



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN: MENCIÓN SEGURIDAD INFORMÁTICA

TEMA:

MARCO DE TRABAJO DE EVALUACIÓN DE LA SEGURIDAD DEL SGSI EN UNA
COOPERATIVA DE AHORRO Y CRÉDITO DEL SEGMENTO 1 BASADO LA NORMA
ISO/IEC 27007:2020 Y ISO/IEC 27004:2016.

Trabajo de Investigación previo a la obtención del Título de Magíster en Computación con
mención Seguridad Informática

AUTOR: Ing. Edison Orlando Túquerres Cancan

DIRECTOR: Msc. Cosme MacArthur Ortega Bustamante

IBARRA - ECUADOR

2024

DEDICATORIA

A mis padres e hijos, por su inquebrantable apoyo y amor incondicional a lo largo de este viaje académico y personal. Su constante aliento y sacrificio han sido la luz que me ha guiado en los momentos más importantes de la vida.

Edison Orlando Túquerres Cancan

AGRADECIMIENTO

Quisiera expresar mi sincero agradecimiento a, mi tutor por su orientación experta y su invaluable consejo durante el desarrollo de este trabajo. Sus conocimientos y dedicación han sido fundamentales para el éxito de esta investigación. Agradezco profundamente a mis amigos y seres queridos por su comprensión, ánimo y palabras de aliento en cada paso del camino. Finalmente, quiero expresar mi gratitud a todas aquellas personas que de alguna manera contribuyeron a la realización de este proyecto, su contribución no ha pasado desapercibida y ha sido fundamental para alcanzar este logro.

Edison Orlando Túquerres Cancan

REPÚBLICA DEL ECUADOR



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

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

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:	100232926-4	
APELLIDOS Y NOMBRES:	Edison Orlando Túquerres Cancan	
DIRECCIÓN:	El limonal 3-80 Y Durazno	
E-MAIL:	edissont@hotmail.com	
TELÉFONO FIJO:	No dispone	TELÉFONO MÓVIL: 0999655086

DATOS DE LA OBRA	
TÍTULO:	Marco de trabajo de evaluación de la seguridad del SGSI en una Cooperativa de Ahorro y Crédito del segmento 1 basado la norma ISO/IEC 27007:2020 Y ISO/IEC 27004:2016.
AUTOR (ES):	Túquerres Cancan Edison Orlando
FECHA: DD/MM/AA	19/02/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	<input type="checkbox"/> PREGRADO <input checked="" type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	Magister en computación con mención en seguridad informática
ASESOR/DIRECTOR:	Msc. Cosme Ortega, Phd. Marco Pusdá

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 13 días del mes de marzo de 2024

EL AUTOR:

Firma:

A handwritten signature in blue ink, consisting of several loops and strokes, positioned to the right of the 'Firma:' label.

Nombre: Edison Orlando Túquerres

CI: 100232926-4

REPÚBLICA DEL ECUADOR



UNIVERSIDAD TÉCNICA DEL NORTE
 Acreditada Resolución Nro. 173-SE-33-CACES-2020
FACULTAD DE POSGRADO



Ibarra, 19 de febrero de 2024


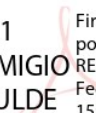
Dra.
 Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado "MARCO DE TRABAJO DE EVALUACIÓN DE LA SEGURIDAD DEL SGSI EN UNA COOPERATIVA DE AHORRO Y CRÉDITO DEL SEGMENTO 1 BASADO LA NORMA ISO/IEC 27007:2020 Y ISO/IEC 27004:2016" del maestrante Túquerres Cancan Edison Orlando, de la Maestría de Computación con mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	Firma
Tutor/a	Msc. Cosme MacArthur Ortega Bustamante	1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE  Firmado digitalmente por 1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE Fecha: 2024.02.19 15:09:34 -05'00'
Asesor/a	Phd. Marco Pusdá Chulde	0401200951 MARCO REMIGIO PUSDA CHULDE  Firmado digitalmente por 0401200951 MARCO REMIGIO PUSDA CHULDE Fecha: 2024.02.19 15:10:56 -05'00'

INDICE DE CONTENIDOS

CAPITULO I	15
EL PROBLEMA	15
1.1. Problema de investigación	15
1.2. Interrogantes de la investigación	16
1.3. Objetivos de la investigación	16
1.3.1. Objetivo general.....	16
1.3.2 Objetivos específicos	16
1.4. Justificación	17
1.4.1. Justificación institucional	17
1.4.2. Justificación metodológica.....	17
1.4.3. Justificación teórica	18
CAPITULO II.....	19
MARCO REFERENCIAL.....	19
2.1. Antecedentes	19
2.2. Marco teórico	22
2.2.1. Introducción al marco teórico	22
2.2.2. Fundamentos de la SI.....	22
2.2.3. Sistemas de gestión de seguridad de la información (SGSI).....	23
2.2.4. Normativas y estándares de SI.....	23
2.2.5. Metodologías de evaluación de seguridad	29
2.2.6. SI en CAC	32
2.3. Marco Legal	38
2.3.1. Introducción al marco legal	38
2.3.2. Marco legal específico para CAC.....	39

CAPÍTULO 3.....	42
METODOLOGÍA.....	42
3.1 Diagnostico del SGSI.....	42
3.1.1 Justificación institucional	42
3.1.2 Justificación metodológica.....	42
3.1.3 Justificación teórica	43
3.1.3 Evaluación de la necesidad del SGSI	43
3.1.4 Análisis de recursos disponibles	43
3.1.5 Identificación de obstáculos.....	43
3.1.6 Valoración de la disposición de la dirección.....	44
3.1.7 Determinación de la conveniencia de la metodología	44
3.2 Identificación de métricas de cumplimiento (etapa diagnóstico inicial)	44
3.3 Metodología (marco de trabajo propuesto).....	46
3.3.1 Marco de trabajo de evaluación de la seguridad.....	47
3.2 Análisis de sustentación de la metodología	68
3.3 Especificación del cumplimiento de objetivos	69
CAPÍTULO 4.....	72
RESULTADOS	72
4.1 Resultados obtenidos aplicados utilizando la metodología	72
4.1.1 Definición de objetivos	72
4.1.2 Diagnóstico del sistema de gestión del SGSI	73
4.1.3 Marco normativo.....	76
4.1.4 Desarrollo de indicadores de desempeño.....	77
4.1.5 Identificación de amenazas y vulnerabilidades.....	87
4.1.6 Evaluación de controles implementados:.....	95

4.1.7 Auditoría interna:	104
4.1.8 Medición del desempeño	106
4.1.9 Mejora continua	107
4.1.10 Documentación y reporte	108
4.1.11 Métricas utilizadas: evaluación específica para instituciones financieras	109
4.2 Resultados obtenidos aplicados utilizando la metodología	111
4.2.1 Definición de objetivos	111
4.2.2 Definición de criterios de evaluación	112
4.2.3 Métricas utilizadas	113
4.2.4 Procedimientos de evaluación	114
4.2.5 Frecuencia de evaluación	115
4.2.6 Documentación de resultados	116
4.2.7 Beneficios esperados	117
CAPÍTULO 5.....	119
MEDIDAS, ACCIONES Y ESTRATEGIAS PARA MEJORAR LA SI Y EL CUMPLIMIENTO NORMATIVO	119
5.1 Políticas y procedimientos actualizados	119
5.2 Formación y concienciación continua	120
5.3 Gestión de la SI.....	120
5.4 Protección de datos personales	121
5.5 Auditorías y revisiones periódicas	121
CONCLUSIONES Y RECOMENDACIONES.....	123
5.1 Conclusiones	123
5.2 Recomendaciones	124

INDICE DE TABLAS

Tabla 1 Checklist Inicial	74
Tabla 2 Checklist para identificación de patrones	74
Tabla 3 Checklist para identificación de tendencias	75
Tabla 4 Checklist para identificación de áreas críticas	75
Tabla 5 Revisión de políticas B3 Etapa inicial	79
Tabla 6 Revisión de políticas B3 Etapa actual.....	79
Tabla 7 Análisis B5 Métrica de Compromiso de la Gestión.....	81
Tabla 8 Análisis de riesgos según MAGERIT V3.0	88
Tabla 9 Evaluación de Efectividad de Salvaguardas	90
Tabla 10 Cálculo del riesgo residual según MAGERIT V3.0.....	91
Tabla 11 Índice IRI.....	96
Tabla 12 Índice ICF	97
Tabla 13 Índice IEC	98
Tabla 14 Índice ICN.....	99
Tabla 15 Índice IVES.....	99
Tabla 16 Índice IESES	100
Tabla 17 Políticas y procedimientos actualizados	119
Tabla 18 Formación y concienciación continua.....	120
Tabla 19 Gestión de la SI	120
Tabla 20 Protección de datos personales	121
Tabla 21 Auditorías y revisiones periódicas	122

INDICE DE FIGURAS

Figura 1 Flujo de la metodología Magerit v3	29
Figura 2 Normativas Técnicas ISO	39
Figura 3 Porcentaje de políticas revisadas – etapa actual	80

INDICE DE ECUACIONES

Ecuación 1 Índice de riesgo inicial (IRI)	63
Ecuación 2 Índice de prioridad de implementación (IPI):	64
Ecuación 3 Índice de concienciación y formación (ICF):	65
Ecuación 4 Índice de cumplimiento de normativas (ICN).....	66
Ecuación 5 Índice de valor de exposición al riesgo (IVES)	66
Ecuación 6 Índice de efectividad de salvaguardas (IESES)	67

REPÚBLICA DEL ECUADOR



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO



**MAESTRÍA EN COMPUTACIÓN CON MENSIÓN EN SEGURIDAD
INFORMÁTICA**

MARCO DE TRABAJO DE EVALUACIÓN DE LA SEGURIDAD DEL SGSI EN UNA
COOPERATIVA DE AHORRO Y CRÉDITO DEL SEGMENTO 1 BASADO LA
NORMA ISO/IEC 27007:2020 Y ISO/IEC 27004:2016.

