperatura proporciona un equilibrio adecuado entre el rendimiento de los servidores y la eficiencia energética. Además, se debe controlar la humedad relativa para que no supere el 60% evitando que surjan problemas de estática y corrosión en los componentes electrónicos de los servidores; para llevar un control de estos niveles, el equipo de aire acondicionado deberá contar con lectores de temperatura y humedad.

La actualización de estos equipos se determinará en base al su rendimiento para cumplir con la normativa técnica en cuanto a refrigeración y humedad; para lograr ampliar su vida útil se debe realizar una planificación de mantenimientos preventivos y en caso de que estos equipos fallen, se contará con un plan de contingencia para reponer de forma inmediata con un equipo nuevo de características similares.

b) Sistemas de alimentación y distribución de energía.

Para estos sistemas también se debe mantener un cronograma de mantenimiento preventivo en el cual se determinará si es necesario tomar medidas correctivas o de actualización o renovación de los dispositivos de alimentación y distribución de energía.

Se debe garantizar que los equipos soporten la capacidad de consumo eléctrico para mantener en funcionamiento todos los equipos instalados en el Data Center y equipos de cómputo conectados a la red regulada. El UPS deberán suministrar energía a todos los equipos críticos, y su capacidad debe satisfacer de tiempo necesario para el restablecimiento del servicio de energía a través de plantas de energía suplementarias.

Obsolescencia tecnológica

Está determinada por el tiempo de funcionalidad, el desgaste natural, las actividades para las cuales se ha adquirido el equipo y el sitio donde se encuentre operando, el cual varía de acuerdo a las características del equipo, en condiciones normales, la obsolescencia se genera por la renovación tecnológica, dificultad para conseguir repuestos y por los requerimientos y exigencias de las necesidades de los usuarios. Para la definición de obsolescencia se determinan los siguientes parámetros:

a) Obsolescencia en equipos de cómputo y periféricos

Los equipos adquiridos por la Cooperativa tendrán un período de obsolescencia determinado de conformidad con las especificaciones técnicas y la valoración del proveedor. La Cooperativa debe considerar desde el punto de vista contable y técnico para cuando haya llegado al límite validar si las prestaciones del equipo siguen siendo normales para los usuarios y tenga el soporte del proveedor, si no cumple con esto se debe tomar la decisión de renovación de los equipos.

b) Obsolescencia en Servidores

La obsolescencia de estos equipos, se considera a partir de las especificaciones técnicas, análisis y concepto técnico realizado al equipo por parte del proveedor, sin embargo, estos equipos pueden funcionar más tiempo del definido si tiene las condiciones físicas y ambientales recomendadas a más de contar con el soporte técnico

y de repuestos del proveedor, si existe inconvenientes con las prestaciones del equipos se debe tomar la decisión de sustituirlo, el equipo reemplazado podría seguir prestando un servicio con funciones que no demanden mayor capacidad de recursos.

c) Obsolescencia de equipos eléctricos para el cuarto técnico

La calidad de la instalación eléctrica es fundamental para el correcto funcionamiento del cuarto técnico, la Cooperativa debe contar con el proveedor que le brinde el mantenimiento de las instalaciones y ejecutar los ajustes y cambios que se considere necesario ajustados a las mejores prácticas.

Renovación y actualización del software

La Cooperativa debe verificar que el software instalado, en equipos de cómputo y servidores, se encuentren legalmente licenciados y durante su vigencia se ejecute la política de renovación y actualización con las últimas versiones de software correspondiente; esta medida es obligatoria, salvo en aquellos casos en los cuales, por limitaciones técnicas en los computadores no se pueda llevar a cabo, en este caso, se debe renovar el equipo de cómputo para evitar fallos que comprometan la seguridad.

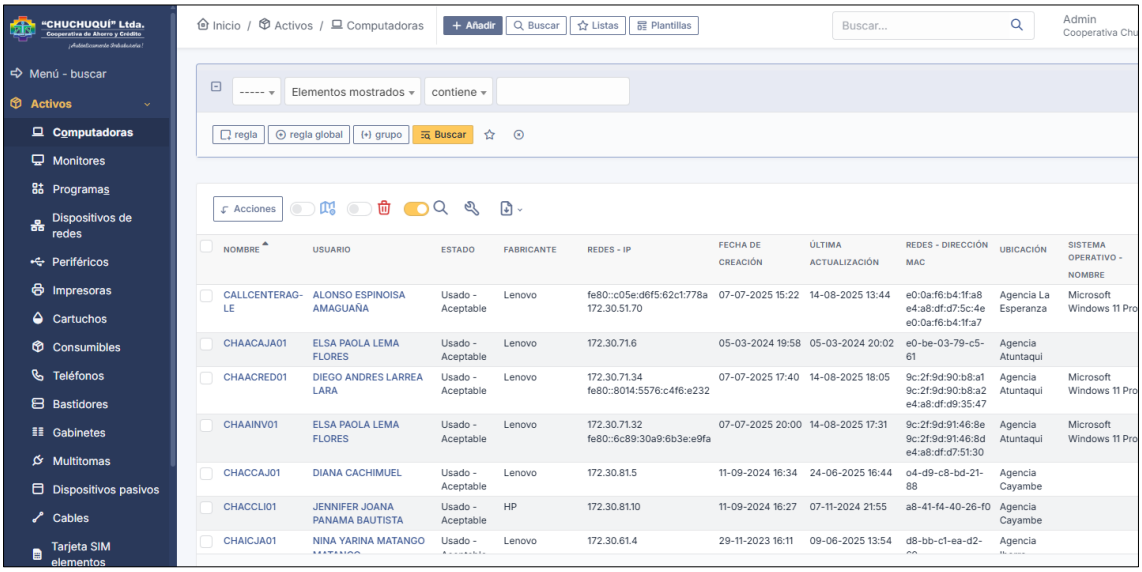
Gestión de redes

- Asegurar que la infraestructura de red esté actualizada.
- Establecer y mantener una arquitectura de red segura.
- Gestionar de forma segura la infraestructura de red conforme a las buenas prácticas.
- Establecer y mantener diagramas de arquitectura.
- Uso de protocolos seguros de administración de redes y comunicaciones.

Otro aspecto importante de la gestión de infraestructura tecnológica que se contempla en la norma de riesgo operativo de la SEPS es mantener un inventario actualizado que considere mínimo: registro, responsable del activo, fecha y control de ingresos y salidas (Superintendencia de Economía Polpular y Solidaria, 2024). Para este cumplimiento también podemos hacer uso del módulo de Activos de la herramienta GLPI, en la cual se encuentran submódulos ya establecidos para el registro de los siguientes tipos de activos: computadoras, monitores, programas, dispositivos de redes, periféricos, impresoras, cartuchos, consumibles, teléfonos, bastidores, gabinetes, dispositivos pasivos, cables y tarjetas SIM.

En el caso del registro de los computadores se lo puede realizar manualmente, pero GLPI cuenta con un agente que se puede instalar en cada equipo de usuario final recopilando toda la información de forma automática, lo que nos permite llevar un control de trazabilidad conociendo a detalle los cambios que ocurren en el equipo, incluso se registran de forma automática los monitores conectados. En la figura 27 se observa ejemplos de levantamiento de información automática de GLPI cumpliendo con lo establecido en la resolución de la SEPS.

Figura 27. Levantamiento de información de computadores en GLPI



Fuente: Propia

3.2.1.8. Política Seguridad de la información para los recursos humanos

Selección y Contratación

- Todos los candidatos deben pasar por un proceso de selección que considere la verificación de antecedentes laborales y legales, acorde a la normativa vigente. A lo cual el responsable de Talento Humano deberá presentar un informe de resultados de la debida diligencia.
- Durante el proceso de contratación, los nuevos empleados deberán firmar acuerdos de confidencialidad y de no divulgación de información.
- Se deberá proporcionar una inducción inicial en la que se incluyan las políticas de seguridad de la información, así como las responsabilidades y obligaciones en el manejo de datos y equipos tecnológicos.

Permanencia y Desarrollo

- Los empleados deben recibir capacitación periódica en temas de seguridad de la información, con énfasis en la identificación de riesgos y amenazas comunes (p. ej., phishing, uso seguro de contraseñas).
- Los accesos a sistemas y datos deben otorgarse bajo el principio de mínimo privilegio y revisarse regularmente para garantizar que correspondan a las responsabilidades del empleado.
- Todo incidente o sospecha de violación a la seguridad de la información debe ser reportado inmediatamente a las áreas responsables.

Desvinculación

- Al finalizar la relación laboral, el responsable de Talento Humano debe notificar de forma inmediata al Departamento de Seguridad de la Información para que se proceda con el bloqueo de todos los accesos a sistemas, redes y recursos tecnológicos que el empleado haya tenido habilitados.
- Se debe realizar un proceso formal de baja, que incluya la revocación de permisos y accesos, garantizando que no existan cuentas activas ni credenciales en uso asociadas al exempleado.
- Los empleados deberán devolver cualquier dispositivo, credencial de acceso físico o documentación confidencial que les haya sido asignado durante su permanencia.
- Se deberá recordar al empleado las obligaciones de confidencialidad y protección de información, las cuales persisten tras su desvinculación.

Roles y Responsabilidades

- Responsable de Talento Humano: Asegurar que los procesos de contratación, permanencia y desvinculación cumplan con los lineamientos establecidos.
- Área de Seguridad de la Información: Proveer capacitación, monitorear el cumplimiento de las políticas y gestionar los accesos a los sistemas de información.
- Empleados: Cumplir con las políticas y reportar cualquier situación que comprometa la seguridad de la información.

3.2.1.9. Política Seguridad Física

Las políticas de Seguridad Física deben alinearse a la resolución SEPS-IGT-IR-IGJ-2018-021, esta resolución establece medidas de seguridad física y electrónica que

las instituciones financieras deben acatar para precautelar la seguridad de los empleados, socios, clientes, usuarios, instalaciones y bienes, así como también las consideraciones para el transporte de efectivo y valores. (Superintendencia de Economía Popular y Solidaria, 2018)

La responsabilidad directa de su cumplimiento es del Oficial de Seguridad Física y Electrónica, quien debe dirigir, gestionar o coordinar los planes de seguridad. A continuación, En la tabla 4 se presenta las exigencias para las instituciones de segmento 3 respecto a seguridad física y electrónica:

Tabla 4. Requisitos de seguridad física y electrónica

Literal	Requerimiento o política de seguridad y protección
a)	Las políticas, normas, principios y procesos conforme a los cuales la cooperativa debe establecer sus medidas de seguridad física y electrónica.
b)	Medidas mínimas de seguridad contempladas en la norma SEPS-IGT-IR-IGJ-2018-021, especificando sus características: dimensiones, calidad de materiales u otros según corresponda.
c)	Medidas de seguridad adicionales a las que se contemplan en la norma SEPS-IGT-IR-IGJ-2018-021, con la finalidad de minimizar posibles riesgos.
d)	Criterios técnicos de la infraestructura de seguridad de sus establecimientos, especialmente de los centros de datos y equipos o dispositivos técnicos de protección para la prestación de servicios
e)	Procedimientos, sistemas y controles operativos destinados a prevenir y detectar irregularidades en la ejecución de las operaciones y en la administración de los recursos, particularmente en lo relacionado con el manejo de efectivo y valores bajo su custodia.
f)	Los sistemas de monitoreo y alarma deberán cumplir con parámetros de calidad y disponibilidad, además de incluir las especificaciones técnicas y tecnológicas necesarias que aseguren la correcta transmisión y emisión de imágenes y señales
g)	Se deberán establecer criterios claros para la contratación de servicios profesionales orientados a brindar seguridad y protección en los diferentes establecimientos
h)	Será obligatorio contar con lineamientos y programas de capacitación e información dirigidos al personal de la entidad, especialmente en lo referente a la preparación para responder ante emergencias, siniestros o delitos. Dichos lineamientos deberán revisarse y actualizarse al menos una vez al año.
i)	La entidad deberá implementar dispositivos, sistemas y procedimientos que permitan controlar de manera adecuada el ingreso y la salida de sus empleados
j)	También deberán existir mecanismos y protocolos para gestionar el acceso y salida de socios, clientes, usuarios, proveedores y personal supervisor

k)	La institución deberá contar con planes de seguridad, contingencia, emergencia y continuidad del negocio frente a siniestros o actos delictivos. La eficacia de dichos planes deberá verificarse mediante simulacros anuales, coordinados con la Policía Nacional, el Cuerpo de Bomberos y la Secretaría Nacional de Gestión de Riesgos, dejando evidencia escrita de su ejecución y evaluación
l)	Los sistemas de alarma y monitoreo deberán contemplar indicadores de calidad y disponibilidad, además de cumplir con los requisitos técnicos necesarios para su correcto funcionamiento
m)	La entidad deberá contar con planes de seguridad y emergencia frente a siniestros o actos delictivos, cuya eficacia se verificará y evaluará mediante la realización de simulacros al menos una vez al año, dejando constancia escrita de su ejecución y de los resultados obtenidos
n)	Es necesario establecer de manera clara las medidas y acciones que se adoptarán en caso de que ocurra un siniestro o un acto delictivo
ñ)	Cada entidad deberá efectuar al menos un simulacro con el fin de comprobar la efectividad de las acciones previstas ante posibles siniestros o hechos delictivos

Fuente: Resolución SEPS-IGT-IR-IGJ-2018-021

3.2.1.10. Política de gestión con terceros

Para dar cumplimiento a la gestión de terceros, la Cooperativa deberá cumplir lo siguiente:

- Calificación de proveedores antes de su contratación por parte del Comité de Contratación de proveedores y Adquisiciones en base a los lineamientos establecidos por la cooperativa en cumplimiento a la norma de riesgo operativo y de prevención de lavado de activos.
- Evaluación periódica del desempeño de los proveedores, evaluando la calidad del servicio y verificando que se cumplan los acuerdos de nivel de servicio (SLA) y las condiciones contractuales.
- Garantizar en los contratos exista una cláusula respecto a sanciones por incumplimiento a las políticas de seguridad de la información.
- Contar con un documento de acuerdo de confidencialidad con los proveedores.

- Control de acceso a los sistemas y redes de la Cooperativa controlado por parte de los proveedores, manteniendo registro de los logs.
- Limitación de los derechos de acceso de los proveedores a la información de la Cooperativa comprando que su acceso sea debidamente justificado.
- Socializar con los proveedores las políticas de seguridad de la Cooperativa para la verificación de su cumplimiento.
- En relación a la protección de los datos personales y financieros de los clientes se debe garantizar un adecuado tratamiento de la información por parte de los proveedores.
- Uso canales seguros o cifrados para proteger la información transmitida entre la Cooperativa y los proveedores.
- Requerimiento de informes periódicos sobre las medidas de seguridad implementadas por los proveedores, especialmente de aquellos que proveen servicios críticos.
- Implementación de políticas de seguridad para la gestión de contraseñas seguras y manejo de credenciales de acceso proporcionadas a los proveedores.
- Capacitación dirigida a empleados sobre el manejo y transmisión de información confidencial con los proveedores.
- Solicitar a los proveedores que concedan a la Cooperativa acceso a los registros de auditoría y a los registros relacionados con la seguridad de la información.
- Exigir a los proveedores la entrega de evidencias que demuestren el cumplimiento de las políticas y procedimientos de seguridad de la información establecidos por la Cooperativa.

- Informar oportunamente a los proveedores sobre cualquier incumplimiento detectado en relación con las políticas de seguridad de la información de la Cooperativa.
- Implementar mecanismos que permitan la revisión y actualización periódica de las políticas y procedimientos asociados a la gestión de proveedores.

3.2.1.11. Política de ciberseguridad

Estas políticas proporcionan medidas de seguridad informática cuya finalidad es minimizar los riesgos de ciber ataques. En tal sentido la Cooperativa deberá cumplir con lo siguiente:

- Debe designar la responsabilidad del Oficial de Seguridad de la Información como figura clave en la gestión de la seguridad institucional quien debe estar adscrito a Gerencia General.
- Detectar riesgos y amenazas relacionados con los servicios internos y expuestos públicamente a internet, así como evaluar vulnerabilidades que permitan identificar debilidades en los sistemas y redes, implementando controles para su mitigación.
- Definir procedimientos que permitan reconocer incidentes de seguridad de la información, asegurando una respuesta ágil y efectiva ante posibles violaciones, con el apoyo de los proveedores de TI. Dichos incidentes deberán informarse a la gerencia y ser gestionados por el Oficial de Seguridad de la Información. Además, deberán incluirse procesos de recuperación de datos y continuidad del negocio.

- Implementar mecanismos que, cuando corresponda, detecten comportamientos anómalos en la red, posibles filtraciones, vulneraciones o fuga de información.
- Incorporar soluciones tecnológicas que prevengan ataques de phishing y la propagación de malware.
- Disponer de herramientas que permitan identificar y contrarrestar ataques de denegación de servicio distribuido (DDoS).
- Establecer medidas de protección perimetral mediante el uso de un firewall que regule el acceso a internet y proteja la red interna.
- Elaborar y ejecutar un plan de Ethical Hacking al menos una vez por año.
- Realizar pruebas de ingeniería social anualmente en la Cooperativa.
- Utilizar sistemas de autenticación robusta antes de permitir el acceso a los sistemas institucionales, incluyendo, cuando sea posible, la autenticación multifactor.
- Garantizar la protección de la información mediante el uso de cifrado, tanto en tránsito como en almacenamiento (discos duros, memorias externas, etc.).
- Aplicar cifrado en dispositivos de almacenamiento para resguardar la información en caso de accesos no autorizados o pérdida física.
- Documentar y aprovechar las lecciones aprendidas de incidentes de seguridad anteriores para fortalecer los procedimientos existentes.
- Definir protocolos de notificación interna y hacia entes reguladores, incluyendo formularios estandarizados y tiempos definidos para la ejecución de dichas notificaciones.
- Restringir el acceso a sistemas y datos únicamente a empleados y proveedores que lo requieran para el desempeño de sus funciones.

- Establecer que cada usuario cuente con credenciales individuales y seguras, con la obligación de cerrar sesión al dejar de usar los sistemas. También deberán aplicarse políticas de control de acceso que refuercen estas medidas.
- Mantener un inventario y clasificación de los activos de información, así como determinar la frecuencia y el alcance de las copias de respaldo. Los responsables de las copias deberán estar claramente identificados y el acceso limitado únicamente a personal autorizado.
- Cumplir con todas las exigencias legales y regulatorias relacionadas con la seguridad de la información, en especial las emitidas por la SEPS y la Ley Orgánica de Protección de Datos Personales.
- Proteger la información clasificada como confidencial mediante cifrado y control de permisos de acceso, almacenándola únicamente en servidores seguros o en la nube bajo control institucional, y compartiéndola solo con usuarios autorizados.
- Establecer políticas y procedimientos que abarquen contraseñas seguras, control de accesos, administración de dispositivos móviles, gestión de aplicaciones internas, aplicación de parches, actualizaciones, gestión de incidentes y relación con proveedores.
- Regular el uso de dispositivos móviles, definiendo controles sobre la instalación de aplicaciones, el acceso a datos y su protección en caso de pérdida o robo.
- Asegurar la aplicación periódica de parches y actualizaciones de seguridad en todos los sistemas y aplicaciones para reducir riesgos frente a nuevas amenazas.

- Implementar al menos dos métodos de autenticación segura en los sistemas de la Cooperativa, requiriendo cambios periódicos de contraseñas y prohibiendo su compartición entre usuarios. El acceso deberá limitarse al personal estrictamente necesario.
- Proteger las páginas web institucionales mediante certificados SSL, asegurando la confidencialidad y encriptación de la información transmitida.
- Exigir a los clientes que utilicen servicios en línea de la Cooperativa el uso de contraseñas seguras y autenticación multifactor, además de establecer tiempos límite de sesión y cierre automático tras periodos de inactividad.
- Establecer políticas para el uso seguro de dispositivos y redes, que incluyan contraseñas seguras y actualizadas, antivirus y software contra malware.
- Realizar evaluaciones de Ethical Hacking tanto en entornos internos como externos, corrigiendo las vulnerabilidades detectadas por el Oficial de Seguridad de la Información.
- Implementar programas de capacitación y concienciación en seguridad de la información para todos los empleados, asegurando que comprendan los riesgos y buenas prácticas.
- Formalizar acuerdos de confidencialidad con socios y colaboradores que tengan acceso a la información institucional, y realizar auditorías periódicas sobre los permisos concedidos para retirarlos cuando ya no sean necesarios.
- Antes de formalizar la relación con proveedores, verificar el cumplimiento de cláusulas de confidencialidad, normas ISO 27001 y disposiciones legales como la Ley de Protección de Datos Personales, como condición indispensable para la vinculación

3.2.2. Procesos

3.2.2.1. Procesos agregadores de valor

El levantamiento de procesos es un factor importante para la gestión de la Seguridad de la información, todo proceso debe estar documentado y analizado por el OSI, para garantizar que no existan brechas en cada uno de estos. Ahora bien, la normativa SEPS 2022-002 nos menciona que el análisis se debe enfocar en los procesos agregadores de valor, que serían los de mayor importancia para la continuidad del negocio.

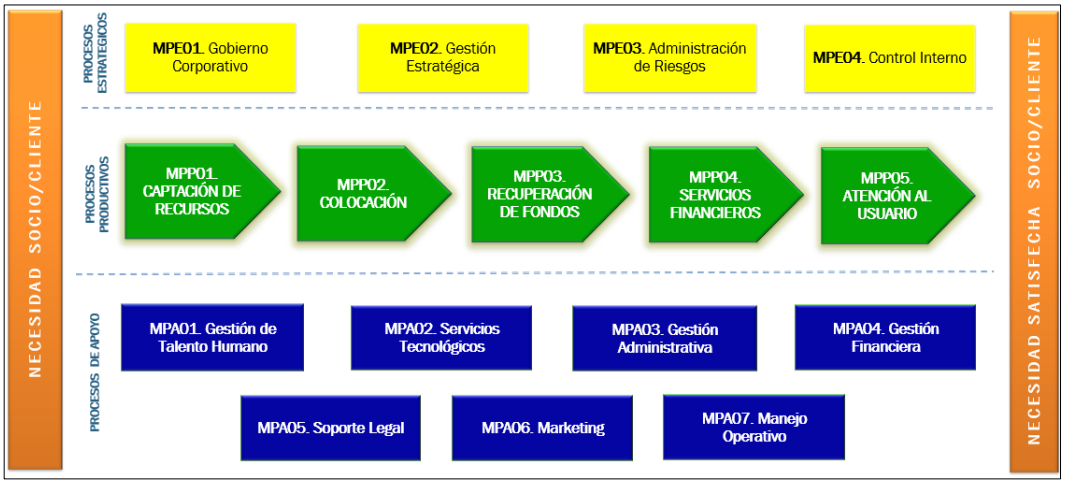
Para tener claro cuales procesos se consideran agregadores de valor se debe iniciar con el levantamiento total de todos los procesos para clasificarlos en tres ramas importantes que deben cubrir las instituciones financieras como se muestra en la figura x, las cuales son:

- Procesos estratégicos
- Procesos productivos
- Procesos de Apoyo

De esta clasificación de procesos, se puede decir que los procesos productivos son los que catalogan como “procesos agregadores de valor”, ya que de estos depende en mucho el giro del negocio, y son en los que se debe poner más énfasis el análisis de la seguridad de la información que en estos se maneja.

En estos procesos productivos es donde se recolecta y almacena la mayor información, especialmente aquella que es proporcionada por los socios y clientes, y es aquí donde entra en juego la Ley Orgánica de Protección de Datos Personales (LOPDP), que va de la mano en el cumplimiento de los controles de seguridad. En la figura 28 se muestra el mapa general de procesos financieros.

Figura 28. Ejemplo de mapa de procesos financieros



Fuente: Cooperativa Chuchuqui Ltda.

Una vez determinado los procesos principales de una institución financiera, se derivan los subprocesos dentro de los cuales se debe tener un esquema de su funcionamiento y las partes que intervienen en todo en proceso. En la figura 29, se presenta un ejemplo de los subprocesos, considerando que dependiendo de la institución y los servicios adicionales que pueden ofrecer al cliente, éstos deberán incluirse en cada caso de estudio.

Figura 29. Ejemplo de subprocesos financieros

Fuente: Cooperativa Chuchuqui Ltda.

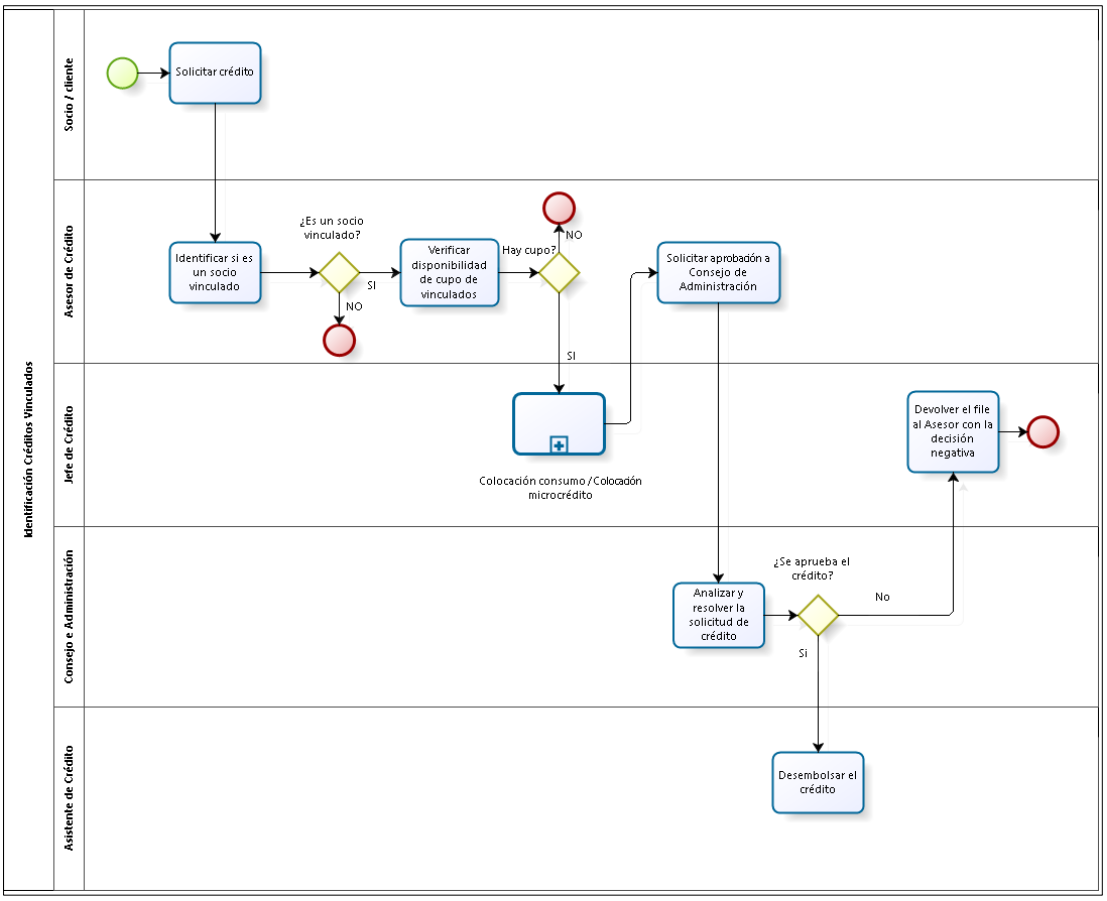
Ahora bien, la normativa SEPS 2022-002 establece que se debe tener un documento en el cual se identifique y defina los procesos agregadores de valor, entonces este documento deberá contener todos los procesos productivos determinados con sus correspondientes subprocesos que contenga por lo mínimo lo que se indica en la figura 30.

Figura 30. Contenido del documento de procesos

Fuente: Autor

Los flujogramas deben ser bastante explícitos de todo el proceso en donde se debe indicar cuales son los actores que intervienen y que función tienen dentro del proceso, como ejemplo se expone en la figura 31 el proceso de identificación de créditos vinculados.

Figura 31. Flujograma de identificación de créditos vinculados.



Fuente: Cooperativa Chuchuqui Ltda.

3.2.2.2. Gestión de Vulnerabilidades

La Gestión de vulnerabilidades según el detalle que se indica en la normativa SEPS 2022-002 más que una gestión de vulnerabilidades se refiere a una gestión de incidentes o hallazgos que se hayan emitido por una Auditoría Informática y en el caso del régimen general también compete a las revisiones de los resultados de las pruebas de penetración que deben realizarse cada año.

Entonces lo que se requiere para dar cumplimiento a este control es presentar documentación de los incidentes o hallazgos generados, para dar seguimiento a las recomendaciones establecidas por el auditor o la empresa de Pentesting. Para esto se debe tener claro cuál es el alcance de las auditorías, para priorizar el análisis a los activos de mayor valor para la continuidad del negocio.

La NIST 800-30 menciona que una vulnerabilidad se considera a las debilidades que puede tener un sistema de información, procesos, controles internos o herramientas de seguridad que pueden ser explotadas por una amenaza. Pero además se debe realizar un análisis más amplio incluso llegando a nivel de las estructuras de gobierno organizacional, como puede ser la falta de estrategias para gestión de riesgos, comunicación deficiente entre agencias, malas decisiones sobre las prioridades relacionada a la misión institucional. Las vulnerabilidades también pueden estar asociadas con terceros o relaciones externas, como son los suministros de energía eléctrica, proveedores de internet, proveedores de infraestructura, etc.

Una vez definido lo que se debe gestionar como vulnerabilidad, se debe tomar en cuenta que para el Segmento 3 no es obligatorio realizar las pruebas de penetración, pero si es necesario que se realicen auditorías informáticas y para ello se debe tomar en cuenta lo que menciona (CERTIPROF , 2022) respecto de lo que la organización debe realizar dentro de una auditoría interna:

- Planificar, establecer, ejecutar y gestionar uno o más esquemas de auditoría, los cuales deben contemplar la periodicidad, los enfoques, las asignaciones de responsabilidades, los criterios de planificación y la presentación de informes. Estos esquemas deben considerar la relevancia de los procedimientos implicados y los hallazgos de auditorías anteriores.
- Definir los criterios y el alcance de cada auditoría.
- Realizar un proceso de selección de los auditores y llevar seguimientos para garantizar la objetividad e imparcialidad del plan de auditoría.
- Informar a alta Gerencia y Consejo de Administración oportunamente de los resultados de las auditorías.

- Mantener registros documentales como prueba de la ejecución del plan de auditoría y de los resultados obtenidos.

Para llevar un buen control de todo lo que se ha mencionado anteriormente es recomendable apoyarse de un sistema o software de gestión de riesgos, en el mercado tecnológico existen muchos a disposición que cuentan con versiones gratuitas que podemos aprovechar sus bondades y como parte de la mejora continua se deberá optar por adquirir las cuentas Enterprise. Para el caso de estudio se utiliza la herramienta ERAMBA con una cuenta community (versión gratuita). Los pasos de instalación se indica en el Anexo VIII y su funcionalidad será explicada más adelante.

Según lo que se determina en el Anexo 1 de la resolución SEPS 2022-002, la gestión de vulnerabilidades para el segmento 3 debe contemplar Auditorías Informáticas y Plan de Mitigación de hallazgos, a continuación, se detalla cada una:

Auditorías informáticas

Cuando recién se publicó la normativa de seguridad, no se tenía bien definido como se debe dar cumplimiento a este punto, solo se mencionaba que se debe realizar revisiones generales con perspectivas internas y externas. Sin embargo, el 13 de abril de 2023 se expide la resolución SEPS-IGT-IGS-INR-INGINT-INSESF-2023-008, en su artículo 18 menciona que el área de Auditoría Interna debe estar conformada por lo menos por el auditor interno y un auditor especializado en temas informáticos, el cual tiene como función realizar auditorías a los sistemas e infraestructura tecnológica de la institución, con el propósito de verificar que los procesos y sistemas se administren de manera eficiente, generando informes en los cuales se identifiquen exposiciones de riesgo de manera oportuna. (Superintendencia de Economía Popular y Solidaria, 2023)

Innovatien establece los pasos generales de la Auditoría Informática basada en las exigencias de la SEPS los cuales se muestran en la figura 32.

Figura 32. Fases del proceso de Auditoría.

Fuente: Innovatien

Los Auditores informáticos se deben realizar su planificación tomando como prioridad las exigencias de la SEPS, luego se considera la normativa interna y buenas prácticas. La planificación se debe realizar anualmente, identificando actividades de periodicidad anual, semestral y trimestral. Los enfoques principales de evaluación que determina Innovatien son los que se muestran en la figura 33.

Figura 33. Fases del proceso de Auditoría.

Fuente: Innovatien

Plan de mitigación de Hallazgos.

El plan de Mitigación de hallazgos se realiza en base a los riesgos identificados por el auditor informático, quien levanta una matriz la cual es reportada a la SEPS, para ello primero debe poner en conocimiento el informe final al responsable o dueño del riesgo, para verificar que se encuentre conforme con los resultados, o de ser el caso se levante una No Conformidad, la cual deberá ser evaluada nuevamente por el auditor.

Una vez determinado los hallazgos y revisados por el personal responsable, el auditor informático debe presentar los hallazgos los cuales deben contener: condición, criterio con el que se evaluó, causa, efecto y recomendación. Los responsables, con la información proporcionada, deberán establecer las estrategias para dar tratamiento al riesgo, presentar las fechas estimadas de finalización y los entregables que se presentará. Y esta información ya debe ser cargada a la SEPS, para dar el seguimiento correspondiente.

A continuación, se presenta un ejemplo de hallazgo con las condiciones mencionadas y los aspectos que deben ser completados por los responsables:

Hallazgo: Pruebas de restauración de respaldos no planificadas.

- Criterio: La resolución SEPS 0116 en su artículo 14, numeral 5, exige procedimientos de respaldo de información periódicos, acorde a los requerimientos legales y de continuidad de negocio, incluyendo la frecuencia de verificación.
- Causa: Falta de planificación formal y procedimientos documentados para pruebas de restauración.
- Efecto: Riesgo de que la recuperación de servicios no sea oportuna o eficaz, afectando la continuidad del negocio.

- Recomendación: Al Gerente General, disponer al jefe de tecnología establecer un plan semestral de pruebas de restauración documentadas, con resultados reportados al comité de tecnologías de la información y comunicación.

Ahora por parte del responsable de cumplimiento se determina lo siguiente:

- Estrategia: Elaborar un plan semestral de pruebas de restauración que incluya sistemas críticos, ejecutar las restauraciones en entornos controlados, documentar los procedimientos y resultados con evidencias, y presentar un informe consolidado al comité de tecnologías de la información y comunicación.
- Fecha inicio: momento desde el que se pone en marcha la estrategia.
- Fecha fin: tiempo máximo para el cumplimiento de la estrategia, el cual debe estar acorde a la criticidad y priorización del hallazgo.
- Entregable: Informe consolidado del responsable de tecnología sobre los resultados de las pruebas de restauración.

3.2.2.3.Adquisición y desarrollo de software; hardware y servicios

En este procedimiento se establecen los lineamientos y actividades necesarias para la adquisición y desarrollo de software, hardware y servicios tecnológicos, alineándose a la normativa de riesgo operativo, prevención de lavado de activos y manual interno de adquisiciones y contratación de proveedores.

Se define las responsabilidades de los actores que intervienen en el proceso de adquisición:

- Gerencia General: aprobar adquisiciones y contrataciones en base a los niveles de autorización (estos niveles se establecen a criterio de cada institución), en la tabla 5 se presenta un ejemplo de niveles de autorización.
- Comité TIC: validar la alineación estratégica y presupuestaria establecida en el PETIC.
- Jefe de Tecnología: liderar procesos de selección, pruebas y validación técnica.
- Oficial de Seguridad de la Información: evaluar riesgos de seguridad y verificar la existencia de cláusulas de seguridades, confidencialidad y protección de datos.
- Área de Compras: gestionar la contratación conforme a normativa interna y legal.
- Auditor Interno**:** verificar cumplimiento de políticas y controles.

Tabla 5. Niveles de autorización

Nivel de Autorización	**Monto de aprobación**	**Modo de revisión**	**Modalidad de contratación**
Asamblea de Representantes	Superior a $50.000	Administrador de Contratos	Concurso Público
Consejo de Administración	Superior a $10.000	Administrador de Contratos	Concurso Público
Gerente General	Hasta $10.000	-Una sola Proforma hasta los 4 SBU -Tres cotizaciones para montos superiores a 4 SBU	Contratación Directa

Fuente: Cooperativa Chuchuqui

Procedimiento

1. Identificación de Necesidades

- El área solicitante debe generar un ticket con el requerimiento formal (hardware, software o servicio)
- El jefe de tecnología debe evaluar la necesidad y de ser el caso también se puede incluir al OSI para garantizar que el requerimiento se alinee al PETIC o PESI.

2. Evaluación de proveedores y ofertas
    - Solicitar mínimo 3 cotizaciones de forma transparente garantizando la igualdad de condiciones.
    - Verificar el cumplimiento de requisitos establecidos en el manual de contratación de proveedores y normativa de la SEPS.
    - Presentar un informe técnico de selección.
3. Validación y aprobación
    - La propuesta es presentada ante el comité de tecnologías de la información y comunicación, quien analizará y emitirá una recomendación dirigida al responsable de adquisiciones, para continuar con el proceso.
    - El responsable de adquisiciones solicitará la autorización correspondiente a Gerencia General.
    - Se ejecuta la contratación siguiendo la política interna.
4. Desarrollo de software
    - Se debe aplicar una metodología de desarrollo seguro por ejemplo DevSecOps.
    - Ejecutar pruebas de seguridad (pentesting o revisión de código por externos).
5. Adquisición de hardware

- Dependiendo de la criticidad se deberá establecer ambientes controlados para la instalación.
- Verificar que la adquisición cumpla con los requisitos de capacidad y rendimiento.
- Establecer plan de mantenimientos preventivos.

6. Servicios
    - Establecer acuerdos de nivel de servicio (SLA) en beneficio de la institución.
    - Establecer cláusulas de confidencialidad y protección de datos.
    - Exigir al proveedor planes de contingencia y continuidad del negocio.
    - Para los casos que aplique, exigir certificaciones ISO, TIER III e informes de auditorías informáticas periódicas (mínimo una vez al año).

3.2.2.4.Planes de Contingencia tecnológica y continuidad del negocio

El objetivo de este control es definir las actividades necesarias para implementar y probar los planes de contingencia informática y continuidad del negocio, enfocándose en la disponibilidad de los servicios críticos de la cooperativa frente a incidentes tecnológicos determinados.

La SEPS en su norma de riesgo operativo determina que las instituciones deben contar con un sistema de gestión de continuidad del negocio de acuerdo a su tamaño y complejidad, de tal manera que garantice la capacidad de operar sin interrupciones y limitar pérdidas en caso de un incidente, para ello se debe contar con los siguientes requisitos: (Superintendencia de Economía Polpular y Solidaria, 2024)

1. Definición de procesos críticos: En base al mapa de procesos institucional, se debe identificar y valorar los procesos críticos. Esta identificación debe tener respaldo del Comité de Administración Integral de Riesgos (CAIR). También se debe realizar un análisis de riesgos estableciendo medidas de tratamiento que incluyan costos de implementación para su planificación y priorización de proyectos de continuidad del negocio, los cuales se deben considerar dentro del PESI y PETIC. (Superintendencia de Economía Polpular y Solidaria, 2024)
2. Un Comité de Continuidad del Negocio: Este Comité se debe conformar por el administrador de riesgos, jefe de tecnología, jefe de negocios, jefe de crédito, jefe administrativo y gerente general. Este grupo de personas se encargan de la gestión de continuidad del negocio, iniciando por la elaboración de los planes, presentación de presupuestos, monitoreo de la implementación, seguimiento de amenazas que pueden afectar a la continuidad de los servicios, evaluar la efectividad de las medidas adoptadas.
3. Políticas y procedimientos: El documento de continuidad del negocio debe incluir políticas y procedimientos que deben ser actualizadas al menos una vez al año o cuando existan cambios significativos. Deben ser puestas a consideración del CAIR y socializadas a todo el personal involucrado en los procesos críticos.
4. Planes de contingencia y continuidad del negocio: las instituciones del segmento 3 están obligadas a implementar planes de contingencia y continuidad del negocio en los cuales se determine las personas, procesos y tecnología que intervienen, con la finalidad de minimizar pérdidas en caso de materializarse una amenaza que provoque interrupciones en el servicio.

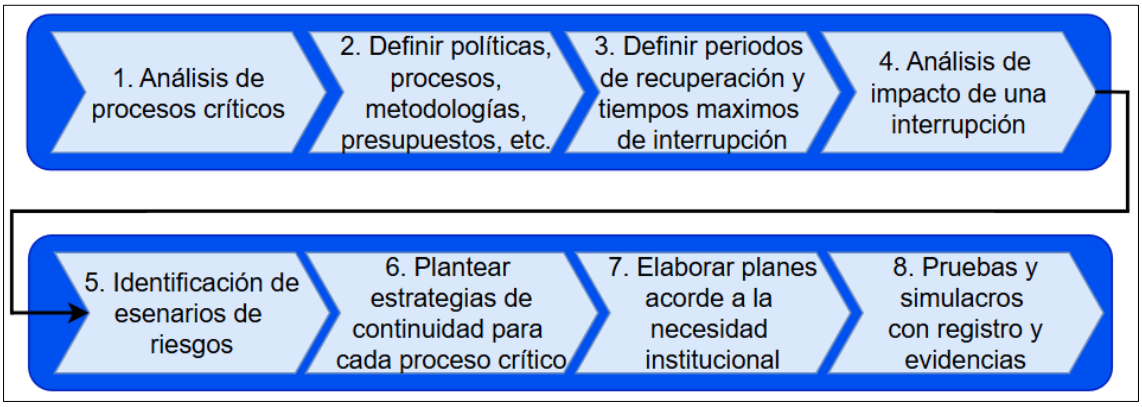
Un buen referente para establecer la continuidad del negocio en el aspecto de tecnologías de la información y ciberseguridad es la ISO/IEC 27031:2025, quien introduce un nuevo concepto IRBC (Preparación de las tecnologías de la información para la continuidad del negocio), y se enfoca en cumplir tres objetivos: (Organización Internacional de Normalización, 2025)

- Objetivo mínimo de continuidad del negocio
- Objetivo de punto de recuperación
- Objetivo de tiempo de recuperación

La ISO/IEC 27031:2025 estable los lineamientos para que la infraestructura tecnológica, arquitectura, procesos y tecnologías relacionadas se encuentren preparadas para responder oportunamente ante un incidente que genere una interrupción intolerable de los servicios tecnológicos o pérdida intolerable de datos. (Organización Internacional de Normalización, 2025)

En base a lo establecido por la SEPS y a la ISO/IEC 27031 se determina el proceso de continuidad de negocio de la figura 34.

Figura 34. Proceso de continuidad del negocio.



Fuente: Propia

3.2.2.5.Cifrado

El procedimiento de cifrado tiene como objetivo proteger la información digital sensible de la cooperativa, para garantizar su confidencialidad e integridad, para el caso de estudio se emplea la herramienta VeraCrypt aplicado a los respaldos de la base de datos del core financiero y al repositorio centralizado, en el cual se maneja información sensible como manuales, informes de auditoría, informes de gestión, entre otros. Cada institución deberá establecer que información requiere ser incluida dentro del proceso de cifrado.

Otro aspecto de cifrado a considerar es la gestión de claves criptográficas como se menciona en el punto 8.4 del Anexo A.1 de la ISO/IEC 27001, para esta gestión también se puede utilizar la herramienta de VeraCrypt solo que en esta ocasión solo se genera un documento de texto plano para el registro de las claves de servicios críticos.

Cifrado con Veracrypt

Para el procedimiento se determina los siguientes responsables:

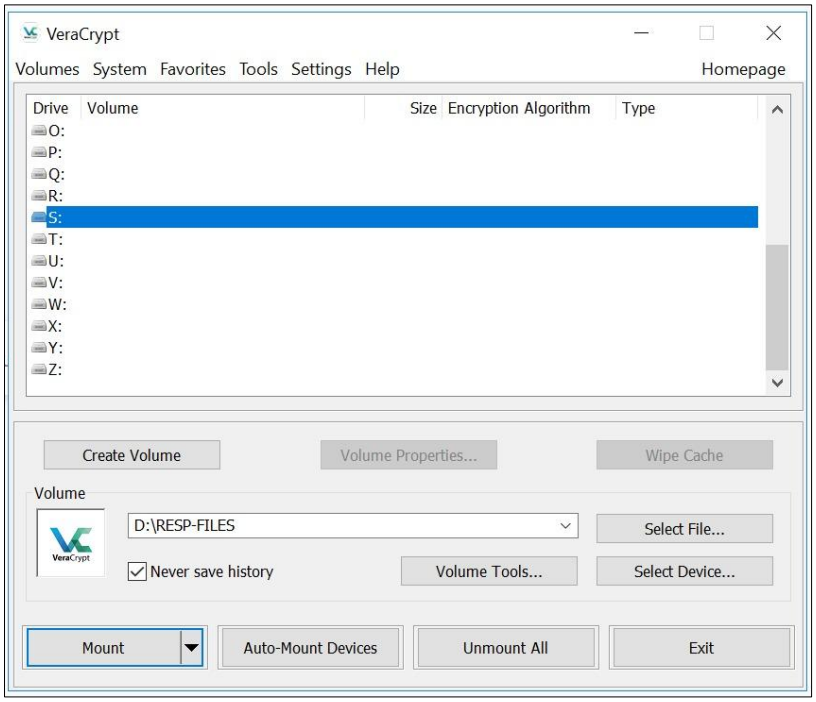
- Oficial de Seguridad de la Información: Se encarga de supervisar la aplicación del procedimiento.
- Jefe de Tecnología: Es el responsable de ejecutar y documentar el proceso de cifrado, se debe incluir dentro de la bitácora de cierre de fin de día.
- Administrador de la base de datos: se encarga de generar los respaldos antes de ser cifrado.
- Auditor Informático: se encarga de verificar la trazabilidad y cumplimiento durante las evaluaciones de auditorías.

Procedimiento

1. Preparación de VeraCrypt

   - Establecer una carpeta independiente tanto para los respaldos del core financiero como para el repositorio centralizado.
   - Establecer y conectar el dispositivo de almacenamiento (disco duro externo con la capacidad suficiente).
   - Verificar que la herramienta VeraCrypt esté instalado y actualizado en el servidor asignado (en la figura 35 se muestra un ejemplo de la herramienta instalada correctamente y lista para ser utilizada).

Figura 35. VeraCrypt.

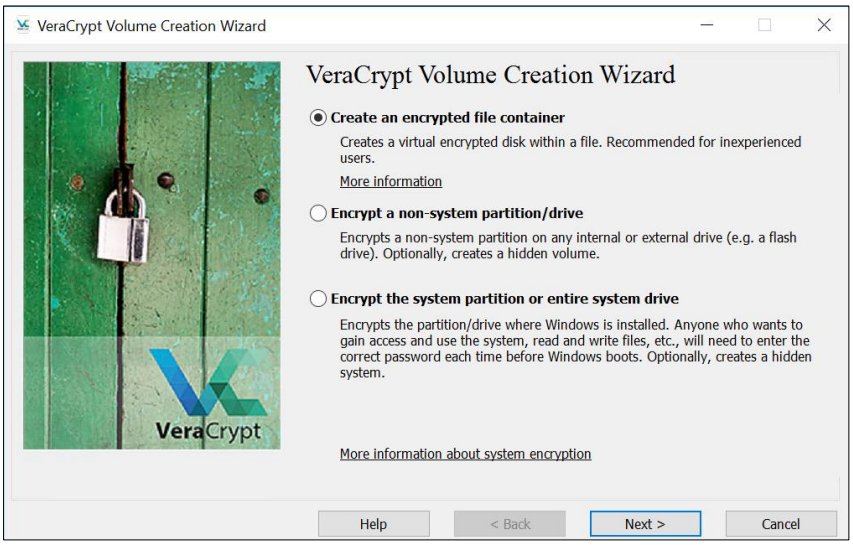


Fuente: Propia

2. Creación de volumen de cifrado

   - Seleccionar la opción de **Create Volume**
   - Seleccionar **Create an encrypted file container** (volumen estándar) como se muestra en la figura 36.

Figura 36. Inicio de creación de volumen encriptado de VeraCrypt.



Fuente: Propia

- Establecer una ubicación y nombre del contenedor, ejemplo: SFWEBCOOP_CH2025.
- Seleccionar algoritmo de cifrado (AES-256 es recomendado).
- Determinar el tamaño del volumen según la necesidad, en el caso de los respaldos del core financiero por su tamaño se ha establecido un tamaño de 2 Tb, y para el repositorio centralizado de 1 Tb.
- Configurar una contraseña la cual debe cumplir con los requisitos mínimos de password seguro (mínimo 12 caracteres, con mayúsculas, minúsculas, números y al menos un caracter especial)
- Seleccionar sistema de archivos (NTFS para archivos mayores a 4GB)
- Finalizar proceso de creación de volumen.

3. Montaje del volumen de cifrado
    - Seleccionar la opción de seleccionar archivo, y buscamos la ubicación del volumen creado.

- Seleccionamos Mount
- Ingresamos la contraseña configurada.
- El volumen aparecerá como una unidad de disco con la asignación de letra que se elija al inicio del montaje.

4. Copia de respaldo
    - Copiar los respaldos generados del core financiero en el volumen montado.
    - Desmontar el volumen encriptado.
5. Seguridad de almacenamiento
    - El disco externo de almacenamiento debe encontrarse en un lugar seguro, de preferencia en el Data Center, para el cual se debe seguir los lineamientos de seguridad correspondientes.
    - El acceso y clave del archivo de cifrado debe ser exclusivo del jefe de tecnología y OSI
6. Registros y evidencias
    - Se debe llevar una bitácora de cifrado, la cual se puede incluir dentro del proceso de fin de día.
    - Se debe presentar evidencias de pruebas de restauración según la planificación establecida por el jefe de tecnología.

3.2.3. Procedimientos

3.2.3.1. Inventario y Clasificación de información

La normativa nos menciona que dentro de lo que respecta al inventario y clasificación de la información se debe establecer tres puntos:

1. Identificación de los tipos de información.
2. Inventario de Activos de Información.

3. Clasificación de los activos de Información.

La clasificación de la información en muchos casos se ha convertido en un elemento obligatorio para la gestión de riesgos de seguridad de la información, sin embargo, muchas organizaciones encuentran muchas dificultades para su implementación, esto radica en que existe poca documentación que presentan un modelo específico para la clasificación de la información, por lo que exige a los profesionales a profundizar en investigación y adaptar a su organización en específico. (Bergquist, Tinet, & Gao, 2022)

En lo que respecta a la clasificación de los activos de información en la tabla 6, podemos observar una referencia de los tipos de activos determinados por (CERTIPROF , 2022).

Tabla 6. Clasificación de los activos de información

Ítem	Código	Clasificación	Tipo
1	IF1	Información Física 1	Documental
2	IF2	Información Física 2	
3	S1	Herramientas para la operación	Software
4	S2	Software Gestión	
5	R1	Red	Infraestructura
6	SL	Servidor Local	
7	EC	Equipo de computo	Equipos
8	AL	Almacenamiento	Almacenamiento
9	CN	Conocimiento del Negocio	Intangible y RH

Fuente: (CERTIPROF , 2022)

El inventario y clasificación aplica a todos los activos de información (físicos y digitales) que circulan o se almacenan en la entidad financiera:

- Información financiera. (Estados financieros, balances, reportes contables, registro de créditos, cuentas por cobrar/pagar)

Comprende todos los registros y documentos que reflejan la situación económica, financiera y contable de la entidad. Esta información debe estar disponible, integra y resguardada para garantizar la transparencia y confiabilidad de los reportes regulatorios.

- Información personal. (clientes, socios, empleados, proveedores)

  Datos que identifican de manera única de los clientes, socios y empleados, así como información sensible relacionada con la actividad financiera o laboral. Es obligatorio garantizar la confidencialidad y la protección de datos personales, evitando accesos indebidos o divulgación no autorizada.

- Información operativa. (Procedimientos internos, manuales de operación, reportes de gestión, cronogramas, actas de reuniones operativas)

  La información relacionada con los procesos, actividades y operaciones diarias de la entidad financiera que permiten el cumplimiento de la misión institucional debe mantenerse actualizada, integra y disponible para asegurar la continuidad operativa y el cumplimiento de los objetivos institucionales.

- Información técnica y de sistemas. (Configuraciones de red, accesos a sistemas, respaldos de bases de datos, manuales técnicos, reportes de monitoreo)

  La información relacionada con los sistemas tecnológicos, infraestructura de TI y soporte técnico que respalda las operaciones de la entidad financiera debe ser protegida respaldando la disponibilidad, integridad y resiliencia de los sistemas críticos, incluyendo controles de acceso y planes de contingencia.

- Documentos legales y contractuales. (Contratos, actas de directorio, convenios, pólizas, escrituras notariales)

La documentación que contemplan requisitos legales y contractuales de la operación financiera debe ser adecuadamente custodiada, autentificada, y mantener un acceso restringido únicamente a personal autorizado.

- Comunicaciones oficiales. (Circulares, comunicados oficiales, boletines internos, notificaciones a la SEPS, publicaciones en la web institucional) Los documentos y medios de comunicación emitidos oficialmente por la entidad financiera hacia los socios, clientes, entes de control y público en general deben ser veraces, oportunos y difundidas por canales autorizados, en línea con las políticas de transparencia y comunicación institucional.

Roles y responsabilidades

La correcta implementación y mantenimiento del inventario y clasificación de la información depende de la participación coordinada de varios roles dentro de la entidad financiera. A continuación, se describe sus responsabilidades especificas en concordancia con la normativa de la SEPS vigente en materia riesgo operativo, riesgo legal y gobierno de tecnologías de la información.

- Oficial de seguridad de la información.
    - Definir y mantener la política de clasificación de la información, asegurando la alineación con las mejores prácticas ISO 27001, ISO 27002 y normativa SEPS.
    - Validar los criterios de confidencialidad, integridad y disponibilidad aplicados a cada activo.
    - Supervisar la correcta aplicación de los niveles de sensibilidad.
    - Verificar que la información crítica este protegido mediante controles técnicos.

  - Coordinar revisiones periódicas de seguridad sobre el inventario.
  - Notificar el comité de riesgos cualquier vulneración o incumplimiento.
- Jefe de TI.
  - Liderar la ejecución del procedimiento de inventario y clasificación de la información.
  - Garantizar que los activos tecnológicos y de información estén debidamente registrados, protegidos y actualizados.
  - Coordinar con cada responsable de área para consolidar la información inventariada.
  - Implementar herramientas y sistemas que permitan registrar y mantener actualizado el inventario.
  - Asegurar el cumplimiento de las políticas de seguridad definidas en la Norma SEPS 0116 y en el PETI.
  - Reportar hallazgos y actualizaciones al comité de riesgos y seguridad.
- Responsable de área.
  - Identificar los activos de información generados, procesados o custodiados por su área.
  - Proporcionar al Jefe de TI y al Oficial de Seguridad la información necesaria para inventariar y clasificar los activos.
  - Asegurar que la información bajo su responsabilidad se almacene en medios autorizados.
  - Reportar cualquier cambio, creación o eliminación de activos de información.

    - Cumplir con las políticas de seguridad y clasificación aprobadas por el Comité de Riesgos.
- Comité de riesgos y seguridad.
    - Revisar y validar la clasificación de la información propuesta por el jefe de TI y el Oficial de Seguridad.
    - Aprobar los niveles de criticidad asignados a cada activo.
    - Definir criterios de tolerancia al riesgo relacionados con la disponibilidad, integridad y confidencialidad de la información.
    - Emitir recomendaciones a la Gerencia General sobre medidas de mitigación y controles adicionales.
    - Supervisar que la gestión de información esté alineada con la estrategia de la entidad y con el marco regulatorio vigente.
- Gerencia general.
    - Aprobar formalmente el inventario de activos de información consolidado.
    - Asegurar la asignación de recursos (financieros, humanos y tecnológicos) para mantener actualizado el inventario.
    - Promover el cumplimiento normativo en materia de seguridad de la información y gestión de riesgos.
    - Respaldar las decisiones del Comité de Riesgos y garantizar su ejecución en la organización.
    - Reportar a la SEPS el cumplimiento de las disposiciones normativas en caso de auditorías o requerimientos.

A continuación, en la tabla 7 se detalla una caracterización del proceso de inventario y clasificación propuesto:

Tabla 7. Caracterización del proceso de Inventario y Clasificación de la información

Campo	Detalle
Código	PR-SI-01
Nombre	Inventario y Clasificación de la Información
Propietario	Oficial de Seguridad de la Información (OSI)
Participantes	Responsables de Área, Seguridad de la Información, Riesgos, Tecnología, Auditoría Informática
Objetivo	Identificar, inventariar y clasificar todos los activos de información para aplicar controles de protección requeridos en base a su criticidad y sensibilidad, alineado a las normativas de la SEPS
Alcance	Toda información (física y digital), sistemas, base de datos, repositorios y documentación en la cooperativa.
Entradas	Listado de información proporcionada por cada área, registros de sistemas (GLPI o ERAMBA), contratos, SLAs, matrices de procesos.
Salidas	Inventario consolidado, Matriz de Clasificación, Matriz de Criticidad.
Clientes del proceso	Comité de Riesgos, Seguridad de la información, Gerencia General, Auditoría Informática, Áreas operativas.
Riesgos del proceso	Omisiones o duplicados de activos de información, clasificación errónea, información sensible sin custodia.
Controles del proceso	Muestreo de calidad, validación por propietarios de la información, conciliación con GLPI o ERAMBA, revisión por el responsable de Riesgos
Recursos y Herramientas	GLPI, ERAMBA o Excel, control de versiones.
Normativa	Norma de Control SEPS (riesgo operativo y Seguridad de la información), políticas internas de seguridad
Frecuencia	Inventario: anual o semestral si se considera que existen cambios significativos
Criterios de éxito	100% activos críticos inventariados y clasificados, 0 activos sin dueño y evidencias verificables
Vinculados	Gestión de Accesos, Gestión de Cambios, Continuidad DRP, Gestión de Proveedores

Fuente Propia

3.2.3.2. Gestión de riesgos

Para la Gestión de riegos nos basaremos en la metodología de la MAGERIT v3 orientándonos en un análisis cualitativo, esto en cuanto se va a considerar el valor de los

activos desde la importancia que estos tienen para institución, ya que existen activos que tal vez por el paso del tiempo su valor cuantitativo se degrada, pero a pesar de llegar a una depreciación total, el activo puede seguir teniendo información que le agrega un valor de importancia a la institución.

Lo primero que se realiza después de tener un levantamiento de los activos como se presentó en el punto 4.2.5 es determinar los criterios de valoración como indica en la siguiente tabla 8.

Tabla 8. Criterios de valoración

VALOR	CRITERIO	
MA: Muy Alto	daño muy grave	5
A: Alto	daño grave	4
M: Medio	daño importante	3
B: Bajo	daño menor	2
MB: Muy Bajo	irrelevante	1

Fuente: Autor

A continuación, se asigna un valor cualitativo al activo, siempre poniendo en suposición de que pasaría si el activo se pierde, en que escala afecta a la continuidad del negocio, reputación o consecuencias económicas, todo esto en base a los cinco principios o pilares de la Seguridad de la Información que nos presenta MAGERIT que son: confidencialidad (C), integridad (I), disponibilidad (D), autenticidad (A) y trazabilidad (T).

En los criterios de valoración del activo existen varios factores que se deben analizar, por ejemplo:

- Los costos de adquisición incluyendo costos por instalación.
- Los costos que puede generar para su recuperación, en el caso de software podría tratarse solo de costos de mano de obra.
- Pérdida de ingresos ocasionados por la indisponibilidad del servicio.

- Sanciones por incumplimiento ante los entes reguladores, leyes o contratos.
- Cascada de daños o afectaciones a otros activos o servicios.
- Daños a personas, ya sea socios, clientes o funcionarios; etc.

Con lo mencionado anteriormente, se presenta unos ejemplos del cálculo del valor del activo en la tabla 9.

Tabla 9. Cálculo del valor del activo

ACTIVO	[C]	[I]	[D]	[A]	[T]	VALOR DEL ACTIVO
[SW] CORE FINANCIERO WEBCOOP	MA	MA	MA	MA	MA	MA
[email] SERVIDOR DE CORREO (ZIMBRA)	MA	MA	M	MA	A	A
[www] INTRANET Y PAGINA WEB	M	MA	M	MA	M	A
[D] BASES DE DATOS	MA	MA	MA	MA	MA	MA
[SW] ACTIVE DIRECTORY	MA	MA	MA	MA	MA	MA
[HW] SERVIDOR DE VIRTUALIZACIÓN (VMware® vSphere)	MA	MA	MA	MA	MA	MA
[SW] CORE FINANCIERO SADFIN	MA	MA	M	MA	M	A
[HW] SERVIDOR DE ALMACENAMIENTO	MA	MA	MA	MA	MA	MA

Fuente: Autor

Una vez que se ha establecido el valor del activo lo siguiente será determinar que amenazas pueden afectar o atentar contra nuestros activos, para este caso se considera las amenazas establecidas por MAGERIT y se analiza si son aplicables o no. Hay amenazas que tienen una probabilidad muy baja de ocurrencia, pero esto no quiere decir que podemos obviar o poner un riesgo 0, de igual manera debe constar dentro de un análisis completo. En la tabla 10 se presentan ejemplos de amenazas para activos, dependiendo de su tipo y como estas afectan a los pilares principales de seguridad de la información causando una degradación del activo.

Tabla 10. Cálculo de la degradación de los activos

ACTIVO	AMENAZA	[C]	[I]	[D]	[A]	[T]	DEGRADACIÓN
	[I.5] Avería de origen físico o lógico	B	A	MA	M	A	A
	[E.2] Errores del administrador	MA	MA	MA	M	A	A

[SW] CORE FINANCIERO WEBCOOP	[E.21] Errores de mantenimiento / actualización de programas (software)	MB	M	MA	B	B	M
[email] SERVIDOR DE CORREO (ZIMBRA)	[A.11] Acceso no autorizado	MA	MA	A	A	A	A
	[A.9] [Re-]encaminamiento de mensajes	MA	MA	MA	M	M	A
	[A.8] Difusión de software dañino	MA	B	B	B	M	M
[www] INTRANET Y PAGINA WEB	[E.20] Vulnerabilidades de los programas (software)	MA	MA	M	A	A	A
	[E.1] Errores de los usuarios	MA	B	B	B	M	M
	[A.18] Destrucción de información	MB	M	MA	MB	M	M
[D] BASES DE DATOS	[A.11] Acceso no autorizado	MA	MA	A	A	A	A
	[E.19] Fugas de información	MA	B	B	M	M	M
	[A.15] Modificación deliberada de la información	B	MA	A	M	M	M
	[A.4] Manipulación de la configuración	B	MA	MA	MA	M	A
[SW] ACTIVE DIRECTORY	[E.20] Vulnerabilidades de los programas (software)	MA	MA	MA	B	B	A
	[I.8] Fallo de servicios de comunicaciones	MB	MB	MA	MB	M	B

Fuente: Autor

Una vez obtenido la valoración de la degradación del activo ya se puede calcular el impacto que la amenaza ocasiona sobre el activo en caso de que esta llegase a ocurrir. En la tabla 11 se indica ejemplos del cálculo del impacto en base al valor del activo afectado por la degradación que causa la amenaza.

Tabla 11. Cálculo del Impacto

ACTIVO	AMENAZA	VALOR DE ACTIVO	DEGRADACIÓN	IMPACTO
[SW] CORE FINANCIERO WEBCOOP	[I.5] Avería de origen físico o lógico	MA	A	MA
	[E.2] Errores del administrador		A	MA
	[E.21] Errores de mantenimiento / actualización de programas (software)		M	A
[email] SERVIDOR DE CORREO (ZIMBRA)	[A.11] Acceso no autorizado	A	A	A
	[A.9] [Re-]encaminamiento de mensajes		A	A
	[A.8] Difusión de software dañino		M	A
[www] INTRANET Y PAGINA WEB	[E.20] Vulnerabilidades de los programas (software)	A	A	A
	[E.1] Errores de los usuarios		M	A
	[A.18] Destrucción de información		M	A
[D] BASES DE DATOS	[A.11] Acceso no autorizado	MA	A	MA
	[E.19] Fugas de información		M	A

	[A.15] Modificación deliberada de la información		M	A
	[A.4] Manipulación de la configuración		A	MA
[SW] ACTIVE DIRECTORY	[E.20] Vulnerabilidades de los programas (software)	MA	A	MA
	[I.8] Fallo de servicios de comunicaciones		B	M

Fuente: Autor

A continuación, una vez obtenido el impacto que la amenaza ocasiona en el activo podemos calcular el riesgo, determinando un nivel de probabilidad de ocurrencia para cada amenaza, tal y como se muestra en los ejemplos de la tabla 12.

Tabla 12. Cálculo de Riesgo

ACTIVO	AMENAZA	IMPACTO	PROBABILIDAD	RIESGO
[SW] CORE FINANCIERO WEBCOOP	[I.5] Avería de origen físico o lógico	MA	M	A
	[E.2] Errores del administrador	MA	M	A
	[E.21] Errores de mantenimiento / actualización de programas (software)	A	M	A
[email] SERVIDOR DE CORREO (ZIMBRA)	[A.11] Acceso no autorizado	A	M	A
	[A.9] [Re-]encaminamiento de mensajes	A	MB	M
	[A.8] Difusión de software dañino	A	M	A
[www] INTRANET Y PAGINA WEB	[E.20] Vulnerabilidades de los programas (software)	A	B	M
	[E.1] Errores de los usuarios	A	MB	M
	[A.18] Destrucción de información	A	MB	M
[D] BASES DE DATOS	[A.11] Acceso no autorizado	MA	B	A
	[E.19] Fugas de información	A	M	A
	[A.15] Modificación deliberada de la información	A	B	M
[SW] ACTIVE DIRECTORY	[A.4] Manipulación de la configuración	MA	B	M
	[E.20] Vulnerabilidades de los programas (software)	MA	M	A
	[I.8] Fallo de servicios de comunicaciones	A	M	A

Fuente: Autor

Una vez obtenida nuestra matriz de riesgo se debe establecer qué tipo de tratamiento se va a asignar a cada riesgo identificado, entre los tipos de tratamiento tenemos:

- Aceptar
- Mitigar
- Reducir
- Transferir

Aceptar. - La institución debe determinar las razones de porque decide aceptar el riesgo y no hacer nada frente a esa amenaza. Una de las razones puede relacionarse al nivel o valoración de dicho riesgo, en el caso de que se encuentre en bajo y muy bajo, pero también puede existir casos que estén en nivel medio en cual se puede analizar la medida de afectación económica en comparación a los costos que puede llegar a tener la implementación de los controles de seguridad específicos para esa amenaza.

Por ejemplo, para la amenaza de con riesgo bajo puede ser una inundación de las instalaciones, este es un tema poco probable que suceda además de tener factores favorables como la ubicación de la institución e históricos que garantizan que la zona no es propensa a tener inundaciones, por lo tanto, el riego es aceptable.

Por otro lado, una amenaza con riesgo medio es la difusión de software maligno por correo electrónico, pero considerando que se ha realizado capacitaciones al personal sobre esta amenaza, la alta gerencia puede aceptar el riesgo, asumiendo que todo el personal se encuentra consciente de este tema, ya que los costos de implementación para un software de detección de malware para correo electrónico son muy elevados.

Mitigar. - Para todos los riegos desde nivel bajo hasta muy alto se debe buscar la manera de implementar controles de seguridad que permitan mitigar la afectación de las amenazas. El objetivo es bloquear casi en su totalidad la probabilidad de que la amenaza se active, no podemos decir que se va a eliminar completamente, ya que el riesgo cero no debe existir.

Por ejemplo, la amenaza de corte de suministro eléctrico en el caso de no existir un control de seguridad, su riesgo puede ser alto, pero se puede mitigar si yo implemento medidas de seguridad que garanticen una redundancia de energía como tener UPS tanto para servidores como para los usuarios finales, además de contar con una planta de energía eléctrica que se active de forma automática, en caso de que la red eléctrica pública haya fallado. En este caso el riego bajaría de ser alto a ser bajo.

Reducir. - En este caso los riesgos simplemente bajarían su valoración, pero estos se mantendrían entre un valor medio y alto, a pesar de haber implementado algún control de seguridad, por lo que se debe dar un seguimiento continuo.

Por ejemplo, la amenaza de robo o intrusión a las instalaciones considerando que la ubicación de la institución se encuentra en una zona de alto riego, donde las estadísticas de delincuencia organizada son muy altas. Si yo implemento controles de seguridad, como contar con seguridad privada las 24h, tener un sistema de video vigilancia enlazado a una central y un sistema robusto de alarmas; el riesgo bajaría de ser muy alto a medio, simplemente por el hecho de que la ubicación es una zona muy peligrosa, en ese caso simplemente se está reduciendo el riesgo.

Transferir. - Este tipo de tratamiento consiste en ceder el riesgo a una tercera parte, que puede ser una empresa contratista que brinde un servicio directo a la institución para lo cual se debe tener un contrato con las cláusulas bien definidas, donde se identifique las posibles amenazas y la responsabilidad de la empresa en caso de una incidencia.

Por ejemplo, uno de los servicios más comunes que las instituciones financieras en el cual transfieren los riesgos a otra empresa es el transporte de valores, si la institución lo hace por sus propios medios, el riesgo de un asalto es muy alto, pero si yo

transfiero ese riesgo a un tercero, debo volver a analizar su valoración tomando en cuenta las medidas de seguridad que la tercera parte expone en el contrato, y en el caso de que no se cumpla con lo estipulado ya será netamente responsabilidad de la empresa contratada.

Ahora bien, con lo explicado anteriormente será indicar que tipo de tratamiento se dará a cada riesgo y que salvaguarda se implementará como control de seguridad para bajar o mantener el criterio de valoración, tal y como se indica en la tabla 13.

Tabla 13. Salvaguardas

ACTIVO	AMENAZA	TRATAMIENTO	SALVAGUARDA
[SW] CORE FINANCIERO WEBCOOP	[I.5] Avería de origen físico o lógico	M	Mantener respaldos de la base de datos y mantener en stock elementos indispensables del servidor
	[E.2] Errores del administrador	M	Establecer un sitio de pruebas para probar posibles cambios antes de pasar al sitio de producción
	[E.21] Errores de mantenimiento / actualización de programas (software)	T	Contar con un contrato claro en el que especifique que el proveedor se responsabiliza de mantener actualizado y parchado el sistema financiero.
[email] SERVIDOR DE CORREO (ZIMBRA)	[A.11] Acceso no autorizado	M	Establecer políticas para el uso responsable de las contraseñas de acceso
	[A.9] [Re-]encaminamiento de mensajes	T	Solicitar al proveedor de comunicaciones que garantice un canal de comunicación seguro
	[A.8] Difusión de software dañino	R	Crear campañas de sensibilización sobre temas de difusión de malware a través de correo electrónico
[www] INTRANET Y PAGINA WEB	[E.20] Vulnerabilidades de los programas (software)	M	Contar con una política de actualización de software
	[E.1] Errores de los usuarios	R	Difundir videos explicativos de cómo utilizar la página web
	[A.18] Destrucción de información	M	Mantener un respaldo de la página web

[D] BASES DE DATOS	[A.11] Acceso no autorizado	M	Establecer una política para el control de usuarios y roles
	[E.19] Fugas de información	R	Capacitar al personal sobre ética profesional y mantener un acuerdo de confidencialidad
	[A.15] Modificación deliberada de la información	M	Mantener respaldos periódicos de la base de datos.
[SW] ACTIVE DIRECTORY	[A.4] Manipulación de la configuración	M	Establecer una política para la gestión de cambios
	[E.20] Vulnerabilidades de los programas (software)	M	Mantener el software actualizado y parchado
	[I.8] Fallo de servicios de comunicaciones	M	Contar con redundancia de enlaces de internet

Fuente: Autor

Determinar las salvaguardas Actuales.

Se debe establecer niveles en los cuales se va a evaluar la efectividad de las salvaguardas midiendo en un factor de 0 a 100% conforme se muestra en la tabla 14.

Tabla 14. Eficacia de la protección

Factor	Nivel	Significado
0%	L0	Inexistente
-	L1	Inicial
-	L2	Reproducible pero incompleto
-	L3	Proceso definido
-	L4	Gestionado y medible
100%	L5	Optimizado

Fuente: Autor

En base al porcentaje de eficacia estimado para cada salvaguarda completamos la tabla 15.

Tabla 15. Eficacia de las salvaguardas

ACTIVO	AMENAZA	SALVAGUARDA	EFICACIA
[SW] CORE FINANCIERO WEBCOOP	[I.5] Avería de origen físico o lógico	Mantener respaldos de la base de datos y mantener en stock elementos indispensables del servidor	L5

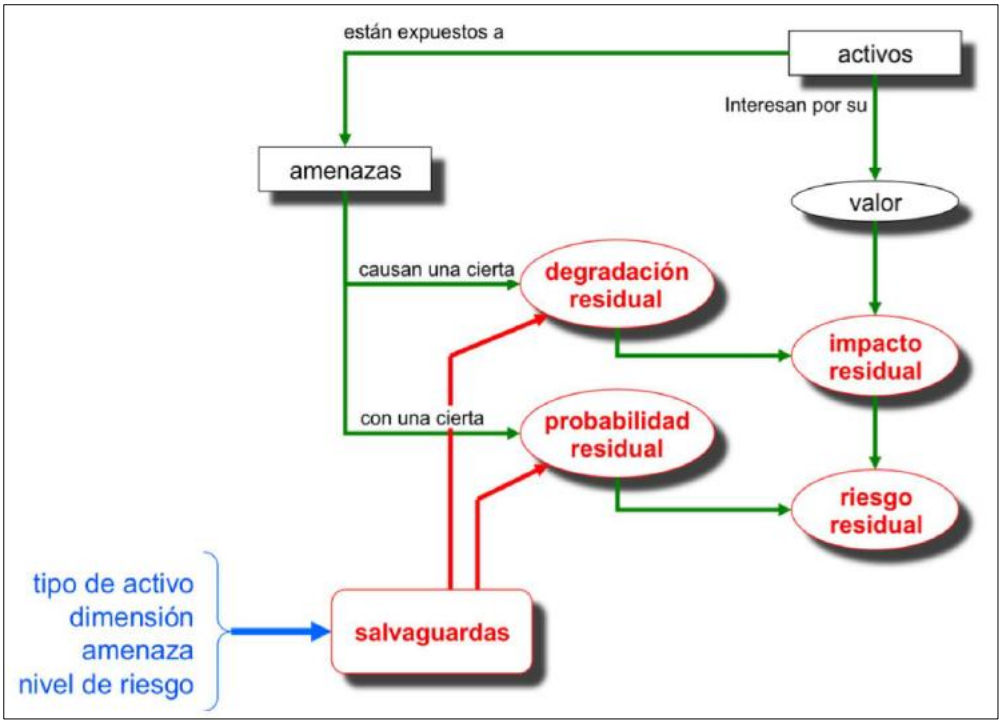
	[E.2] Errores del administrador	Establecer un sitio de pruebas para probar posibles cambios antes de pasar al sitio de producción	L5
	[E.21] Errores de mantenimiento / actualización de programas (software)	Contar con un contrato claro en el que especifique que el proveedor se responsabiliza de mantener actualizado y parchado el sistema financiero.	L4
	[A.11] Acceso no autorizado	Establecer políticas para el uso responsable de las contraseñas de acceso	L5
[email] SERVIDOR DE CORREO (ZIMBRA)	[A.9] [Re-]encaminamiento de mensajes	Solicitar al proveedor de comunicaciones que garantice un canal de comunicación seguro	L3
	[A.8] Difusión de software dañino	Crear campañas de sensibilización sobre temas de difusión de malware a través de correo electrónico	L3
	[E.20] Vulnerabilidades de los programas (software)	Contar con una política de actualización de software	L3
[www] INTRANET Y PAGINA WEB	[E.1] Errores de los usuarios	Difundir videos explicativos de cómo utilizar la página web	L3
	[A.18] Destrucción de información	Mantener un respaldo de la página web	L5
	[A.11] Acceso no autorizado	Establecer una política para el control de usuarios y roles	L4
[D] BASES DE DATOS	[E.19] Fugas de información	Capacitar al personal sobre ética profesional y mantener un acuerdo de confidencialidad	L4
	[A.15] Modificación deliberada de la información	Mantener respaldos periódicos de la base de datos.	L5
	[A.4] Manipulación de la configuración	Establecer una política para la gestión de cambios	L4
[SW] ACTIVE DIRECTORY	[E.20] Vulnerabilidades de los programas (software)	Mantener el software actualizado y parchado	L4
	[I.8] Fallo de servicios de comunicaciones	Contar con redundancia de enlaces de internet	L5

Fuente: Autor

Según la metodología MAGERIT v3, el riesgo residual se obtiene una vez evaluada la eficacia de las salvaguardas o controles implementados sobre los activos

analizados. Este cálculo parte del riesgo inherente, es decir, el nivel de riesgo existente antes de aplicar medidas de protección y se ajusta considerando el grado en que las salvaguardas reducen la probabilidad o el impacto de las amenazas. En la figura 37 se muestra los elementos de análisis del riesgo residual determinado por MAGERIT v3 y en la tabla 16 se muestra ejemplos de la aplicación para determinar el impacto residual.