Autor: Edison Orlando Túquerres

Director: Msc. Cosme Ortega

Año: 2024

RESUMEN

El presente estudio se centra en la evaluación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) en Cooperativas de Ahorro y Crédito (CAC), específicamente en el Segmento 1. Se ha desarrollado un marco de trabajo de evaluación basado en normativas y estándares reconocidos internacionalmente, como la ISO/IEC 27001, la ISO/IEC 27004 y Magerit v3. El objetivo general es implementar este marco para identificar el nivel de cumplimiento del SGSI en las CAC del Segmento 1.

Para lograr este objetivo, se han definido objetivos específicos que incluyen diagnosticar el SGSI implementado con respecto a la Resolución No. SEPS 2022-002, identificar métricas de cumplimiento apoyadas en la norma ISO/IEC 27004:2016, desarrollar el marco de trabajo de evaluación de la seguridad y evaluarlo mediante una prueba de concepto.

En términos metodológicos, se realiza un diagnóstico inicial del SGSI, se identifican

métricas de cumplimiento y se desarrolla el marco de trabajo de evaluación. Posteriormente, se lleva a cabo una evaluación de la efectividad del marco mediante una prueba de concepto. Los resultados obtenidos muestran un avance positivo en la seguridad de la información, con una mayor concienciación y formación del personal, una reducción significativa de riesgos y un cumplimiento normativo más sólido. Sin embargo, también se identifican áreas de mejora, como la necesidad de fortalecer ciertos controles de seguridad y mantener un seguimiento constante de los cambios legales y regulaciones relacionadas con la seguridad de la información.

Este estudio ofrece una contribución significativa al campo de la seguridad de la información en las CAC del Segmento 1, al proporcionar un marco de trabajo de evaluación y recomendaciones específicas para mejorar el SGSI y garantizar un cumplimiento normativo efectivo. Las conclusiones y recomendaciones ofrecidas servirán como guía para futuras investigaciones y prácticas en este ámbito.

Palabras clave: Seguridad de la Información, Sistema de Gestión, Cooperativas de Ahorro y Crédito, Normativas, Evaluación de Seguridad.

ABSTRACT

This study focuses on evaluating and improving the Information Security Management System (ISMS) in Savings and Credit Cooperatives (CAC), specifically in Segment 1. An evaluation framework has been developed based on regulations and internationally recognized standards, such as ISO/IEC 27001, ISO/IEC 27004, and Magerit v3. The general objective is to implement this framework to identify the level of ISMS compliance in the CACs of Segment 1. To achieve this objective, specific objectives have been defined that include diagnosing the ISMS implemented concerning Resolution No. SEPS 2022-002, identifying compliance metrics supported by the ISO/IEC 27004:2016 standard, developing the evaluation framework for security, and evaluating it through a proof of concept.

In methodological terms, an initial diagnosis of the ISMS is carried out, compliance metrics are identified, and the evaluation framework is developed. Subsequently, an evaluation of the framework's effectiveness is carried out through a proof of concept.

The results obtained show positive progress in information security, with greater awareness and training of staff, a significant reduction in risks, and stronger regulatory compliance. However, areas for improvement are also identified, such as the need to strengthen certain security controls and maintain constant monitoring of legal changes and regulations related to information security. This study offers a significant contribution to the field of information security in Segment 1 CACs by providing an evaluation framework and specific recommendations to improve the ISMS and ensure effective regulatory compliance. The conclusions and recommendations offered will serve as a guide for future research and practices in this area.

Keywords: Information Security, Management System, Savings and Credit Cooperatives, Regulations, Security Evaluation.

CAPITULO I

EL PROBLEMA

1.1. Problema de investigación

Conforme al creciente desarrollo tecnológico se ha producido un significativo efecto en las diversas actividades económicas que son parte del diario convivir del ser humano; en este sentido, se ha identificado la necesidad de los sistemas de información como herramienta válida para el desempeño de las organizaciones financieras.

El avance del denominado sistema de información se ha posicionado en el enfoque de procesos que estructuran las empresas, lo cual, se orienta a responder a los requerimientos del mercado y se soporta en el nivel de acceso a internet que dispone el cliente de una entidad.

Con el transcurrir del tiempo, ha sido evidente el desarrollo de normativas ISO (IEC 27007:2020 ISO/IEC 27004:2016) en función de constituirse en herramientas de gestión para todo tipo de las organizaciones, de todas maneras, su aplicación aún no llega a ser de uso común para los establecimientos. Así mismo, se ha determinado la existencia de empresas que persiguen consolidarse en el mercado para lo cual, la realización de procesos es un tema fundamental y en este ámbito es significativo el manejo de datos debidamente protegidos como parte de su potencial análisis y consecuente toma de decisiones.

En el asunto de entidades financieras como una Cooperativa de Ahorro y Crédito (CAC), ellas no escapan del ámbito de acción que se vincula al manejo de información relevante para el cliente interno y externo del establecimiento, sin embargo, no se caracterizan por disponer de ámbito de trabajo proactivo y que se encuentre en condición de responder de manera efectiva a las potenciales amenazas informáticas.

Por lo indicado, es preponderante el planteamiento de un SGSI que responda a las necesidades de una CAC con el fin de gestionar el nivel confidencial y la accesibilidad de los

datos que se manejan a nivel de clientes y como parte propiamente de su operación, con lo cual, es factible la reducción de eventuales riesgos en la información.

1.2. Interrogantes de la investigación

Las preguntas asociadas a la presente investigación se vinculan sobre cada uno de los objetivos específicos, con lo cual, se tiene:

- Cuál es el estado del procedimiento de la Norma de Control de la Seguridad de la Información (SI) de las CAC de Segmento 1, en relación con la Resolución No. SEPS 2022-002?
- Qué métricas de cumplimiento son necesarias para la ejecución del SGSI establecido en la norma ISO/IEC 27004:2016
- Cuál es el marco de trabajo de evaluación de la seguridad que se requiere desarrollar en soporte a la ISO/IEC 27007:2020 e ISO/IEC 27004 y Magerit v3?
- ¿Cómo se conoce el incremento o decremento del nivel de cumplimiento del SGSI en una CAC?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Implementar un marco de trabajo de evaluación para identificar el nivel de cumplimiento de implementación del SGSI en CAC del Segmento 1.

1.3.2 Objetivos específicos

- Diagnosticar el SGSI implementado con respecto a la Resolución No. SEPS 2022-002 cómo Norma de Control de la SI en CAC de segmento 1.
- Identificar métricas de cumplimiento de la implementación del SGSI apoyado en la norma ISO/IEC 27004:2016

- Desarrollar un marco de trabajo de evaluación de la seguridad basado en la ISO/IEC 27007: 2020. ISO/IEC 27004 y Magerit v3.
- Evaluar el marco con una prueba de concepto para verificar el incremento o decremento del nivel de cumplimiento del SGSI.

1.4. Justificación

1.4.1. Justificación institucional

A nivel de las CAC, las cuales, son de incidencia significativa en la economía de índole popular debido a su aplicación estratégica en grupos minoritarios de la población, es relevante la disposición del SGSI, pues el ámbito de la solidaridad y cooperación sobre organizaciones sociales y emprendimientos productivos requieren de un efectivo manejo de la información encomendada por sus clientes y que generen la consecuente confianza de los diversos participantes.

1.4.2. Justificación metodológica

Dentro de la actual investigación, los Sistemas de Información son identificados como parte de una variable independiente en su gestión, por lo mismo, dispone de una incidencia en la gestión por procesos de una organización. Dicho de otra manera, es indispensable una efectiva planificación que involucre el proceso en que se realiza en el proceso de toma de disposiciones en función del análisis de datos y del nivel de cumplimiento de los requerimientos asociados a las normativas ISO/IEC 27007: 2020. ISO/IEC 27004. La investigación se orienta a la creación de un SGSI que facilite una evaluación sobre su nivel de cumplimiento y el consecuente control y mejora de sus procesos, lo cual, se constituye en un tema de interés para el cliente interno y externo del establecimiento.

1.4.3. Justificación teórica

La investigación se orienta a resultados que motiven la identificación de ventajas inherentes a la presencia de un SGSI dentro de una actividad económica como la desarrollada por las CAC, por lo mismo, es factible la creación de un ámbito de trabajo proactivo dentro del desempeño de los procesos que son parte de la entidad financiera. Es necesario tener en cuenta que los sistemas de información (SI) facilitan el proceso de datos, por lo mismo, los mencionados SI son identificados como la columna vertebral de una organización. En consecuencia, el erróneo funcionamiento de los sistemas motiva la presencia de fallas y potencial incremento de riesgos sobre la información que se maneja. Por lo indicado, es significativo contar con un efectivo control de los SI, lo cual, involucra un grado de seguridad en el uso de los datos. Adicionalmente este trabajo de investigación contribuye a la línea de Seguridad de la Información.