Figura 37. Elementos de análisis de riesgo residual



Fuente: MAGERIT v3

Tabla 16. Determinación del Impacto Residual

ACTIVO	AMENAZA	SALVAGUARDA	VALOR DE ACTIVO	DEGRADACIÓN	IMPACTO
[SW] CORE FINANCIERO WEBCOOP	[I.5] Avería de origen físico o lógico	Mantener respaldos de la base de datos y mantener en stock elementos indispensables del servidor	MA	Antes: A Ahora: M	Antes: MA Ahora: A
	[E.2] Errores del administrador	Establecer un sitio de pruebas para probar posibles cambios antes de pasar al sitio de producción		Antes: A Ahora: B	Antes: MA Ahora: M

[email] SERVIDOR DE CORREO (ZIMBRA)	[E.21] Errores de mantenimiento / actualización de programas (software)	Contar con un contrato claro en el que especifique que el proveedor se responsabiliza de mantener actualizado y parchado el sistema financiero.	A	Antes: M Ahora: M	Antes: A Ahora: A
	[A.11] Acceso no autorizado	Establecer políticas para el uso responsable de las contraseñas de acceso		Antes: A Ahora: B	Antes: A Ahora: M
	[A.9] [Re-]encaminamiento de mensajes	Solicitar al proveedor de comunicaciones que garantice un canal de comunicación seguro		Antes: A Ahora: A	Antes: A Ahora: A
	[A.8] Difusión de software dañino	Crear campañas de sensibilización sobre temas de difusión de malware a través de correo electrónico		Antes: M Ahora: B	Antes: A Ahora: M
[www] INTRANET Y PAGINA WEB	[E.20] Vulnerabilidades de los programas (software)	Contar con una política de actualización de software	A	Antes: A Ahora: M	Antes: A Ahora: M
	[E.1] Errores de los usuarios	Difundir videos explicativos de como utilizar la pagina web		Antes: M Ahora: M	Antes: A Ahora: A
	[A.18] Destrucción de información	Mantener un respaldo de la página web		Antes: M Ahora: B	Antes: A Ahora: M
[D] BASES DE DATOS	[A.11] Acceso no autorizado	Establecer una politica para el control de usuarios y roles	MA	Antes: A Ahora: M	Antes: MA Ahora: A
	[E.19] Fugas de información	Capacitar al personal sobre ética profesional y mantener un acuerdo de confidencialidad		Antes: M Ahora: M	Antes: A Ahora: A
	[A.15] Modificación deliberada de la información	Mantener respaldos periódicos de la base de datos.		Antes: M Ahora: B	Antes: A Ahora: M
	[A.4] Manipulación de la configuración	Establecer una política para la gestión de cambios		Antes: A Ahora: M	Antes: MA Ahora: A
[SW] ACTIVE DIRECTORY	[E.20] Vulnerabilidades de los programas (software)	Mantener el software actualizado y parchado	MA	Antes: A Ahora: A	Antes: MA Ahora: MA
	[I.8] Fallo de servicios de comunicaciones	Contar con redundancia de enlaces de internet		Antes: B Ahora: B	Antes: M Ahora: M

Fuente: Autor

Estimar el Riesgo Residual

El cálculo del riesgo residual en la metodología MAGERIT v3 consiste en repetir la estimación del riesgo inicial considerando los cambios generados por la

aplicación de salvaguardas. Dado que los activos y sus dependencias permanecen iguales, lo que varía es la magnitud de la degradación y la probabilidad de ocurrencia de las amenazas, las cuales se recalculan para obtener el impacto y la probabilidad residuales.

La magnitud de la degradación residual se toma como base para el impacto, mientras que la probabilidad residual se ajusta en función de la eficacia de las salvaguardas, entendida como la diferencia entre una eficacia perfecta y la eficacia real alcanzada. De esta forma, el riesgo residual refleja el nivel de exposición que permanece tras aplicar las medidas de seguridad. En la tabla 17 se muestra ejemplos del cálculo del riesgo residual.

Tabla 17. Determinación del riesgo residual

ACTIVO	AMENAZA	SALVAGUARDA	IMPACTO	PROBABILIDAD	RIESGO
[SW] CORE FINANCIERO WEBCOOP	[I.5] Avería de origen físico o lógico	Mantener respaldos de la base de datos y mantener en stock elementos indispensables del servidor	Antes: MA Ahora: A	M	Antes: A Ahora: A
	[E.2] Errores del administrador	Establecer un sitio de pruebas para probar posibles cambios antes de pasar al sitio de producción	Antes: MA Ahora: M	M	Antes: A Ahora: M
	[E.21] Errores de mantenimiento / actualización de programas (software)	Contar con un contrato claro en el que especifique que el proveedor se responsabiliza de mantener actualizado y parchado el sistema financiero.	Antes: A Ahora: A	M	Antes: A Antes: A
[email] SERVIDOR DE CORREO (ZIMBRA)	[A.11] Acceso no autorizado	Establecer políticas para el uso responsable de las contraseñas de acceso	Antes: A Ahora: M	M	Antes: A Ahora: M
	[A.9] [Re-]encaminamiento de mensajes	Solicitar al proveedor de comunicaciones que garantice un canal de comunicación seguro	Antes: A Ahora: A	MB	Antes: M Ahora: M

	[A.8] Difusión de software dañino	Crear campañas de sensibilización sobre temas de difusión de malware a través de correo electrónico	Antes: A Ahora: M	M	Antes: A Ahora: M
[www] INTRANET Y PAGINA WEB	[E.20] Vulnerabilidades de los programas (software)	Contar con una política de actualización de software	Antes: A Ahora: M	B	Antes: M Ahora: M
	[E.1] Errores de los usuarios	Difundir videos explicativos de cómo utilizar la página web	Antes: A Ahora: A	MB	Antes: M Ahora: M
[D] BASES DE DATOS	[A.18] Destrucción de información	Mantener un respaldo de la página web	Antes: A Ahora: M	MB	Antes: M Ahora: B
	[A.11] Acceso no autorizado	Establecer una política para el control de usuarios y roles	Antes: MA Ahora: A	B	Antes: A Ahora: M
	[E.19] Fugas de información	Capacitar al personal sobre ética profesional y mantener un acuerdo de confidencialidad	Antes: A Ahora: A	M	Antes: A Ahora: A
	[A.15] Modificación deliberada de la información	Mantener respaldos periódicos de la base de datos.	Antes: A Ahora: M	B	Antes: M Ahora: B
[SW] ACTIVE DIRECTORY	[A.4] Manipulación de la configuración	Establecer una política para la gestión de cambios	Antes: MA Ahora: A	B	Antes: M Ahora: M
	[E.20] Vulnerabilidades de los programas (software)	Mantener el software actualizado y parchado	Antes: MA Ahora: MA	M	Antes: A Ahora: A
	[I.8] Fallo de servicios de comunicaciones	Contar con redundancia de enlaces de internet	Antes: M Ahora: M	M	Antes: A Ahora: M

Fuente: Autor

3.2.3.3. Herramienta de Gestión de riesgos ERAMBA

ERAMBA es un software GRC (Governance, Risk, and Compliance), gratuito con una eficacia probada por varios expertos que forman parte de su comunidad, su objetivo es ayudar a numerosas organizaciones de todo el mundo a certificar estándares

relacionados a la gestión de riesgo en seguridad de la información, crear modelos de riesgo, gestión de incidentes y dar seguimiento a proyectos tecnológicos. (Ri, 2025)

En la figura 38 se puede observar la aceptación de la comunidad en base a su interacción en descargas e instalaciones.

Figura 38. Interacciones de la comunidad con la herramienta ERAMBA

Fuente: www.eramba.org

Contar con una herramienta de gestión nos ayuda a dar un seguimiento más adecuada a los procesos, procedimientos y tareas de tecnología, aspectos que por lo general se tiene en hojas de cálculo o documentos sueltos, pero ERAMBA permite su actualización y dar seguimiento adecuado a través de su interfaz.

Esta herramienta permite gestionar los riegos asociados a las unidades de negocio de una organización en los siguientes aspectos: (Ri, 2025)

- Creación y mantenimiento de un Registro de Riesgos
- Propiedad y tratamiento del riesgo de seguimiento
- Marcos de riesgo compatibles con ISO, etc.

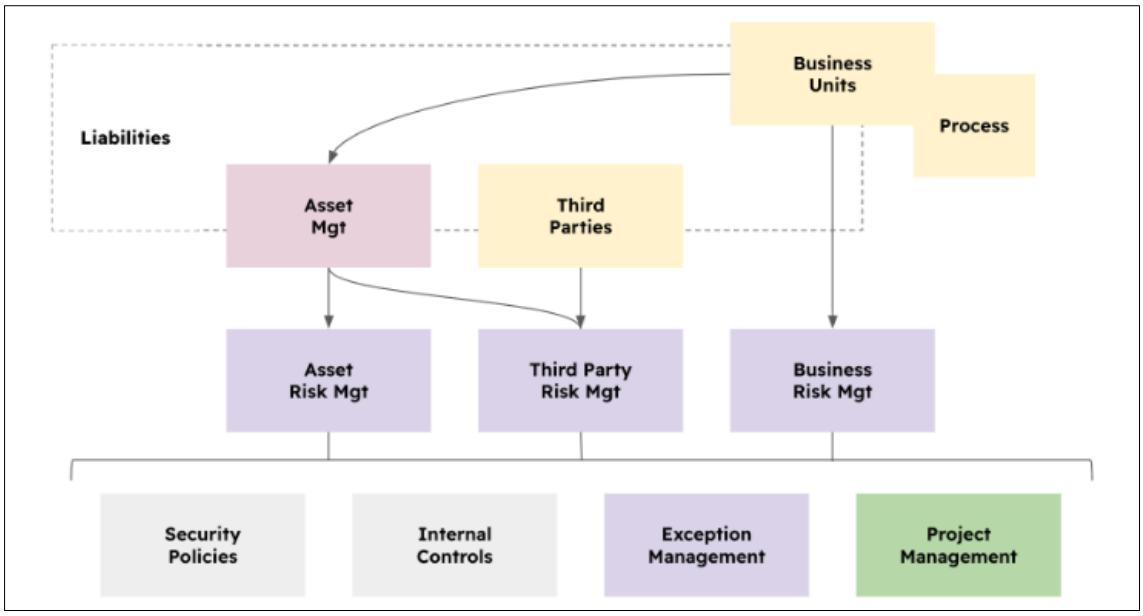
- Administrar políticas y sus revisiones
- Gestionar los controles internos y sus auditorías
- Administrar excepciones y sus revisiones
- Gestionar proyectos y sus revisiones
- Gestionar planes de continuidad

Para poder cumplir con lo mencionado anteriormente, ERAMBA cuneta con los siguientes módulos: (Ri, 2025)

- Organización / Unidades de Negocio
- Organización / Unidades de Negocio / Proceso
- Organización / Terceros
- Organización / Pasivos
- Gestión de activos / Activos
- Gestión de riesgos / Gestión de riesgos de activos
- Gestión de riesgos / Gestión de riesgos de terceros
- Gestión de riesgos / Análisis del impacto empresarial
- Gestión de riesgos / Excepciones de riesgo
- Catálogo de Controles / Controles Internos
- Catálogo de controles / Políticas de seguridad
- Operaciones de seguridad / Gestión de proyectos

Dentro de la herramienta los aspectos básicos para la gestión de riesgos se relacionan entre sí, lo que permite gestionar estos componentes de manera estructurada, asegurando que cada elemento aporte a la estrategia de gestión de riesgos. En la figura 39 se muestra la relación básica.

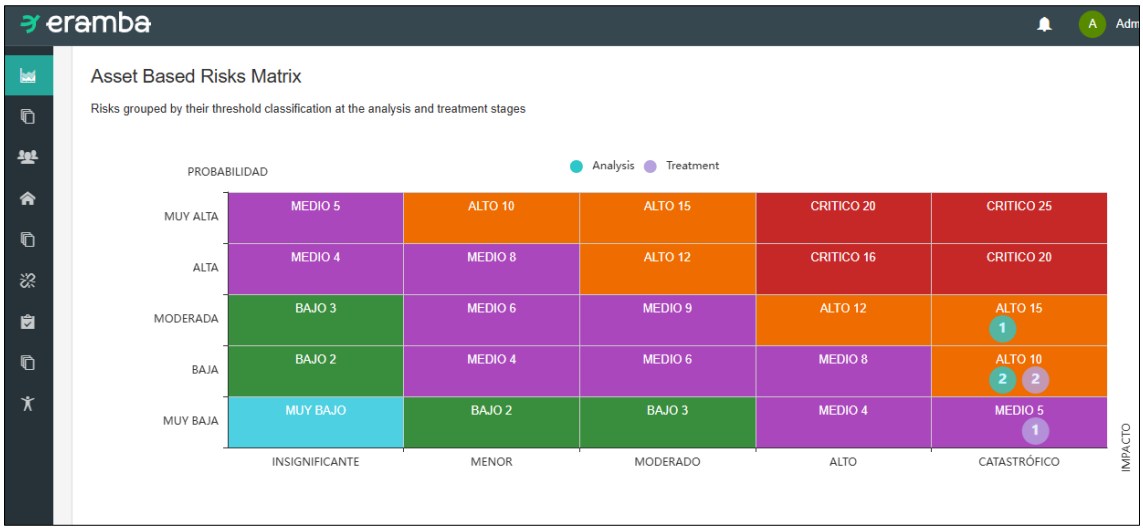
Figura 39. Diagrama de relación básica de elementos de gestión de riesgos



Fuente: Eramba.org

Tras haber expuesto las principales ventajas que ofrece ERAMBA como herramienta de gestión de riesgos y cumplimiento, a continuación, se presenta su aplicación práctica dentro de la Cooperativa en cumplimiento de la Gestión del Sistema de Seguridad de la Información (SGSI). En primera instancia en el ingreso a la plataforma vamos a encontrar el panel principal, donde se aprecia un resumen de toda la gestión, podemos ver las tareas (expiradas, en proceso y futuras), si tenemos la versión gratuita estas graficas no suelen verse por completo; también se puede visualizar la matriz de riesgo basada en activos como se muestra en la Figura 40.

Figura 40. Matriz de riesgo basada en activos en el Panel principal de ERAMBA

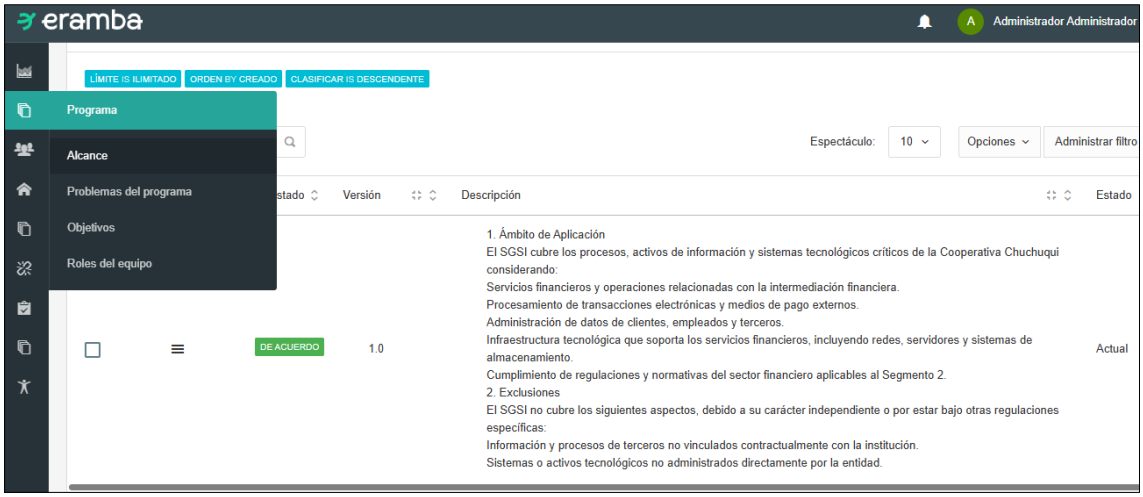


Fuente: Propia

Módulo de Programa de ERAMBA

En el módulo de Programa vamos a encontrar los submódulos de Alcance, Problemas del programa, Objetivos y Roles de equipo, como se muestra en la Figura 41.

Figura 41. Módulo de Programa de ERAMBA



Fuente: propia

En el alcance del SGSI se debe establecer el ámbito de aplicación describiendo las áreas que intervienen, procesos, sistemas, toda información relevante que interviene en al análisis del SGSI incluyendo las sucursales de la cooperativa. También se puede detallar las exclusiones, aspectos que no se consideran con su debida justificación.

En problemas del programa se debe definir las limitaciones u obstáculos internos y externos que pueden afectar al cumplimiento de los objetivos planteados, por ejemplo:

- Problema externo: El código fuente del core financiero es administrado solo por el proveedor, por lo que cualquier cambio está bajo su dependencia.
- Problema interno: Infraestructura tecnológica obsoleta, el uso de hadware y software desactualizado incrementa las vulnerabilidades en la institución

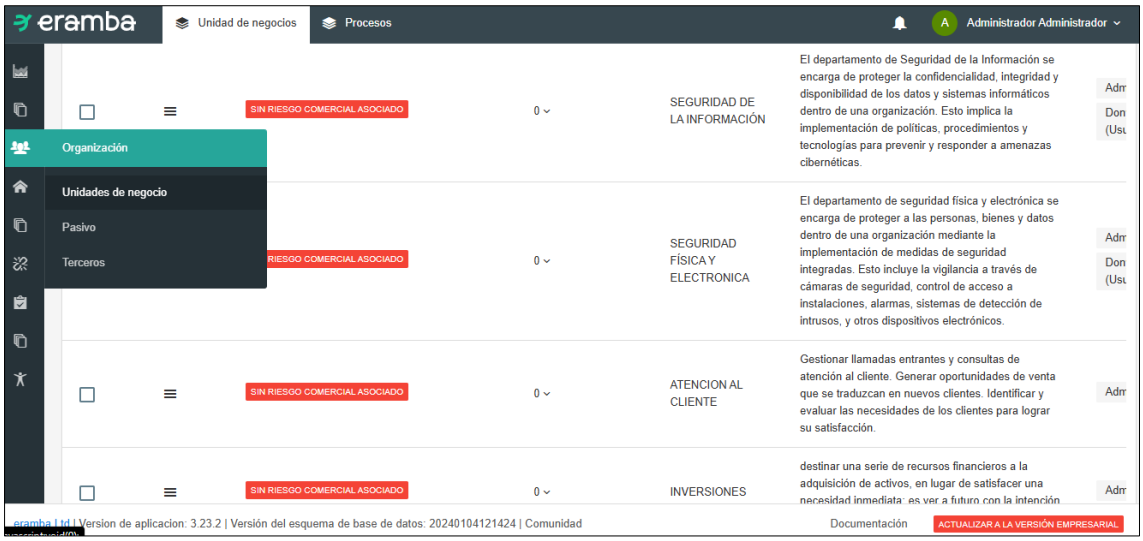
Los objetivos deben estar alineados a la estrategia institucional y al cumplimiento normativo vigente, definiendo de manera específica la finalidad del SGSI que en sí radica en la protección de la información crítica o sensible de la institución frente a amenazas y vulnerabilidades.

En roles de equipo se debe documentar las funciones y responsabilidades de los actores que intervienen en el SGSI. Estos roles deben estar alineados a lo que se establece en la resolución SEPS 2022-002.

Módulo de Organización de ERAMBA

El módulo de organización permite ingresar las unidades de negocio o departamentos que conforman la cooperativa, las obligaciones y Terceros, como se muestra en la Figura 42.

Figura 42. Módulo de Organización de ERAMBA

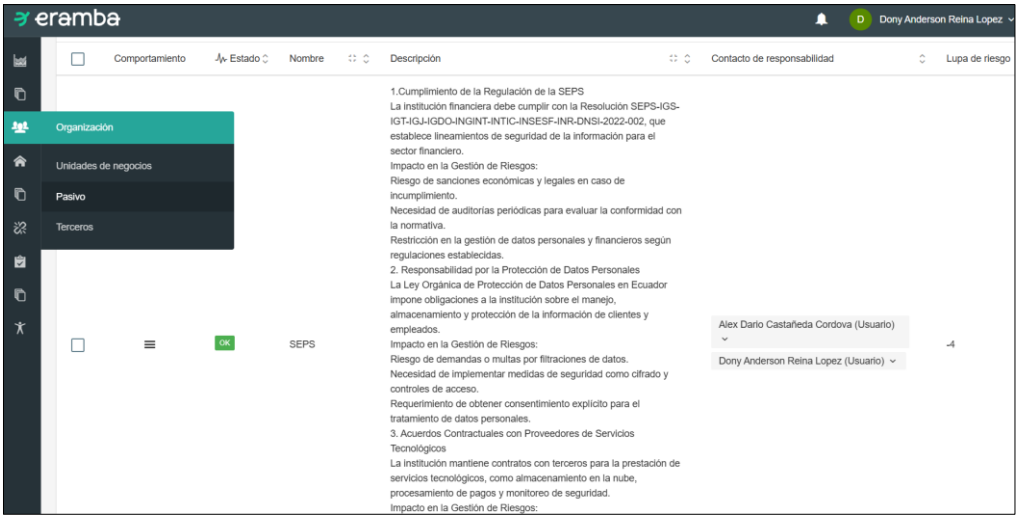


Fuente Propia.

El apartado de unidades de negocio permite describir los procesos de cada unidad que se emplean para el análisis de impacto empresarial determinando el RTO ((Recovery Time Objective) y MTO (Maximum Tolerable Outage).

En la sección de pasivo se describe las restricciones o limitaciones legales, las cuales utilizan para delimitar el alcance del SGSI. En este caso se va a identificar las normativas internas y externas como se observa en el ejemplo de la figura 43.

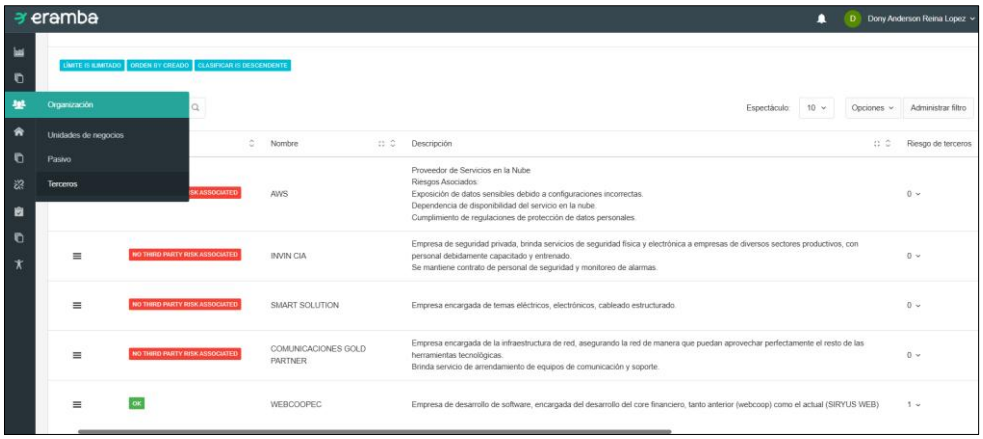
Figura 43. Registro de pasivos (limitaciones legales) en ERAMBA



Fuente: Propia

En el apartado de terceros, lo ideal sería enlistar a todos los proveedores con los que la institución tenga relación, pero si no se cuenta con recursos humanos para poder gestionar de forma adecuada a terceros, se debe establecer un alcance para considerar solo a los proveedores de servicios críticos. En la figura 44 se observa un ejemplo del registro de terceros, los cuales hasta no identificar un riesgo asociado aparece en rojo para dar a entender que aún no se gestiona de forma adecuada al proveedor.

Figura 44. Registro de terceros en ERAMBA

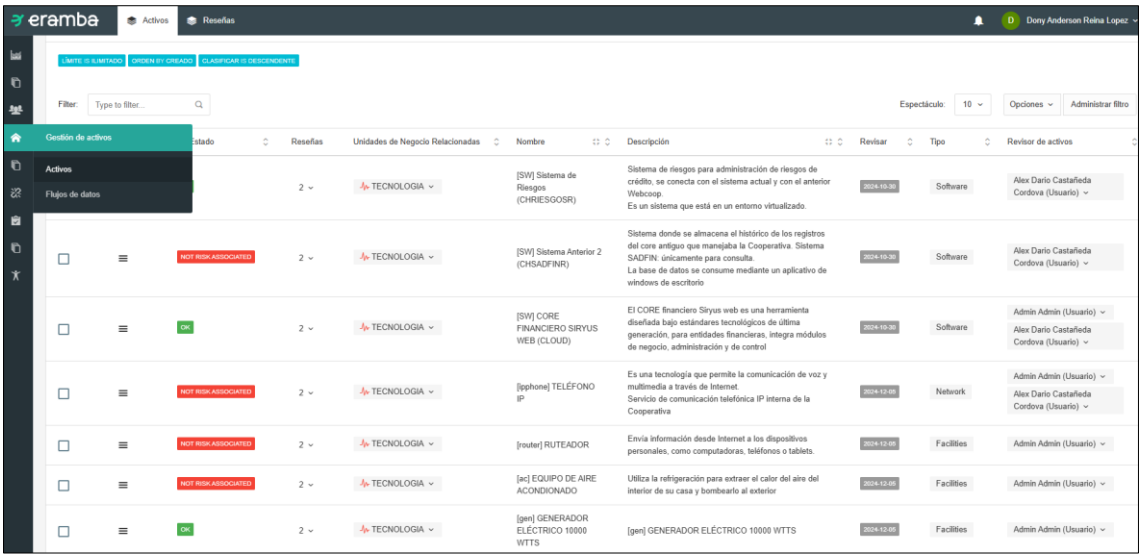


Fuente: Propia

Módulo de Gestión de Activos de ERAMBA

En el módulo de gestión de activos, encontramos los submódulos de Activos y Flujos de datos. En Activos vamos a poder registrar todos los activos de información que se ha identificado, los cuales aparecen en rojo hasta no tener asociado un riesgo como se observa en la figura 45.

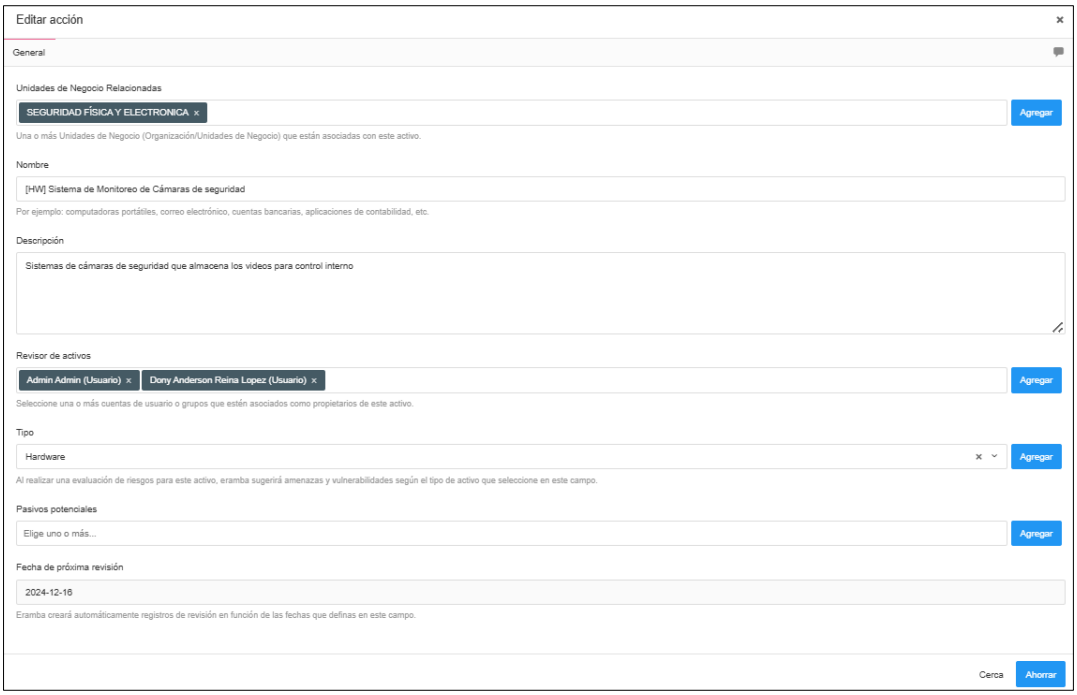
Figura 45. Módulo de Gestión de Activos de ERAMBA



Fuente Propia

Para ingresar un nuevo activo lo primero que nos requiere es la información de la unidad de negocio a la que está asociado el activo, esto es indispensable para conocer su ubicación, luego nos solicita el nombre que se le asigna, una descripción, el nombre del responsable del activo, el tipo de activo, pasivos potenciales (para conocer si está bajo una limitación legal) y fecha de próxima revisión (se la puede utilizar para gestionar acciones como mantenimiento o revisión de las medidas de seguridad). En la figura 46 se presenta un ejemplo de registro de un nuevo activo de información.

Figura 46. Ejemplo de registro de activo en ERAMBA



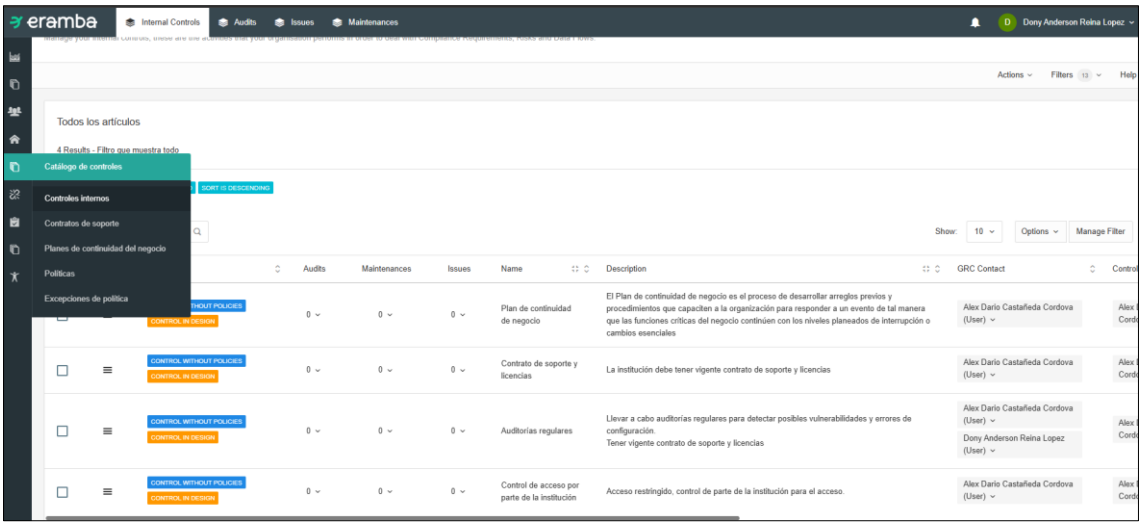
Fuente: Propia

Respecto al submódulo de flujo de datos, se refiere a los activos relacionados con base de datos, los cuales pueden requerir una gestión adicional de GDPR (Gestión de Riesgos de Protección de Datos), para lo cual el DPO (Oficial de Protección de Datos) es el responsable, por lo cual no se considera dentro de este estudio ya que no está dentro del alcance del trabajo de investigación.

Módulo de Catálogo de Controles de ERAMBA

En el módulo de Catálogo de Controles, como se observa en la figura 47 podemos registrar toda la información de la institución relacionada a la implementación controles de seguridad, políticas de seguridad aprobadas, contratos con los proveedores de servicios críticos, SLAs tanto internos como con terceros, planes de continuidad del negocio. Esta información puede ser de manera textual, en la cual se describa los puntos relevantes, o también podemos cargar el documento asociado. En el caso de los planes de continuidad nos permite registrar los costos o presupuestos requeridos.

Figura 47. Módulo de Catálogo de Controles de ERAMBA

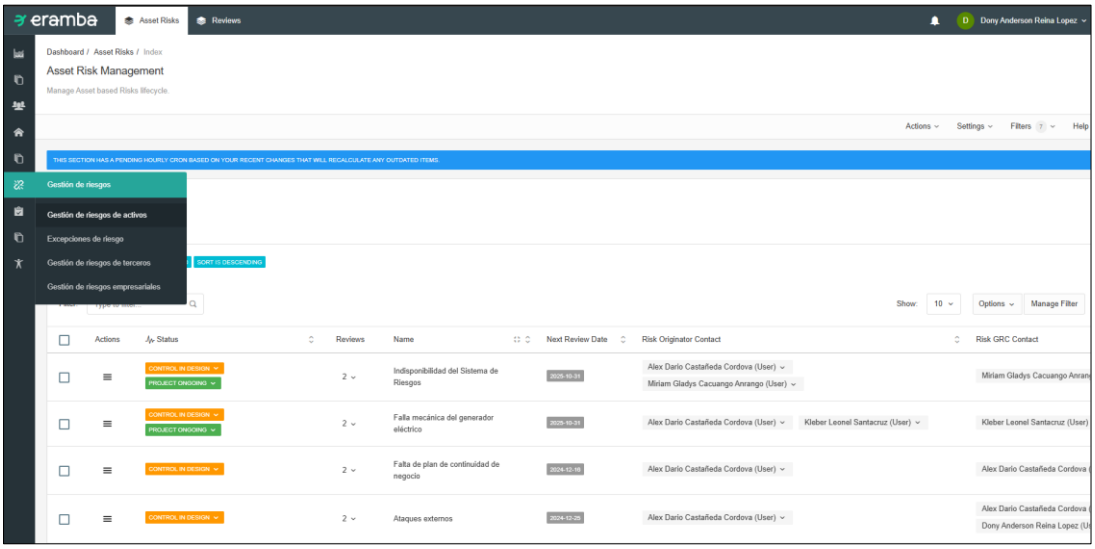


Fuente: Propia

Módulo de Gestión de Riesgos

En este módulo ERAMBA nos muestra tres enfoques para la gestión de riesgos como se observa en la figura 48 (gestión de riesgos de activos, gestión de riesgos con terceros y gestión de riesgos empresariales).

Figura 48. Módulo de Gestión de Riesgos de ERAMBA



Fuente: Propia

Para iniciar cualquiera de las gestiones de riesgo, el punto de partida es identificar la clasificación y los tipos de clasificación.

- Tipos de clasificación: se refiere en base a que vamos a calcular del riesgo, que en este caso solo vamos a utilizar el impacto y la probabilidad.
- Clasificación: se refiere a los niveles de valoración que se da a cada tipo de clasificación, por ejemplo, en la figura 49 se muestra los niveles de valoración del impacto.

Figura 49. Valoración del impacto en ERAMBA

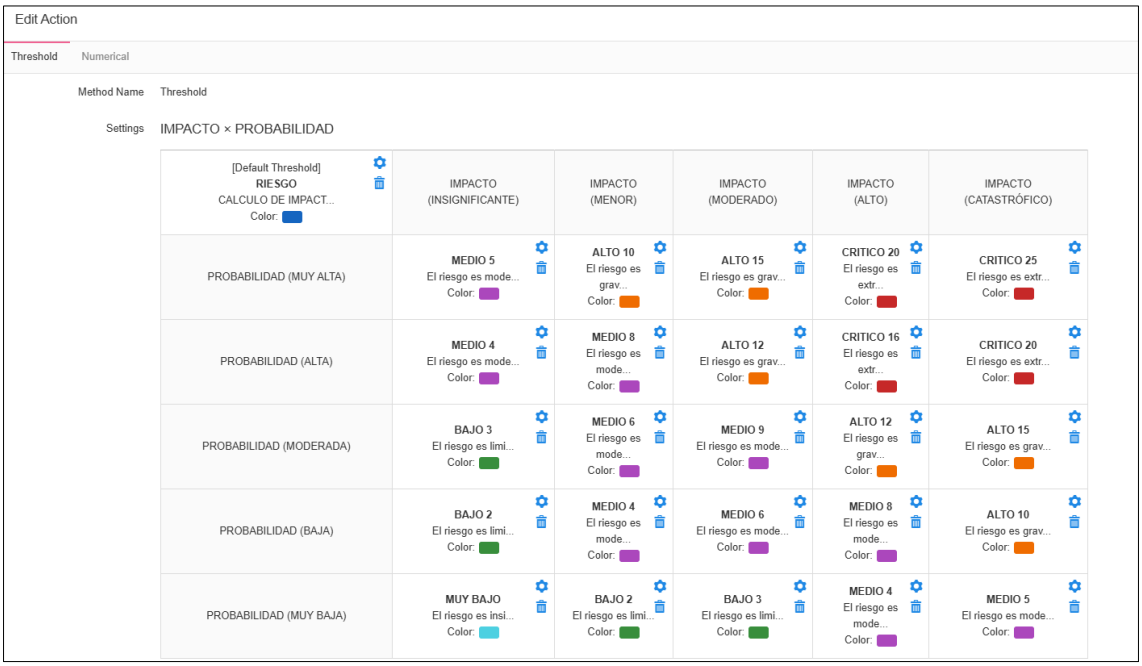
Risk Classifications

Actions	Classification Type	Name	Criteria	Value
≡	IMPACTO	CATASTRÓFICO	En caso de que el activo tenga un incidente y sus consecuencias son extremadamente graves que pueden afectar totalmente al giro de negocio de la organización o a un daño irreparable. Ejemplos: Pérdida total de datos críticos sin posibilidad de recuperación, compromisos masivos de seguridad que llevan a la bancarrota o cierre de la organización, pérdida de vidas humanas. Consecuencias: Pérdida total de la confianza de los clientes, sanciones legales severas, daños irreparables a la reputación.	5
≡	IMPACTO	ALTO	En caso de que el activo tenga un incidente su impacto es muy grave, con consecuencias serias pero no necesariamente irreparables. Requiere una acción inmediata para mitigar daños. Ejemplos: Pérdida significativa de datos, compromisos importantes de seguridad que afectan considerablemente a la organización, fallos en servicios clave. Consecuencias: Pérdida considerable de ingresos, daño significativo a la reputación, sanciones legales importantes, interrupciones graves en las operaciones.	4
≡	IMPACTO	MODERADO	El evento tiene un impacto notable pero manejable. La organización puede recuperarse con recursos internos sin afectar su operación general a largo plazo. Ejemplos: Pérdida de datos de respaldo, compromisos de seguridad con alcance limitado, interrupciones temporales en servicios no críticos. Consecuencias: Daños financieros moderados, daño a la reputación recuperable, interrupciones manejables en las operaciones.	3
≡	IMPACTO	MENOR	El impacto es limitado y la organización puede gestionarlo con poca o ninguna interrupción a sus operaciones normales. Ejemplos: Incidentes menores de seguridad, pérdida temporal de acceso a datos no críticos, fallos en sistemas de bajo impacto. Consecuencias: Impacto financiero mínimo, daño a la reputación poco significativo, interrupciones menores en las operaciones.	2
≡	IMPACTO	INSIGNIFICANTE	El impacto es casi nulo o no afecta de manera perceptible a la organización. Ejemplos: Incidentes de seguridad sin pérdida de datos ni compromisos, fallos menores en sistemas sin impacto operacional. Consecuencias: Sin impacto financiero, sin daño a la reputación, operaciones continúan normalmente.	1

Fuente: Propia

A continuación, se establece el apetito de riesgo donde se estable la matriz en base a la cual se va a calcular el riesgo, se debe ir armando los valores de la matriz con una descripción de cada uno (por ejemplo, riesgo Muy Alto con valoración 25 significa que el riesgo es crítico y ocasiona interrupciones en los servicios), en la figura 50 se presenta un ejemplo de matriz de apetito de riesgo.

Figura 50. Ejemplo de matriz de apetito de riesgo en ERAMBA



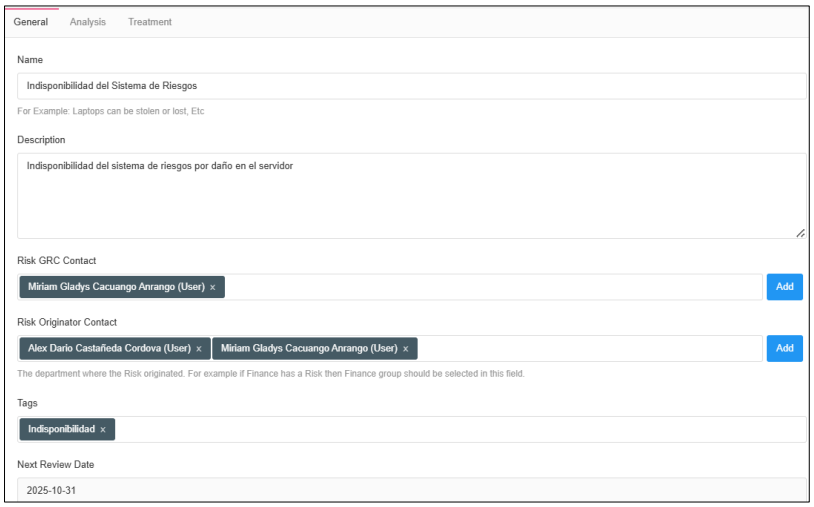
Fuente: Propia

De esta misma forma lo podemos hacer para los tres enfoques de gestión de riesgos, y conforme se vayan registrando los riesgos identificados, estos se van a ir visualizando en el dasboard.

En el registro de los riesgos se consideran tres aspectos:

- General: el nombre del riesgo identificado, una descripción, el responsable de la gestión de riesgos, el funcionario responsable que se asocia con el origen del riesgo, asignación de etiquetas para el riesgo y una fecha próxima para la siguiente revisión. En la figura 51 se presenta un ejemplo de registro general de riesgo.

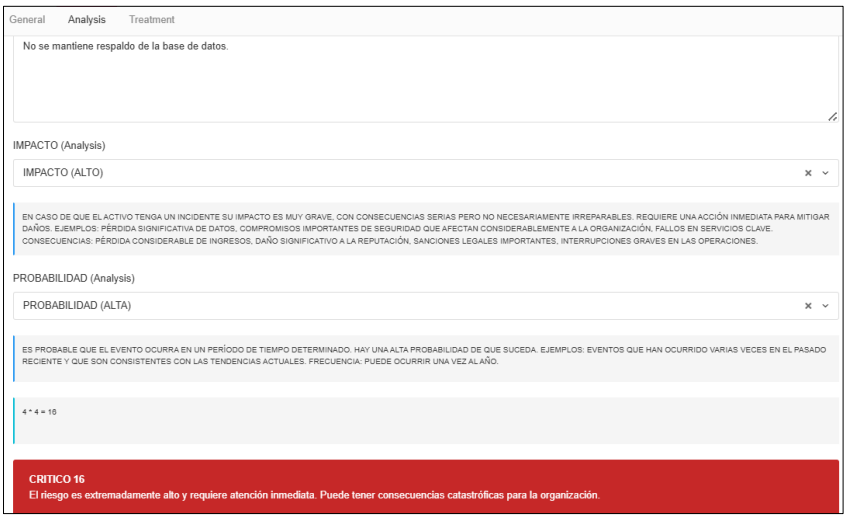
Figura 51. Registro de aspectos generales del riesgo en ERAMBA



Fuente: Propia

- Análisis: se registra el activo, tercero o unidad de negocio asociado al riesgo, una descripción de la amenaza, una descripción de la vulnerabilidad, la valoración el impacto y la valoración de la probabilidad. En la figura 52 se muestra un ejemplo de análisis de riesgo.

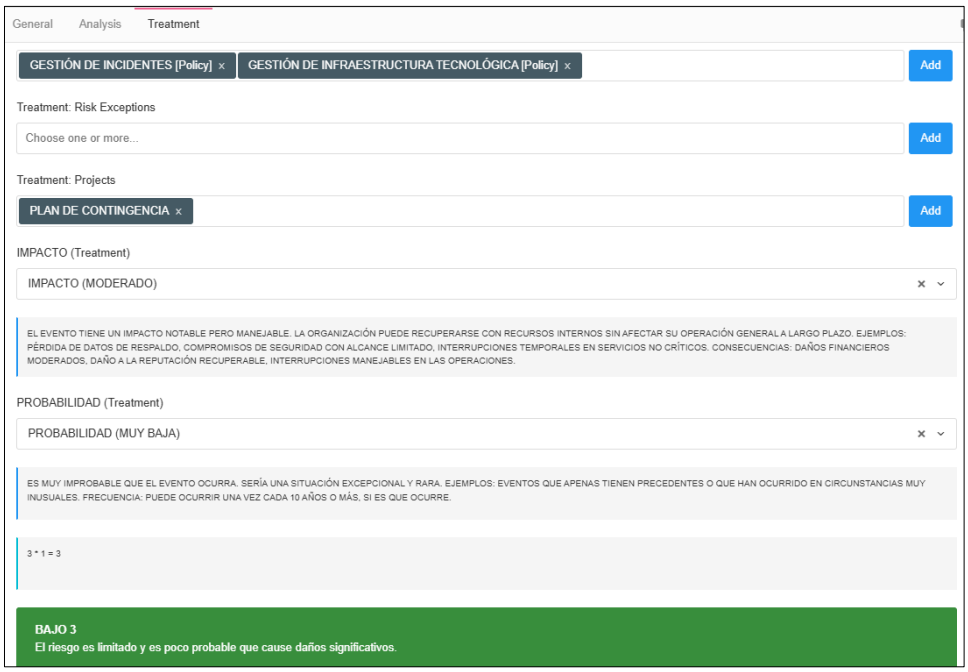
Figura 52. Ejemplo de registro de análisis de riesgo en ERAMBA



Fuente: Propia

- Tratamiento: Se registra el tipo de tratamiento (aceptar, reducir, mitigar o transferir), los controles asociados, las políticas asociadas, los proyectos asociados, y la valoración del impacto y probabilidad luego del tratamiento. En la figura 53 se presenta un ejemplo de tratamiento de riesgo.

Figura 53. Ejemplo de tratamiento de riesgo en ERAMBA



Fuente: Propia

3.2.3.4. Respaldos y resguardo de información sensible o crítica

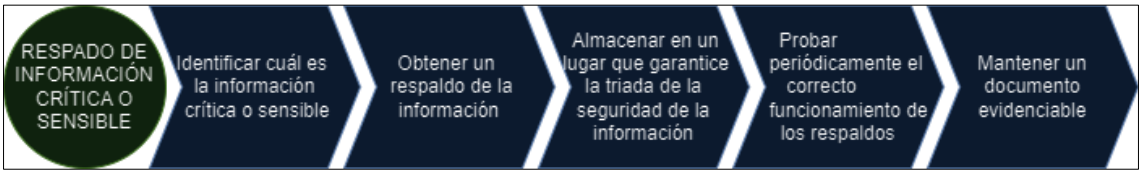
Según lo establecido en la normativa SEPS 2022-002, las instituciones financieras bajo la regulación de la Superintendencia de Economía Popular y Solidaría deben:

- Respaldar la información sensible o crítica ya sea física o digital, en lugares que garanticen su protección considerando la triada de la seguridad de la información.

- Mantener un documento evidenciable que compruebe que los respaldos almacenados funcionen correctamente.

En la figura 54 se presenta el proceso de respaldo de información.

Figura 54. Proceso de respaldo de información



Fuente: Autor

La mayor parte o por no decir toda la información crítica o sensible de las instituciones financieras es aquella que se maneja dentro del "core financiero", por lo cual se debe tener una política que garantice la obtención de un respaldo periódico de la base de datos, en el sector financiero es obligatorio que se realice a diario y cada vez que exista un proceso crítico que se ejecute. Por ejemplo, el cierre de fin de día es un proceso crítico que realizan todas las instituciones financieras antes de cambiar de fecha contable, también existen procesos que no son tan continuados, pero también se debe obtener un respaldo de la base de datos antes de ser ejecutados como es la capitalización de intereses de forma masiva o cambios en la parametrización del sistema por temas normativos.

Para los respaldos obtenidos se deben realizar las siguientes acciones:

- Verificar los incrementales de los respaldos diarios y semanales completos de servidores críticos.
- Respaldar en medios externos etiquetados y almacenados en sitios seguros implementado técnicas de cifrado de la información.
- Custodia física de los discos externos y mantener una bitácora de registro.

- Copias adicionales en la nube, para el caso de estudio la cooperativa Chuchuqui emplea OneDrive.

Respecto a la técnica de cifrado de los respaldos de información se puede utilizar la herramienta Veracrypt que es gratuita open source, para crear un contenedor que nos permita almacenar los respaldos de manera segura.

También se deben identificar otros activos de información sensible que requieran la generación de respaldos, como puede ser el caso de máquinas virtualizadas que se puede utilizar herramientas de respaldo automático como Veem Backup, para el caso de estudio en la tabla 18 se ha identificado las siguientes máquinas virtuales con su determinada frecuencia de respaldo:

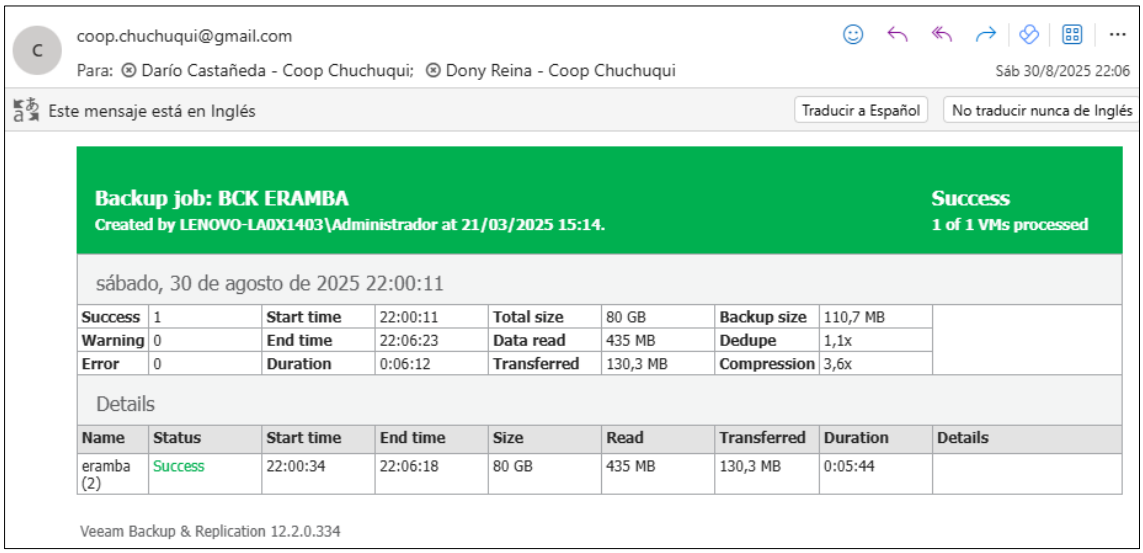
Tabla 18. Respados planificados en Veem Backup

Nombre de Maquina virtual	Descripción	Frecuencia
CHAPP	Servidor de aplicaciones	Diaria
CHAD	Active Directory	Semanal
CHERAMBA	Sistema de ERAMBA (SGSI)	Semanal
CHMAILR	Servidor de correo electrónico	Diaria
CHRIESGOR	Sistema de Riesgos	Mensual
CHRESP	Sistema Financiero anterior	Semanal

Fuente: Propia

Dentro de la gestión de respaldos presentada, existen las que se realizan de forma manual que es el caso de los respaldos del core financiero y la carga a la nube también es manual, y está la forma automatizada a través de Veem Backup que genera respaldos planificados y su carga en la nube es automática y envía un correo con el reporte de generación de respaldo como se observa un ejemplo en la figura 55.

Figura 55. Ejemplo de confirmación de respaldo de Veem Backup



coop.chuchuqui@gmail.com

Para: Darío Castañeda - Coop Chuchuqui; Dony Reina - Coop Chuchuqui

Sáb 30/8/2025 22:06

Este mensaje está en Inglés | Traducir a Español | No traducir nunca de Inglés

Backup job: BCK ERAMBA
Created by LENOVO-LA0X1403\Administrador at 21/03/2025 15:14.

Success
1 of 1 VMs processed

sábado, 30 de agosto de 2025 22:00:11

Success	1	Start time	22:00:11	Total size	80 GB	Backup size	110,7 MB
Warning	0	End time	22:06:23	Data read	435 MB	Dedupe	1,1x
Error	0	Duration	0:06:12	Transferred	130,3 MB	Compression	3,6x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
eramba (2)	Success	22:00:34	22:06:18	80 GB	435 MB	130,3 MB	0:05:44	

Veeam Backup & Replication 12.2.0.334

Fuente: Propia

3.2.3.5. Cultura de seguridad de la información

La cultura de seguridad de la información se fundamenta en lo establecido en la resolución SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116 en su artículo 8, donde menciona que las instituciones deben diseñar, programar y coordinar planes de capacitación permanentes, los cuales deben ser dirigidos a todos sus órganos internos, empleados, funcionarios o servidores. Las capacitaciones deben cumplir al menos con las siguientes condiciones (1Superintendencia de Economía Popular y Solidaria, 2024):

- Ser impartidas durante el proceso de inducción a los nuevos empleados.
- Ser impartidas periódicamente a todos los empleados.
- Contar con mecanismos de evaluación (cuestionarios, simulación de escenarios).
- Mantener registro del personal capacitado.

En base a lo establecido por la SEPS se debe elaborar el plan de capacitación con la finalidad de fortalecer la capacidad de los funcionarios mediante conocimientos, habilidades y actitudes en el entorno de seguridad de la información. Una consideración

importante el desarrollo del material de capacitación, el cual no debe generar desinterés por parte de los funcionarios, sino que sea entendible con ejemplos prácticos.

La capacitación al ser dirigida a todos los funcionarios es necesario que se explique la responsabilidad compartida y la importancia que todos tienen dentro del SGSI. Los temas para considerar pueden ser los siguientes:

- Gestión de Contraseñas seguras.
- Malware y sus diferentes tipos.
- Políticas internas relacionadas con Seguridad de la Información.
- Correcto uso de correo electrónico e identificación de correos maliciosos.
- Uso adecuado de Internet.
- Política de escritorios limpios.
- Sanciones por incumplimiento de las Políticas.
- Ejemplos de amenazas y vulnerabilidades comunes.
- Uso y manejo de inventario de activos de información.
- Software permitido y prohibido en la Cooperativa.
- Controles de acceso a los sistemas críticos.
- Ingeniería social.
- Gestión de Incidentes (cómo reportar, a quién reportar, qué se puede reportar).
- Roles y responsabilidades en la Cooperativa.

Implementación.

1. Socialización del plan con la alta dirección

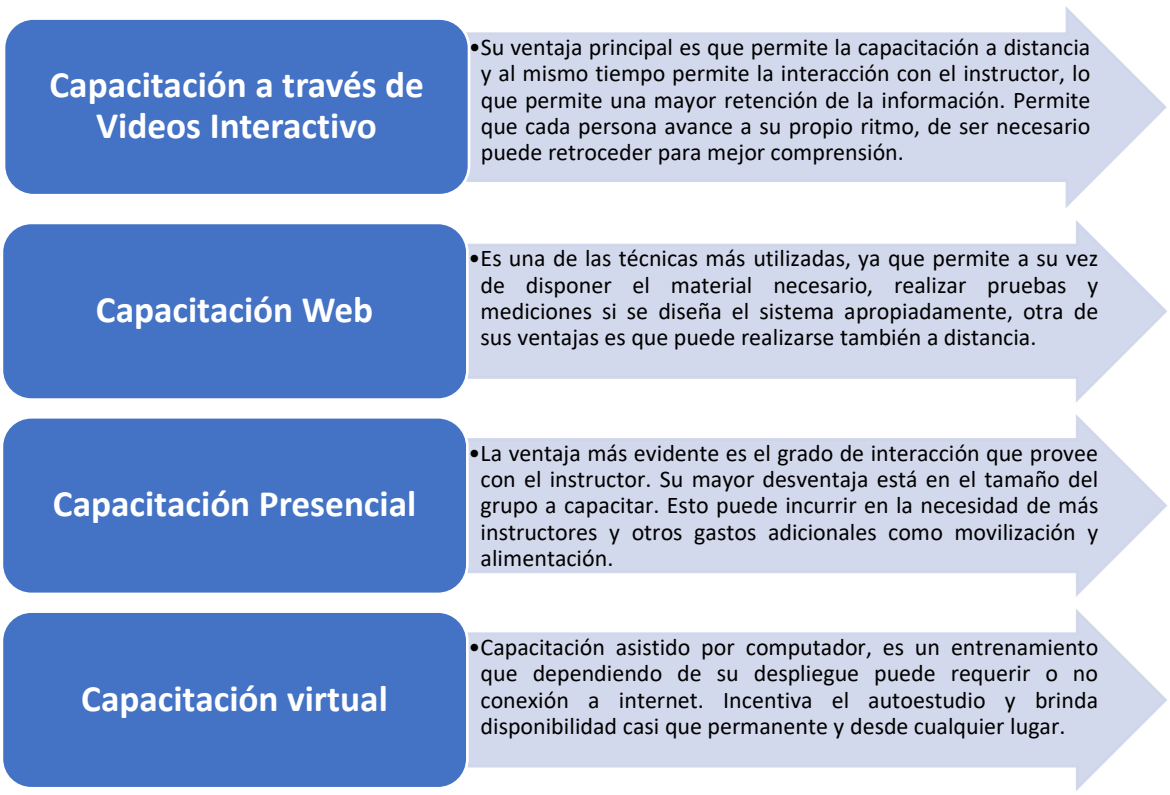
Lo primero que debe hacerse es socializar el programa que se diseñó en las fases anteriores, para así asegurar el apoyo y los recursos necesarios por parte de la Gerencia General para la ejecución.

Una vez se logra la aprobación por parte de la alta dirección, la implementación puede dar inicio (desarrollando o contratando los materiales propuestos para cada fin). A continuación, se definen técnicas que permiten difundir o comunicar la información.

2. Técnicas recomendadas para la comunicación de material de capacitación.

Las técnicas de capacitación deben aprovechar al máximo los avances tecnológicos, empleando herramientas que brinden facilidad de uso y acceso, escalabilidad. Dentro de las técnicas más comunes y efectivas se muestran en la figura 56.

Figura 56. Técnicas más comunes de fomentar la cultura de SI



Fuente: Propia

3. Evidencias de la asistencia a capacitaciones y el compromiso con la entidad

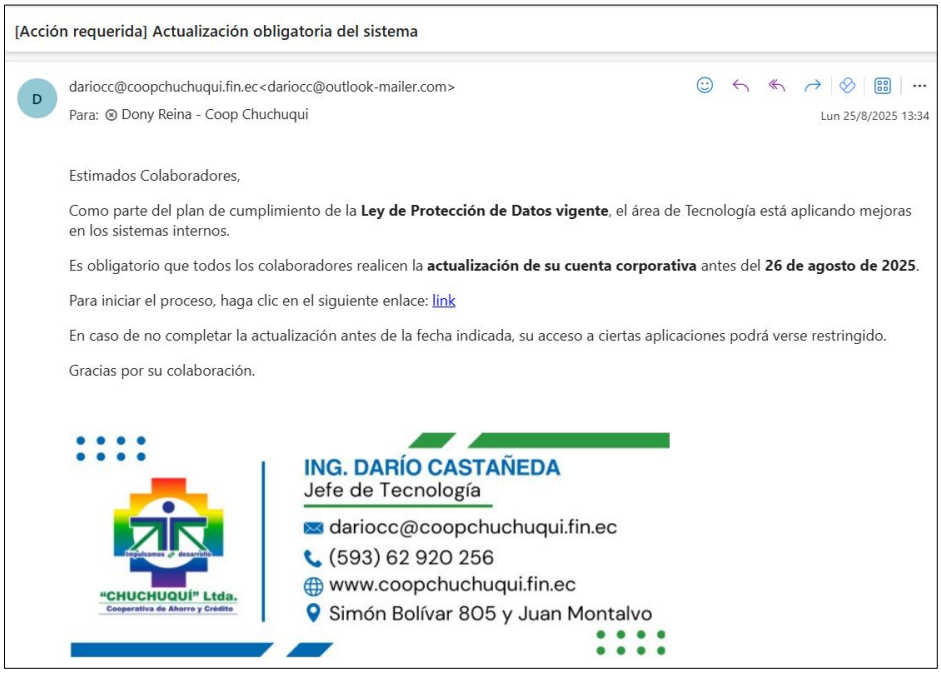
Los usuarios que asistan a las capacitaciones deben certificar su asistencia y asumir sus respectivos compromisos con la preservación de la seguridad de la información en la institución (cumpliendo con las políticas de seguridad internas).

4. Pruebas de seguridad

Es importante realizar simulacros periódicos donde se pueda evaluar y fortalecer los conocimientos de las capacitaciones realizadas. Adicionalmente, se puede elaborar pruebas escritas, para evaluar la capacidad de retención de la información.

Un ejemplo de simulacro es una prueba de phishing utilizado la identidad de un funcionario de la cooperativa, en la figura 57 se muestra un ejemplo en el cual se utilizó la identidad del jefe de tecnología solicitando una actualización.

Figura 57. Ejemplo de simulación de phishing



Fuente: Propia

Como se observa en la imagen anterior el correo está suplantando la identidad del jefe de tecnología, pero también se observa en el remitente que el correo original de envío es diferente al institucional. Los resultados de esta práctica se muestran en la figura 58.

Figura 58. Resultados de simulación de phishing

Fuente: Propia

Se ejecuto una campaña de Phishing a un total de 47 usuarios, únicamente 45 correos fueron entregados de los cuales solo 24 usuarios abrieron el correo. De esos 24 usuarios que abrieron el correo solo 23 usuarios dieron clic al link de la campaña y 12 usuarios finalizaron el entrenamiento. Estos resultados deben ser socializados para fortalecer los conocimientos del personal.

3.2.3.6. Gestión de accesos tecnológicos

El proceso de gestión de accesos tecnológicos define las actividades para la asignación, modificación y eliminación de accesos a los servicios críticos o información sensible de la institución. La ISO/IEC 27001 en su Anexo A, punto 5.15 se describe el control de acceso el cual menciona que “las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar en función de los requisitos del negocio y de seguridad de la *información*”.

En el alcance de este procedimiento se debe establecer a que activos o información sensible aplica, a continuación, se presenta ejemplos de activos que necesitan gestión de accesos:

- Core financiero
- Active Directory
- Correo institucional
- Repositorio Centralizado
- Servidores
- Data Center
- Aplicaciones internas

Los actores que intervienen en este proceso son:

- OSI: Se encarga de verificar el cumplimiento, monitorear las bitácoras de acceso, verificar los privilegios de acceso e identificar posibles riesgos asociados.
- Jefe de Tecnología: Ejecutar la gestión de accesos y mantener registros de los usuarios habilitados para cada servicio o activo de información.
- Gerencia General: Disponer la habilitación de accesos críticos.
- Auditor Informático: Verificar el cumplimiento.
- Usuarios: Hacer el correcto uso de las credenciales de acceso, manteniendo la confidencialidad y no transferencia a terceros.

Proceso

1. Solicitud de acceso

- El usuario o jefe inmediato hace la solicitud de acceso justificando su necesidad.
- El OSI revisa la justificación de acceso y dispone al jefe de TI la creación del usuario.
- Solo para casos de accesos críticos, se requerirá la autorización de gerencia general, como el acceso al core financiero, o acceso a áreas de valores.

2. Creación y asignación
    - El jefe de TI hace la entrega de las credenciales de acceso con acta entrega de respaldo.
    - En el caso de asignación de privilegios como en el caso de core financiero, el responsable de TTHH deberá comunicar el rol que se debe asignar en base a las funciones a desempeñar.
    - Se entregará las credenciales al usuario, y se le capacitará sobre las seguridades que debe contemplar para evitar posibles riesgos.
3. Revisión periódica de accesos
    - Con periodicidad trimestral el OSI y Jefe de Tecnología revisarán accesos y verificarán que no exista anomalías en los registros de bitácora y logs.
    - Verificar que los accesos temporales sean eliminados cuando finalice su vigencia.
4. Modificación de accesos
    - Para los casos de rotación de funciones, el responsable de TTHH deberá solicitar la modificación de los privilegios de acceso.

- El acceso anterior debe darse de baja, antes de asignar los nuevos privilegios, tomando en cuenta que la SEPS no permite que un funcionario tenga dos perfiles dentro del core financiero.

5. Revocación de accesos
    - Por desvinculación laboral: El responsable de TTHH debe notificar la salida del personal al jefe de tecnología, quien debe desactivar los accesos el mismo.
    - Por incumplimiento de políticas: El OSI solicitará la revocación inmediata y el funcionario deberá ser sancionado de acuerdo al reglamento interno de trabajo.
6. Controles adicionales
    - Las sesiones se deben bloquear tras un tiempo establecido de inactividad, por ejemplo, para los equipos informáticos de usuario final puede ser de 3 minutos, para el core financiero puede ser de 20 minutos. Estos tiempos se definirán por criterio del OSI
    - Control adecuado sobre cuentas genéricas, como la verificación periódica de los logs y bitácoras.
    - Integración con sistemas de monitoreo y alertas.

3.2.3.7. Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios tecnologías de la información

El propósito de este control es definir las acciones necesarias para solicitar, evaluar, aprobar, implementar y documentar cambios tecnológicos y mantenimiento de hardware, software y servicios de TI. La ISO/IEC 27001 en su punto 6.3 menciona que "*cuando la organización determina la necesidad de cambios en el sistema de gestión de*

seguridad de la información, los cambios deben llevarse a cabo de manera planificada".

Una gestión de cambios planificada nos permite evaluar las consecuencias que se pueden derivar y determinar medidas de mitigación de riesgos según sea necesario.

El alcance de este control se aplica a:

- Sistemas críticos (core financiero, base de datos, canales digitales, Active Directoty, Correo institucional, servidor de virtualización, entre otros que se considere como críticos)
- Infraestructura tecnológica (servidores, firewalls, equipos de comunicación, almacenamiento, redes, etc.)
- Servicios tecnológicos contratados (almacenamiento en la nube, networking, internet, etc.)
- Se considera cambios realizados tanto por el personal de TI como de proveedores externos.

Responsables.

- Persona que solicita el cambio: funcionario que identifica una necesidad de cambio.
- Jefe de tecnología: evalúa la necesidad del cambio, realiza un análisis de factibilidad y coordina la ejecución.
- OSI: evalúa posibles riesgos que afecten a la seguridad de la información.
- Comité TIC y Comité de Seguridad de la información: considera los análisis presentados y aprueba los cambios (solo en caso de sean cambios de alto impacto).

- Auditor informático: Verifica el cumplimiento del proceso.

Tipos de cambios

- Cambio estándar: de bajo riesgo, puede ser recurrente como actualizaciones menores por ejemplo la actualización de Sublime Text o WinSCP. Para este tipo de cambios no se requiere autorización de ningún comité.
- Cambio normal: es necesario un análisis previo y pruebas en entorno controlado, se requiere aprobación. Por ejemplo, migración de un servidor.
- Cambio urgente: se aplica cuando ocurren incidentes lo que deriva una emergencia. Por ejemplo, aplicación de parches de seguridad.

Procedimiento

1. Solicitud del cambio
    - El solicitante debe generar un ticket adjuntando el formulario de solicitud de cambio el cual contiene: descripción de cambio, justificación, sistemas o activos comprometidos, riesgos identificados, planificación de respaldo.
2. Evaluación
    - El jefe de tecnología evalúa la necesidad del cambio y presenta un informe de factibilidad.
    - El OSI evalúa los riesgos de seguridad y continuidad de los servicios.
    - Se asigna una clasificación (estándar, normal o urgente)
3. Aprobación
    - Estándar: autorizado por el jefe de tecnología
    - Normal: aprobado por el comité TIC

- Urgente: se notifica al comité TIC pero la autorización la realiza Gerencia General

4. Planificación
    - El jefe de tecnología debe elaborar un cronograma de planificación que contenga: Fecha y hora de ejecución, asignación del responsable y plan de respaldo antes de la ejecución.
    - De ser necesario, realizar pruebas en ambiente controlado.
    - Documentar el proceso en caso de incidencias.
5. Verificación
    - Verificar el correcto funcionamiento del sistema o activo afectado.
    - Documentar los resultados.
    - El OSI y usuario de cambio deben confirmar que la implementación sea adecuada.
    - El Jefe de tecnología cierra formalmente el cambio.

Respecto al mantenimiento, en la resolución de riesgo operativo de la SEPS se determina que las instituciones deben garantizar el mantenimiento de las aplicaciones para que satisfagan los objetivos del negocio, para ello se debe realizar una planificación anual de mantenimiento en base a lo que determine en la normativa interna de cada institución.

Los mantenimientos se aplican a toda la infraestructura tecnológica y pueden ser de tipo correctivo, preventivo y adaptativo, los cuales deben garantizar la calidad del servicio. Se debe mantener una bitácora de mantenimiento y documentación necesaria para mantener evidencia en caso de que solicite auditoría interna.

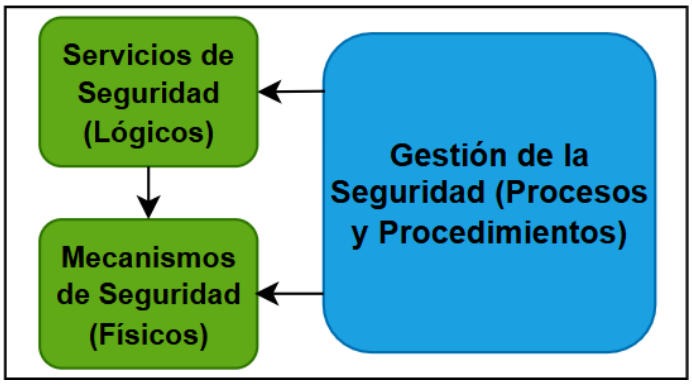
3.2.4. Controles tecnológicos

3.2.4.1. Arquitectura Segura

La SEPS determina que las instituciones financieras "*deberán diseñar, implementar y gestionar, la arquitectura segura para proteger los activos digitales en función de la particularidad tecnológica*", para ello es necesario tener una metodología de apoyo, para poder diseñar una arquitectura segura, que se ajuste al giro de negocio, y la más acertada es SABSA (Arquitectura de Seguridad Empresarial Aplicada de Sherwood). (SABSA Institute, 2018)

SABSA es una metodología originaria de Reino Unido, pero es reconocida a nivel mundial con una aceptación de alrededor de 50 países. Es de uso gratuito y mantiene un desarrollo continuo para satisfacer las necesidades empresariales. Uno de los sectores empresariales en los que se enfoca esta metodología es la banca (instituciones financieras), por lo que es muy aplicable en este caso de estudio. Se fundamenta en tres elementos de seguridad que estable la norma ISO 7498-2, indispensables en el diseño de una arquitectura segura los cuales se indican en la Figura 59. (SABSA Institute, 2018)

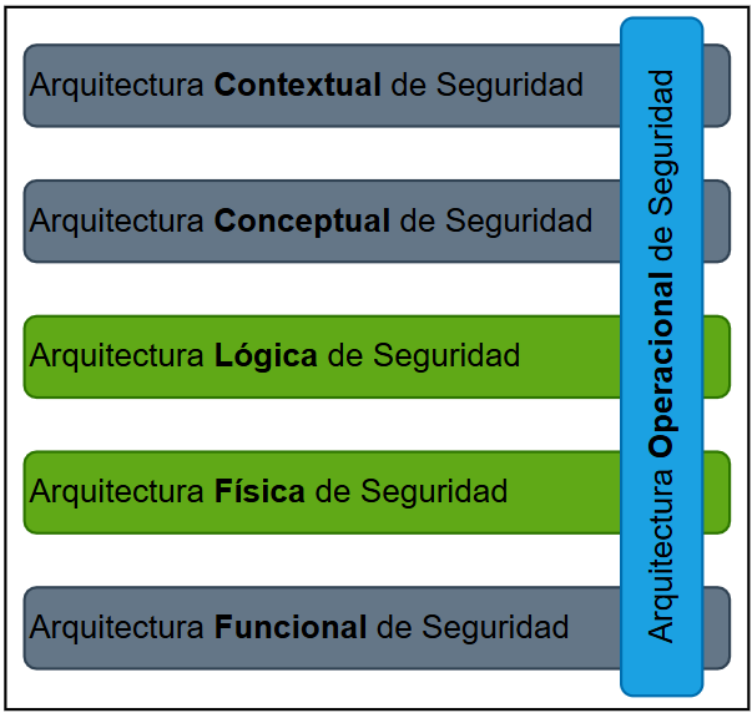
Figura 59. Relaciones conceptuales fundamentales de seguridad



Fuente: SABSA – W101 Diseñando un mundo digital seguro

A partir de la relación presentada en la figura anterior, la metodología determina un modelo en capas incluyendo aspectos de negocio, estrategia institucional y productos como se muestra en la figura 60. Este modelo establece lineamientos a considerar en cada capa, con el propósito de garantizar una arquitectura tecnológica segura.

Figura 60. Modelo en Capas SABSA



Fuente: SABSA – W101 Diseñando un mundo digital seguro

SABSA presenta perspectivas diferentes de las partes interesadas dentro de la institución en relación con la seguridad de la información. A continuación, se presenta un resumen de cada una:

Perspectiva del negocio (Arquitectura Contextual de Seguridad): Se le denomina de esta manera ya que se encarga del análisis del contexto del negocio, con una visión de gerente o de las personas que tienen el conocimiento y la experiencia para dirigir la institución, con la finalidad de establecer las estrategias institucionales y toma de decisiones relevantes. Al hablar de toma de decisiones de importancia también se incluye que se debe tener la capacidad de asumir los riesgos del giro del negocio y el

aporte que dan los profesionales en esta perspectiva es de suma importancia para que la arquitecta de seguridad cubra las necesidades del negocio. (SABSA Institute, 2018)

Perspectiva del Arquitecto (Arquitectura Conceptual de Seguridad): SABSA describe al arquitecto como una persona con gran creatividad y visión, capaz de enfrentar retos complejos preparando el terreno para que otros profesionales con conocimientos específicos, vayan cumpliendo tareas puntuales. Define elementos de concepto global que guían selección y organización de los elementos necesarios para el cumplimiento de las capas inferiores.

Perspectiva del diseñador (Arquitectura lógica): Está relacionada con el entorno virtual, se enfoca en los elementos lógicos de la arquitectura, como la información, procesos o funciones de aplicaciones y sistemas. El diseñador es quien toma la posta del arquitecto, donde interpreta la visión conceptual y la transforma en una estructura lógica para diseñar un sistema real. Se aplica términos de seguridad lógica y flujo de control lógico. (SABSA Institute, 2018)

Perspectiva del Constructor (Arquitectura Física): El rol del constructor es establecer los elementos físicos sobre los cuales el diseño lógico cobra vida. Se aplica la seguridad física, como controles de acceso, sistemas de seguridad electrónica, puntos de comunicación, infraestructura tecnológica.

Perspectiva del Técnico (Arquitectura Funcional): El personal tiene conocimientos técnicos y habilidades para integrar, configurar y unir elementos para entregar productos o servicios finales. Se relaciona con la seguridad en aspectos más específicos de hardware, software y servicios.

Perspectiva de Gerente (Arquitectura Operacional o de Gestión): Cuando se finaliza todo el proceso de la construcción y puesta en marcha de un sistema, se debe designar al encargado de su operación durante su vida útil, a esta persona se le denomina gerente de operaciones. La gestión de la seguridad es uno de sus roles para mantener condiciones aceptables de funcionamiento mediante monitoreo continuo.

De estas perspectivas SABSA desarrolla su matriz de arquitectura segura en contestación a las preguntas qué, por qué, cómo, quien, dónde y cuándo, como se muestra en la Tabla 19.