CAPITULO II

MARCO REFERENCIAL

2.1. Antecedentes

En el criterio de Gómez (2018) la información que manejan las organizaciones es cada vez más significativa, esto al margen de su razón de ser y del propio sector de aplicación; por lo que, se sitúa como un activo de naturaleza intangible que es capaz de proporcionar una ventaja competitiva. El adecuado tratamiento de lo indicado requiere del uso de herramientas tecnológicas que brinden facilidades al procesamiento de datos, generación de informes y consecuentes decisiones. La aplicación tecnológica actual ha impulsado el desempeño y desarrollo de las organizaciones; por lo tanto, es un factor que ha multiplicado el margen de los riesgos informáticos debido al auge desmedido de la era digital y uso del internet. La propuesta respondió a la ausencia de procesos de auditoria en el medio de lo que se conoce como seguridad informática. La investigación dispuso como propósito la contribución a la determinación de las amenazas y vulnerabilidades en pro de la mitigación de los riesgos informáticos en base al diseño de una metodología que audite la inclusión de criterios de seguridad sobre la prestación de servicios en base al manejo de información. En el método se establecieron tres dimensiones relevantes para el desarrollo de una auditoria. Cada dimensión estableció un criterio que fue sujeto de evaluación por la verificación de controles informáticos. Los mencionados controles fueron definidos por requisitos que validen su implementación. La verificación de la metodología aplicó instrumentos de medición previamente diseñados que facilitaron la identificación de los hallazgos.

En el punto de vista de Cruz y Fukuzaki (2018) es factible la delineación y ejecución de un SGSI con la finalidad de la protección del activo de la información que influye de forma directa con el acatamiento de los objetivos empresariales. La metodología sobre el SGSI se soportó en el método Deming, lo cual, es sugerido en la ISO/IEC 27001; de esta manera, se

identificaron los activos de información y consecuente clasificación para conocer el impacto de una pérdida de información. Los controles se motivaron en la guía ISO/IEC 27002. El resultado se orientó a la implementación de un SGSI y minimización de riesgos y vulnerabilidades sobre la información de la entidad MEDCAM Perú S.A.C. así, se logró la confidencialidad, disponibilidad e integridad. Se concluyó el beneficio relevante al aseguramiento de los activos de información que maneja la entidad.

Para Yáñez (2018) la aplicación de un SGSI en una entidad de economía utilizó herramientas Open Source y la elaboración de modelos de desarrollo de mejora en función del cumplimiento de objetivos de control asociados a la norma ISO27001:2013. El trabajo se orientó a la gestión de los principales hallazgos de seguridad existentes en el establecimiento y que fueron parte del desarrollo del Ciclo PDCA del SGSI. Se priorizaron los hallazgos y se incorporaron las recomendaciones efectuadas por la DIPRES, adicionalmente, participó el Comité correspondiente del establecimiento. Se definieron políticas y procedimientos en base al contenido del SGSI cuya finalidad era la administración, monitoreo, control y mejora aplicable al ámbito de la seguridad. La metodología que se manejó se estableció en la aprobación de los métodos inherentes a la usanza de sistemáticas y ordenamientos de SI. Se propuso que las técnicas del SGSI se soporte en el control de riesgos, por lo tanto, los procesos estratégicos fueron priorizados por la exposición al riesgo. Se logró la optimización de los recursos necesarios en los proyectos de seguridad de datos y se favoreció el entendimiento del personal.

Por otra parte, Yáñez (2018) evaluó la implementación del SGSI en base a auditorías internas y externas. Las auditorías fueron independientes al equipo que participó en el SGSI y se concluyó que el manejo de la información estaba en el nivel medio. Sin embargo, en el arranque del trabajo no existía un SGSI efectivo para el resguardo de la información. A nivel

de recomendaciones se determinó el establecimiento y difusión de políticas y ordenamientos de la SI, gestión de objetivos asociados a la normativa ISO27001:2013.

En la visión de Rozo (2018) es necesario considerar el análisis, implementación, desarrollo y revisión de la aplicación de un SGSI dentro de una entidad privada o pública, este aspecto permitía el fortalecimiento de políticas y de procesos vinculados a la seguridad de su información, calidad en los procesos y confianza hacia los clientes y directivos. El desarrollo gigantesco de la tecnología potencializa el fraude y la exposición no autorizada sobre los datos y activos que maneja una organización, por lo tanto, es de vital importancia una preparación de los establecimientos para reaccionar a eventos inesperados en la conducción de la información.

Para García (2018) las diferentes organizaciones y su sistema de información se encuentra expuestos al sinnúmero de amenazas, las cuales, aprovechan las vulnerabilidades que son parte de su actividad económica y que las convierten en recursos de información esenciales por aspectos de engaño, vigilancia clandestina y acciones sabotadoras. Este particular repercute en los costos económicos y afectan de manera considerable la imagen que presentan la organización hacia el mercado. En este sentido, se tornaba prioritario el soporte y control de los procesos tecnológicos que son parte de las labores de una cooperativa, así como el diseño de un SSGSI en función del establecimiento de directrices y procesos establecidos por la organización.

Para Sánchez (2018) se debe tener claro los desafíos inherentes a la seguridad informática, lo cual, requiere del manejo adecuado de la informática de la entidad, es decir, es indispensable la seguridad en la red de datos de modo que el intercambio de información esté debidamente protegido y no se comprometa la integridad de la información nativa de actividades administrativas y financieras como es el caso de una Cooperativa. En este sentido, se determinaron seguridades a tomar en cuenta como salvaguardas de una entidad financiera y estas acciones se enfocaron en el cuidado de las direcciones IP, firewall físico, protocolos de

seguridad debidamente documentados, claves de seguridad, actualización de los planes de capacitación del personal, entre otros.

2.2. Marco teórico

2.2.1. Introducción al marco teórico

La cimentación del marco teórico es fundamental para conocer los fundamentos de la SI y su implementación en las CAC. Como señala Johnson (2018), el marco teórico es "el conjunto de conceptos, teorías y modelos que ayudan a comprender el fenómeno bajo estudio". En lo que se respecta a la SI, esta comprensión es fundamental para abordar eficazmente los desafíos y amenazas que enfrentan las organizaciones.

2.2.2. Fundamentos de la SI

La información segura es un concepto central en cualquier empresa u organización moderna. Según Tipton y Krause (2017) , se refiere a la custodia de los diferentes tipos de activos de información frente a algún tipo de acceso no autorizado, así como la divulgación, la interrupción o destrucción. Esta protección se fundamentó en tres pilares fundamentales, conocidos como el triángulo de la información segura: confiabilidad, integridad y disponibilidad.

La confidencialidad se asegura mediante la condición del acceso a la información solo a aquellos que tienen autorización. La integridad garantiza que los datos o información no sea transformada por personas no autorizadas, y con respecto a que esté disponible la información cuando se necesita. Estos principios son esenciales para resguardar los datos de los clientes y la integridad de las operaciones en una cooperativa de ahorro y crédito.

2.2.3. Sistemas de gestión de seguridad de la información (SGSI)

Un SGSI es una estructura organizativa que contiene políticas, procesos, instrucciones y recursos para administrar la SI de manera efectiva (ISO/IEC 27001:2013). La ejecución de un SGSI en una cooperativa de ahorro y crédito ofrece varios beneficios. Según Von Solms y Van Niekerk (2013), estos beneficios incluyen la reducción de riesgos, así como también un aumento en la eficiencia de las operaciones y el acatamiento de requisitos legales y regulatorios.

Dentro de un SGSI, la guía ISO/IEC 27001 determina elementos importantes, como la enunciación de una política de seguridad, la gestión de riesgos y ocurrencias. La norma proporciona un trazo sólido para implementar y mantener la SI en cualquier organización (ISO/IEC 27001:2013).

2.2.4. Normativas y estándares de SI

Guía ISO/IEC 27001:2013 – Requisitos que se necesita para un SGSI

La guía ISO/IEC 27001:2013 es uno de los estándares internacionales más significativos en el ámbito de la SI, ya que determina los requisitos fundamentales para el cumplimiento en un SGSI. Esta guía proporciona un enfoque organizado y sistemático para colaborar a las entidades a tratar los riesgos de SI, desde su identificación y evaluación (ISO/IEC 27001:2013).

Identificación de requisitos y componentes clave

- a. **Política de SI:** La norma solicita a que las organizaciones instituyan una política de SI que manifieste la responsabilidad con el resguardo de lo que son los activos de información (AI), así como el acatamiento de los requisitos legales y ordenaciones aplicables.
- b. **Evaluación de riesgos:** Las organizaciones deben realizar una evaluación de los riesgos para que se pueda identificar y comprender las amenazas, así como las vulnerabilidades que pueden afectar de alguna manera la SI.

- c. **Tratamiento de riesgos:** Cuando los riesgos se identifican, las organizaciones deben decidir cómo tratarlos. Es decir, lo que puede circunscribir en la ejecución de controles de seguridad, la aceptación del riesgo o la transferencia del riesgo a terceros.
- d. **Implementación de controles:** La norma facilita un conjunto de diferentes tipos de controles en donde las organizaciones pueden efectuar para mitigar los riesgos. Estos controles envuelven aspectos como las acciones de accesos, la seguridad física, la gestión de incidentes y otros.
- e. **Revisión y mejora continua:** La norma requiere que las organizaciones revisen y mejoren continuamente su SGSI para garantizar su efectividad a lo largo del tiempo.

Beneficios ISO/IEC 27001:2013:

- a. **Mejora en la seguridad:** Ayuda a distintas entidades u organizaciones a fortalecer sus prácticas de SI y reducir los riesgos de incidentes de seguridad.
- b. **Cumplimiento legal:** Ayuda a que se realice de forma ordenada el cumplimiento de exigencias legales y regulatorias relacionados con la SI.
- c. **Confianza de los Stakeholders:** Mejora la certidumbre de los clientes, distintas partes interesadas al señalar un compromiso claro con la SI.
- d. **Gestión eficaz de riesgos:** Suministra un marco sólido para el encargo de los riesgos de la SI.

Guía ISO/IEC 27007:2020 - Pautas para auditoría SGSI

La guía (ISO/IEC 27007:2020) se enfoca en proporcionar directrices para conducir a cabo auditorías efectivas de SGSI. Esta norma es esencial para afirmar que un SGSI esté operando correctamente y de cumplimiento con los requerimientos de la ISO/IEC 27001. La norma facilita orientación sobre cómo cumplir las auditorías de forma efectivas de SGSI.

Componentes clave de la ISO/IEC 27007:2020

- a. Alcance de la auditoría:** Define la importancia y las directrices de la auditoría, incluyendo los elementos específicos del SGSI que se evaluarán.
- b. Planificación de la auditoría:** Detalla los pasos necesarios para planificar una auditoría de SGSI efectiva, incluyendo la selección de auditores competentes y la definición de criterios de auditoría.
- c. Realización de la auditoría:** Describe cómo llevar a cabo la auditoría, incluyendo la recopilación de evidencia y la evaluación de los controles de SI.
- d. Informe de auditoría:** Establece los requisitos para la elaboración de informes de auditoría que incluyan hallazgos, conclusiones y recomendaciones.
- e. Seguimiento de la auditoría:** Proporciona orientación sobre cómo seguir los resultados de la auditoría y verificar la implementación de acciones correctivas.

Beneficios de la ISO/IEC 27007:2020:

- a. Mejora de la efectividad de las auditorías:** Ayuda a garantizar que las auditorías de SGSI sean más efectivas y eficientes.
- b. Cumplimiento normativo:** Contribuye al cumplimiento de forma continua de los requerimientos de la ISO/IEC 27001 y otras regulaciones aplicables.
- c. Gestión de incidentes continuada:** Facilita la tipificación y mitigación de riesgos de SI a través de auditorías regulares.

Norma ISO/IEC 27004:2016 - medición y métricas de SI

La norma (ISO/IEC 27004:2016) se enfoca en proporcionar orientación sobre cómo medir y evaluar el desempeño de un SGSI y sus controles. Esta norma es esencial para garantizar que un SGSI esté cumpliendo sus objetivos y que se mejore continuamente su efectividad (ISO/IEC 27004:2016).

Aspectos Clave de la ISO/IEC 27004:2016

- a. Establecimiento de métricas:** Describe cómo identificar, seleccionar y establecer métricas de SI que sean relevantes para la organización.
- b. Recopilación de datos:** Proporciona directrices sobre la recopilación de datos necesarios para medir el desempeño del SGSI y las inspecciones de seguridad.
- c. Análisis de datos:** Detalla cómo analizar los datos recopilados para valorar el desempeño y la actividad de los controles de seguridad.
- d. Elaboración de informes:** Define cómo elaborar informes que presenten las métricas y resultados de manera clara y comprensible.
- e. Mejora continua:** Ayuda a las organizaciones a utilizar los resultados de las métricas para mejorar continuamente su SGSI y la SI.

Beneficios de la ISO/IEC 27004:2016:

- a. Mejora basada en datos:** Proporciona una estructura que sirve como guía para el proceso de toma de decisiones enfocado en datos sólidos sobre la SI.
- b. Transparencia y comunicación:** Ayuda a comunicar de manera efectiva el estado de la SI a las partes interesadas.
- c. Mejora continua:** Contribuye al progreso continuo de las revisiones de seguridad y del SGSI en su asociación.

COBIT (Objetivos de revisión de la información y tecnologías afines)

COBIT es una estructura de trabajo largamente utilizado en todo el mundo que se centra en lo que se denomina gobierno y lo que se conoce como gestión de las TI. Fue perfeccionado por ISACA (Asociación de Auditoría y Revisión de SI) y suministra un conjunto de principios y directrices para ayudar a las empresas o instituciones a lograr un gobierno efectivo y una gestión de TI que se alinee con los objetivos del negocio (ISACA, 2021).

Componentes clave de COBIT

- a. **Dominios de Gobierno y Gestión:** COBIT se organiza en dominios que cubren áreas críticas de gobierno y gestión de TI, como la entrega de servicios, la evaluación de riesgos (GR) y el proceso de aseguramiento de la calidad (AC).
- b. **Procesos y objetivos de control:** Dentro de cada dominio, COBIT define procesos de TI específicos y establece objetivos de control que deben cumplirse para avalar el acatamiento de los requisitos y la entrega de valor a la organización.
- c. **Marco de referencia:** COBIT proporciona una estructura de referencia para la implementación de mejores prácticas en TI, incluyendo estándares y directrices aplicables.
- d. **Enfoque en resultados de negocio:** Uno de los aspectos más destacados de COBIT es su enfoque en la alineación de la TI con las metas del negocio. Esto promueve a las organizaciones a medir el valor que aporta la TI y a tomar decisiones informadas.

Beneficios de COBIT

- a. **Mejora del Gobierno de TI:** COBIT ayuda a las organizaciones a establecer un gobierno de TI sólido que sea efectivo y eficiente.
- b. **Reducción de Riesgos:** Proporciona una dirección estructurada para la realización de tratamiento de riesgos relacionados con la TI, lo que ayuda a minimizar las amenazas y vulnerabilidades.
- c. **Alineación con el Negocio:** Facilita la alineación de la TI con los objetivos estratégicos del negocio.

NIST (Instituto Nacional de Estándares y Tecnología) - Norma de Ciber seguridad de NIST

La norma es una guía detallada desarrollada por el NIST de USA. Este marco se centra en la GR cibernéticos y proporciona pautas específicas para facilitar a las organizaciones a proteger sus sistemas y datos de las amenazas cibernéticas (NIST, 2020).

Componentes clave del marco de ciberseguridad de NIST

- a. **Identificar:** Este paso implica la identificación de activos críticos, amenazas, vulnerabilidades y riesgos cibernéticos. Se centra en comprender y catalogar los activos de información y evaluar los riesgos asociados.
- b. **Proteger:** El siguiente paso se describe a la implementación de medidas de protección para reducir los riesgos identificados. Esto incluye controles de seguridad, políticas y procedimientos.
- c. **Detectar:** Aquí se aborda la localización temprana de amenazas y vulnerabilidades. Incluye la implementación de sistemas de monitoreo y detección de incidentes.
- d. **Responder:** Cuando se detecta una amenaza, este paso se enfoca en la respuesta rápida y efectiva para mitigar el impacto. Se establecen planes de respuesta a incidentes.
- e. **Recuperar:** Finalmente, se aborda la recuperación de los sistemas y datos afectados después de un incidente de ciberseguridad. Esto implica la restauración de la operatividad normal.

Beneficios del marco de ciberseguridad de NIST:

- a. **Enfoque integral:** Proporciona un enfoque completo y estructurado para gestionar la ciberseguridad desde la identificación hasta la recuperación.
- b. **Adaptabilidad:** Es escalable y adaptable a diferentes tipos y tamaños de organizaciones.
- c. **Estándar reconocido:** Es ampliamente reconocido y utilizado tanto en USA como a nivel internacional.

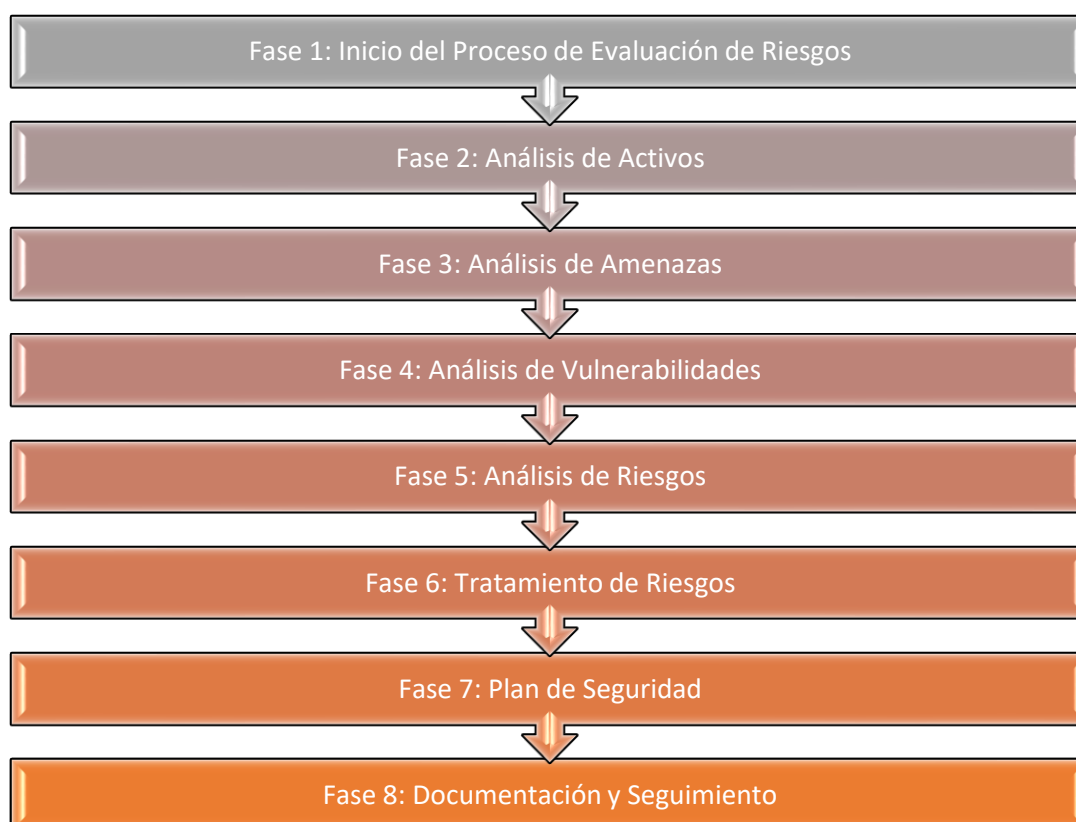
Además de las normas ISO, otros marcos de trabajo relevantes incluyen COBIT, que se centra en la gestión de TI y el gobierno, y la normativa de Ciberseguridad de NIST, que ofrece directrices detalladas para realizar el trabajo de riesgos cibernéticos.