Tabla 19: Matriz de arquitectura SABSA

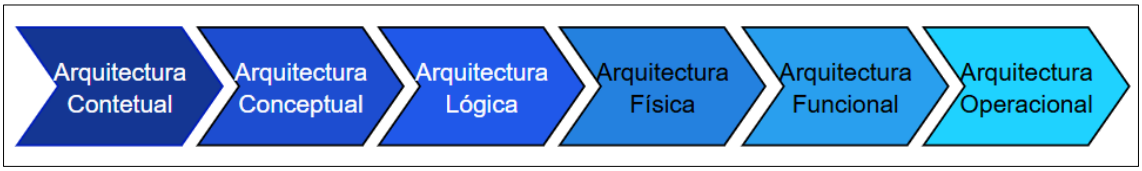
Arquitectura	ACTIVOS (Qué)	MOTIVACIÓN (Por qué)	PROCESOS (Cómo)	PERSONAS (Quién)	UBICACIÓN (Dónde)	TIEMPO (Cuándo)
ARQUITECTURA CONTEXTUAL	Decisiones de negocio y objetivos	Riesgo de negocio	Meta-procesos de negocio	Gobernanza organizacional y de la empresa extendida	Geografía del negocio	Dependencias de tiempo del negocio
	Valor del negocio; Taxonomía de asuntos/estrategias, incluyendo metas y objetivos, factores de éxito, metas	Inventario de oportunidades y amenazas	Cadenas de valor del negocio; Capacidades de negocio	Estructura organizacional y empresa extendida	Inventario de edificios, sitios, territorios, jurisdicciones, etc.	Dependencias temporales de metas y cadenas de valor del negocio
	Estrategia y objetivos de valor de negocio	Estrategia y objetivos de gestión de riesgos	Estrategias para procesos	Gobernanza de seguridad y riesgos; Marco de confianza	Marco de dominios	Marco de gestión del tiempo
ARQUITECTURA CONCEPTUAL	Taxonomía de atributos de negocio y perfil con objetivos de desempeño integrados	Objetivos, habilitación y control; Políticas de aseguramiento; Estrategias de gestión de riesgos; Estrategia de arquitectura de riesgos; Marco de aseguramiento de riesgos	Inventario de todos los procesos operativos (SI, manuales); Mapeo de procesos y flujos de trabajo	Gobernanza de seguridad; Proveedores de servicios internos y externos; Marcos de relaciones de confianza	Conceptos y marcos de dominio de seguridad	Marco de ciclo de vida; Marco de atributos de desempeño
	Activos de información	Políticas de gestión de riesgos	Mapas de procesos y servicios	Relaciones de confianza	Mapas de dominio	Calendario y programación
ARQUITECTURA LÓGICA	Inventario de activos de información; Modelo de información del negocio	Modelos de riesgos; Políticas de riesgos; Criterios de aseguramiento (política de aseguramiento requerida)	Flujos de información; Flujos funcionales; Servicios de información; Catálogo de servicios; Aplicaciones, utilidades y servicios comunitarios	Autoridades de dominio; Entidad de gobernanza comunitaria; Modelos de autoridad de confianza	Definiciones de dominio; Interfaces; Estándares	Inicio, tiempos de vida y fechas límite

	Activos de información	Prácticas de gestión de riesgos	Mecanismos de procesos	Infraestructura	Infraestructura	Programación de procesos
ARQUITECTURA FÍSICA	Registros de información e inventario de infraestructura de información	Reglas y procedimientos de gestión de riesgos; Metadatos	Procedimientos de trabajo; Sistemas de seguridad; Controles físicos; Controles de puntos de comunicación	Interfaces de usuario para sistemas heredados; Sistemas; Identidad y acceso	Espacios de trabajo; Hosts; Ubicación de dispositivos y redes	Programación y secuencias de procesos y sesiones
	Componentes de activos	Componentes de gestión de riesgos y estándares	Componentes y estándares de procesos	Componentes y estándares humanos	Componentes y estándares de localización	Componentes y estándares de tiempo y secuencia
ARQUITECTURA DE COMPONENTES	Productos y herramientas; Repositorios de datos; Procesadores de registros	Herramientas analíticas de gestión de riesgos; Registros de riesgos; Herramientas de monitoreo	Protocolos y estándares de procesos para entrega de servicios; Paquetes de aplicaciones	Identidades; Biografías; Roles; Funciones; Acciones; Controles de acceso	Direcciones; Hosts; Direcciones y localizadores; Configuración de la red	Horarios; Relojes; Temporizadores
	Gestión de entrega y continuidad	Políticas de gestión operativa de riesgos	Gestión del ciclo de vida de procesos	Gestión de recursos humanos y personal	Gestión del entorno	Gestión de tiempo y desempeño
ARQUITECTURA DE GESTIÓN	Aseguramiento de la entrega y continuidad	Evaluación de riesgos; Monitoreo y reportes de riesgos; Tratamiento de riesgos	Gestión de desarrollo, mantenimiento y soporte de sistemas, aplicaciones y servicios	Gestión de recursos humanos; Gestión de personal de la empresa extendida y relaciones empresariales	Gestión de edificios, sitios, plataformas y redes	Gestión del calendario y programación

Fuente: SABSA – W101 Diseñando un mundo digital seguro

La matriz de arquitectura presentada se puede ir desarrollando de forma vertical o de forma horizontal, dependiendo de la planificación de cada institución, pero siempre manteniendo la trazabilidad que se muestra en la figura 61.

Figura 61. Trazabilidad de cumplimiento de arquitectura SABSA



Fuente: SABSA – W101 Diseñando un mundo digital seguro

Además, SABSA estable un esquema general de actividades que deben realizar los diferentes directivos que intervienen en la arquitectura de seguridad de una organización. Para este caso se ha realizado una adaptación de la matriz para que se acople al sector financiero popular y solidario, manteniendo los enfoques que establece SABSA como se muestra en la tabla 20.

Tabla 20. Visión ejecutiva basado en SABSA

Enfoque	Consejo de Administración	Gerente General (CEO)	Contador General (CFO)	Administrador de Riesgos (CRO)	Oficial de Seguridad de la Información (OSI)	Jefe de Tecnología (CIO/CTO)
Negocio	Define la estrategia y aprueba planes (PETIC, PESI, SGSI). Garantiza que TI y riesgos estén alineados a la estrategia institucional.	Ejecuta la estrategia aprobada, asegura que los recursos estén disponibles para la operación.	Garantiza registros contables veraces, reportes financieros confiables y soporte a decisiones estratégicas.	Alinea gestión de riesgos con objetivos estratégicos institucionales; monitorea riesgos estratégicos y operativos.	Define políticas de seguridad de la información que respalden la continuidad del negocio.	Implementa sistemas y plataformas que soporten operaciones del core financiero, canales digitales y socios.
Riesgo	Supervisa la gestión de riesgo institucional; recibe reportes del Comité de Riesgos.	Administra riesgos operativos y tecnológicos en el día a día. Escala incidencias críticas al Consejo.	Vigila riesgos financieros, fraudes contables y cumplimiento tributario.	Identifica, mide, controla y monitorea riesgos (operativos, financieros, tecnológicos).	Evalúa riesgos de seguridad, propone controles (ISO 27001, SEPS 2022-002).	Evalúa riesgos tecnológicos: disponibilidad, ciberseguridad, obsolescencia, continuidad.

Integral (alcance escalable)	Exige que la gestión de riesgos abarque a toda la cooperativa (negocio, TI, seguridad, finanzas).	Coordina que todas las áreas integren sus planes (finanzas, riesgos, TI, seguridad).	Integra contabilidad con áreas de riesgos y tecnología para escalabilidad de reportes.	Promueve la adopción de metodologías (MAGERIT, ISO 27005) que cubran riesgos en todos los niveles.	Articula seguridad de la información con TI, riesgos y cumplimiento.	Escala infraestructura tecnológica (servidores, nube, redes) de acuerdo con necesidades futuras.
Modular (agilidad)	Aprueba modelos de gestión que permitan crecimiento progresivo (ej. Implementación gradual del SGSI).	Promueve agilidad organizacional y reasignación de recursos según prioridades.	Flexibiliza reportes financieros para adaptarse a cambios regulatorios o tecnológicos.	Diseña módulos de riesgo por procesos (crédito, liquidez, TI, seguridad).	Diseña políticas modulares (ej. Controles por dominios: acceso, continuidad, ciberseguridad).	Implementa soluciones tecnológicas por fases (virtualización, cloud, automatización).
Auditable (cumplimiento con autoridades)	Asegura que las decisiones y políticas permitan rendición de cuentas a SEPS y auditorías externas.	Entrega evidencias a SEPS, auditores internos y externos sobre cumplimiento normativo.	Garantiza reportes financieros auditables y presentados en tiempo y forma.	Mantiene matrices de riesgo auditables y reportes periódicos (SEPS, Comité de Riesgos).	Mantiene documentación del SGSI y registros de controles implementados.	Registra bitácoras técnicas, respaldos y evidencias de operación para auditoría.
Transparencia (trazabilidad)	Exige reportes claros, trazables y comparables.	Asegura trazabilidad de decisiones y de recursos asignados a proyectos y operaciones.	Transparencia en registros contables, soportados con evidencias digitales y físicas.	Documenta todo el ciclo de gestión de riesgos (identificación, control, seguimiento).	Mantiene trazabilidad de incidentes y accesos en sistemas críticos.	Garantiza trazabilidad técnica en cambios de infraestructura, software y configuraciones.

Fuente: SABSA – W101 Diseñando un mundo digital seguro

Una vez establecido la metodología de trabajo, se debe garantizar que las acciones determinadas ayuden al cumplimiento normativo. La SEPS determina que la arquitectura debe contener:

a) Una estrategia de defensa en profundidad;

   La estrategia de defensa en profundidad comprende de múltiples capas de protección que tienen como objetivo salvaguardar la información y la infraestructura tecnológica. El término radica en que si un control falla, existen otros adicionales que pueden hacer frente a una amenaza (por

ejemplo, si el firewall de una institución no aplica correctamente las políticas de bloqueo de páginas no seguras, el antivirus puede ayudar controlar que la navegación sea segura).

b) Controles de flujo de información;

Estos controles tienen como objetivo restringir y monitorear la transmisión de información, para garantizar la confidencialidad, integridad y disponibilidad.

Lo que se logra con el control de flujo de información es evitar fugas de información sensible, asegurando que dicha información fluya solo entre el personal autorizado según los privilegios del usuario. También permite visualizar la trazabilidad de la información (quien accede, quien modifica hacia donde se transfiere). El control más común que se aplica es DLP (Data Loss Prevention).

En la Tabla 21, se presenta un ejemplo de levantamiento de activo de información sensible con la aplicación de un control de flujo de información.

Tabla 21. Matriz e control de flujo de información

Activo de Información Crítico	Flujo de Información	Riesgo Asociado	Control Aplicado	Responsable
Base de datos del Core Financiero	Transmisión de datos entre core y generación de reportes	Fuga, robo o alteración de información sensible	Autenticación de usuarios con MFA, privilegio de acceso en base al rol.	Jefe de Tecnología, administrador de base de datos

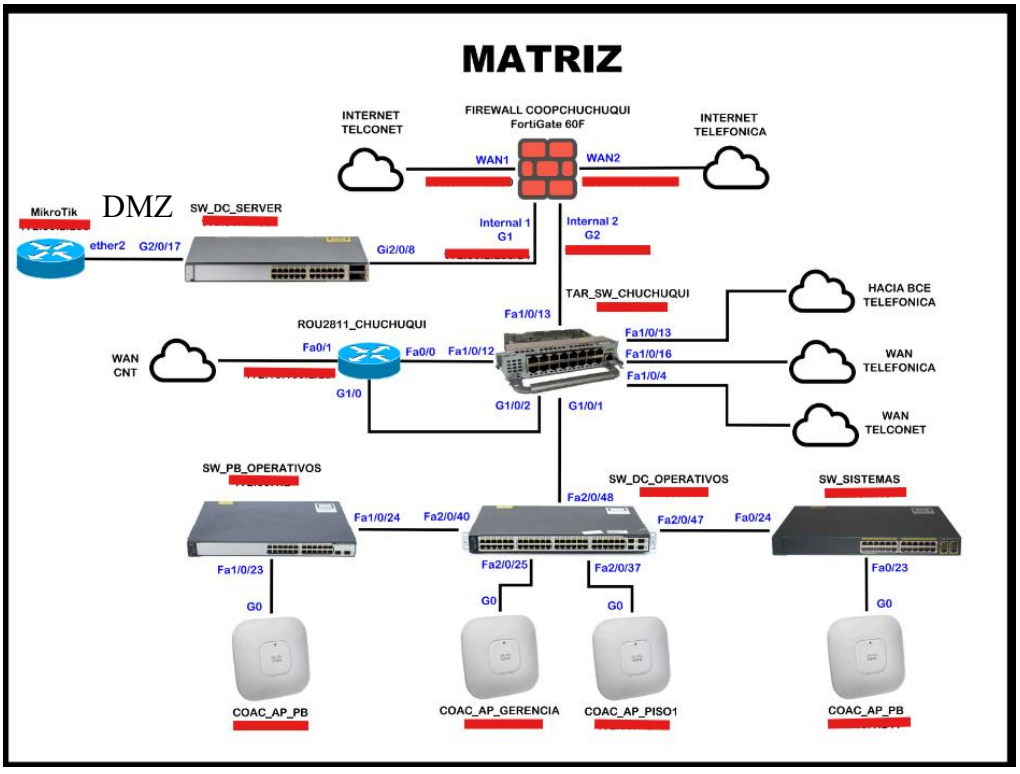
Repositorio centralizado de archivos	Todos los usuarios pueden acceder a la información del repositorio, la cual puede ser sensible, como informes de gestión.	Acceso no autorizado, robo de información	Clasificación de la información, asignación de permisos de solo lectura.	Oficial de Seguridad de la información.

Fuente: Propia

c) Aislamiento y Segmentación;

Este control consiste en separar los recursos del resto de la infraestructura para evitar riesgos como, fuga de información, accesos no autorizados, propagación de malware. El primer paso es establecer de forma adecuada la topología de red, considerando una DMZ como se observa en la figura 62.

Figura 62. Topología de red.



Fuente: Cooperativa Chuchuqui Ltda.

Luego de establecer la topología se debe implementar la segmentación de red a través de VLANs. En la tabla 22 se presenta un ejemplo de segmentación de red.

Tabla 22. Segmentación mediante VLANs

VLAN	Descripción	Red (subnet)	Función o aplicación
1	Datos de usuario final	172.xx.xx.xx/24	Usuarios y estaciones finales
2	Servidores	172.xx.xx.xx/24	Servidores internos críticos
3	Operativos	172.xx.xx.xx/24	Procesos Operativos
4	Invitados	172.xx.xx.xx/24	Red para visitantes, aislada de la red interna
5	Telefonía IP	172.xx.xx.xx/24	Tráfico de voz con calidad garantizada
20	Banco Central del Ecuador	172.xx.xx.xx/24	Conexión exclusiva para el Banco Central
25	Enlace telefónica	172.xx.xx.xx/24	Enlace WAN hacia telefónica
30	Enlace telconet	172.xx.xx.xx/24	Enlace WAN hacia telconet

Fuente: propia

d) Monitoreo y detección;

El control de monitoreo y detección se lo analiza detalladamente en el punto 3.2.4.2.

e) Técnicas de Cifrado

El control de cifrado se detalla en el punto 3.2.2.4

3.2.4.2. Monitoreo y Detección

Fundamentación Normativa

El monitoreo y detección de eventos tecnológicos constituye un componente esencial de la gestión del riesgo operativo en las entidades financieras. La Resolución SEPS-2022-002 determina la obligación de mantener registros de logs de infraestructura crítica que incluyan, al menos: hora del evento, cambios en permisos de archivos,

periodos de operación, accesos de usuarios, modificaciones de datos, errores, violaciones y tareas fallidas.

Asimismo, la normativa dispone que los registros deben permitir la detección, análisis y depuración de incidentes, de modo que se garantice la trazabilidad de la información y el cumplimiento en auditorías internas y externas.

A nivel internacional, diversos marcos normativos respaldan esta exigencia:

- ISO/IEC 27001 (A.12.4: Registro y monitoreo de eventos).
- COBIT 2019 (DSS05: Gestión de la seguridad de los sistemas y servicios).
- ITIL v4 (Prácticas de gestión de incidentes, problemas y eventos).

Estos lineamientos consolidan la necesidad de contar con un sistema de monitoreo robusto que asegure la confidencialidad, integridad y disponibilidad (CID) de la información crítica.

Marco Conceptual

A continuación, se presentan los conceptos clave necesarios para la comparación de herramientas de monitoreo y detección:

- Monitoreo: proceso de recopilación y análisis de registros (logs) de eventos en sistemas y redes.
- Correlación de eventos: técnica para identificar patrones anómalos en diferentes activos.
- SIEM (Security Information and Event Management): plataforma para centralizar, correlacionar y analizar los registros de logs.

- XDR (Extended Detection and Response): evolución que integra múltiples vectores (endpoint, red, nube).
- SOAR (Security Orchestration, Automation and Response): herramientas que automatizan respuestas ante incidentes.
- OT/NDR: monitoreo en entornos industriales y detección en redes.

Metodología de Evaluación

Para la evaluación de las herramientas de monitoreo y detección se establecieron los siguientes criterios:

- Cumplimiento normativo: Alineación con la Resolución SEPS-2022-002 e ISO 27001.
- Capacidades técnicas: Funcionalidades SIEM, XDR, SOAR, IA/ML, OT/NDR.
- Nivel de apertura: Disponibilidad de soluciones Open Source frente a sistemas cerrados.
- Facilidad de auditoría: Capacidad de generar reportes y dashboards ejecutivos.
- Escalabilidad y soporte: Adaptabilidad al crecimiento institucional.
- Costos asociados: Diferencia entre soluciones open source y comerciales.

La evaluación se basó en documentación oficial de los fabricantes alineada a las exigencias de la SEPS e ISO/IEC 27001.

Análisis Comparativo de Herramientas

En la tabla 23 se presenta la comparación general de capacidades

Tabla 23. Comparación de capacidades de herramientas de monitoreo

Plataforma	**SIEM**	**XDR**	**SOAR**	**IA/ML**	**OT/NDR**
Stellar Cyber	✓	✓	✓	✓	✓
Microsoft XDR	✓	✓	X	✓	X
Palo Alto Cortex	✓	✓	✓	✓	✓
CrowdStrike	X	✓	X	✓	X
IBM QRadar XDR	✓	✓	✓	✓	✓
Elastic Security	✓	✓	X	✓	✓
Sumo Logic	✓	✓	✓	✓	X
SentinelOne	X	✓	X	✓	✓
Trellix	✓	✓	✓	✓	✓
Wazuh (OpenSrc)	✓	✓	X	X	X

Fuente: Propia

En la tabla 24 se presenta la evaluación individual de las herramientas

Tabla 24. Evaluación Individual de herramientas de monitoreo

Plataforma	Descripción Técnica	Fortalezas	Limitaciones
Stellar Cyber	Plataforma comercial con apertura alta; integra SIEM, XDR, SOAR e IA/ML.	Automatización avanzada, dashboards listos, normalización automática de logs, orientada a auditorías.	Requiere inversión en licenciamiento y soporte especializado.
Microsoft XDR	Solución enfocada a entornos Microsoft.	Integración nativa con Microsoft 365 y Azure.	Ecosistema cerrado, limitada apertura, dependencia de Microsoft.
Palo Alto Cortex	SIEM/XDR avanzado con correlación de amenazas.	Alta capacidad de detección y uso de IA.	Costos de licenciamiento elevados.
CrowdStrike	Reconocida en EDR, especializada en endpoint.	Excelente en protección de endpoints y amenazas persistentes.	Limitada correlación de logs y escasa cobertura OT/NDR.
IBM QRadar XDR	Plataforma consolidada y escalable.	Integración robusta, alta escalabilidad, adecuada para corporaciones grandes.	Alto costo y complejidad en implementación.

Elastic Security	Solución open source flexible.	Adaptable, amplia comunidad, costo reducido.	SOAR limitado, requiere expertise técnico avanzado.
Sumo Logic	Servicio cloud-native de monitoreo.	Dashboards potentes, análisis rápido en la nube.	Dependencia total de la nube, puede afectar entornos regulados.
SentinelOne	XDR con fuerte soporte en IA.	Detección automatizada y rápida en endpoints. Cuenta con funciones (SOAR) para automatizar respuestas en endpoints.	Apertura media, menos flexible que alternativas open source.
Trellix	Solución intermedia de seguridad integrada.	Cobertura completa de funciones de seguridad.	Menor presencia en el mercado, ecosistema menos maduro.
Wazuh	Plataforma open source con cobertura SIEM y XDR básica.	Flexible, sin costo de licencias, amplia comunidad, cumplimiento normativo.	Requiere integración externa (TheHive, Cortex) para flujo completo de incidentes.

Fuente: Propia

En la tabla 25 se presenta la comparación de Stellar Cyber vs Wazuh con criterio de cumplimiento normativo.

Tabla 25. Comparación Stellar vs Wazuh

Criterio Normativo	Wazuh (Open Source)	Stellar Cyber (Comercial)
Registro de logs	Centraliza logs de servidores, redes y aplicaciones.	Consolida y normaliza logs automáticamente.
Monitoreo de actividad	Detecta anomalías con reglas y alertas (manual).	Detecta anomalías con IA/ML y dashboards listos.
Gestión de incidentes	Necesita integración externa (TheHive/Cortex).	SOAR integrado, flujo automático de respuesta.
Cumplimiento regulatorio	Incluye plantillas para ISO 27001, PCI DSS, HIPAA, GDPR.	Reportes listos para ISO 27001 y marcos financieros.
Evidencia para auditoría	Exporta reportes de logs y alertas.	Exporta dashboards ejecutivos y reportes técnicos listos.

Fuente: propia

Riesgos en caso de no Implementar

La ausencia de implementación conlleva riesgos significativos, entre los cuales destacan:

- Pérdida de trazabilidad en incidentes: sin registros de logs, es imposible reconstruir ataques o fallas.
- Sanciones regulatorias: incumplir la Resolución SEPS-0116 puede derivar en sanciones económicas o administrativas.
- Incremento del riesgo operativo y reputacional: los incidentes no detectados pueden afectar la confianza de socios y clientes.

Selección y Justificación

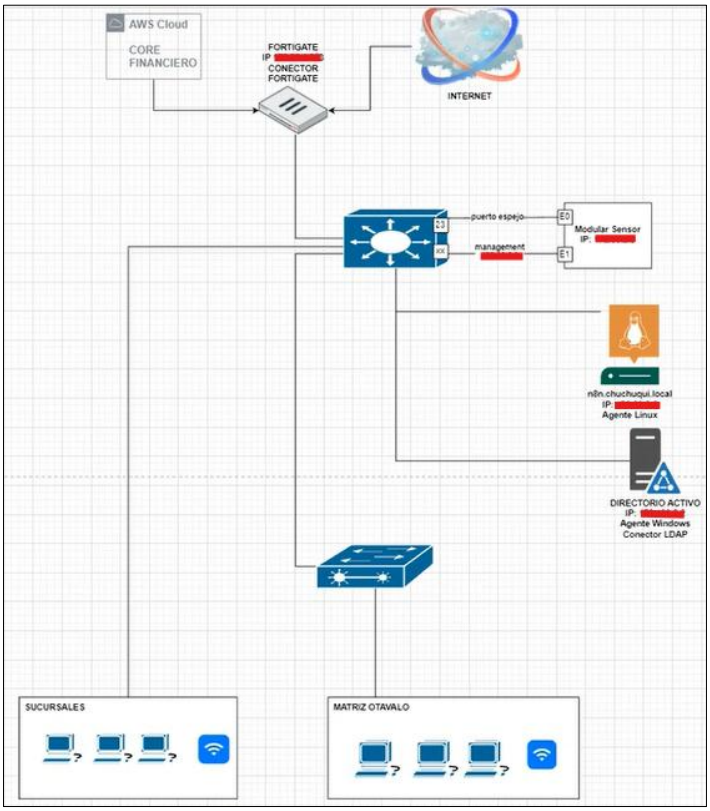
Del análisis realizado se concluye lo siguiente:

- Stellar Cyber es la herramienta más completa y alineada a las necesidades institucionales, ya que:
  - Automatiza la normalización de logs.
  - Integra capacidades de IA/ML para la detección de anomalías.
  - Incorpora SOAR nativamente, reduciendo tiempos de respuesta.
  - Presenta dashboards listos para auditoría, lo que asegura cumplimiento de SEPS e ISO 27001.
  - No obstante, debe considerarse que implica un costo de licenciamiento y soporte más elevado en comparación con soluciones open source.
- Wazuh constituye la mejor alternativa open source, adecuada para escenarios de restricción presupuestaria. Su principal ventaja es la adaptabilidad y el respaldo de una amplia comunidad, además de su alineación a los requerimientos normativos; sin embargo, demanda un esfuerzo técnico adicional al momento de integrar la gestión de incidentes.

Si bien existen las otras soluciones presentadas, que también son muy reconocidas, estas tienen limitaciones respecto a la falta de flexibilidad, la adaptabilidad con otras marcas o precios muy elevados, lo que no se ajusta al contexto de instituciones de segmento 3.

Stellar Cyber para el monitoreo necesita estar implementado en un host con dos interfases de red donde una se conecta directamente al switch core y el otro de la misma manera, pero empleando un puerto espejo como se observa en la topología de la figura 63. Una de sus principales funciones es el NDR (Detección y Respuesta de Red), haciendo un análisis profundo de paquetes desde capa 2 hasta capa 7, observando todas las firmas maliciosas y conexiones, evaluando el comportamiento de todo el tráfico que pasa por el switch core.

Figura 63. Topología de conexión con Stellar Cyber



Fuente: Propia

Stellar Cyber trabaja con un framework propio que establece una cadena de ataque denominada XDR Kill Chain, que refleja cómo va haciendo el progreso del ataque o de los intentos que pueden darse, esta cadena se conforma por cinco etapas como se muestra en la figura 64.

Figura 64. Topología de conexión con Stellar Cyber

Fuente: Propia

La XDR Kill Chaine es un modelo de ataque alineado con el marco MITRE ATT&CK, creado con la finalidad de describir de forma clara y comprensible cada fase de las amenazas actuales. En la plataforma de Stellar Cyber, todas las alertas generadas se vinculan directamente con esta cadena, lo que permite identificar de inmediato la evolución de un ataque y obtener una visión completa de la progresión, en la tabla 26 se presenta un resumen de cada etapa. (Stelar Cyber, 2025)

Tabla 26. Etapas del modelo Kill Chain de Stellar Cyber

Etapa	Descripción	Tácticas / técnicas asociadas	Ejemplos

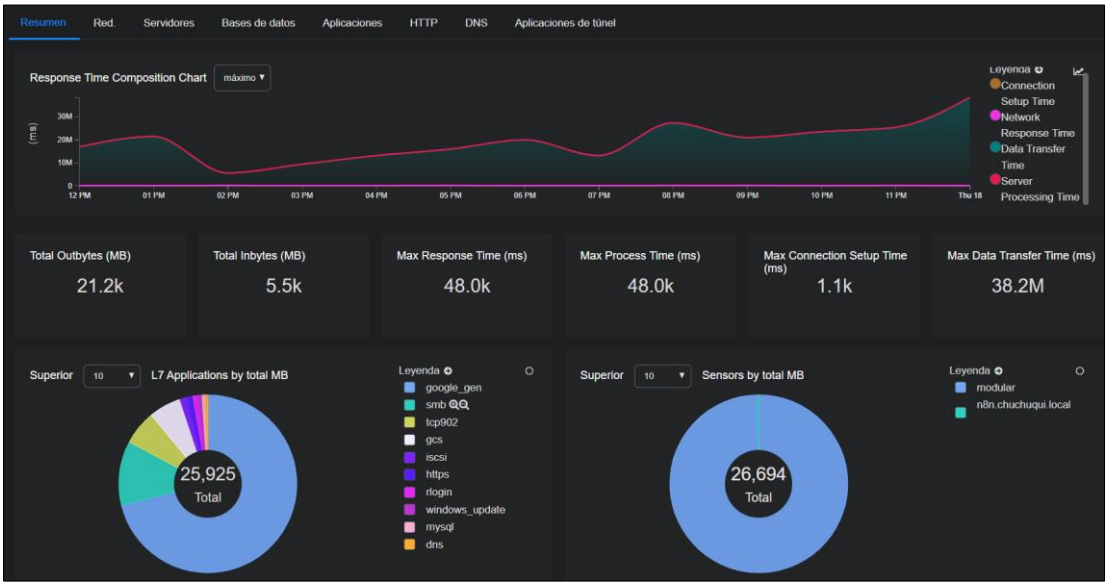
1. Primeros intentos	Es la etapa en la que el atacante hace un reconocimiento de acceso externo. Empieza el ataque desde fuera de la red en busca de vulnerabilidades como puertos abiertos, credenciales expuestas, phishing, etc.	Tácticas MITRE tales como: Reconnaissance, Resource Development, Initial Access, External Credential Access. Las herramientas/alertas de Stellar que participan: External XDR NBA (Network Behavior Analytics), External XDR UBA (User Behavior Analytics), XDR SBA (Sensor Behavior Analytics). (Stellar Cyber Knowledge Base)	Ejemplos: escaneo de puertos externos, intentos de login desde IPs desconocidas con el uso de bibliotecas de password comunes o por defecto, envíos de phishing, uso de herramientas de reconocimiento externo.
2. Posición sostenida	El atacante trata de mantener una conexión estable dentro de la red o sistema, resistiendo a los controles defensivos, y ejecutar código o malware que le permita avanzar con el ataque. No solo acceso momentáneo, sino persistencia.	Tácticas como Persistence, Execution, Defense Evasion, Command & Control. También alertas de XDR Malware, XDR Intel y XDR EBA. (Stellar Cyber Knowledge Base)	Ejemplos: instalación de troyanos que sobreviven reinicios, creación de cuentas para mantener acceso con privilegios elevados, establecer comunicación hacia servidores de control.
3. Exploración	Una vez que el atacante está dentro, analiza el entorno interno: descubre recursos, mapea la red interna, identifica activos críticos. Esto con la finalidad de preparar el terreno para acciones posteriores.	Tácticas MITRE como Discovery, Collection; alertas relacionadas con Internal NBA (Network Behavior Analytics).	Ejemplos: escaneo interno para encontrar servidores vulnerables, copia de archivos, mapeo de red interna, recolección de información sobre configuraciones o permisos.
4. Propagación	Durante esta etapa, el atacante realiza desplazamiento lateral por la red, para conseguir más privilegios y comprometer otros equipos adicionales. No se conforma con una simple exploración, sino que desea tomar el control de recursos críticos.	Tácticas como movimiento lateral, Escalada de privilegios, Acceso a credenciales internas. Alertas con Internal XDR Malware, Internal UBA, etc.	Ejemplo: uso de credenciales robadas para ingresar a otros servidores, propagación de malware interno, movimientos entre dominios, escalación de privilegios para tener mayor control.

5. Exfiltración e impacto	Es la fase final, donde el atacante intenta robar datos importantes, filtrar información sensible o causar daño (ransomware, destrucción de datos, sabotaje), provocando una mala reputación.	Tácticas MITRE: Exfiltration. Alertas relacionadas con acciones finales como anomalías de archivos, copias externas, cifrado de datos, uso de servicios externos para fuga de información.	Ejemplos: Publicación de datos sensibles, cifrado de archivos para pedir rescate, destrucción o modificación de archivos críticos, denegación de servicio.

Fuente: Stellar Cyber

Stellar Cyber permite visualizar el estado de toda la red, servidores, Bases de datos, aplicaciones, HTTP, DNS y aplicaciones de túnel como se observa en la figura 65, todo esto en base al tráfico que pasa por el switch core, pero también tiene la factibilidad de conectarse con otras herramientas como antivirus, firewall lo que permite tener una mejor perspectiva de lo que está pasando en la red y poder realizar una correlación de eventos.

Figura 65. Resumen del comportamiento de red en Stellar Cyber

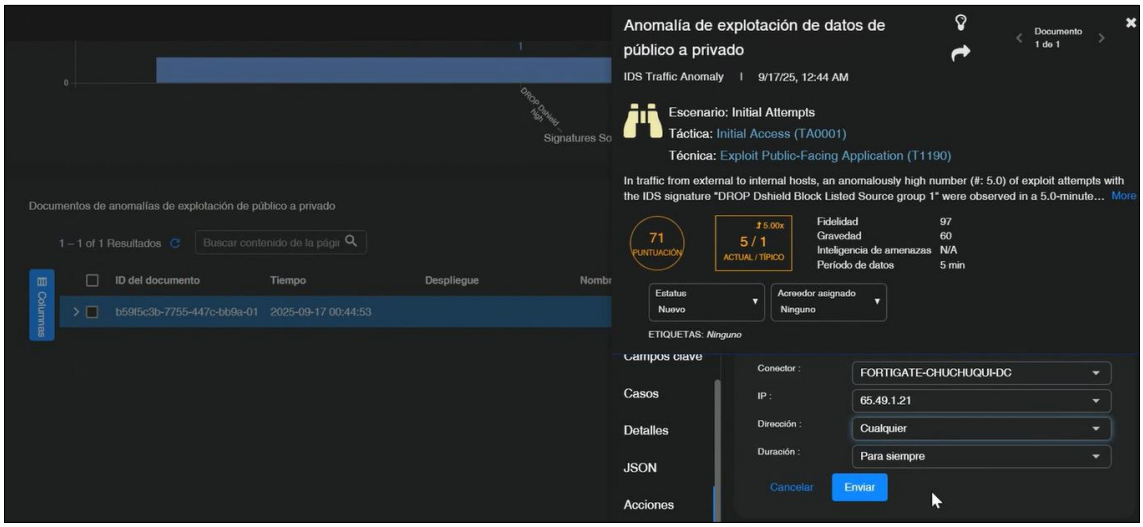


Fuente: Propia

Otra ventaja de Stellar es que, al interconectarse con el firewall, es capaz de crear reglas de protección en caso de identificar alguna amenaza, como es el bloqueo de IPs que están intentando filtrarse en la red, las cuales ya se encuentran identificadas con

mala reputación. En la figura 66 se puede observar un ejemplo creación de una regla de bloqueo de una IP desde Stellar Cyber aplicando al firewall.

Figura 66. Creación de regla de bloqueo desde Stellar Cyber



Fuente: Propia

La documentación relevante para la implementación de controles de seguridad alineado el cumplimiento de la resolución de la SEPS 2022-002 se puede encontrar el siguiente enlace: https://drive.google.com/drive/folders/1UWmONdZVM_XylCo6o1D3QTdQmZ8MqROT?usp=drive_link

CAPITULO V

4. EVALUACIÓN DE RESULTADOS DE IMPLEMENTACIÓN

La metodología utilizada para la evaluación es Mehari, cuya gestión consiste en identificar las situaciones riesgo y tomar decisiones específicas que se adapten a cada situación. (CLUSIF, 2010)

Para cumplir con lo establecido en la metodología se presenta una matriz de evaluación de cada control de la norma de Seguridad de la información SEPS 2022-002, y se analiza el nivel de madurez de implementación (No existe, inicial, parcialmente, definido, administrado, optimizado). En base a estos 5 criterios se determina la madurez del control en la escala del 0 al 5 como se indica en la Tabla 27.

Tabla 27. Niveles de madurez de implementación

% Cumplimiento	Nivel de Madurez	Descripción
0% al 9%	0	**0. No existe. -** Carencia completa de cualquier proceso o documentación evidenciable. La institución no ha reconocido siquiera la urgencia de implementación
10% al 30%	1	**1. Inicial. -** Existe evidencia de que la institución ha reconocido la urgencia de implementación, se presenta una planificación de lo que va a implementar. El enfoque administrativo puede ser desorganizado.
31% al 50%	2	**2. Parcialmente. -** los procesos se encuentran parcialmente implementados, no se encuentra una documentación completa por lo que no se puede realizar pruebas, evaluaciones o mediciones de la implementación.
51% al 70%	3	**3. Definido. -** Los procedimientos están documentados completamente, sin embargo, existen aspectos de mejora o no se ha dado un seguimiento de cumplimiento. Aunque el control no es tan efectivo, ayuda a formalizar o fortalecer las prácticas existentes.
71% al 94%	4	**4. Administrado. -** Los procedimientos pueden ser monitoreados y medidos, permitiendo aplicar correcciones cuando no se cumplen de manera efectiva. Se promueve la mejora continua, pero el control no es completamente efectivo.
94% al 100%	5	**5. Optimizado. -** Los controles alcanzan un nivel de mejores prácticas, con base en mejoras continuas y evaluación de resultados. Se integran herramientas para automatizar trabajos, mejorar la calidad y la eficiencia, lo que permite a la institución adaptarse con rapidez a los cambios tecnológicos o normativos.

Fuente: Propia

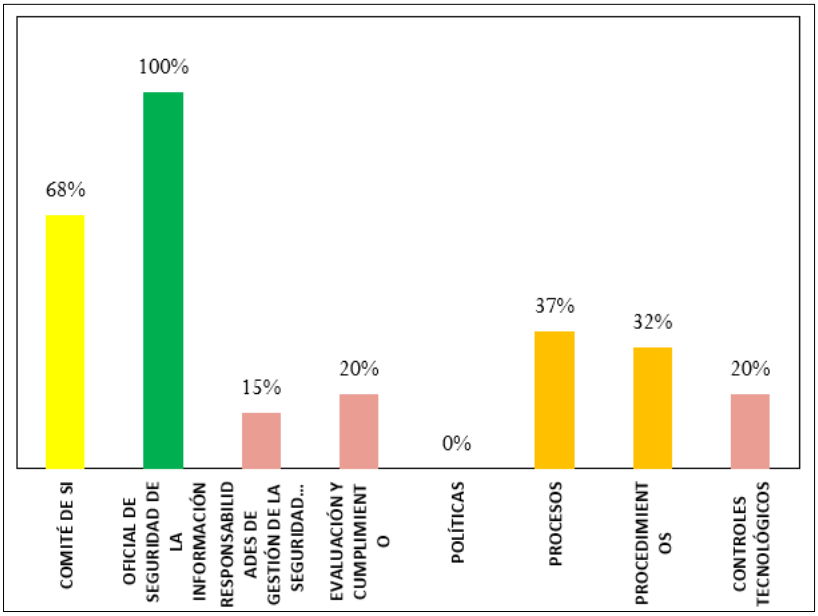
Con base a la tabla de los niveles de madurez de implementación de los controles de seguridad, se evalúa en primera instancia el estado inicial del caso de estudio, considerando todo lo establecido en la normativa de la SEPS 2022-002. Esta evaluación inicial se encuentra en el Anexo IX. Sin embargo, en la tabla 28 y figura 67 se presenta un resumen de la evaluación inicial.

Tabla 28. Resumen de estado inicial de implementación

# Sección	Nombre	% implementación
1	COMITÉ DE SI	68%
2	OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	100%
3	RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	15%
4	EVALUACIÓN Y CUMPLIMIENTO	20%
5	POLÍTICAS	0%
6	PROCESOS	37%
7	PROCEDIMIENTOS	32%
8	CONTROLES TECNOLÓGICOS	20%
TOTAL		**36%**

Fuente: Propia

Figura 67. Diagrama de barras de implementación inicial



Fuente: Propia

Mehari menciona que es importante realizar una identificación de riegos, identificando amenazas y vulnerabilidades dentro de escenarios determinados, para ello se ha realizado un levantamiento de las amenazas o vulnerabilidades asociadas,

considerando la causa de donde se deriva la estimación de la probabilidad, impacto y valoración del riego. La matriz de cálculo de riesgo inicial se encuentra en el Anexo X.