Estas normas, en conjunto, proporcionan una estructura sólida para la ejecución, auditoría y medición efectiva de un SGSI, lo que es importante para avalar la protección de la información en una CAC.

2.2.5. Metodologías de evaluación de seguridad

La metodología Magerit v3 es un enfoque ampliamente utilizado para la evaluación de riesgos de SI. Magerit, cuyo nombre procede de las palabras metodología de estudio y gestión de contingencias de los SI, se enfoca en la tipificación de activos, ataques, vulnerabilidades y la valoración de la probabilidad e impacto de los riesgos. Magerit se enfoca en identificar activos, amenazas, vulnerabilidades y evaluar el impacto y la probabilidad de que se presenten los riesgos (MEYSS, 2019). La metodología es especialmente útil para comprender y abordar los riesgos específicos que afronta una cooperativa de ahorro y crédito. A continuación, se detalla el flujo de la metodología Magerit v3 en forma detallada (Magerit, 2023):

Figura 1 Flujo de la metodología Magerit v3



Fuente: (Magerit, 2023)

A continuación, se detalla el flujo de la metodología Magerit v3 en forma detallada:

Fase 1: Inicio del Proceso de evaluación de riesgos

1.1 Preparación: En esta etapa inicial, se instituyen los propósitos y alcances del proceso de evaluación de riesgos. Esto implica definir qué sistemas de información se evaluarán y los criterios para la evaluación.

Fase 2: Análisis de activos

2.1 Identificación de Activos: Se reconocen y catalogan los activos críticos de información que se encuentran en el ámbito de estudio. Esto incluye datos, sistemas, hardware, software y cualquier otro elemento relevante.

Fase 3: Análisis de amenazas

3.1 Tipificación de ataques: Se reconocen todas los posibles ataques que suelen perjudicar a los activos de información. Dichas amenazas pueden contener ataques cibernéticos, desastres naturales, errores humanos, etc.

Fase 4: Análisis de vulnerabilidades

4.1 Identificación de Vulnerabilidades: Se examinan las vulnerabilidades o debilidades que podrían ser explotadas por las amenazas identificadas en la fase anterior. Estas vulnerabilidades pueden estar relacionadas con la tecnología, los procesos o las personas.

Fase 5: Análisis de Riesgos

5.1 Evaluación de riesgos: En esta etapa, se evalúan los riesgos identificados. Esto se hace calculando la casualidad de que una amenaza abuse de una debilidad y la repercusión que podría tener en los activos. de información. La probabilidad e impacto se califican en una escala.

5.2 Cálculo de Riesgos: Se calcula el riesgo multiplicando la probabilidad por el impacto. Esto ayuda a priorizar los riesgos según su gravedad.

Fase 6: Tratamiento de riesgos

6.1 Identificación de protocolos o medidas de seguridad: Se proponen y eligen regímenes de protección para tratar los riesgos identificados. Dichas medidas pueden contener controles de seguridad, políticas, procedimientos y otros enfoques.

6.2 Análisis de Costo-Beneficio: Se evalúa el costo y el beneficio de implementar las medidas de seguridad propuestas. Esto ayuda a tomar decisiones informadas sobre qué medidas implementar.

Fase 7: Plan de seguridad

7.1 Desarrollo del Plan de Seguridad: Se crea un plan de protección que incluye todas las medidas de protección a implementar, los plazos y los responsables de su ejecución.

Fase 8: Documentación y seguimiento

8.1 Documentación: Se documentan todas las secuelas del proceso de valoración de riesgos, incluyendo la tipificación de activos, ataques, vulnerabilidades, riesgos, medidas de seguridad y el plan de seguridad.

8.2 Seguimiento y Revisión: Se determina un proceso continuo de seguimiento y reconocimiento de la SI para afirmar que las medidas implementadas sean efectivas y adecuadas a lo largo del tiempo.

La metodología Magerit v3 proporciona una dirección estructurada y completa para la valoración y gestión de posibles ataques o amenazas de SI, lo que concede a las organizaciones identificar, analizar y tratar de manera efectiva los riesgos que podrían afectar sus activos de información y la persistencia de sus operaciones.

Otras metodologías de evaluación, como OCTAVE y NIST SP 800-30, también son aplicables en la evaluación de la SI y pueden adaptarse según las necesidades específicas de la organización (CERT, 2021) (NIST, 2020).

2.2.6. SI en CAC

Las CAC derivan principalmente dependiente de los sistemas de información para gestionar cuentas, transacciones y servicios financieros. Los datos sensibles y críticos para estas instituciones incluyen información financiera de los clientes, datos personales y detalles de transacciones. Además, las CAC enfrentan desafíos específicos de seguridad, como el fraude financiero y la falta de resguardar la confiabilidad de los datos de los integrantes. La comprensión de estos desafíos es esencial para la realización efectiva de un SGSI en este entorno.

2.2.7 Casos de estudio

Caso de Estudio: Análisis y Gestión de Riesgos de los Sistemas de la CAC Jardín Azuayo manejando la Metodología MAGERIT

Introducción: La CAC Jardín Azuayo, ubicada en la región de Azuay en Ecuador, ha experimentado un crecimiento sostenido en sus operaciones y una creciente dependencia de sistemas de información para brindar servicios a sus socios y clientes (Lucero & Valverde , 2012). Con el propósito de asegurar la disponibilidad, confiabilidad e integridad de los datos de sus miembros y enfrentar los desafíos de seguridad cibernética en constante evolución, la cooperativa ha emprendido un proyecto de análisis y tratamiento de amenazas de seguridad de la información utilizando la metodología MAGERIT versión 2.

Contexto:

Nombre: CAC Jardín Azuayo.

Ubicación: Región de Azuay, Ecuador.

Objetivo: Evaluar y estimar los riesgos de seguridad de la información en los sistemas de la cooperativa utilizando la metodología MAGERIT versión 2.

Desarrollo del Proyecto:

Fase 1:

- Planificación del Proyecto: Se estableció el marco general del proyecto, definiendo los objetivos, la importancia y los recursos necesarios para la evaluación de riesgos.

Fase 2:

- Análisis de riesgos: Tipificación de Activos: Se catalogaron todos los activos críticos de información, incluyendo los datos financieros de los socios, registros de transacciones, sistemas de información y la infraestructura tecnológica.
- Identificación de amenazas: Se identificaron una serie de amenazas potenciales, como ataques cibernéticos, malware, errores humanos y desastres naturales, que podrían afectar a los recursos de información esenciales de la cooperativa.
- Identificación de debilidades o vulnerabilidades: Se realizaron evaluaciones exhaustivas para identificar las vulnerabilidades en la infraestructura tecnológica, incluyendo posibles brechas de seguridad y debilidades en los sistemas.

Fase 3: Gestión de Riesgos

- Evaluación de peligros: Se evaluó la posibilidad y el impacto de las amenazas identificadas en relación con las vulnerabilidades. Los riesgos se calificaron en una escala para priorizarlos.
- Tratamiento de riesgos: Se desarrolló un plan para implementar acciones de seguridad adecuadas, como la mejora de las políticas de seguridad, la actualización de sistemas y la implementación de controles de acceso más rigurosos.

Herramienta utilizada: PILAR Basic

Para conseguir se realiza la valoración de amenazas en el SI, para lo cual se implementó la herramienta PILAR Basic. Esta herramienta permitió conjugar los activos del sistema, identificar amenazas y sugerir salvaguardas para minimizar el riesgo.

Resultados y Beneficios:

- La evaluación de riesgos reveló áreas críticas de vulnerabilidad y riesgo para la cooperativa.
- Se implementaron medidas de seguridad efectivas para mitigar los riesgos identificados.
- La cooperativa mejoró su capacidad para revelar, advertir, reconocer y responder a amenazas cibernéticas.
- Se logró un mayor nivel de confianza de los socios y clientes en la seguridad de sus datos financieros.
- La cooperativa cumplió con las regulaciones de SI y los requisitos legales relacionados.

La aplicación de la metodología MAGERIT versión 2 en la CAC Jardín Azuayo permitió una evaluación integral y efectiva de los riesgos de SI, fortaleciendo así la defensa de los activos y la confianza de los miembros y clientes. Esta iniciativa demuestra el compromiso de la cooperativa con la SI en un entorno financiero en constante evolución.

Caso de estudio: Valoración de amenazas de los SI de Audioauto S.A. utilizando MAGERIT V3.0 y COBIT V4.1

Contexto: Audioauto S.A. es una compañía que trabaja en el sector automotriz y que depende principalmente de los SI para gestionar sus operaciones. La organización ha emprendido un proyecto de evaluación de los riesgos de SI con el objetivo de establecer el entorno actual de

riesgo en la que se encuentran sus sistemas y establecer acciones para controlar y mitigar estas amenazas (Cruz & Chamorro, 2012). La metodología MAGERIT V3.0 y los Objetivos de Control de COBIT V4.1 se utilizan como marcos de trabajo para este análisis.

Desarrollo del Proyecto:

Fase 1: Identificación de Activos y Dimensiones de Seguridad

- Se realizó un registro de datos de la estructura interna de la institución para identificar los principales activos de (TI), procesos de negocio y SI.
- Se enfocaron en las dimensiones de seguridad sugeridas por MAGERIT: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad para evaluar y gestionar el riesgo.

Fase 2: Caracterización y Valoración de Activos

- Se aplicó MAGERIT para caracterizar y valorar cuantitativamente los activos de TI. Esto implicó determinar su valor y su interrelación con los procesos de negocio.
- Se identificaron los posibles ataques de los que podrían estar expuestos estos activos y se evaluaron las salvaguardas existentes y las que podrían implementarse para mitigar los riesgos.

Fase 3: Evaluación de Efectividad y Riesgo

- Se estimó la eficacia de las salvaguardas existentes en comparación a los riesgos identificados.
- Se calculó el impacto potencial derivado de la posible ejecución de las amenazas y se determinaron los niveles de riesgo asociados.

Fase 4: Optimización del Riesgo según COBIT

- Desde la perspectiva de la Optimización del Riesgo de COBIT, se evaluaron las dimensiones Financiera, Cliente e Interna.
- Se identificaron debilidades relacionadas con el Gobierno y Gestión de TI en función de los objetivos denominados de control dentro de COBIT V4.1.

Resultados y beneficios:

- La evaluación de riesgos reveló áreas críticas de vulnerabilidad y riesgo en los SI de Audioauto S.A.
- Se implementaron medidas de seguridad efectivas para aminorar los riesgos identificados y mejorar la privacidad, integridad, disponibilidad y otras dimensiones de seguridad.
- La empresa pudo tomar decisiones informadas sobre la priorización de la optimización del riesgo en áreas específicas relacionadas con el gobierno y gestión de TI.
- Se logró un mayor nivel de seguridad y fidelidad en los SI de la empresa.
- La empresa se alineó con las principales prácticas de manejo de amenazas y SI, lo que le permitió ejecutar con regulaciones y requisitos legales.

La valoración de amenazas de SI en Audioauto S.A. manejando las metodologías MAGERIT V3.0 y COBIT V4.1 permitió una identificación efectiva de riesgos y la ejecución de medidas de seguridad adecuadas, mejorando la seguridad de los sistemas de información y fortaleciendo la gestión de TI en la empresa.

Caso de estudio: Auditoría sobre la Coop. “Surangay” Ltda.

En el caso de Valverde (2022) se trabajó una auditoría sobre la Coop. “Surangay” Ltda., siendo el período en cuestión el 2020; en este sentido, se requirió de procedimientos asociados a la auditoría en busca del control y mejora de la efectividad y ética del establecimiento. Se complementó el análisis con un flujo de información nativo de fuentes primarias y secundarias del establecimiento que facilitaron la aplicación de entrevistas con los responsables. Se revisó

la documentación pertinente inherente a los formatos facilitados por la SEPS. Como en los resultados se determinó el diagnóstico del control interno en función de los controles de los procedimientos informáticos de información, la evaluación ubicó un nivel de riesgo moderado, se identificaron debilidades y se priorizó la inexistencia de un manual de control interno. De manera cuantitativa, se utilizaron indicadores de gestión ligados a la actividad del establecimiento. Finalizada la auditoría, se establecieron hallazgos asociados al cumplimiento de objetivos y metas organizacionales.

Para Pilla (2019) la naturaleza de la información que maneja una organización es un activo relevante dentro de su actividad económica, pues esta, es susceptible de ser vulnerada por la intervención de grupos delincuenciales, lo cual, se constituye en un factor capaz de motivar pérdidas incalculables. A manera de referencia se tiene un informe desarrollado por la International Communication Union (ITU) que ubicó al Ecuador en el lugar 14 a nivel de Latinoamérica y en el sitio 98 en el mundo, esto en respecto a la gestión de políticas de ciberseguridad. El ranking establecido por el ITU induce que el Ecuador necesita trabajar en el diseño y realización de políticas en pro de prevenir potenciales ataques cibernéticos que perjudiquen la estructura organizacional a nivel directiva, trabajadores, clientes y proveedores. La problemática requirió de un diseño de política destinada al proceso TI de la Cooperativa, lo cual, se fundamentó en la normativa ISO/IEC 27002:2013. La propuesta se orientó a reducir la existencia de potenciales puntos vulnerables en los sistemas de información, así mismo, se establecieron dominios, objetivos y controles para la seguridad de datos. Se efectuó un diagnóstico de la informática del proceso de TI. Los resultados se agruparon en la matriz de riesgos de Deloitte y del Bco. de España, este particular detalló los recursos de información y los riesgos a ser evaluados. En función de la ISO 27002:2013, se identificaron controles destinados a controlar los eventos de alto riesgo; y al final, se determinó la política de SI para

el sector de Tecnología de Información. Se recomendó, una política a ser revisada y aprobada por el CA y luego difundida al personal de Cooperativa.

2.3. Marco Legal

2.3.1. Introducción al marco legal

El marco legal juega un papel crucial en la SI de las CAC, ya que establece los requisitos y regulaciones que deben cumplir. Este apartado proporciona una visión general de la importancia del marco legal en la SI. La Constitución vigente de Ecuador se determinó como la ordenación de la norma jurídica en la sistematización jurídico del país, con lo cual, prima sobre los diversos convenios y tratados a nivel internacional excepto en temas de Derechos Humanos, así como los Art. 3, 16, 66 (Núm. 19 y 21), 158, 313 y 393 (Registro Oficial, 2008) El Acuerdo Ministerial 006-2021 del Ministerio de Telecomunicaciones (MINTEL, 2021) determinó la Política de Ciberseguridad que se enfocó en el lineamiento necesario para un disponer de un Ecuador Ciber seguro que permita garantizar el Estado, a la vez que proteja los servicios, la infraestructura y la correspondiente seguridad de la comunidad. En este sentido el Gobierno Nacional determinó una gestión fundamentada en pilares como la ciber seguridad, el sistema de información, la protección del servicio digital, la soberanía, la seguridad pública y de los ciudadanos.

El Código Orgánico Integral Penal que constituye el agrupamiento de las normas jurídicas asociadas a faltas sujetas de sanciones, por lo que, es un documento legislativo que determina delitos y penas en función del código penal del Ecuador por temas como el manejo errado de información personal que es parte del desarrollo de una actividad (COIP, 2021).

A nivel de normas técnicas es válido considerar a (ISO, 2022):

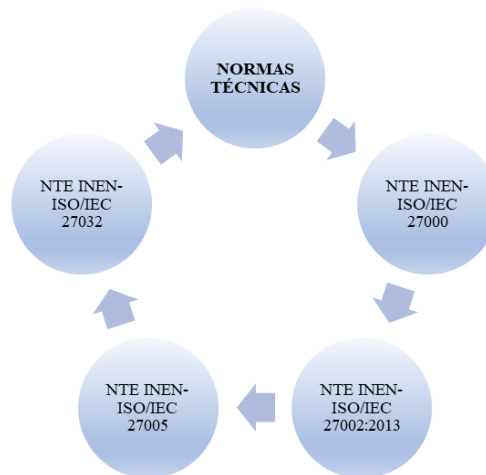
NTE INEN-ISO/IEC 27000.

NTE INEN-ISO/IEC 27002:2013.

NTE INEN-ISO/IEC 27005.

NTE INEN-ISO/IEC 27032.

Figura 2 Normativas Técnicas ISO



Fuente: (ISO, 2022)

La Ley Orgánica específicamente sobre la Identidad y Datos Civiles busca el garantizar el derecho a la identidad de los individuos en base al registro de los hechos consecuentes de la subsistencia de la población y cuyo manejo debe garantizar la ausencia de un manejo doloso de información de interés.

La Ley de la Seguridad que es Pública y es del Estado que controla seguridad integra del Estado ecuatoriano en base a derechos y justicia sobre sus habitantes, de esa manera, se garantiza el orden público y el buen vivir de personas naturales y jurídicas (Registro Oficial , 2016).

2.3.2. Marco legal específico para CAC

Es importante subrayar que las CAC están sujetas a regulaciones específicas en función de la jurisdicción y el país en el que operen. Estas regulaciones abordan temas relacionados con la SI y los SGSI de manera detallada. Se debe determinar y analizar estas regulaciones específicas para avalar el acatamiento y la seguridad de la información.

Marco legal específico para CAC en Ecuador

En el contexto de Ecuador, las CAC están sujetas a regulaciones específicas emitidas por la SEPS. La SEPS es la entidad reguladora encargada de supervisar y regular las actividades de las CAC en el país (SEPS, 2023).