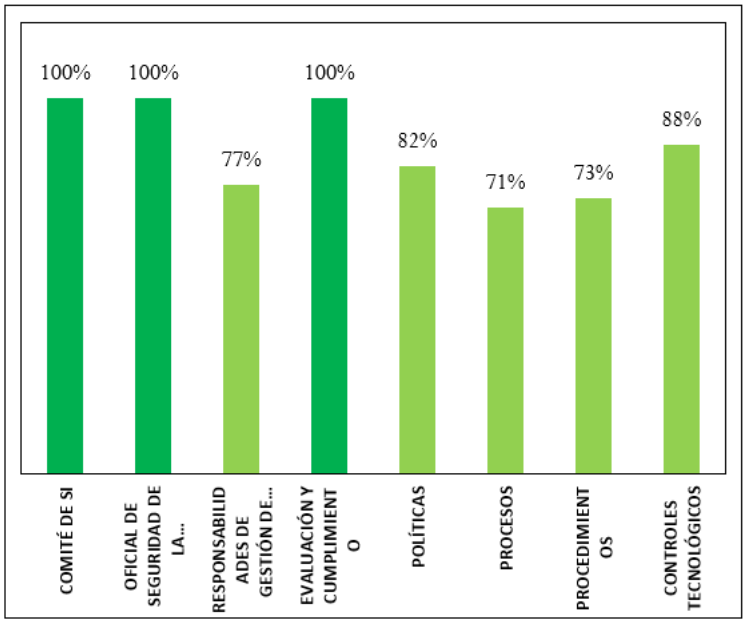
Una vez que se identifica los riesgos se empieza a trabajar en la implementación de los controles de seguridad dando una prioridad a las actividades que generan in riesgo muy alto y alto. De la implementación realizada se determina la evaluación final de implementación de cada control. La evaluación se encuentra en el Anexo XI, sin embargo, en la Tabla 29 y Figura 68 se muestra un resumen de implementación final con una comparativa de estado inicial.

Tabla 29. Resumen de estado final de implementación

# Sección	Nombre	% implementación inicial	% implementación Final
1	COMITÉ DE SI	68%	100%
2	OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	100%	100%
3	RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	15%	77%
4	EVALUACIÓN Y CUMPLIMIENTO	20%	100%
5	POLÍTICAS	0%	82%
6	PROCESOS	37%	71%
7	PROCEDIMIENTOS	32%	73%
8	CONTROLES TECNOLÓGICOS	20%	88%
TOTAL		**36%**	**84%**

Fuente: Propia

Figura 68. Diagrama de barras de implementación final



Fuente: Propia

Para finalizar la evaluación, se determina el riego inherente obtenido con la implementación de los controles, la matriz de riesgo final se encuentra en el Anexo XII.

5. CONCLUSIONES

El presente trabajo de investigación es de gran utilidad para el cumplimiento de la normativa de seguridad de la información SEPS 2022-002, gracias al diseño de un framework de implementación de controles de seguridad fundamentado en normativas nacionales e internacionales, marcos de referencia de buenas prácticas y herramientas previamente evaluadas, permitiendo mejorar la gestión de seguridad de la información para cooperativas de ahorro y crédito de segmento 3.

Se llevó a cabo un estudio documental con la ayuda de la herramienta Parsifal, de donde se genera una matriz que relaciona los documentos relevantes con los controles de seguridad establecidos en el Anexo 1 de la resolución SEPS 2022-002. A

partir de esta relación se permite extraer aportes significativos que fundamentan la estructura del framework propuesto.

El diseño del framework propuesto para la implementación de controles de seguridad se fundamenta principalmente en la metodología MAGERIT v3, pero también se alinea con marcos internacionales como ISO/IEC 27001, ITIL v4 y SABSA, con lo cual asegura un correcto cumplimiento normativo, fomenta una cultura de seguridad de la información y contribuye a la continuidad el negocio.

Se evalúa cualitativamente los resultados de la implementación considerando la metodología Mehari, donde se identifica los riesgos asociados a cada control de seguridad y como estos aportan a reducir el riesgo residual, para ello se compara la situación actual con los resultados obtenidos de la madurez y efectividad de los controles.

6. RECOMENDACIONES

- El framework de implementación de los controles de seguridad, se encuentra generalizado para que se adapte a cualquier cooperativa de segmento 3, por lo que se recomienda que se realice una evaluación individual para que se alinee a las necesidades y objetivos estratégicos de cada institución.
- Se recomienda trabajar con cada unidad institucional para el levantamiento y clasificación de la información, para garantizar que no se omita ningún activo de información de relevancia, ya que cada unidad es responsable de la generación, tratamiento y aseguramiento.
- Se recomienda que el control de accesos físicos de debe coordinar con el Oficial de Seguridad Física y Electrónica, considerando adicionalmente a lo establecido en las normativas de la SEPS los requisitos impuestos por el

COSP, ya que de estos depende la obtención del Certificado de Seguridad y continuidad del funcionamiento de la institución.

- Se recomienda que el plan de concienciación de seguridad de la información se incluya dentro del plan de capacitación institucional, para evitar conflictos con el cronograma de planificación.
- Se recomienda considerar dentro del control de arquitectura segura, aspectos de gobernanza como lo propone la metodología SABSA, y no simplemente lo que se estable en la resolución SEPS 2022-002, para garantizar su alineación con los objetivos estratégicos institucionales.

REFERENCIAS

Andersson, S. (2023). Problems in information classification: insights frompractice. *Information and Computer Security*, 449-462.

Arias, F. G. (2016). *El proyecto de investigación.* Carácas: Editorial Episteme.

Asamblea Nacional Constituyente de la República del Ecuador. (2008). *Constitución de la República del Ecuador.* Quito: Ecuador: Asamblea Nacional Constituyente.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Monetario y Financiero del Ecuador.* Quito: Ecuador: Asamblea Nacional del Ecuador.

AXELOS. (2019). *ITIL Foundation: ITIL 4 Edition.* Norwich: The Stationery Office (TSO).

Axis comunications. (2021). *La digitalización y la ciberseguridad del controlde acceso físico.* Lund.

Bergquist, J.-H., Tinet, S., & Gao, S. (2022). An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality. *Information and Computer Security*, 153-172.

Bergström, E., & Åhlfeldt, R. M. (2014). *Information Classification Issues.* Skövde: University of Skövde.

Caldas Urduy, J. C. (2020). *Evaluación de control de acceso en CORREVAL.* Bogotá: Universidad Piloto de Colombia.

CERTIPROF . (2022). *ISO 27001 INTERNAL AUDITOR / LEAD AUDITOR.* Sunrise.

CLUSIF. (2010). *MEHARI 2010 Risk analysis and treatment Guide.* Paris: rue de Mogador.

COAC CHUCHUQUI LTDA. (2023). *Cooperativa de Ahorro y Crédito Chuchuqui Ltda.* Obtenido de http://www.coopchuchuqui.fin.ec/?page_id=35666

CRESPO OROZCO, J. N. (2022). *Analisis de amenazas y vulnerabilidades de la gestion de procesos del sistema informático en la cooperativa de taxi San Fernando de Babahoyo.* Babahoyo: Universidad Técnica de Babahoyo.

Durán Mongue, E., Santos Pasamontes, M., Salas Gutiérrez, G., & Aragón Ramirez, A. (2023). *Brecha de género en Ciencia y Tecnología en Costa Rica.* San José: CONARE - PEN.

García, A. &. (2021). *Fundamentos del análisis de datos en investigación.* Editorial Ciencias Sociales.

Grupo ESG Innova. (23 de 09 de 2021). *pmg-ssi*. Obtenido de ESGINNOVA GROUP: https://www.pmg-ssi.com/2021/09/metodologia-mehari-para-el-analisis-de-riesgos-en-sgsi/

ISOTools. (26 de Agosto de 2021). *Seguridad de la Información*. Obtenido de Seguridad de la Información y Ciberseguridad: https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/

López, A., & Fernandez, M. (2022). *Metodologías avanzadas en la recolección y análisis de datos.* Editorial Académica.

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Ministerio de Telecomunicaciones. (2020). *Guía para la Gestión de Riesgos de Seguridad de la Información.* Quito.

MSB – Myndigheten för samhällsskydd och beredskap. (25 de 06 de 2024). *Metodstödet för systematiskt informationssäkerhetsarbete*. Obtenido de https://metodstod-informationssakerhet.msb.se/sv/utforma/klassningsmodell/

Mucha Hospinal, L. F., Chamorro Mejía, R., Oseda Lazo, M. E., & Alania Contreras, R. D. (2021). Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado. 52-53.

Naciones Unidas Ecuador. (2021). *NACIONES UNIDAS ECUADOR*. Obtenido de https://ecuador.un.org/es/sdgs/16

National Institute of Standars and Technology (NIST). (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: MD 20899-8930.

Nuñez Santamaría, A. C. (2022). *Plan De Contingencia Informático Basado En La Norma ISO 24762:2008 Para El Departamento De Tecnologías De La Información Del Gobierno Autónomo Descentralizado De La Municipalidad De Ambato.* Ambato: Universidad Técnica de Ambato.

Paltín León , M. R. (2022). *Aplicabilidad del sistema de gestión de calidad ISO 9001:2015 en los procesos agregadores de valor de los registros de la propiedad del Ecuador.* Quito: Universidad Central del Ecuador.

Parsifal. (05 de Septiembre de 2021). *About Parsifal*. Obtenido de https://parsif.al/about/

Ri, E. (12 de 02 de 2025). *GRC Solution ERAMBA*. Obtenido de https://www.eramba.org/

SABSA Institute. (2018). *Architecting a Secure Digital World.* Hove: The SABSA Press™.

Salazar Méndez, Y. (02 de octubre de 2022). *PRIMICIAS*. Obtenido de https://www.primicias.ec/noticias/firmas/estadisticas-censo2022-afroecuatorianos-inec/

SEPS. (2022). *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.* Quito.

SEPS. (2023). *SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA*. Obtenido de https://www.seps.gob.ec/institucion/que-es-la-seps/

Subsecretaria de Desarrollo Regional y Administrativo del Gobierno de Chile. (25 de 07 de 2023). POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN. *Resolución Gubernamental*. Santiago, Chile.

Superintendencia de Economía Polpular y Solidaria. (06 de 07 de 2024). NORMA DE CONTROL PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO. Quito, Pichincha, Ecuador.

Superintendencia de Economía Popular y Solidaria. (2018). *Norma de control respecto de la Seguridad Física y Electrónica.* Quito.

Vacca, J. R. (2020). *Computer and Information Security Handbook.* Burlington: Morgan Kaufmann.

Zamora Pomaquiza, D. J. (2023). *AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SERVICIOS TECNOLÓGICOS EN EL GADIPCS SUSCAL.* Cañar: UNIVERSIDAD CATÓLICA DE CUENCA.

ANEXOS

ANEXO I

Informe de resultado de Parsifal

CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN SEPS 2022-002

Dony Reina

CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN SEPS 2022-002 PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO DE SEGMENTO 3 MEDIANTE EL DISEÑO DE UN FRAMEWORK UTILIZANDO LA METODOLOGÍA MAGERIT

Planning

Evaluar controles de seguridad de acuerdo con normativas y herramientas establecidas en un framework para el cumplimiento de la normativa de Seguridad de la Información SEPS 2022-002, a partir del enfoque cualitativo aplicada en una Cooperativa de Ahorro y Crédito de Segmento 3

PICOC

- **Population:** Information security, financial institutions, financial sector, Risk management
- **Intervention:** Magerit
- **Comparison:** ISO 27001
- **Outcome:** evaluation of security controls
- **Context:** Information security management in financial institutions

Research Questions

1. What information security guidelines do the regulations for financial institutions have?
2. which information security risk management methodologies are most suitable for financial institutions?
3. How to evaluate the effectiveness of the implemented security controls?

Keywords and Synonyms

Keyword	Synonyms

Search String

"information security" AND ("financial institutions" OR "bank" OR "financial sector" OR "finance") AND ("risk management" OR "security risk management") OR "MAGERIT"

Sources

- IEEE Digital Library (http://ieeexplore.ieee.org)
- Science@Direct (http://www.sciencedirect.com)
- Scopus (http://www.scopus.com)

Selection Criteria

Inclusion Criteria:

- Related content

Exclusion Criteria:

- Before 2020
- Not related

Quality Assessment Checklist

Questions:

- What information security guidelines do the regulations for financial institutions have?
- which information security risk management methodologies are most suitable for financial institutions?
- How to evaluate the effectiveness of the implemented security controls?

Answers:

- Yes
- Partially
- No

Data Extraction Form

- What information security guidelines do the regulations for financial institutions have?
- which information security risk management methodologies are most suitable for financial institutions?
- How to evaluate the effectiveness of the implemented security controls?

Conducting

Digital Libraries Search Strings

Imported Studies

- **IEEE Digital Library:** 26
- **Science@Direct:** 70
- **Scopus:** 81

ANEXO II

Tabla 30. Documentos Seleccionados

CÓDIGO	TÍTULO	AUTOR	INFORMACIÓN RELEVANTE
A1	Norma de control respecto a la seguridad de la información en las entidades del sector financiero popular y solidario.	Superintendencia de Economía Popular y Solidaria (SEPS).	Esta normativa tiene por objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y la empresas, deben definir e implementar con el fin de resguardar y proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad.
A2	Magerit - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los sistemas de Información	Ministerio de Haciendas y Administraciones Públicas de España	MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información
A3	Guía para la realización de Evaluaciones de Riesgos NIST 800-30	National Institute of Standards and Technology (NIST)	La evaluación de riesgos es un componente clave de un proceso holístico de gestión de riesgos para toda la organización. Los procesos de gestión de riesgos incluyen: enmarcar el riesgo, evaluación del riesgo, responder al riesgo, y seguimiento del riesgo.
A4	ISO/IEC 27001: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.	ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	Proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.
A5	ISO/IEC 27005: Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de riesgos de seguridad de la información.	ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	Contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI)

A6	ISO/IEC 27005: Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de riesgos de seguridad de la información.	ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	Contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI)
A7	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	Subsecretaria de Desarrollo Regional y Administrativo – Gobierno de Chile	Asegurar el conocimiento y acceso, a través de los medios con que cuente la Institución, a la Política General de Seguridad de la Información y sus instrumentos asociados, de manera comprensible y pertinente a la labor de todas las personas involucradas en el sistema. Ejecutar, aplicar e implementar medidas acordes a las directrices gubernamentales en materia de ciberseguridad. (Subsecretaria de Desarrollo Regional y Administrativo del Gobierno de Chile, 2023)
A8	Klassningsmodell	MSB – Myndigheten för samhällsskydd och beredskap	Esta guía le ayudará a diseñar un modelo para clasificar la información. La clasificación ayuda a una organización a valorar su información de manera uniforme según los requisitos internos y externos de confidencialidad, precisión y disponibilidad. Los resultados de la clasificación, junto con la evaluación de riesgos, proporcionan una base para seleccionar medidas de seguridad suficientes para la información. (MSB – Myndigheten för samhällsskydd och beredskap, 2024)
A9	ISO/IEC 22301:2025 Ciberseguridad: preparación de las tecnologías de la información y la comunicación para la continuidad del negocio	ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission)	Las interrupciones de los servicios de TIC, afectan la continuidad de las operaciones intitucionales. Por lo tanto, la gestión de las TIC y la continuidad de negocio relacionada, y la preparación de las tecnologías de seguridad, constituyen un componente clave para mantener la continuidad del negocio.
A10	SABSA Arquitectura de Seguridad Empresarial Aplicada de Sherwood	SABSA Institute	SABSA es una metodología de arquitectura segura originaria de Reino Unido, pero es reconocida a nivel mundial con una aceptación de alrededor de 50 países. SABSA presenta perspectivas diferentes de las partes interesadas dentro de la institución en relación con la seguridad de la información
A11	ITIL v4	Axelos Global Best Practice	ITIL v4 es un marco de buenas prácticas enfocado en la gestión de servicios de TI. Proporciona lineamientos tecnológicos que se adaptan con las necesidades del negocio. Su fundamenta en el ciclo de vida del servicio y en el valor del sistema de servicio

A12	RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116	Superintendencia de Economía Popular y Solidaria (SEPS).	tiene por objeto normar la administración de riesgo operativo, contempla muchos factores tecnológicos y no tecnológicos que pueden generar riesgo operativo.
A13	GLPI (Gestionnaire Libre de Parc Informatique)	GLPI (Gestionnaire Libre de Parc Informatique)	Es un software de gestión de servicios de código abierto, permite gestionar hardware, software y centros de datos. Permite recopilar la información completa del inventario tecnológico a través de un agente.
A14	ERAMBA	ERAMBA	Eramba es una plataforma de gestión de gobierno, riesgo y cumplimiento (GRC). Es de código abierto, su implementación y administración se adapta a marcos de referencia como MAGERIT, ISO/IEC 27001, ISO 9001, entre otros.
A15	Stellar Cyber	Stellar Cyber	es una plataforma de ciberseguridad tipo Open XDR (Extended Detection and Response) que integra en un único ecosistema la detección, correlación y respuesta frente a amenazas

Fuente: (Google Scholar), (INEN), (SCOPUS), SEPS

ANEXO II

Tabla 31. Matriz de investigación

Framework/Artículo / Tema	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15
Seguridad de la información	X	X	X	X		X			X	X	X	X		X	X
Clasificación de información	X	X	X	X			X	X	X		X			X	
Gestión de riesgos de seguridad de la información.	X	X	X	X	X	X					X	X	X	X	
Control de accesos físicos y tecnológicos	X		X	X								X			
Gestión de incidentes	X		X	X	X						X	X	X	X	X
Gestión de software	X			X	X						X	X	X		
Gestión de infraestructura tecnológica	X		X	X	X	X			X		X	X	X	X	X
Seguridad física	X	X	X	X								X			
Gestión con terceros	X	X	X	X							X	X	X	X	

Ciberseguridad	X			X							X			X	
Identificación de los procesos agregadores de valor	X		X	X					X						
Auditorias informáticas	X		X	X	X									X	
Plan de mitigación de los hallazgos	X		X	X	X									X	
Procedimiento de adquisición, desarrollo de software y mantenimiento de sistemas informáticos, hardware y servicios	X		X	X							X	X			
Planes, procesos y procedimientos de Contingencia tecnológica y continuidad del negocio	X		X	X	X			X	X		X	X			
Identificación de tipos de información	X	X		X	X	X								X	
Inventario de activos de información.	X	X		X	X	X		X			X	X	X	X	
Clasificación de activos de información.	X	X		X	X	X		X			X	X	X	X	
Análisis y evaluación de riesgos de las aplicaciones, servicios y activos de seguridad de la información.	X		X	X	X	X					X	X			
Procedimientos y mecanismos de resguardo de información física y digital, sensible o crítica	X		X	X	X							X			
Plan de capacitación de seguridad de la Información.	X		X	X	X							X			
Procedimiento de control de accesos	X		X	X	X										
Procedimiento para gestión de la configuración	X			X	X						X				
Procedimiento para gestión de cambios y control de versiones en los servicios de tecnologías de la información.	X		X	X							X	X			
Arquitectura segura	X			X						X	X				X
Monitoreo y detección	X			X								X			X

ANEXO III

Validación del Instrumento de Investigación

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN
(CUESTIONARIO - ENCUESTA)

Proyecto:	CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN SEPS 2022-002 PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO DE SEGMENTO 3
Autor:	Dony Anderson Reina López
Objetivo:	Obtener la opinión de profesionales que trabajan en el campo de la Seguridad de la Información dentro del sector financiero, específicamente expertos que laboran para instituciones que se encuentran bajo la regulación de la Superintendencia de Economía Popular y Solidaria cuyo enfoque es la Normativa de Seguridad de la Información SEPS 2022-002

Fecha de envío para la evaluación del experto:	09 de febrero de 2023
Fecha de revisión del experto:	7 de marzo de 2024

En la siguiente matriz marque con una X el criterio de evaluación según corresponda en cada ítem. De ser necesario realice la observación en el apartado correspondiente.

INSTRUMENTO DE EVALUACIÓN CUALITATIVO			
ITEMS	**CRITERIOS DE EVALUACIÓN**		
	MUCHO	**POCO**	**NADA**
Instrucción breve, clara y completa.	X		
Formulación clara de cada pregunta.	X		
Comprensión de cada pregunta.	X		
Coherencia de las preguntas en relación con el objetivo.	X		
Relevancia del contenido	X		
Orden y secuencia de las preguntas	X		
Número de preguntas óptimo	X		

Observaciones:

_____

_____

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

A continuación, marque con una X en el criterio de evaluación según el análisis de cada pregunta que conforma el cuestionario, las cuales se encuentran representadas en el siguiente instrumento de evaluación como ítem. De ser necesario realice la observación en el casillero correspondiente.

INSTRUMENTO DE EVALUACION CUANTITATIVO				
CRITERIOS DE EVALUACIÓN				OBSERVACIONES
Ítem	Dejar	Modificar	Eliminar	
1	X			
2	X			
3	X			
4	X			
5	X			
6	X			
7	X			
8	X			
9		X		Si esta "En desacuerdo" ó "Muy en desacuerdo", indicar el porqué
10		X		Si no está de acuerdo, indicar el porqué
11		X		Si el cumplimiento es "Medianamente Suficiente", "Poco" y "Muy Poco", explicar el porqué
12	X			
13	X			
14	X			
15	X			
16	X			

Firma del Evaluador
C.C.: 1714425392

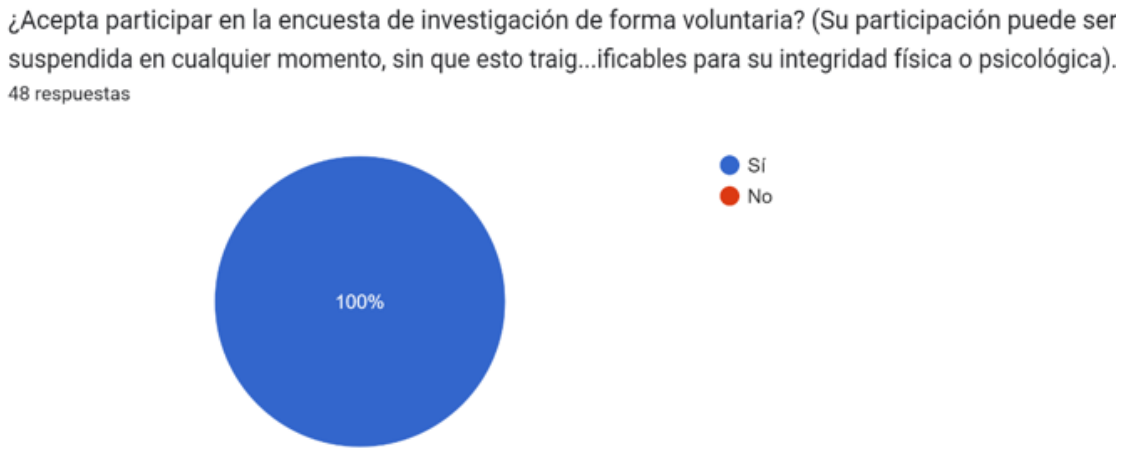
Apellidos y nombres completos	CAIZA VILLAGÓMEZ KARLA FERNANDA
Título académico	ING. SISTEMAS
Institución de Educación Superior	UNIVERSIDAD ISRAEL
Correo electrónico	karlacaiza@hotmail.com
Teléfono	0995812399

ANEXO IV

Análisis de resultados de la encuesta

La primera pregunta se trata de la aceptación de los profesionales para participar en la encuesta de forma libre y voluntaria en la que se obtiene un resultado del 100% de aceptación, lo que no dice que todos los participantes no tienen ninguna objeción sobre en cooperar con el tema de investigación. Esto da a entender que la trama de la encuesta es de interés para los profesionales de seguridad de la información del sector financiero como se puede observar en la figura 69 y tabla 32.

Figura 69. Resultados de la pregunta 1



Fuente: Autor

Tabla 32. Pregunta 1

Pregunta 1	**Frecuencia**	**Porcentaje**
Si	48	100%
No	0	0%
Total	**48**	**100%**

Elaborado por: El autor

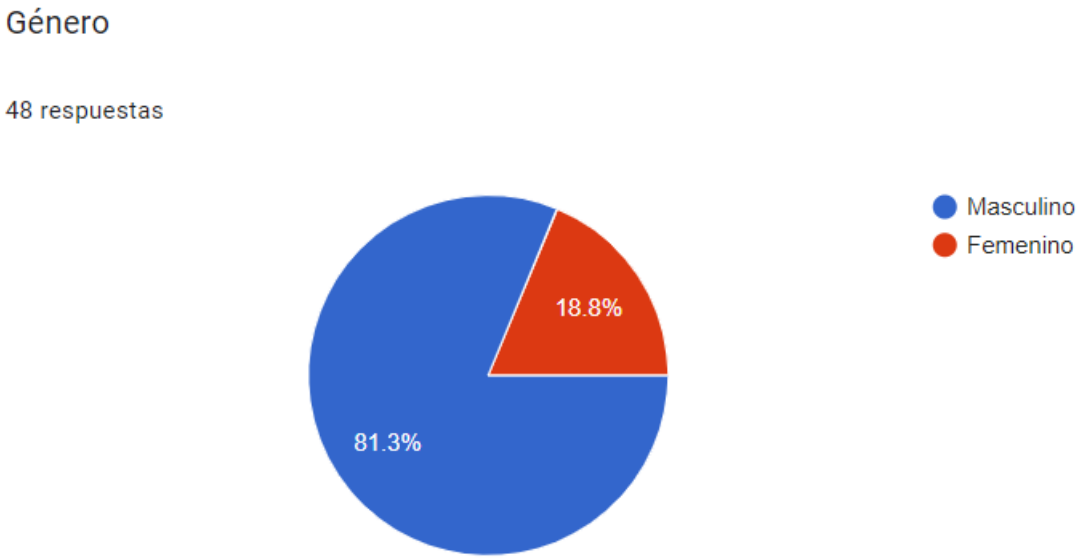
La segunda pregunta es respecto al género de los participantes la cual esta orientada a identificar la diversidad dentro del campo de la seguridad de la información, sabiendo que dentro de las carreras técnicas o de ingeniería, de forma histórica se ha tenido una participación baja del sector femenino.

En los resultados de la pregunta dos que se refleja en la figura 70 y tabla 33, se muestra que los profesionales dedicados a la seguridad de la información del sector financiero encuestado en un 18.8% son mujeres, frente a un 81.2% de hombres, lo que nos da a entender que los resultados son similares con la tendencia global en ramas de

tecnología, un claro ejemplo de esta investigación sobre la brecha de participación de las mujeres a nivel profesional en la TIC's menciona (Durán Mongue, Santos Pasamontes, Salas Gutiérrez, & Aragón Ramirez, 2023) que menciona que el 31.7% de participación femenina se encuentra entre las disciplinas de ciencia y tecnología.

Estos resultados deben ser tomados en cuenta para poder generar estrategias que incentiven a la diversidad e inclusión que fomente a aumentar la participación de mujeres en la seguridad de la información.

Figura 70. Resultados de la pregunta 2.



Fuente: Autor

Tabla 33. Pregunta 2

Pregunta 2	**Frecuencia**	**Porcentaje**
Masculino	39	18.75%
Femenino	9	81.25%
Total	**48**	**100%**

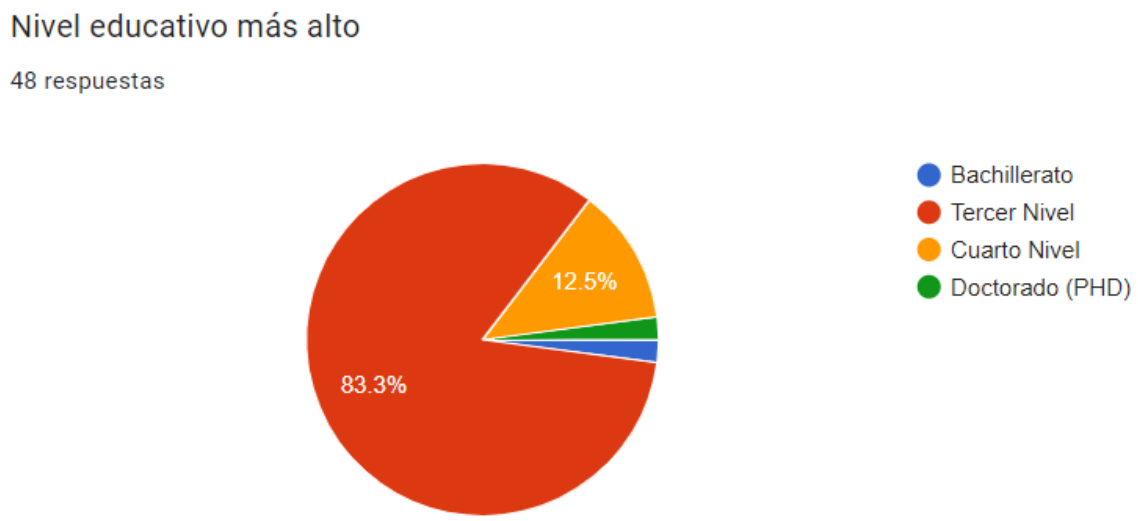
Elaborado por: El autor

La tercera pregunta es respecto al nivel educativo que tienen los profesionales o encargados de seguridad de la información. Esta pregunta hace referencia a la exigencia que se presenta en la normativa SEPS 2022-002 que menciona que los OSI deben tener como mínimo un título de tercer nivel.

El nivel académico de los oficiales de seguridad se puede usar como indicados para evaluar las competencias técnicas que poseen lo que es muy importante en el sector financiero. Para ello se presentan los siguientes resultados como se indica en la figura

71 y tabla 34, donde se aprecia que la mayoría posee un título de tercer nivel (83.3%), seguido de un 12.5% que tienen un título de cuarto nivel, un 2.1% posee un Doctorado que es el nivel académico más alto, pero también se observa que existe un 2.1% que solo tiene Bachillerato. Este último se encuentra incumpliendo lo que se menciona en la normativa, por lo que se espera que sea un profesional que se encuentre próximo a la obtención de un título de tercer nivel, ya que la experiencia y cursos de capacitación no son válidos para el cumplimiento de esta exigencia.

Figura 71. Resultados de la pregunta 3.



Fuente: Autor

Tabla 34. Pregunta 3

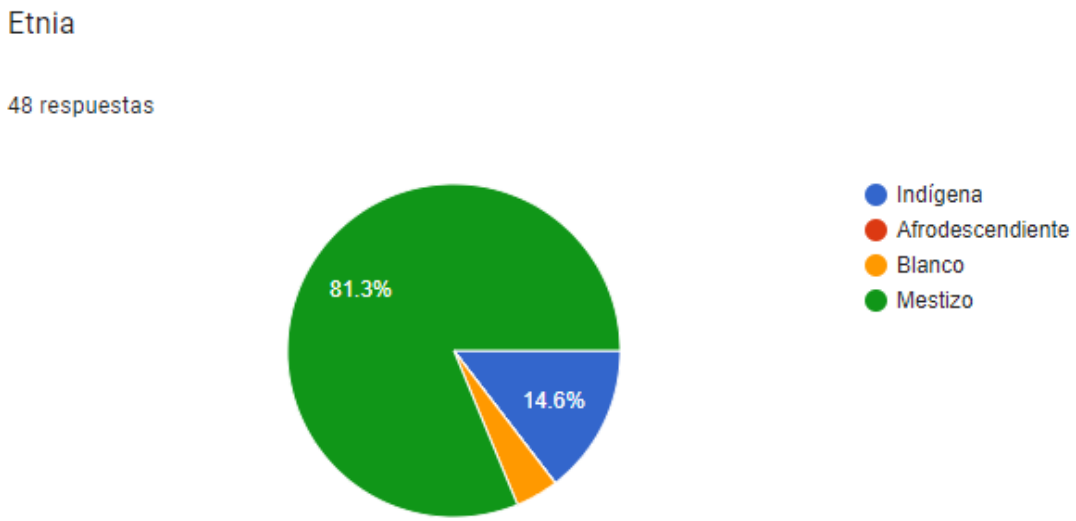
Pregunta 3	**Frecuencia**	**Porcentaje**
Bachillerato	1	2.08%
Tercer Nivel	40	83.34%
Cuarto Nivel	6	12.5%
Doctorado (PHD)	1	2.08%
Total	**48**	**100%**

Elaborado por: El autor

La cuarta pregunta hace referencia a la Etnia de los oficiales de seguridad, que al igual a la pregunta 2, se pretende evaluar la diversidad e inclusión social en temas de tecnología, según los resultados que se muestran en la imagen 72 y tabla 35, se observa que si existe diversidad de etnias en base al porcentaje de nuestra cultura, sin embargo existe un 0% para personas afrodescendientes, lo que se puede justificar que la muestra (48 profesionales) no pudo ser lo suficiente grande para poder establecer la diversidad completa en el campo, también se debe considerar que el porcentaje de las personas

afrodescendientes en el Ecuador según (Salazar Méndez, 2022) es alrededor de 4.8%, que es un porcentaje muy bajo.

Figura 72. Resultados de la pregunta 4.



Fuente: Autor

Tabla 35. Pregunta 4

Pregunta 4	**Frecuencia**	**Porcentaje**
Indígena	7	14.58%
Afrodescendiente	0	0.00%
Blanco	2	4.17%
Mestizo	39	81.25%
Total	**48**	**100%**

Elaborado por: El autor

La quinta pregunta está orientada a saber si las personas a las cuales va dirigida la encuesta concuerdan con el sector de estudio establecido en el alcance de la investigación como se observa en la figura 73 y tabla 36, se obtiene que el 100% de los profesionales encuestados pertenecen a instituciones financieras del segmento 3 cumpliendo en su totalidad con la muestra requerida.

Figura 73. Resultados de la pregunta 5.

Fuente: Autor

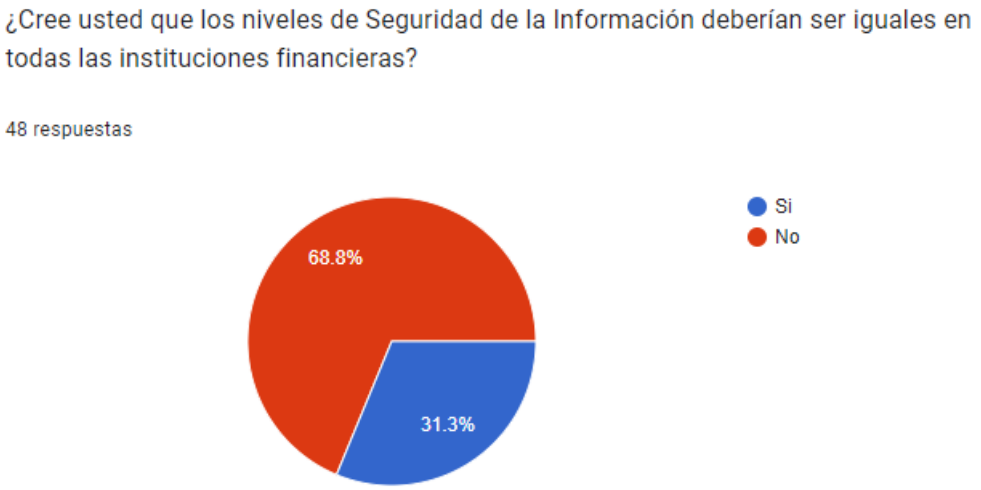
Tabla 36. Pregunta 5

Pregunta 5	**Frecuencia**	**Porcentaje**
Segmento 1	48	100.00%
Segmento 2	0	0.00%
Segmento 3	0	0.00%
Segmento 4	0	0.00%
Segmento 5	0	0.00%
Total	**48**	**100%**

Elaborado por: El autor

La sexta pregunta pretende descubrir la opinión de los profesionales sobre si los niveles de Seguridad de la Información deberían ser iguales en todas las instituciones financieras, a lo cual según se observa los resultados en la figura 74 y tabla 37, el 68.75% opina que no deben ser igual con una justificación de que cada institución financiera a pesar de tener la misma actividad económica, tiene muchas diferencias que influyen en variaciones en base a la realidad de cada empresa, mientras que el 31.25% opina que si deben ser iguales justificando que todas deben tener los mismos niveles de cumplimiento.

Figura 74. Resultados de la pregunta 6.



Fuente: Autor

Tabla 37. Pregunta 6

Pregunta 6	**Frecuencia**	**Porcentaje**
Si	33	68.75%
No	15	31.25%
Total	**48**	**100%**

Elaborado por: El autor

La séptima pregunta es sobre qué tipo de estudio recomiendan los encuestados para realizar proyectos de seguridad de la información, donde en la figura 75 y tabla 38 se observa que existe bastante diversidad de opiniones sobresaliendo la investigación Documental con el 37.5%, seguido de la Investigación Cualitativa con un 27.1%, lo que incentiva a que este trabajo se oriente hacia esas dos primeras opiniones.

Figura 75. Resultados de la pregunta 7.

Tabla 38. Pregunta 7

Pregunta 7	Frecuencia	Porcentaje
Investigación Documental	18	37.50%
Investigación de Campo	5	10.42%
Investigación Experimental	4	8.33%
Investigación Cualitativa	13	27.08%
Investigación Cuantitativa	8	16.67
Otros	0	0.00%
Total	**48**	**100%**

Elaborado por: El autor

La octava pregunta se enfoca en saber qué nivel de conocimiento tienen los profesionales de seguridad sobre la normativa SEPS 2022-002, en base a todos los controles que esta contiene, en la cual se obtiene los resultados que se muestran en la figura 76 y tabla 39, donde se evidencia que existe un buen porcentaje de alto conocimiento en el tema, sin embargo existe un 18.8% que menciona que el conocimiento que tiene es nivel medio, por lo que es necesario de parte de la superintendencia de economía popular y solidaria que se mantenga un programa de capacitación continua sobre temas de cumplimiento de la normativa, incluso un tipo conversatorio para conocer las dudas y recomendaciones de los profesionales de las diferentes instituciones bajo su regulación.

Figura 76. Resultados de la pregunta 8.

Fuente: Autor

Tabla 39. Pregunta 8

Pregunta 8	Frecuencia	Porcentaje
Alto	39	81.25%
Medio	9	18.75%
Bajo	0	0.00%

Total	**48**	**100%**

Elaborado por: El autor

La novena pregunta busca saber si los encuestados están de acuerdo con los requisitos de la Normativa SEPS 2022-002 en la cual según los resultados que se muestran en la figura 77 y tabla 40, el 45.8% está de acuerdo lo cual no supera la mitad de los encuestados, y solamente el 4.2% están muy de acuerdo, lo que da a entender que a opinión de los profesionales de seguridad existen aspectos que se pueden mejorar de la normativa y según la justificación a la pregunta, la mayoría menciona que es necesario especificar algunos requisitos de la normativa.

Algo que se puede destacar es que no existe ninguna respuesta en muy desacuerdo, y en desacuerdo existe solo un 10.4%, lo que indica que la normativa en cierta medida se encuentra bien estructurada, pero necesita una revisión en profundidad como parte de un proceso de retroalimentación y mejora continua.

Figura 77. Resultados de la pregunta 9.

Fuente: Autor

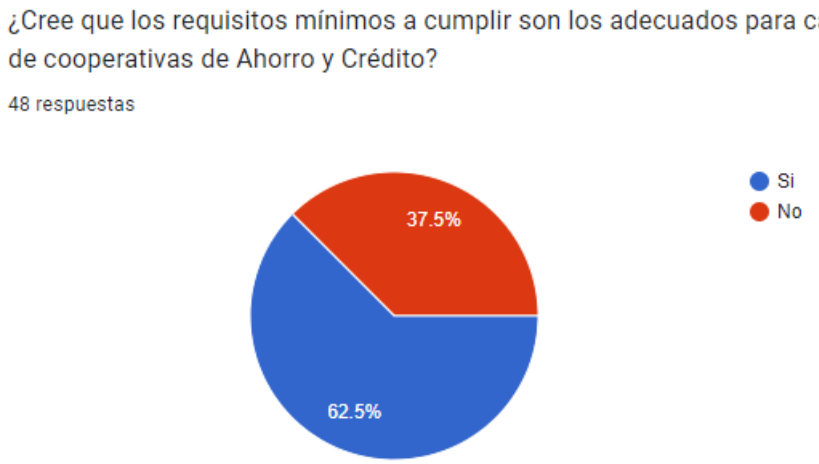
Tabla 40. Pregunta 9

Pregunta 9	**Frecuencia**	**Porcentaje**
Muy de acuerdo	2	4.17%
De acuerdo	22	45.83%
Indiferente	19	39.58%
En desacuerdo	5	10.42%
Muy en desacuerdo	0	0.00%
Total	**48**	**100%**

Elaborado por: El autor

La décima pregunta es de si los encuestados creen que los requisitos a cumplir son adecuados para cada segmento de cooperativa de ahorro y crédito, en la cual según la figura 78 y tabla 41, el 62.5% menciona si son adecuados mientras que el 37.5% opina que no son adecuados, lo que indica que la normativa en su mayoría se encuentra bien determinado su cumplimiento pero se debería analizar un pequeño ajuste en algunos requisitos dependiendo del segmento o tal vez establecer ciertos lineamientos por segmento en ciertos controles, por ejemplo en el caso de Pruebas de Penetración, se podría establecer alcances específicos para cada segmento.

Figura 78. Resultados de la pregunta 10



Fuente: Autor

Tabla 41. Pregunta 10

Pregunta 10	**Frecuencia**	**Porcentaje**
Si	30	62.50%
No	18	37.50%
Total	**48**	**100%**

Elaborado por: El autor

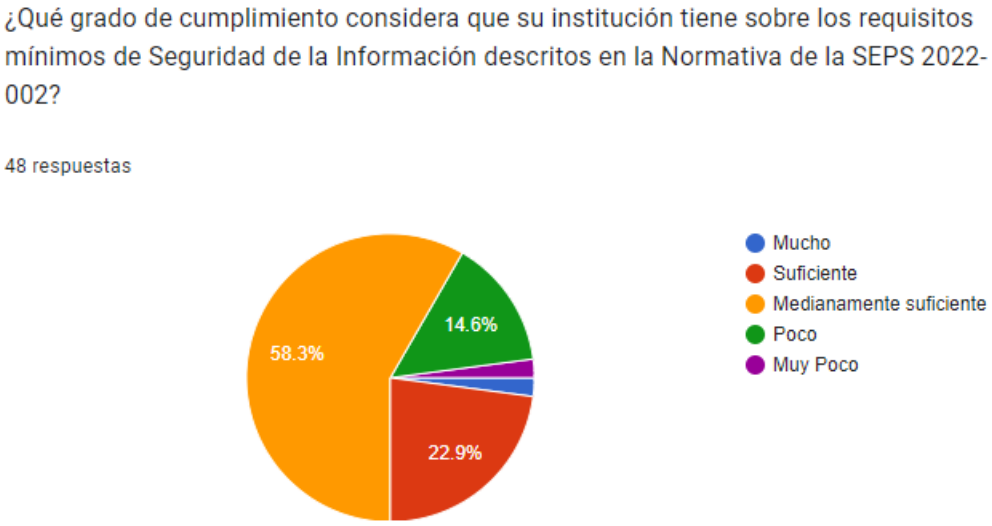
La pregunta onceava pretende conocer el nivel de cumplimiento que tienen las instituciones hasta la fecha de la encuesta considerando que para el segmento 3, el plazo máximo de cumplimiento es hasta mayo de 2025, y también poder conocer las causas que pueden ocasionar que no se complete el 100% la implementación de la normativa.

En la figura 79 y tabla 42 podemos apreciar que la mayoría (58.3%), piensa que su cumplimiento es medianamente suficiente seguido por un 22.9% que menciona que su cumplimiento es suficiente. Ahora bien, hay otros casos en los que no han podido tener un cumplimiento amplio de la normativa y algunos de los factores que se mencionan en

la justificación es la falta de apoyo de alta gerencia y falta de capacitación en algunos aspectos.

Si bien es cierto que aún hay tiempo para dar cumplimiento es necesario ya tener un buen porcentaje de implementación, y el tema de falta de apoyo de alta gerencia es algo muy común todas las instituciones, por cual es necesario poder socializar bien el alcance de la normativa y los beneficios que logran al cumplir con lo establecido y los riesgos que conlleva el no acatar las disposiciones de la SEPS.

Figura 79. Resultados de la pregunta 11



Fuente: Autor

Tabla 42. Pregunta 11

Pregunta 11	**Frecuencia**	**Porcentaje**
Mucho	1	2.08%
Suficiente	11	22.92%
Medianamente suficiente	28	58.33%
Poco	7	14.58%
Muy poco	1	2.08%
Total	**48**	**100%**

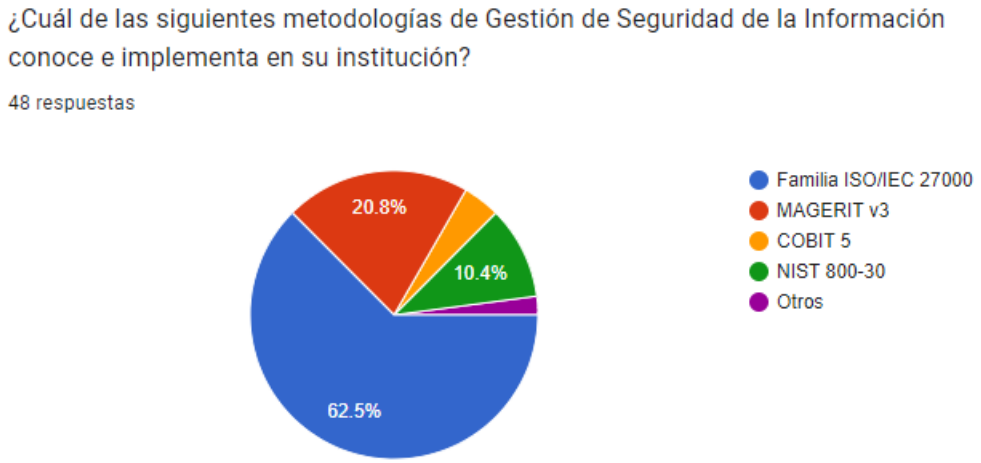
Elaborado por: El autor

La pregunta doceava busca conocer que metodología de Gestión de Seguridad de la información es más común en el sector financiero, ya que existen varias que se pueden adaptar a la normativa, incluso se puede hacer una combinación entre algunas de ellas.

En la figura 80 y tabla 43 se puede observar los resultados donde en la mayoría (62.5%) utiliza la familia de la ISO/IEC 27000, en este punto se debe aclarar que se puso como opción esta norma internacional, ya que muchos profesionales le confunden como una metodología, pero la verdad es que no se puede catalogar como tal. Por ejemplo, la ISO/IEC 27005 es una norma o guía que apoya o direcciona a las instituciones a identificar, evaluar, tartar y monitorear los riesgos informáticos, pero no es una metodología por sí misma.

En base a lo mencionado anteriormente, descartando a la familia ISO/IEC 27000 la metodología de MAGERIT v3 es la mayormente puntuada o conocida por los encuestados, ratificando ser una metodología muy aceptada en habla hispana.

Figura 80. Resultados de la pregunta 12



Fuente: Autor

Tabla 43. Pregunta 12

Pregunta 12	**Frecuencia**	**Porcentaje**
Familia ISO/IEC 27000	30	62.50%
MAGERIT v3	10	20.83%
COBIT 5	2	4.17%
NIST 800-30	5	10.42%
Otros	1	2.08%
Total	**48**	**100%**

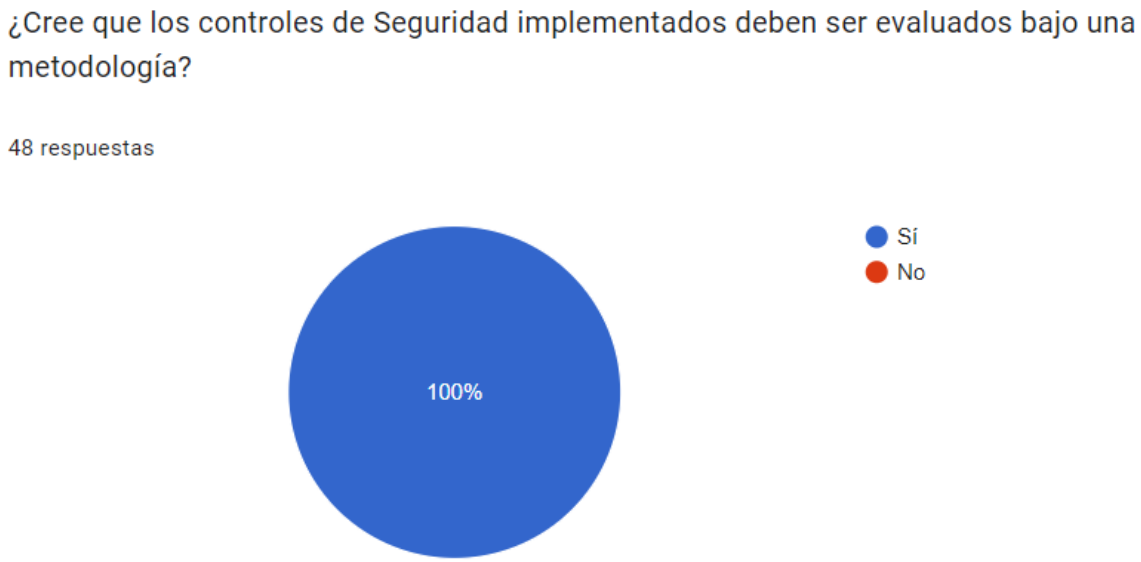
Elaborado por: El autor

La pregunta treceava hace referencia a la opinión de los encuestados de si es creen que es necesario tener una metodología para evaluar la implementación de los controles de seguridad, ya que no es suficiente con implementar solo para dar cumplimiento, sino que es importante evaluarlos como parte del proceso de mejora continua.

En la figura 81 y tabla 44 se muestran los resultados, donde se evidencia claramente que todos los encuestados se encuentran a favor del uso de una metodología de evaluación de los resultados con un 100% de aceptación, lo cual se recomienda realizar como punto adicional a la implementación de la normativa SEPS 2022-002.

Para este trabajo de titulación se utilizará la metodología Mehari, que es una herramienta que permite identificar, evaluar y tratar los riesgos de seguridad de la información de manera detallada, estableciendo planes de acción en base a las prioridades asignadas a cada riesgo.

Figura 81. Resultados de la pregunta 13



Fuente: Autor

Tabla 44. Pregunta 13

Pregunta 13	**Frecuencia**	**Porcentaje**
Si	48	100.00%
No	0	0.00%
Total	**48**	**100%**

Elaborado por: El autor

La pregunta decimocuarta busca conocer la opinión de los encuestados sobre si creen que la normativa SEPS 2022-002 se encuentra bien definida y no necesita ninguna mejora, con la finalidad de analizar la aceptación que tiene con criterio de la experiencia profesional.

En la figura 82 y tabla 45 se muestran los resultados, donde se puede evidenciar que el 89,6% creen que la normativa no está bien definida, lo que da a entender que existen

aspectos que se pueden mejorar, por lo que el ente regulador debería hacer un acercamiento más directo y así poder establecer los puntos que requieren una revisión.

Figura 82. Resultados de la pregunta 14

Fuente: Autor

Tabla 45. Pregunta 14

Pregunta 14	**Frecuencia**	**Porcentaje**
Si	5	10.4%
No	43	89.6%
Total	**48**	**100%**

Elaborado por: El autor

La pregunta decimoquinta busca conocer si la metodología de evaluación de riesgos propuesta por la SEPS en el Anexo 2 tiene total aceptación por los profesionales de seguridad, considerando que se ajuste a la realidad institucional.

En la figura 83 y tabla 46 se muestran los resultados, donde se observa que tiene una gran aceptación con el 72.9%, sin embargo la diferencia piensa que no es adecuado, esto puede se causado en base a la metodología de evaluación que se esté utilizando y eso ya depende del criterio de cada profesional, solo que la metodología que se emplee debe tener una gran aceptación en la sociedad.

Figura 83. Resultados de la pregunta 15

Fuente: Autor

Tabla 46. Pregunta 15

Pregunta 14	**Frecuencia**	**Porcentaje**
Si	35	72.9%
No	13	27.1%
Total	**48**	**100%**

Elaborado por: El autor

ANEXO V

PLAN DE TRABAJO DE SEGURIDAD DE LA INFORMACIÓN

Periodo anual		Actividades	MES 1				MES 2				MES 3				MES 4				MES 5				MES 6				MES 7				MES 8				MES 9				MES 10				MES 11				MES 12			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
A. POLÍTICAS, PROCESO Y PROCEDIMIENTOS, ROLES Y RESPONSABILIDADES.																																																
1	Política	Elaboración de la Política de Seguridad de la Información	X	X																																												
		Elaboración de la Política para la Clasificación de la información			X	X																																											
		Elaboración de la Política de Gestión de Riesgos de Seguridad de la información					X	X																																								
		Elaboración de la Política de Control de accesos físicos y tecnológicos							X	X																																					
		Elaboración de la Política de Gestión de Incidentes									X	X																																			
		Elaboración de la Política de Gestión de Software											X	X																																	
		Elaboración de la Política de Gestión de Infraestructura Tecnológica													X	X																															
		Elaboración de la Política de Seguridad de la Información para Recursos Humanos															X	X																													
		Elaboración de la Política de Seguridad física																	X	X																												
		Elaboración de la Política de Gestión con terceros																			X	X																										
		Elaboración de la Política de Ciberseguridad																					X	X																								
2	Planificación	Elaborar y aprobar el Plan de Gestión de Riesgos de Seguridad de la Información.																							X	X	X	X																			
3	Organización	Efectuar pautas para analizar los avances obtenidos y verificar en base a la planinificación								X																X								X												X
		Sesionar al menos dos veces al año																						X																				X			
4	Integración - Implementación	Elaborar un Plan de Capacitacion, para dar competencias al personal					X																																								

5	Verificación - Auditorías Internas Índices de Eficacia del Plan de Gestión	Verificar la efectividad de las medidas implementadas por el Oficial de Seguridad de la Información (OSI);																																													X	X	
6	Mejoramiento Continuo	Verificar e implementar acciones de mejora continua																					X																								X	
B.	**PROCESOS**																																																	
1	Identificación de los procesos agregadores de valor	Elaborar un documento de identificación de procesos agregadores de valor																										X	X	X	X																		
2	Gestión de vulnerabilidades	Difundir resultados de mediciones																					X																								X	
3	Adquisición y desarrollo de software; hardware y servicios	Definir el Procedimiento de adquisición, desarrollo de software y mantenimiento de sistemas informáticos, hardware y servicios.																														X	X																
4	Planes de contingencia tecnológica y continuidad del negocio	Elaborar planes, procesos y procedimientos de Contingencia tecnológica y continuidad del negocio																																X	X	X													
5	Cifrado	Procedimientos de Cifrado de la información sensible o crítica, conforme al análisis de riesgos de seguridad de la información																																			X												
		Verificar periódicamente la vigencia de los elementos cifrados.										X											X											X												X		
C.	**PROCEDIMIENTOS**																																																	
1	Inventario y Clasificación de la Información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tiposy activos de infomación considerando los criterios de disponibilidad, confidencialidad e integridad así como su custodio, responsable y ubicación.			X	X																																											
2	Gestión de Riesgo	Disponer de un documento evidenciable en el cual se evalúen vulnerabilidades y amenazas con el fin de detenninar el nivel de riesgo					X	X	X	X																																							
3	Respaldos y resguardo de información sensible o crítica.	Respaldar la información sensible o crítica (física y digital) en lugares y ubicaciones adecuadas													X	X																																	

4	Cultura de seguridad de la Información	Evaluar periodicamente el Plan de Capacitación de Seguridad de la Información																						X																										X
5	Control de accesos tecnológicos	Definir los perfiles y roles asignados al personal y establecer el procedimiento para su administración							X	X																																								
6	Gestión de Configuración	Implementar procedimientos para la gestión de configuraciones del activo de tecnologías de información.																																			X	X												
7	Gestion de cambios, control de versiones …	Implementar procedimientos de gestión de cambios y control de versiones en el que se registren las autorizaciones, ajustes y variaciones que se realicen en los servicios de tecnología, de una manera ordenada y controlada.																																					X	X								
D.	**CONTROLES TECNOLÓGICOS**																																																	
1	Arquitectura Segura	Diseñar, implementar y gestionar, la arquitectura segura para proteger los activos digitales en función de la particularidad tecnológica																																							X	X	X	X				
2	Monitoreo y Detección	Implementar sistemas que mantengan registros de logs correlacionados de la infraestructura crítica, que permitan su detección, análisis y depuración																																											X	X	X	X

ANEXO VI

Tabla 47. Guía de implementación resumida

MATRIZ DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN			
CONTROL	OBJETIVO	ACTIVIDADES	ENTREGABLE
POLÍTICAS			
Política General de Seguridad de la Información	Definir la estructura de gobierno de seguridad de la información, principios y lineamientos generales	Elaborar la política general, definir, objetivos, alcance, documentos de referencia, definiciones, roles y responsabilidades, directrices para la aplicación, evaluación, revisión, sanciones y excepciones.	Documento aprobado, por Consejo de Administración.
Clasificación de la Información	Identificar, categorizar y garantizar la protección de la información según el nivel de sensibilidad y criticidad.	Definir categorías, aplicar en inventarios. Establecer una matriz de clasificación. Etiquetar documentos.	Documento aprobado, por Consejo de Administración.
Gestión de riesgos de seguridad de la Información	Brindar lineamientos para identificar, evaluar y tratar riesgos de seguridad.	Aplicar metodología (MAGERIT) para establecer matrices de gestión de riesgo, identificando, amenazas, vulnerabilidades. Determinar el valor de los activos, degradación causada por las amenazas, impacto, probabilidad y riesgo. Implementación de salvaguardas, evaluar la efectividad de las salvaguardas, cálculo del riesgo inherente.	Documento aprobado, por Consejo de Administración.
Control de accesos físicos y tecnológicos	Establecer medidas de protección para prevenir el acceso no autorizado a la información sensible o crítica	Implementar controles de acceso físico, MFA, revisión periódica de accesos, implementación de sistemas de CCTV y sistemas de intrusión e incendios.	Documento aprobado, por Consejo de Administración.
Gestión de incidentes	Detectar, responder, mitigar daños y recuperación de servicios oportunamente ante incidentes.	Establecer una categorización de los incidentes. Definir procedimiento, habilitar canal de reporte (GLPI). Elaborar informes técnicos para conocimiento del CSI.	Documento aprobado, por Consejo de Administración.
Gestión de software	Proporcionar medidas de seguridad en el proceso de adquisición, desarrollo, instalación, actualización o eliminación de software	Gestionar el software en todo el ciclo de vida: diseño de soluciones, desarrollo, pruebas, gestión de repositorios, creación de paquetes en caso de que aplique, control de versiones, retiro de software obsoleto.	Documento aprobado, por Consejo de Administración.

Gestión infraestructura tecnológica	Garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada	Monitoreo de servidores y redes, respaldos y redundancia. Mantenimientos preventivos. Actualización y renovación de equipos. Análisis de capacidad y rendimiento. Monitoreo periódico de toda la infraestructura de Data Center.	Documento aprobado, por Consejo de Administración.
Gestión de seguridad para Recursos Humanos	Incluir seguridad en el ciclo de vida laboral.	Establecer políticas en: Selección y contratación, Permanencia y desarrollo, Desvinculación.Definir roles y responsabilidades relacionadas a seguridad de la información.	Documento aprobado, por Consejo de Administración.
Seguridad Física	Precautelar la seguridad de los empleados, socios, clientes, usuarios, instalaciones y bienes, así como también las consideraciones para el transporte de efectivo y valores	Cumplimiento con lo establecido en la Resolución SEPS-IGT-IR-IGJ-2018-021: Medidas generales de seguridad física. Manual y políticas de seguridad física. Personal de Seguridad. Bóvedas y cajas fuertes. Sistemas de alarmas. Sistemas de video vigilancia. Cajeros automáticos. Transporte y fondos de valores.	Documento aprobado, por Consejo de Administración.
Gestión con terceros	Controlar riesgos en proveedores externos.	Firmar acuerdos de confidencialidad. Calificación de proveedores. Evaluación periódica de desempeño. Verificar cumplimiento de SLAs. Control de acceso a la información sensible por parte de terceros. Limitación de derechos de acceso. Garantizar un tratamiento adecuado de la información por parte de terceros. Uso de canales de comunicación seguros o cifrados. Exigir informes de medidas de seguridad.	Documento aprobado, por Consejo de Administración.
Ciberseguridad	Prevenir, minimizar y responder a amenazas cibernéticas.	Lineamientos para detectar riesgos y amenazas considerando la implementación de firewall, IDS/IPS, SIEM, antivirus, XDR.	Documento aprobado, por Consejo de Administración.
PROCESOS			
Identificación de procesos agregadores de valor	Determinar procesos críticos que soportan el negocio.	Mapear procesos clave como transacciones de canales digitales, captación, colocación.	Mapa de procesos documentado.

Gestión de vulnerabilidades - Auditorías Informáticas	Detectar debilidades en la gestión de seguridad de la información.	Realizar auditorías internas y externas periódicas.	Informes de auditoría, reportes de vulnerabilidades.
Gestión de vulnerabilidades - Plan de mitigación de hallazgos	Reducir riesgos mediante acciones correctivas.	Elaborar planes o estrategias de mitigación para hallazgos. Definir fechas de solución y entregables.	Planes de acción aprobados, evidencias de ejecución.
Adquisición y desarrollo de hardware, software y servicios	Asegurar adquisiciones con criterios de seguridad.	Definir procedimiento que se alinee al manual de adquisiciones institucional y a la resolución de riesgo operativo vigente.Presentar informes al CSI y Comité de Adquisiciones.	Procedimientos aprobados.
Planes de Contingencia Tecnológica y continuidad del negocio	Definir las actividades necesarias para implementar y probar los planes de contingencia informática y continuidad del negocio garantizando continuidad de servicios frente a desastres.	Diseñar PCN y DRP, realizar simulacros periódicos.	Planes aprobados. Reportes e informes de simulacros.
Cifrado	Proteger información sensible en tránsito y reposo.	Implementar cifrado en bases de datos, correos y discos. Gestión de claves criptográficas.	Políticas y procedimientos de cifrado. Verificación de configuraciones.
PROCEDIMIENTOS			
Inventario y Clasificación de información - Identificación de tipos de información	Definir categorías de información según naturaleza.	Realizar identificación documental y digital, para su posterior categorización.	Informe de identificación.
Inventario y Clasificación de información - Inventario de activos de información	Mantener listado actualizado de activos.	Usar herramientas como GLPI. Verificación de activos cada 6 meses.	Inventario actualizado y firmado.
Inventario y Clasificación de información - Clasificación de activos de información	Asignar criticidad a cada activo.	Aplicar niveles: Crítico, Muy Alto, Alto, Medio, Bajo.	Matriz de clasificación, custodios asignados.
Gestión de Riesgos	Administrar riesgos tecnológicos y de ciberseguridad.	Elaborar matriz de riesgos, aplicar controles. Gestionar los riesgos con el uso de una herramienta como ERAMBA. Determinar riesgos por cada activo de información.	Matriz actualizada, reportes de tratamiento y seguimiento.

Respaldo y resguardo de información sensible o crítica	Garantizar copias confiables y seguras.	Establece el proceso para la generación de respaldos. Automatizar procesos de respaldos. Garantizar el resguardo y disponibilidad de los respaldos. Verificar periódicamente la restauración.	Registros de respaldos y resultados de pruebas de restauración.
Cultura de Seguridad de la información	Diseñar, programar y coordinar planes de capacitación permanentes.	Diseñar programas de capacitación. Establecer un cronograma anual de capacitación. Ejecutar campañas y capacitaciones periódicas.	Registros de participación, material de difusión.
Gestión de accesos tecnológicos	Controlar accesos a sistemas y aplicaciones sensibles.	Identificar activos de información sensible o crítica.Gestionar las solicitudes de acceso, creación y asignación de privilegios, revisión y monitoreo periódica, modificación y revocación de accesos.	Bitácoras de accesos, informes de auditoría.Listado de usuarios y privilegios de acceso a información sensible o crítica.
Gestión de configuración	Mantener configuraciones seguras y estandarizadas.	Documentar y revisar configuraciones críticas.	Informes de configuración, checklist de revisión.
Gestión de cambios, control de versiones y mantenimiento	Definir las acciones necesarias para solicitar, evaluar, aprobar, implementar y documentar cambios tecnológicos y mantenimiento de hardware, software y servicios de TI	Determinar los tipos de cambios. Gestionar las solicitudes de cambios, evaluación, aprobación, planificación y verificación. Identificar los riegos que pueden generar los cambios por su naturaleza o criticidad de la información. Establecer un cronograma anual de mantenimientos preventivos y correctivos.	Informes de gestión de cambios, registros de mantenimiento y control de versiones.
CONTROLES TECNOLÓGICOS			
Arquitectura segura	Diseñar infraestructura con seguridad integrada.	Determinar la metodología de arquitectura segura. Aplicar segmentación de red, DMZ. Establecer estrategias de defensa en profundidad. Controles de flujo de información, para evitar fugas de información, o accesos no autorizados.	Metodología de arquitectura aprobada por el Comité de Seguridad de la Información.
Monitoreo y detección	Detectar amenazas y anomalías en tiempo real.	Implementar SIEM/XDR, logs centralizados, gestión de alertas de seguridad.	Sistema de monitoreo funcional. Informe de registro de alertas.

Fuente: Propia

ANEXO VII

Política General de Seguridad de la Información

1. Objetivos de la política

1.1. Objetivo General

Definir la estructura de gobierno de seguridad de la información, principios y lineamientos generales para la Gestión de Seguridad de la Información de la Cooperativa de Ahorro y Crédito [nombre de la institución]

1.2. Objetivos Específicos

- Definir e implementar políticas y controles de seguridad de la información con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de todo activo de información de la cooperativa.
- Diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI), con la finalidad de controlar, monitorear y evaluar periódicamente la aplicación de controles y políticas de seguridad mediante la gestión de riegos.
- Definir una estructura organizacional alineada a la normativa de la SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002, determinando los roles y responsabilidades de gestión de seguridad.
- Garantizar el acceso y conocimiento de esta política a todas las partes interesadas incluyendo funcionarios, socios, clientes y proveedores, a través de los medios con los que cuente la cooperativa.

2. Alcance

La Política General de Seguridad de la Información de la cooperativa [nombre de la institución] se aplica a todo el personal, socios, clientes y proveedores que tengan acceso a los activos de información de la cooperativa, para lo cual se debe suscribir acuerdos correspondientes.

3. Documentos de referencia

- Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.
- Resolución SEPS-IGT-IGS-INR-INGINT-INSESF-2023-008
- Resolución SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116
- Resolución SEPS-IGT-IGS-INR-INGINT-INSESF-2023-015
- Resolución SEPS-IGT-IR-IGJ-2018-021
- Ley Orgánica de Protección de Datos Personales 2021 (LOPDP)
- Normativa de la Junta de Política y Regulación Financiera (JPRF)
- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información
- ISO/IEC 27002:2022 – Controles de seguridad de la información (referencia para la política)
- ISO 22301:2025 – Ciberseguridad: Continuidad del negocio (relacionada con disponibilidad)
- ITIL Foundation, ITIL 4 Edition.

4. Definiciones

- SGSI. – Sistema de Gestión de seguridad de la información, su propósito es garantizar que los datos y activos informáticos se gestionen de manera segura frente a amenazas internas y externas, mediante un enfoque basado en riesgos y mejora continua, está conformado por políticas, procesos, recursos y controles orientados a proteger la confidencialidad, integridad y disponibilidad de la información. (INEN, 2022)
- SEPS. – Superintendencia de Economía Popular y solidaria, es el organismo de control del Ecuador encargado de supervisar, regular y vigilar a las entidades que forman parte del sector financiero popular y

solidario, como cooperativas de ahorro y crédito, asociaciones y mutualistas. (SEPS, 2023)

- Seguridad de la Información. – ISACA, 2023 establece un concepto de en base a los tres pilares de seguridad que menciona que la seguridad de la información asegura que solo las personas autorizadas (confidencialidad) tengan acceso a la información precisa y completa (Integridad) cuando sea necesario (disponibilidad).
- Activo de información. - es todo recurso que posee valor para la organización y que resulta indispensable para el desarrollo de sus actividades. No se limita únicamente a los datos, sino que abarca sistemas, aplicaciones, infraestructuras, servicios, procesos y personas que los operan. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)
- Confidencialidad. - es la propiedad de la información que garantiza que los datos solo sean accesibles por personas autorizadas, evitando su divulgación indebida o el acceso no autorizado. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)
- Integridad. - es la propiedad de la información y de los sistemas que asegura que los datos se mantienen exactos, completos y confiables, evitando alteraciones no autorizadas ya sea de manera intencional o accidental. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)
- Disponibilidad. - es la propiedad de la información, los sistemas y los servicios para que estén accesibles y utilizables por los usuarios

autorizados en el momento en que se requieran. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

5. Roles y Responsabilidades

Los roles y responsabilidades se describen en la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002, que son:

Consejo de Administración

- Aprobar el Plan Estratégico de Seguridad de la Información, asegurando que se encuentre articulado con la planificación estratégica de la entidad, de las empresas relacionadas y de la CONAFIPS.
- Autorizar la asignación de los recursos humanos, técnicos y financieros requeridos para la adecuada implementación y sostenibilidad de la seguridad de la información.
- Validar y aprobar las políticas, procesos, procedimientos, así como la definición de roles y responsabilidades vinculados a la gestión de la seguridad de la información.
- Respaldar la ejecución del Plan de Capacitación y Sensibilización, destinado a fortalecer la cultura de seguridad en toda la organización.
- Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información, garantizando que se contemplen las medidas necesarias para la identificación, tratamiento y mitigación de riesgos.

Fuente: Resolución SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002, Artículo 20, literal 1

Comité de Seguridad de la Información

- Autorizar la asignación de los recursos humanos, tecnológicos y financieros requeridos para la gestión de la seguridad de la información, asegurando que su utilización contribuya de manera eficiente y eficaz al cumplimiento de los objetivos estratégicos de la entidad y de sus empresas vinculadas.
- Aprobar y mantener actualizadas las políticas, procedimientos, funciones y responsabilidades relacionadas con la gestión de la seguridad de la información.
- Respaldar la ejecución de los programas de concienciación y capacitación en seguridad de la información, orientados a fortalecer la cultura organizacional en esta materia.
- Validar el Plan de Gestión de Riesgos de Seguridad de la Información, verificando que se encuentre alineado con el Plan Integral de Administración de Riesgos de la entidad y sus empresas.

Fuente: Resolución SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002, Artículo 20, literal 2

Gerente General

- Dirigir la gestión de la seguridad de la información, en concordancia con las resoluciones del Consejo de Administración o del Directorio y con lo establecido en la normativa vigente.
- Nombrar a la persona responsable de ejercer las funciones de Oficial de Seguridad de la Información (OSI).

- Impulsar la participación comprometida de todas las partes interesadas que intervienen en el desarrollo y administración de la seguridad de la información.

Fuente: Resolución SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002, Artículo 20, literal 3

Oficial de Seguridad de la Información

- Definir, elaborar, supervisar y mantener actualizadas las políticas, metodologías, procesos, procedimientos, planes y controles vinculados con la seguridad de la información, garantizando además su adecuada difusión entre el personal de la entidad y de las empresas relacionadas.
- Gestionar la solicitud de recursos humanos, tecnológicos y financieros necesarios para la seguridad de la información, asegurando que su uso sea eficiente y eficaz, en coherencia con los objetivos estratégicos institucionales.
- Diseñar y presentar al Consejo de Administración las políticas, procesos, procedimientos, roles y responsabilidades relacionados con la seguridad de la información, para su revisión y aprobación.
- Planificar, desarrollar y ejecutar programas de capacitación y concienciación en materia de seguridad de la información, dirigidos al personal de la organización.
- Coordinar y dar seguimiento, junto con los responsables de los procesos del negocio, a la implementación de controles de seguridad de la información definidos en el plan de gestión de riesgos, así como diseñar, evaluar y comunicar dicho plan de manera periódica.

- Coordinar las distintas actividades necesarias para la gestión de la seguridad de la información dentro de la institución.
- Aplicar los procedimientos y lineamientos establecidos en caso de identificarse incidentes de seguridad de la información.
- Reportar, conforme a la normativa vigente, aquellos incidentes de seguridad catalogados como críticos o sensibles a las instituciones públicas competentes.
- Contribuir en la identificación y evaluación de amenazas relacionadas con la seguridad de la información y proponer medidas de mitigación apropiadas.
- Brindar asesoría en materia de seguridad de la información mediante su participación en proyectos que impliquen el tratamiento de datos sensibles o críticos, tanto de la institución como de socios, clientes o usuarios.
- Recomendar medidas correctivas adicionales en seguridad de la información, asegurando su alineación con el Anexo 1 de la normativa aplicable y con las buenas prácticas reconocidas.
- Verificar que los servicios prestados por proveedores externos ya sean personas naturales o jurídicas, cumplan con las políticas de seguridad de la información de la institución.
- Generar y mantener la documentación que evidencie la gestión de la seguridad de la información, asegurando trazabilidad y soporte para auditorías o revisiones regulatorias.

Fuente: Resolución SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002, Artículo 20, literal 4

Auditor Interno

- Supervisar y evaluar la eficacia de las medidas de seguridad implementadas por el Oficial de Seguridad de la Información (OSI).
- Resguardar los informes derivados de auditorías o exámenes especiales realizados por el OSI, asegurando su disponibilidad para la Superintendencia de Economía Popular y Solidaria cuando esta lo solicite.
- Emitir recomendaciones de mejora o acciones correctivas dirigidas al Oficial de Seguridad de la Información (OSI).

Fuente: Resolución SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002, Artículo 20, literal 5

6. Directrices para la aplicación de la política

Información de la cooperativa: se considera un activo intangible esencial para la cooperativa, por lo que todo acceso, uso y tratamiento deberá alinearse con las políticas y normas internas de seguridad de la información. La responsabilidad de protegerla recae en los propietarios de los activos, quienes deberán aplicar medidas de acuerdo con su valor y criticidad, cumpliendo con lo dispuesto en las políticas institucionales, los procedimientos y las directrices aprobadas por la cooperativa.

Gestión de riesgo: para cada activo de información de la cooperativa se debe realizar una evaluación de riesgos aplicando la metodología MAGERIT v3, con el fin de garantizar un tratamiento adecuado frente a posibles amenazas. Dicho enfoque contempla la identificación de los activos, el análisis de su valor, la detección de vulnerabilidades y amenazas, así como la estimación del impacto y

la probabilidad de ocurrencia de incidentes. A partir de estos resultados se definen salvaguardas y planes de mitigación que permiten priorizar las acciones de seguridad, asegurando que la protección de la información esté en concordancia con la relevancia del activo y los objetivos estratégicos y regulatorios de la institución. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

Acciones de mitigación de riesgos: En el marco de la metodología MAGERIT v3, las acciones de mitigación de riesgos se orientan a reducir la probabilidad de ocurrencia o el impacto de los incidentes que puedan afectar a los activos de información y puede ser (mitigar, reducir, aceptar y transferir). Estas medidas incluyen la implementación de salvaguardas, tales como controles de acceso, cifrado, planes de respaldo, segmentación de redes, políticas de uso, concienciación del personal y procedimientos de continuidad. La selección de las acciones se basa en la valoración previa de los riesgos y se debe priorizar aquellas que ofrezcan mayor eficacia en relación con el costo beneficio, contribuyendo así a una gestión de la seguridad de la información efectiva. (Ministerio de Hacienda y Administraciones Públicas de España, 2012)

7. Evaluación del cumplimiento

   La evaluación del cumplimiento de la normativa SEPS 2022-002 se realiza mediante una matriz de riesgos, la cual permite medir el nivel de avance en la implementación de los controles de seguridad. Para ello se utiliza la metodología MEHARI, que facilita identificar las amenazas y vulnerabilidades asociadas a cada activo, evaluar la efectividad de las medidas aplicadas y calcular un porcentaje de madurez que refleja el grado de alineación con los requisitos normativos. Este enfoque no solo proporciona una visión objetiva del estado

actual del SGSI, sino que también orienta la priorización de acciones correctivas y de mejora continua en la cooperativa. (CLUSIF, 2010)

8. Revisión de la política

   Para garantizar la aplicación correcta y el uso adecuado de los recursos de esta política, así como de los documentos derivados de ella (políticas generales, procesos y procedimientos) y de todos los componentes del Sistema de Gestión de Seguridad de la Información (SGSI), se dispone que su cumplimiento sea revisado de forma periódica (mínimo 2 veces al año), o cuando exista un cambio significativo, como cambios normativos o tecnológicos.

9. Vulneración de las políticas de Seguridad de la Información

   Cualquier incumplimiento con la Política General de Seguridad de la Información, políticas específicas, procesos y procedimientos establecidos por la cooperativa, serán sancionados conforme a lo establecido en el Reglamento Interno de Trabajo vigente, considerando como falta grave.