Roles de la SEPS:

Supervisión y regulación: La SEPS tiene la responsabilidad de supervisar y reglamentar las operaciones de las CAC para garantizar su solidez financiera y la protección de los intereses de los miembros y depositantes.

Emisión de normativas: La SEPS emite regulaciones y resoluciones que establecen los requisitos y estándares que las CAC deben cumplir. Estas regulaciones incluyen disposiciones específicas relacionadas con la SI y la GR.

Resolución No. SEPS 2022-002 y su impacto

Dentro del marco legal específico para CAC en Ecuador, se destaca la Resolución No. SEPS 2022-002 emitida por la SEPS. Esta resolución establece requisitos y disposiciones importantes relacionados con la SI y la GR cibernéticos para las CAC en el país.

Algunos aspectos clave de la (Resolución No. SEPS 2022-002, 2022) incluyen:

Requisitos de SI: La resolución establece requisitos específicos relacionados con la SI, como la custodia de datos sensibles de los socios y clientes, la diligencia de accesos y la detección y respuesta a eventualidades de seguridad.

Evaluación y gestión de riesgos cibernéticos: La resolución requiere que las CAC realicen evaluaciones periódicas de riesgos cibernéticos y tomen medidas para mitigar esos riesgos.

Notificación de incidentes de seguridad: Se establece pautas para la notificación obligatoria de incidentes de seguridad a la SEPS y a las partes interesadas relevantes.

Cumplimiento y auditorías: La resolución requiere que las CAC cumplan con ciertos estándares de SI y sometan a auditorías regulares para verificar el cumplimiento.

Legislación de defensa de datos en Ecuador

Además de las regulaciones específicas emitidas por la SEPS, las CAC en Ecuador también están sujetas a la legislación nacional para lo que es la protección de datos y privacidad. Esta legislación establece requisitos relacionados con la recopilación, almacenamiento y manejo de datos personales de los socios y clientes de las cooperativas.

El marco legal específico para las CAC en Ecuador incluye regulaciones emitidas por la SEPS, como la Resolución No. SEPS 2022-002, que establece requisitos y estándares afines con la SI y la diligencia de riesgos cibernéticos. Además, la legislación nacional de defensa de datos y privacidad también es relevante para estas organizaciones en términos de manejo de datos personales. Estos aspectos legales son cruciales para avalar la protección de la información y la defensa de los socios y clientes de las CAC en Ecuador.

CAPÍTULO 3

METODOLOGÍA

La metodología de evaluación realizada se fundamenta en la integración de estándares reconocidos a nivel internacional, tales como ISO 27004, ISO 27007, MAGERIT, y la Norma de Control Respecto a la SI SEPS 2022-002. A continuación, se muestra una guía estructurada para realizar la evaluación del SGSI:

3.1 Diagnóstico del SGSI

La justificación y el diagnóstico de viabilidad para la implementación de la metodología propuesta en la cooperativa se sustentan en la realidad específica de la organización, destacando hechos encontrados durante el análisis y evaluación.

3.1.1 Justificación institucional

Durante la revisión de la infraestructura informática de la cooperativa, se identificó una creciente dependencia de sistemas digitales para gestionar información financiera y personal de los miembros. La exposición a amenazas cibernéticas y la exigencia de salvaguardar datos confidenciales se han tornado más evidentes con el tiempo, justificando la urgencia de fortalecer la seguridad de la información.

3.1.2 Justificación metodológica

La cooperativa ha experimentado dificultades para abordar de forma estructurada y efectiva los desafíos de SI. Incidentes pasados, como tentativas de acceso no autorizado y pérdida de datos, resaltan la exigencia de adoptar un enfoque más sistemático y metodológico para gestionar los riesgos de seguridad.

3.1.3 Justificación teórica

La revisión de prácticas y normativas actuales reveló una brecha en la alineación con los estándares principalmente internacionales SI. La falta de una metodología coherente asentada en marcos reconocidos teóricamente ha dejado a la cooperativa en desventaja en términos de seguridad, respaldando la necesidad de una fundamentación teórica sólida.

3.1.3 Evaluación de la necesidad del SGSI

El análisis de incidentes previos y la tipificación de recursos críticos pusieron de manifiesto la vulnerabilidad actual de la cooperativa. La necesidad de implementar un SGSI se evidencia al considerar las posibles consecuencias financieras y reputacionales de incidentes de seguridad (Ver Anexo 1)

3.1.4 Análisis de recursos disponibles

La cooperativa cuenta con un equipo de profesionales comprometidos, pero se observa una carencia de recursos específicos dedicados a la SI. La evaluación de los recursos disponibles destaca la exigencia de asignar adecuadamente personal y presupuesto para la implementación del SGSI.

3.1.5 Identificación de obstáculos

Durante las conversaciones con el personal, se identificaron posibles obstáculos, como la falta de metodologías y métricas que midan las actividades en riesgo y procesos que permitan hacer los seguimientos necesarios en temas de seguridad. Este análisis temprano permite diseñar estrategias de comunicación y capacitación para superar estos desafíos.

3.1.6 Valoración de la disposición de la dirección

Las entrevistas con la dirección revelaron un interés creciente en fortalecer la SI. La disposición y apoyo de la dirección se reflejan en la asignación de recursos y en la inclusión de la SI en la agenda estratégica.

3.1.7 Determinación de la conveniencia de la metodología

El conjunto de hechos encontrados respalda la determinación de que la metodología propuesta y el desarrollo de métricas es conveniente para la cooperativa. Ya que se alinea con las necesidades identificadas, supera obstáculos conocidos y aprovecha el respaldo y la disposición de la alta dirección, estableciendo las bases para una implementación exitosa.

3.2 Identificación de métricas de cumplimiento (etapa diagnóstico inicial)

La identificación de métricas de cumplimiento resulta primordial para evaluar la eficacia y eficiencia del SGSI. Estas métricas ofrecen indicadores cuantitativos que permiten medir el grado de acatamiento de las normativas y otros aspectos relacionados con la SI en la cooperativa.

Métrica 1: Frecuencia de revisión de normativas

Esta métrica se describe a la frecuencia con la que se ejecutan revisiones exhaustivas de las normativas aplicadas. Actualmente, la cooperativa no tiene un cronograma claro y definido para estas revisiones, especialmente en cuanto a la periodicidad que debería seguirse, ya sea mensual, trimestral o anual.

Métrica 2: Número de cambios o actualizaciones en las normativas identificadas

Esta métrica cuantifica la dinámica de las normativas, indicando cuántas veces se han producido cambios o actualizaciones. En la actualidad, no existe un número elevado que podría sugerir un entorno normativo volátil, lo cual requeriría una atención más diligente y una rápida adaptación a los cambios.

Marco de trabajo de evaluación de la seguridad

Métrica 3: Tiempo dedicado a la evaluación y selección del marco de trabajo

Esta métrica mide la cantidad de tiempo que se invierte en la evaluación de diferentes marcos de trabajo antes de seleccionar el más adecuado. Actualmente, la cooperativa solo incluye las horas de trabajo, reuniones y cualquier otro esfuerzo dedicado a esta actividad.

Métrica 4: Grado de adaptación del marco de trabajo a las necesidades específicas de la cooperativa

Se refiere a la medida en que el marco de trabajo seleccionado se ajusta y satisface las necesidades específicas de la cooperativa. Actualmente no dispone de un marco de trabajo establecido.

Normativas aplicadas (implementación)

Métrica 5: Porcentaje de procedimientos implementados

Esta métrica cuantifica el progreso en la implementación de procedimientos establecidos por las normativas. Actualmente la cooperativa tiene un alto porcentaje, lo que indica un sólido cumplimiento. Cabe aclarar que actualmente se realizan procesos superficiales en donde no tiene procedimientos detallados en donde se establezca métricas como tal implementadas.

Métrica 6: Frecuencia de auditorías internas para valorar el cumplimiento

Mide con qué asiduidad se realiza auditorías internas para evaluar el cumplimiento con las normativas. En la actualidad en la cooperativa, no se realizan auditorías de forma detallada y sistemática; solo se lleva a cabo una revisión de procesos que indica el compromiso de la alta gerencia por evaluar de forma general, no específica.

Métrica 7: Número de objetivos establecidos

Cuantifica la cantidad de objetivos específicos que se establecen para el marco de trabajo. Actualmente la cooperativa, los objetivos no están claros en específico y no son

medibles en forma de un marco de trabajo metodológico. Además, no están definidos con plazos.

Métrica 8: Porcentaje de objetivos alcanzados

Evalúa qué tan exitosa es la cooperativa en alcanzar los objetivos establecidos. Este porcentaje proporciona una visión clara del rendimiento y la eficacia del marco de trabajo en la práctica.

La Métrica 8 representa un indicador crucial para medir la eficacia de la implementación del marco de trabajo en la cooperativa. Este porcentaje no solo brinda una evaluación cuantitativa del rendimiento, sino que también proporciona una visión integral de hasta qué punto se han realizado los objetivos establecidos.