10. Excepciones

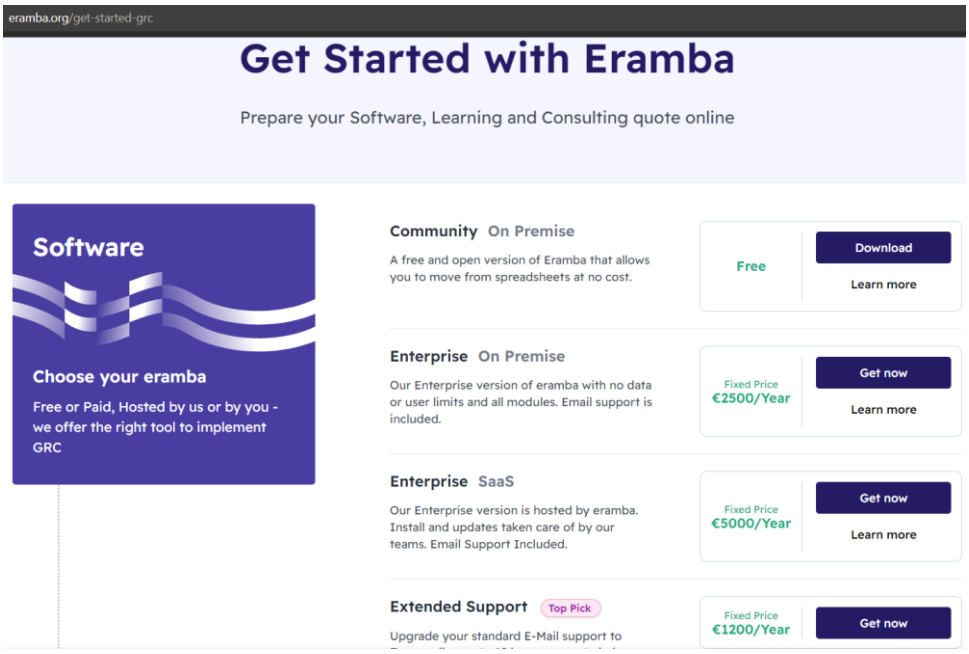
    La Política General de Seguridad no estable excepciones, sin embargo, se evaluará para su eventual admisión siempre y cuando existan casos justificados.

ANEXO VIII

Instalación de ERAMBA

Nos dirigimos a la página oficial de ERAMBA https://www.eramba.org/ donde encontraremos todas las versiones disponibles como se muestra en la figura 84, para iniciar por primera vez hasta familiarizarse con el software se recomienda iniciar con la versión gratuita.

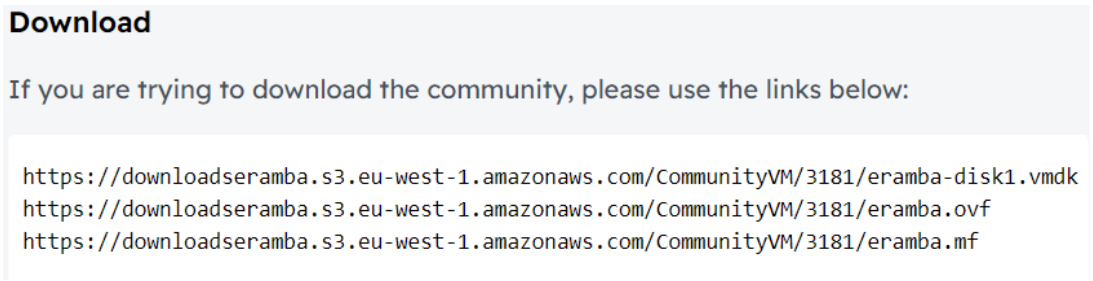
Figura 84. Página oficial para descarga de ERAMBA



Fuente: https://www.eramba.org/

Al seleccionar la versión deseada, no redirige a una Guía de instalación donde nos indicará paso a paso lo que se debe realizar, y también nos indica los enlaces de descarga como se muestra en la figura 85.

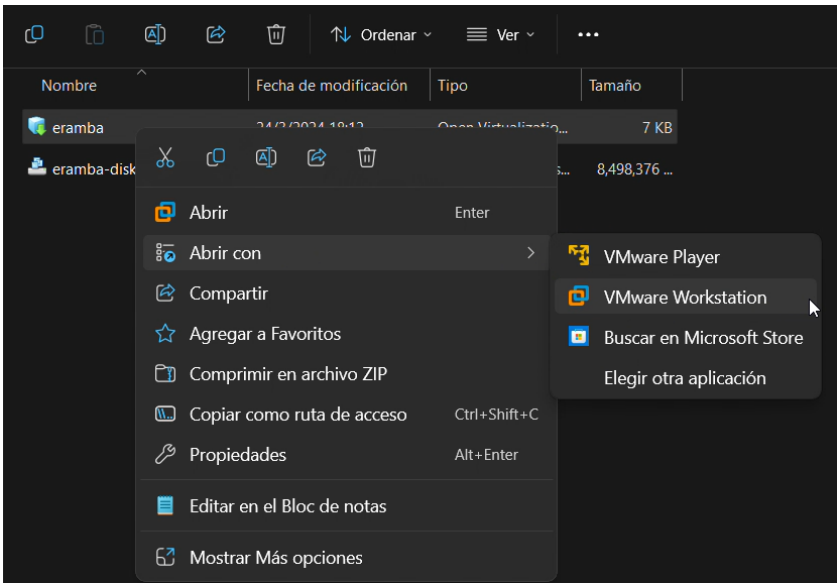
Figura 85. Enlaces de descarga ERAMBA



Fuente: https://www.eramba.org/

Una vez que tenemos los archivos descargados, la forma más fácil para cargar la máquina virtual en VMware es haciendo click derecho en el archivo y seleccionar “Abrir con” y nos permite escoger nuestro software de virtualización, como se muestra en la figura 86.

Figura 86. Carga de ERAMBA a software de virtualización



Fuente: Autor

Ya en el software de virtualización empezará a correr ERAMBA, como se muestra en la figura 87.

Figura 87. Arranque de máquina virtual ERAMBA

Fuente: Autor

Una vez completada la inicialización de la máquina virtual, nos aparece una pantalla con la información de la versión de software que utiliza que en este caso de trata de Ubuntu 22.04.1 y nos solicita un usuario y password como se observa en la figura 88, cuyas credenciales por defecto son:

- usuario: eramba
- password: eramba

Figura 88. Ventana para logueo de ERAMBA

Fuente: Autor

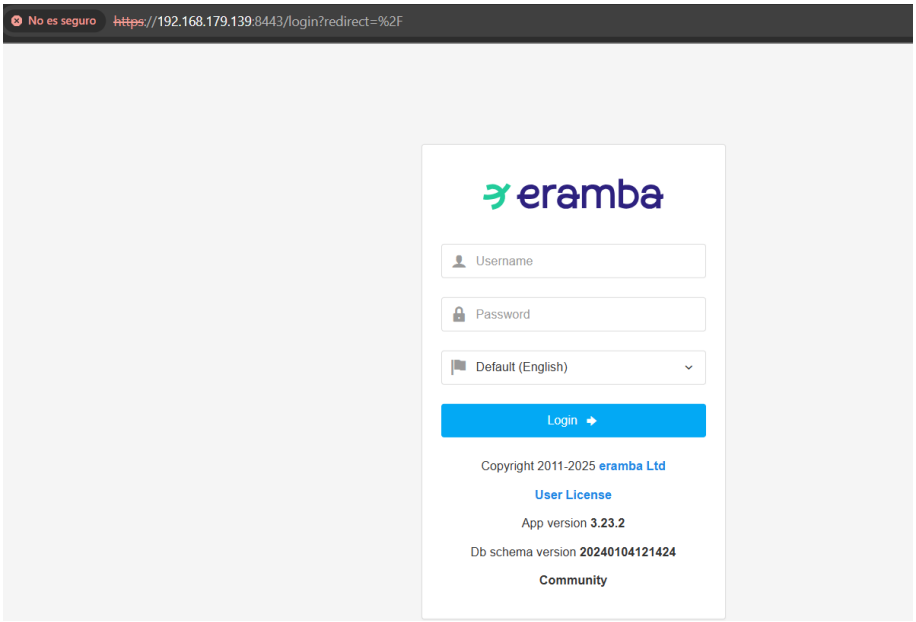
Una vez logueado correctamente, se muestra la dirección IP que se ha asignado a la máquina virtual de ERAMBA y el resultado de una prueba de conexión a internet como se observa en la figura 89.

Figura 89. Ventana inicial de ERAMBA

Fuente: Autor

Una vez completo el proceso de instalación ya podemos ingresar en el navegador la dirección IP que arroja la máquina virtual utilizando el puerto 8443 como se muestra en la figura 90.

Figura 90. Acceso a ERAMBA a través del navegador



Fuente: Autor

ANEXO IX

Tabla 48. Matriz de evaluación de estado inicial

Tipificación	# Sección	Clausula	Descripción de control	Estado	%	Observación
EVALUACIÓN DE CUMPLIMIENTO PARA REGIMEN ESPECIAL						
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 15 Se debe contar con un comité de Seguridad de la información	Determinar la conformación del comité, alineado a la normativa	No existe	100 %	Se encuentra formalizado
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 16 Se debe sesionar al menos dos veces al año	Verificar constancia de sesiones	Parcialmente	35%	Solo se ha realizado una reunión del comité para la designación de responsabilidades.
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN					68%	
OFICIAL DE SEGURIDAD DE LA	CAPITULO III	Art. 17 Se debe contar con un Oficial	Determinar la existencia de un Oficial de Seguridad	Optimizado	100 %	OSI cumple con todos los requisitos

INFORMACIÓN		de Seguridad de la Información	de la Información con título de tercer nivel y capacitación de 40 horas en seguridad		100 %	
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN						
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 1 – Consejo de Administración o directorio	El directorio debe aprobar PESI, recursos humanos, técnicos y financieros, políticas, procesos, procedimientos, plan de concienciación y formación, Gestión de riesgos.	Parcialmente	35%	No existen muchas acciones relacionadas a seguridad, más allá de la aprobación del CSI y aprobación de políticas de seguridad de la información inmersas en el manual de Tecnología
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 2 – Comité de Seguridad de la Información	Debe proponer al Directorio el PESI, Los recursos humanos, técnicos y financieros, políticas, procedimientos, roles y responsabilidades, Plan de concienciación, plan de gestión de riesgos	No existe	0%	El comité aún no se ha reunido con la finalidad de gestionar sus responsabilidades
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 3 - Gerente General	Liderar la gestión de seguridad de la información, designar al oficial de seguridad, coordinar la participación de todas las partes.	Parcialmente	35%	Solamente se cumplido con la asignación del OSI
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 4 – Oficial de Seguridad de la Información	Desarrollar, gestionar, monitorear el PESI, Diseñar y proponer las políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad, solicitar asignación de recursos, desarrollar y ejecutar Planes de concienciación	No existe	5%	El OSI recién empieza a revisar la situación actual de la institución
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 5 – Auditor Interno	Verificar la efectividad de las medidas implementadas por la unidad de Seguridad de la información	No existe	0%	No se ha realizado evaluaciones respecto a seguridad de la información
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					15%	

EVALUACIÓN Y CUMPLIMIENTO	CAPITULO III	Art. 13 evaluaciones, revisiones, pruebas, exámenes y actualizaciones anualmente	Verificar la documentación de evaluaciones, revisiones, pruebas, exámenes y actualizaciones	Inicial	20%	El OSI recién empieza a revisar la situación actual de la institución
		EVALUACIÓN Y CUMPLIMIENTO			20%	
			EVALUACIÓN DE ANEXO 1			
POLÍTICAS	Anexo 1	Política General de SI	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Clasificación de la Información	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Gestión de riesgos de seguridad de la Información	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Control de accesos físicos y tecnológicos	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Gestión de incidentes	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Gestión de software	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Gestión infraestructura tecnológica	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Gestión de seguridad para Recursos Humanos	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Seguridad Física	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Gestión con terceros	Política aprobada y socializada	No existe	0%	No existe
POLÍTICAS	Anexo 1	Ciberseguridad	Política aprobada y socializada	No existe	0%	No existe
		POLÍTICAS			0%	
PROCESOS	Anexo 1	Identificación de procesos agregadores de valor	Verificar existencia de documento de procesos agregadores de valor	Definido	70%	Necesita actualización por los cambios normativos, no se incluye procesos relacionados con la seguridad de la Información
PROCESOS	Anexo 1	Gestión de vulnerabilidades – Auditorías Informáticas	Auditorías internas y externas	No existe	0%	No se ha realizado ninguna Auditoría Informática
PROCESOS	Anexo 1	Gestión de vulnerabilidades – Plan de mitigación de hallazgos	Plan de hallazgos para mitigar los resultados de las auditorías o pruebas de Pentesting	No existe	0%	Al no existir Auditoría, tampoco existe un Plan de mitigación de hallazgos

PROCESOS	Anexo 1	Adquisición y desarrollo de hadware, software y servicios	Disponer de procedimientos para la adquisición y desarrollo de software, hadware y servicios en la que se incluyan temas relacionados a la seguridad	Parcialmente	50%	Existen procedimientos dentro del manual de Tecnología y manual de Adquisiciones, pero no se consideran puntos relacionados con seguridad de la información.
PROCESOS	Anexo 1	Planes de Contingencia Tecnológica y continuidad del negocio	Elaborar Planes de Contingencia Tecnológica y continuidad del negocio	Parcialmente	50%	La institución cuenta con un Plan de continuidad de Negocio y Plan de recuperación de desastres, pero no se consideran temas de seguridad de la información
PROCESOS	Anexo 1	Cifrado	Procedimientos de cifrado de información sensible o crítica	Parcialmente	50%	Se realiza cifrado con VeraCript para los respaldos de base del core financiero, pero no considera el resto de información sensible
PROCESOS					37%	
PROCEDIMIENTOS	Anexos 1	Inventario y Clasificación de información – Identificación de tipos de información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos de activos de información considerando los criterios de disponibilidad, integridad y confidencialidad.	No existe	0%	No se dispone de ningún documento de Identificación de tipos de información
PROCEDIMIENTOS	Anexos 1	Inventario y Clasificación de información – Inventario de activos de información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos de activos de información considerando los criterios de disponibilidad, integridad y confidencialidad.	Inicial	30%	No se dispone de ningún documento de Inventario de activos de información, pero se cuenta con inventario de activos tecnológicos en general sin ningún tipo de análisis

PROCEDIMIENTOS	Anexos 1	Inventario y Clasificación de información – Clasificación de activos de información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos de activos de información considerando los criterios de disponibilidad, integridad y confidencialidad.	No existe	0%	No se dispone de ningún documento de clasificación de activos de información
PROCEDIMIENTOS	Anexos 1	Gestión de Riesgos	Documento evidenciable en el cual se evalúen vulnerabilidades y amenazas con el fin de determinar el nivel de riesgo	No existe	0%	No se cuenta con un documento evidenciable de evaluación de vulnerabilidades y amenazas
PROCEDIMIENTOS	Anexos 1	Respaldo y resguardo de información sensible o crítica	Respaldar la información sensible o crítica (física o digital) en lugares y ubicaciones adecuadas.	Definido	70%	El proceso si existe dentro del Manual de Tecnología, pero no se considera toda la información sensible
PROCEDIMIENTOS	Anexos 1	Cultura de Seguridad de la información	Evaluar periódicamente el plan de capacitación, definir indicadores de madurez.	No existe	0%	No existe un plan de capacitación de seguridad de la información
PROCEDIMIENTOS	Anexos 1	Gestión de accesos tecnológicos	Procedimiento de control de accesos	Parcialmente	50%	Existen los lineamientos generales dentro del manual de Seguridad física y electrónica, pero es necesario realizar de forma específica para ciertos accesos a información sensible.
PROCEDIMIENTOS	Anexos 1	Gestión de configuración	Procedimiento de gestión de configuración de activos tecnológicos	Definido	70%	Se cuenta con el proceso de configuración dentro del Manual de tecnología, pero requiere mejora
PROCEDIMIENTOS	Anexos 1	Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios de tecnología	Procedimiento de gestión de cambios, control de versiones en el que se registren las autorizaciones, ajustes y variaciones que se realicen en los servicios de tecnología	Definido	70%	Se cuenta con el proceso de gestión de cambios dentro del Manual de tecnología, pero requiere mejora
PROCEDIMIENTOS					32%	

CONTROLES TECNOLÓGICOS	Anexos 1	Arquitectura segura	La arquitectura debe tener una estrategia de defensa a profundidad y controles de flujo de información, aislamiento y segmentación, monitoreo y detección, y técnicas de cifrado.	Inicial	20%	Se cuenta con segmentación de red, pero no existe una arquitectura de seguridad definida
CONTROLES TECNOLÓGICOS	Anexos 1	Monitoreo y detección	Implementar sistemas que mantengan registros de logs, correlacionados de la infraestructura crítica que permitan su detección, análisis y depuración.	Inicial	20%	Solo se cuenta con información básica dentro del manual de tecnología, y los sistemas críticos cuentan con registros de logs, pero es necesario la adquisición de un software de monitoreo
		CONTROLES TECNOLÓGICOS			20%	

Fuente: Propia

ANEXO X

Tabla 49. Matriz de riesgo inicial

Tipificación	Clausula	Nivel de madurez	Amenaza o vulnerabilidad asociada	CAUSA	[P]	[I]	[R]
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Art. 15 Se debe contar con un comité de Seguridad de la información	5	Descoordinación en la gestión de SI, incumplimiento normativo, sanciones SEPS	Falta de gobernanza, ausencia de responsables claros	Media	Alto	Alto
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Art. 16 Se debe sesionar al menos dos veces al año	2	Riesgos no gestionados a tiempo, falta de evidencias para auditoría	Falta de seguimiento periódico, decisiones sin trazabilidad	Alta	Alto	Alto
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN		3					
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	Art. 17 Se debe contar con un Oficial de Seguridad de la Información	5	Gestión ineficaz del SGSI, incumplimiento normativo, exposición a incidentes	Designación de personal no calificado	Media	Muy alto	Alto
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN		5					

RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 1 - Consejo de Administración o directorio	2	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Alto	Alto
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 2 - Comité de Seguridad de la Información	0	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Alto	Alto
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 3 -Gerente General	2	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Alto	Alto
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 4 - Oficial de Seguridad de la Información	0	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Alto	Alto
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 5 - Auditor Interno	0	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Alto	Alto
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		1					
EVALUACIÓN Y CUMPLIMIENTO	Art. 13 evaluaciones, revisiones, pruebas, examenes y actualizaciones anualmente	1	Riesgos no detectados, planes ineficaces, vulnerabilidad ante incidentes	No ejecutar pruebas o hacerlo parcialmente	Alta	Alto	Alto
EVALUACIÓN Y CUMPLIMIENTO		1					
POLÍTICAS	Politica General de SI	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Clasificación de la Información	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto

POLÍTICAS	Gestión de riesgos de seguridad de la Información	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Control de accesos físicos y tecnológicos	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Gestión de incidentes	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Gestión de software	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Gestión infraestructura tecnológica	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Gestión de seguridad para Recursos Humanos	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Seguridad Física	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Gestión con terceros	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS	Ciberseguridad	0	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Muy Alto	Alto
POLÍTICAS		0					
PROCESOS	Identificación de procesos agregadores de valor	3	Ineficiencia operativa, dificultad en priorizar recursos y controles	No identificación de procesos críticos	Media	Alto	Alto

PROCESOS	Gestión de vulnerabilidades - Auditorías Informáticas	0	Exposición a ciberataques, pérdida de información, interrupción de servicios	Vulnerabilidades técnicas sin identificar ni corregir	Alta	Muy Alto	Muy Alto
PROCESOS	Gestión de vulnerabilidades - Plan de mitigación de hallazgos	0	Exposición a ciberataques, pérdida de información, interrupción de servicios	Vulnerabilidades técnicas sin identificar ni corregir	Alta	Muy Alto	Muy Alto
PROCESOS	Adquisición y desarrollo de hadware, software y servicios	2	Adquisición de tecnología ineficientes, brechas de seguridad en sistemas	Falta de criterios de seguridad en compras o desarrollos	Media	Alto	Alto
PROCESOS	Planes de Contingencia Tecnológica y continuidad del negocio	2	Interrupción prolongada de operaciones, afectación de socios, sanciones regulatorias	No contar con planes probados	Media	Muy alto	Muy alto
PROCESOS	Cifrado	2	Filtración de información, pérdida de confidencialidad.	Datos almacenados o transmitidos en texto plano	Alta	Muy Alto	Alto
PROCESOS		2					
PROCEDIMIENTOS	Inventario y Clasificación de información - Identificación de tipos de información	0	Pérdida de control sobre activos, dificultad para priorizar medidas de seguridad	No identificar activos ni su criticidad	Alta	Alto	Alto
PROCEDIMIENTOS	Inventario y Clasificación de información - Inventario de activos de información	1	Falta de visión integral del riesgo, decisiones sin base, incumplimiento normativo	No identificar activos ni su criticidad	Alta	Alto	Alto
PROCEDIMIENTOS	Inventario y Clasificación de información - Clasificación de activos de información	0	Falta de visión integral del riesgo, decisiones sin base, incumplimiento normativo	No identificar activos ni su criticidad	Alta	Alto	Alto
PROCEDIMIENTOS	Gestión de Riesgos	0	Falta de visión integral del riesgo, decisiones sin base, incumplimiento SEPS	No se han evaluado amenazas y vulnerabilidades	Media	Muy Alto	Alto
PROCEDIMIENTOS	Respaldo y resguardo de información sensible o crítica	3	Pérdida de datos críticos, indisponibilidad de servicios por periodos largos	Respaldo incompleto o en sitios no seguros	Alta	Muy Alto	Muy alto
PROCEDIMIENTOS	Cultura de Seguridad de la información	0	Riesgos internos elevados (phishing, mal uso de sistemas)	Capacitación insuficiente, usuarios poco conscientes	Media	Alto	Alto

PROCEDIMIENTOS	Gestión de accesos tecnológicos	2	Accesos no autorizados, fraude interno, fuga de información	Usuarios con privilegios excesivos o sin control de de la trazabilidad de la información	Alta	Muy alto	Alto
PROCEDIMIENTOS	Gestión de configuración	3	Fallas de configuración, afectación a los servicios.	Cambios no controlados en sistemas	Media	Alto	Alto
PROCEDIMIENTOS	Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios de tecnología	3	Interrupciones de servicio, errores no rastreables, pérdida de integridad	No analizar, registrar ni autorizar cambios	Alta	Alto	Alto
PROCEDIMIENTOS		2					
CONTROLES TECNOLÓGICOS	Arquitectura segura	1	Expansión rápida de ataques, caída de servicios críticos	Red sin segmentación, falta de aislamiento	Media	Muy Alto	Alto
CONTROLES TECNOLÓGICOS	Monitoreo y detección	1	Incidentes no detectados a tiempo, retraso en respuesta, mayor impacto de ataques	Ausencia de correlación de logs, falta de SIEM	Alta	Muy Alto	Muy Alto

Fuente: Propia

ANEXO XI

Tabla 50. Matriz de evaluación final

Tipificación	# Sección	Clausula	Descripción de control	Estado	%	Observación
EVALUACIÓN DE CUMPLIMIENTO PARA REGIMEN ESPECIAL						
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 15 Se debe contar con un comité de Seguridad de la información	Determinar la conformación del comité, alineado a la normativa	Optimizado	100 %	Se encuentra formalizado.
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 16 Se debe sesionar al menos dos veces al año	Verificar constancia de sesiones	Optimizado	100 %	Se cumple con lo establecido de al menos 2 veces al año
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN					100 %	
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 17 Se debe contar con un Oficial de Seguridad de la Información	Determinar la existencia de un Oficial de Seguridad de la Información con título de tercer nivel y capacitación de 40 horas en seguridad	Optimizado	100 %	OSI cumple con todos los requisitos

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN					100 %	
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 1 - Consejo de Administración o directorio	El directorio debe aprobar PESI, recursos humanos, técnicos y financieros, políticas, procesos, procedimientos, plan de concienciación y formación, Gestión de riesgos.	Definido	60%	Manuales de políticas y Procedimientos aprobados, pero no se aprueban planes que están pendientes de elaboración hasta la publicación del nuevo PEI
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 2 - Comité de Seguridad de la Información	Debe proponer al Directorio el PESI, Los recursos humanos, técnicos y financieros, políticas, procedimientos, roles y responsabilidades, Plan de concienciación, plan de gestión de riesgos	Definido	60%	Manuales de políticas y Procedimientos elaborados, pero no se aprueban planes que están pendientes de elaboración hasta la publicación del nuevo PEI
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 3 - Gerente General	Liderar la gestión de seguridad de la información, designar al oficial de seguridad, coordinar la participación de todas las partes.	Optimizado	100 %	Cumple con todo lo mencionado, se verifica su participación en las actas del comité
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 4 - Oficial de Seguridad de la Información	Desarrollar, gestionar, monitorear el PESI, Diseñar y proponer las políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad, solicitar asignación de recursos, desarrollar y ejecutar Planes de concienciación	Definido	65%	Manuales de políticas y Procedimientos elaborados, pero no se aprueban planes que están pendientes de elaboración hasta la publicación del nuevo PEI y falta de gestión de riesgos de seguridad
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	CAPITULO III	Art. 12, numeral 5	Auditor Interno	Optimizado	100 %	Se tiene una planificación anual que se viene cumpliendo adecuadamente
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					77%	

EVALUACIÓN Y CUMPLIMIENTO	CAPITULO III	Art. 13 evaluaciones, revisiones, pruebas, exámenes y actualizaciones anualmente	Verificar la documentación de evaluaciones, revisiones, pruebas, exámenes y actualizaciones	Administrado	100 %	Se presenta una matriz de evaluación, las revisiones son comunicadas a Gerencia y al Comité de Seguridad de la información
EVALUACIÓN Y CUMPLIMIENTO					100 %	
EVALUACIÓN DE ANEXO 1						
POLÍTICAS	Anexo 1	Política General de SI	Política aprobada y socializada	Optimizado	100 %	Política aprobada y socializada
POLÍTICAS	Anexo 1	Clasificación de la Información	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Gestión de riesgos de seguridad de la Información	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Control de accesos físicos y tecnológicos	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Gestión de incidentes	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Gestión de software	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Gestión infraestructura tecnológica	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización

POLÍTICAS	Anexo 1	Gestión de seguridad para Recursos Humanos	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Seguridad Física	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Gestión con terceros	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
POLÍTICAS	Anexo 1	Ciberseguridad	Política aprobada y socializada	Administrado	80%	Política aprobada y socializada, pero la ejecución y seguimiento de cumplimiento depende de la organización
		POLÍTICAS			82%	
PROCESOS	Anexo 1	Identificación de procesos agregadores de valor	Verificar existencia de documento de procesos agregadores de valor	Administrado	80%	Necesita verificación con el manual de procesos de cada institución
PROCESOS	Anexo 1	Gestión de vulnerabilidades - Auditorías Informáticas	Auditorías internas y externas	Definido	70%	Se mantiene una planificación de Auditoría interna pero no se ha ejecutado una auditoría externa netamente a tecnología y seguridad de la información
PROCESOS	Anexo 1	Gestión de vulnerabilidades - Plan de mitigación de hallazgos	Plan de hallazgos para mitigar los resultados de las auditorías o pruebas de Pentesting	Administrado	90%	Aún no se cumple la mitigación de hallazgos de Pentesting
PROCESOS	Anexo 1	Adquisición y desarrollo de hadware, software y servicios	Disponer de procedimientos para la adquisición y desarrollo de software, hadware y servicios en la que se incluyan temas relacionados a la seguridad	Definido	65%	Cuenta con lineamientos, pero no se establece un esquema del proceso

PROCESOS	Anexo 1	Planes de Contingencia Tecnológica y continuidad del negocio	Elaborar Planes de Contingencia Tecnológica y continuidad del negocio	Definido	70%	Existen Los planes aprobados, pero no se ajustan a la realidad institucional, además no se evidencia que existen pruebas documentadas
PROCESOS	Anexo 1	Cifrado	Procedimientos de cifrado de información sensible o crítica	Parcialmente	50%	Se realiza cifrado con Veracript pero no se cuenta con un procedimiento formal
		PROCESOS			71%	
PROCEDIMIENTOS	Anexos 1	Inventario y Clasificación de información - Identificación de tipos de información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos de activos de información considerando los criterios de disponibilidad, integridad y confidencialidad.	Definido	70%	Se cuenta con lineamientos para la identificación de los tipos de activos, pero no existe un procedimiento como tal
PROCEDIMIENTOS	Anexos 1	Inventario y Clasificación de información - Inventario de activos de información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos de activos de información considerando los criterios de disponibilidad, integridad y confidencialidad.	Definido	70%	Se cuenta con un levantamiento de activos de información, pero requiere una actualización
PROCEDIMIENTOS	Anexos 1	Inventario y Clasificación de información - Clasificación de activos de información	Disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos de activos de información considerando los criterios de disponibilidad, integridad y confidencialidad.	Definido	70%	Se cuenta con una clasificación de activos de información, pero requiere una actualización
PROCEDIMIENTOS	Anexos 1	Gestión de Riesgos	Documento evidenciable en el cual se evalúan vulnerabilidades y amenazas con el fin de determinar el nivel de riesgo	Administrado	80%	Se tiene una matriz de riesgo, pero necesita, revisión, mejora y actualización

PROCEDIMIENTOS	Anexos 1	Respaldo y resguardo de información sensible o crítica	Respaldar la información sensible o crítica (física o digital) en lugares y ubicaciones adecuadas.	Administrado	75%	Proceso se lo realiza de forma adecuada, pero no existe un proceso actualizado, ni tampoco existe evidencia documentada de su verificación
PROCEDIMIENTOS	Anexos 1	Cultura de Seguridad de la información	Evaluar periódicamente el plan de capacitación, definir indicadores de madurez.	Administrado	75%	Es necesario mejorar la cultura de capacitación hacia socios y clientes.
PROCEDIMIENTOS	Anexos 1	Gestión de accesos tecnológicos	Procedimiento de control de accesos	Definido	70%	Existen los lineamientos generales, pero es necesario realizar de forma específica para ciertos accesos sensibles.
PROCEDIMIENTOS	Anexos 1	Gestión de configuración	Procedimiento de gestión de configuración de activos tecnológicos	Administrado	80%	Se cuenta con el proceso de configuración, pero no se presenta un esquema
PROCEDIMIENTOS	Anexos 1	Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios de tecnología	Procedimiento de gestión de cambios, control de versiones en el que se registren las autorizaciones, ajustes y variaciones que se realicen en los servicios de tecnología	Definido	70%	Se cuenta con el proceso de gestión de cambios, pero no se presenta un esquema
		PROCEDIMIENTOS			73%	
CONTROLES TECNOLÓGICOS	Anexos 1	Arquitectura segura	La arquitectura debe tener una estrategia de defensa a profundidad y controles de flujo de información, aislamiento y segmentación, monitoreo y detección, y técnicas de cifrado.	Parcialmente	40%	Solo se tiene información general de la arquitectura

CONTROLES TECNOLÓGICOS	Anexos 1	Monitoreo y detección	Implementar sistemas que mantengan registros de logs, correlacionados de la infraestructura crítica que permitan su detección, análisis y depuración.	Inicial	20%	Solo se cuenta con información básica, es necesario la adquisición de un software de monitoreo
CONTROLES TECNOLÓGICOS					30%	

Fuente: Propia

ANEXO XII

Tabla 51. Matriz de riesgos final

Tipificación	Clausula	%	AMENAZA O VULNERABILIDAD ASOCIADA	CAUSA	[P]	[I]	[R]
EVALUACIÓN DE CUMPLIMIENTO PARA REGIMEN ESPECIAL							
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Art. 15 Se debe contar con un comité de Seguridad de la información	100 %	Descoordinación en la gestión de SI, incumplimiento normativo, sanciones SEPS	Falta de gobernanza, ausencia de responsables claros	Media	Antes: A Ahora: MB	Antes: A Ahora: B
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Art. 16 Se debe sesionar al menos dos veces al año	100 %	Riesgos no gestionados a tiempo, falta de evidencias para auditoría	Falta de seguimiento periódico, decisiones sin trazabilidad	Alta	Antes: A Ahora: MB	Antes: A Ahora: M
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN		100 %					
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	Art. 17 Se debe contar con un Oficial de Seguridad de la Información	100 %	Gestión ineficaz del SGSI, incumplimiento normativo, exposición a incidentes	Designación de personal no calificado	Media	Antes: MA Ahora: M	Antes: A Ahora: M
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN		100 %					
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 1 - Consejo de Administración o directorio	60%	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Antes: A Ahora: M	Antes: A Ahora: M

RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 2 - Comité de Seguridad de la Información	60%	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Antes: A Ahora: M	Antes: A Ahora: M
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 3 - Gerente General	100 %	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Antes: A Ahora: M	Antes: A Ahora: M
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 4 - Oficial de Seguridad de la Información	65%	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Antes: AAhora: M	Antes: AAhora: M
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Art. 12, numeral 5 - Auditor Interno	100 %	Omisión responsabilidades, aumento del riesgo operativo	Falta de claridad en las funciones	Media	Antes: A Ahora: B	Antes: A Ahora: M
RESPONSABILIDADES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		77%					
EVALUACIÓN Y CUMPLIMIENTO	Art. 13 evaluaciones, revisiones, pruebas, examenes y actualizaciones anualmente	100 %	Riesgos no detectados, planes ineficaces, vulnerabilidad ante incidentes	No ejecutar pruebas o hacerlo parcialmente	Alta	Antes: A Ahora: B	Antes: A Ahora: M
EVALUACIÓN Y CUMPLIMIENTO		100 %					

EVALUACIÓN DE ANEXO 1

POLÍTICAS	Politica General de SI	100 %	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Clasificación de la Información	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Gestión de riesgos de seguridad de la Información	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Control de accesos físicos y tecnológicos	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Gestión de incidentes	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MAAhora: B	Antes: AAhora: M
POLÍTICAS	Gestión de software	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Gestión infraestructura tecnológica	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M

POLÍTICAS	Gestión de seguridad para Recursos Humanos	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Seguridad Física	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Gestión con terceros	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS	Ciberseguridad	80%	Desconocimiento por parte de usuarios, incumplimiento regulatorio, exposición a ataques	Ausencia de políticas formales o falta de socialización	Alta	Antes: MA Ahora: B	Antes: A Ahora: M
POLÍTICAS		82%					
PROCESOS	Identificación de procesos agregadores de valor	80%	Ineficiencia operativa, dificultad en priorizar recursos y controles	No identificación de procesos críticos	Media	Antes: A Ahora: A	Antes: A Ahora: A
PROCESOS	Gestión de vulnerabilidades - Auditorías Informáticas	70%	Exposición a ciberataques, pérdida de información, interrupción de servicios	Vulnerabilidades técnicas sin identificar ni corregir	Alta	Antes: MAAhora: M	Antes: MA Ahora: A
PROCESOS	Gestión de vulnerabilidades - Plan de mitigación de hallazgos	90%	Exposición a ciberataques, pérdida de información, interrupción de servicios	Vulnerabilidades técnicas sin identificar ni corregir	Alta	Antes: MA Ahora: A	Antes: MA Ahora: A

PROCESOS	Adquisición y desarrollo de hadware, software y servicios	65%	Adquisición de tecnología ineficientes, brechas de seguridad en sistemas	Falta de criterios de seguridad en compras o desarrollos	Media	Antes: A Ahora: B	Antes: A Ahora: M
PROCESOS	Planes de Contingencia Tecnológica y continuidad del negocio	70%	Interrupción prolongada de operaciones, afectación de socios, sanciones regulatorias	No contar con planes probados	Media	Antes: MA Ahora: A	Antes: MA Ahora: A
PROCESOS	Cifrado	50%	Filtración de información, pérdida de confidencialidad.	Datos almacenados o transmitidos en texto plano	Alta	Antes: A Ahora: MB	Antes: A Ahora: B
PROCESOS		71%					
PROCEDIMIENTOS	Inventario y Clasificación de información - Identificación de tipos de información	70%	Pérdida de control sobre activos, dificultad para priorizar medidas de seguridad	No identificar activos ni su criticidad	Alta	Antes: A Ahora: B	Antes: A Ahora: M
PROCEDIMIENTOS	Inventario y Clasificación de información - Inventario de activos de información	70%	Falta de visión integral del riesgo, decisiones sin base, incumplimiento normativo	No identificar activos ni su criticidad	Alta	Antes: AAhora: B	Antes: A Ahora: M

PROCEDIMIENTOS	Inventario y Clasificación de información - Clasificación de activos de información	70%	Falta de visión integral del riesgo, decisiones sin base, incumplimiento normativo	No identificar activos ni su criticidad	Alta	Antes: A Ahora: B	Antes: A Ahora: M
PROCEDIMIENTOS	Gestión de Riesgos	80%	Falta de visión integral del riesgo, decisiones sin base, incumplimiento SEPS	No evaluar amenazas y vulnerabilidades	Media	Antes: A Ahora: M	Antes: A Ahora: M
PROCEDIMIENTOS	Respaldo y resguardo de información sensible o crítica	75%	Pérdida de datos críticos, indisponibilidad de servicios por periodos largos	Respaldo incompleto o en sitios no seguros	Alta	Antes: MA Ahora: M	Antes: MA Ahora: A
PROCEDIMIENTOS	Cultura de Seguridad de la información	75%	Riesgos internos elevados (phishing, mal uso de sistemas)	Capacitación insuficiente, usuarios poco conscientes	Media	Antes: A Ahora: MB	Antes: A Ahora: B
PROCEDIMIENTOS	Gestión de accesos tecnológicos	70%	Accesos no autorizados, fraude interno, fuga de información	Usuarios con privilegios excesivos o sin control de de la trazabilidad de la información	Alta	Antes: MA Ahora: M	Antes: A Ahora: A
PROCEDIMIENTOS	Gestión de configuración	80%	Fallas de configuración, afectación a los servicios.	Cambios no controlados en sistemas	Media	Antes: A Ahora: M	Antes: A Ahora: M
PROCEDIMIENTOS	Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios de tecnología	70%	Interrupciones de servicio, errores no rastreables, pérdida de integridad	No analizar, registrar ni autorizar cambios	Alta	Antes: AAhora: B	Antes: AAhora: M

PROCEDIMIENTOS		73%					
CONTROLES TECNOLÓGICOS	Arquitectura segura	90%	Expansión rápida de ataques, caída de servicios críticos	Red sin segmentación, falta de aislamiento	Media	Antes: MA Ahora: M	Antes: A Ahora: M
CONTROLES TECNOLÓGICOS	Monitoreo y detección	85%	Incidentes no detectados a tiempo, retraso en respuesta, mayor impacto de ataques	Ausencia de correlación de logs, falta de SIEM	Alta	Antes: MA Ahora: B	Antes: MA Ahora: M

Fuente: propia