Justificación de la implementación de las métricas

En la actualidad, la cooperativa carece de un marco de trabajo o un sistema estructurado para medir y evaluar de manera sistemática el valor de éxito en el beneficio de sus objetivos específicos. La introducción de estas métricas se vuelve imperativa para abordar esta laguna y establecer un enfoque cuantitativo que permita no solo establecer metas claras sino también medir y mejorar continuamente el desempeño en función de resultados tangibles. Al incorporar estas métricas, la cooperativa no solo adquirirá la capacidad de cuantificar sus logros, sino que también identificará áreas específicas que requieren mayor atención y desarrollo. Esta métrica no solo se convierte en una herramienta para evaluar el cumplimiento de objetivos, sino también en un motor de mejora continua, impulsando a la cooperativa hacia prácticas más efectivas y resultados más exitosos en el ámbito de SI.

3.3 Metodología (marco de trabajo propuesto)

En esta subsección, se describe en detalle el marco de trabajo de evaluación de la seguridad desarrollado para alcanzar con los propósitos de la investigación. Este marco se fundamenta en las normativas aplicadas, la distribución organizativa de la entidad, los métodos,

los procedimientos y las herramientas y tecnologías utilizadas. A continuación, se proporciona una explicación detallada de cada componente:

3.3.1 Marco de trabajo de evaluación de la seguridad

Paso 1. Especificación de Normativas

Marco normativo

En el ámbito de las COAC, el marco normativo para la SI se fundamenta en normativas internacionales y locales, asegurando una orientación integral en el manejo de amenazas y la protección de la información. Entre las normativas clave se encuentran la ISO 27001, SEPS 2022-002, la ISO 27004 y la ISO 27007.

Descripción de las Normativas

En esta sección, se detalla las normativas específicas que han influido en la concepción del marco de trabajo.

- ISO 27001: Esta normativa internacional proporciona los requerimientos para instituir, realizar, proteger y mejorar continuamente un SGSI. Se incorpora en nuestro marco de trabajo para establecer los estándares necesarios en la gestión de la SI.
- ISO/IEC 27004: Es una guía internacional que suministra pautas y directrices para determinar, efectuar, cuidar y optimizar un sistema de gestión de la SGSI. Esta norma se centra específicamente en la medición de la efectividad y el desempeño del SGSI a través de la definición y aplicación de métricas de SI. Su enfoque está dirigido a ofrecer a las organizaciones a evaluar la eficacia de sus controles y procesos de seguridad, permitiéndoles tomar decisiones informadas para fortalecer su postura de seguridad y adaptarse a las variabilidades en el entorno de amenazas. ISO/IEC 27004 es una herramienta valiosa para la mejora continua de la SI al proporcionar un marco sistemático para medir, evaluar y optimizar el SGSI.

Incorporación de Normativas al Marco propuesto

El marco de trabajo implementado se rige por un conjunto exhaustivo de procedimientos y estándares seleccionados en el campo de la SI. La conformidad con las siguientes normativas y estándares específicos ha sido incorporada para asegurar una evaluación integral y alineada con las mejores prácticas reconocidas a nivel mundial:

- ISO/IEC 27007:2020: El estándar facilita pautas para la auditoría de SGSI, asegurando que la valoración se efectúe de manera sistemática y eficiente. La integración de ISO/IEC 27007 garantiza la aplicación de enfoques disciplinados y procesos auditables en la evaluación de la seguridad.
- ISO/IEC 27004: En consonancia con esta normativa, se establecen métricas y técnicas para la medición del desempeño del SGSI. La aplicación de ISO/IEC 27004 permite una evaluación cuantitativa y cualitativa, proporcionando una comprensión detallada del rendimiento de los controles de seguridad implementados.
- Magerit v3: Este marco de riesgos y encargo de la SI, desarrollado por el Centro Criptológico Nacional (CCN) de España, el cual se utiliza para reconocer, examinar y gestionar los riesgos de seguridad. La integración de Magerit v3 asegura una evaluación exhaustiva de amenazas y vulnerabilidades, permitiendo la priorización de medidas correctivas basadas en el riesgo.
- SEPS 2022-002: Esta normativa específica se integra para cumplir con los requisitos normativos particulares de la cooperativa, asegurando la conformidad con las regulaciones locales y las necesidades específicas del entorno operativo.

La elección de estas normativas y estándares se traduce en un enfoque robusto y completo para la evaluación de la seguridad, abarcando aspectos de auditoría, medición del desempeño y gestión de riesgos. Esta combinación de normativas establece una base sólida que

cumple con los requisitos internacionales y promueve la adopción de las principales prácticas en la SI.

Paso 2. Determinación de objetivos del marco de trabajo

Los objetivos del marco de trabajo incluyen la comprobación de la efectividad de las inspecciones implementados, la evaluación de la adaptabilidad del marco de trabajo a cambios en el entorno, la medición del cumplimiento de requisitos normativos y la identificación de áreas específicas que requieran mejoras continuas. Cada uno de estos objetivos ha sido cuidadosamente diseñado para contribuir a la evaluación integral de la SI. A continuación, se detallan los objetivos específicos del marco de trabajo:

a) Verificación de la eficacia de los controles implementados:

- Evaluar la actividad de las inspecciones de seguridad implementados en el entorno del SGSI.
- Identificar y analizar el rendimiento de cada control en términos de mitigación de riesgos y protección de la información.

b) Evaluación de la adaptabilidad del marco de trabajo a cambios en el entorno:

- Analizar la capacidad del marco de trabajo para adaptarse a cambios en el entorno operativo, como actualizaciones tecnológicas, nuevas amenazas o modificaciones en los procesos organizativos.
- Proporcionar mecanismos para evaluar la flexibilidad y la adaptabilidad del marco de trabajo en respuesta a cambios significativos.

c) Medición del cumplimiento de requisitos normativos:

- Evaluar el grado de conformidad del SGSI con las normativas y estándares aplicables, incluyendo ISO/IEC 27001, ISO/IEC 27007:2020, ISO/IEC 27004 y Magerit v3. Incluye la conformidad con regulaciones locales, en donde se busca

cumplir con los requisitos específicos de la normativa local como el caso del Ecuador la SEPS 2022-002.

- Proporcionar métricas claras que indiquen el nivel de adhesión a los requisitos normativos establecidos.

d) Identificación de áreas que requieran mejoras continuas:

- Realizar un análisis detallado para identificar áreas específicas del SGSI que puedan beneficiarse de mejoras continuas.
- Proveer recomendaciones concretas y acciones correctivas para abordar deficiencias identificadas, fomentando un ciclo de mejora continua.

Estos objetivos se integran de manera sinérgica para brindar una evaluación completa y efectiva de la SI, contribuyendo así a la obtención de los propósitos generales de la investigación.

Paso 3. Definición de responsables

Estructura organizativa

La estructura organizativa delineada en el marco de trabajo establece un marco claro y definido para el proceso de evaluación de seguridad. Cada elemento de esta estructura desempeña un encargo esencial en la ejecución y seguimiento efectivo de los controles de SI. A continuación, se proporciona una descripción detallada de la estructura organizativa:

a) Responsables de la gestión de la SI:

Este componente clave de la estructura organizativa recae en individuos o equipos encargados de la labor integral de la SI en la organización. Sus responsabilidades abarcan la supervisión directa de la implementación de controles, la identificación proactiva de riesgos y la coordinación de acciones correctivas.

b) Auditores internos:

Los auditores internos desempeñan un papel crítico en la estructura, llevando a cabo evaluaciones periódicas e imparciales del sistema de gestión de SI. Su función incluye la revisión detallada de los controles implementados, la verificación de la conformidad con normativas y estándares, y la emisión de informes de auditoría.

c) Otros actores relevantes:

Además de los roles mencionados, se consideran otros actores relevantes que pueden variar según la estructura organizativa específica de la entidad. Estos pueden incluir, por ejemplo, personal de TI, equipos de respuesta a incidentes, y cualquier otro grupo directa o indirectamente involucrado en la SI.

La colaboración efectiva entre estos actores en la estructura organizativa garantiza una implementación coherente y eficiente de los controles de seguridad. Además, clarifica las líneas de responsabilidad, facilitando la comunicación efectiva y fortalece la posibilidad de la organización para abordar los desafíos en materia de SI.

Paso 4. Especificación de procesos a realizar

La eficacia del marco de trabajo radica en la rigurosidad de sus procesos y procedimientos, diseñados para abordar cada aspecto crítico de la evaluación de seguridad. En la continuación, se detalla la estructura de los procesos y los procedimientos incorporados en el marco de trabajo:

a) Identificación de amenazas y vulnerabilidades:

- Se establece un proceso detallado para la tipificación proactiva de amenazas y vulnerabilidades en el entorno de la organización.
- Métodos como el análisis de riesgos según MAGERIT V3.0 se aplican para evaluar la posibilidad y el impacto de posibles eventos adversos.

- b) Implementación de controles: Se describen los ordenamientos para la implementación efectiva de controles de seguridad, abordando las vulnerabilidades identificadas y mitigando los riesgos evaluados.
- c) Auditoría interna: Se establecen procesos específicos para la realización de auditorías internas, abarcando la recopilación de datos conforme a ISO/IEC 27007:2020 y la evaluación de la efectividad de las salvaguardas.
- d) Medición del desempeño: Los procedimientos detallados para la compilación de datos según ISO/IEC 27004 permiten medir el cumplimiento del sistema de gestión de SI.
- e) Mejora continua: Se definen los pasos para la evaluación periódica, la implementación de acciones correctivas y el empleo a cambios en el entorno operativo, asegurando una mejora continua del sistema.

Procedimientos detallados:

- Auditoría interna: Se especifican los pasos precisos para la recopilación de datos según ISO/IEC 27007:2020, la evaluación de la efectividad de las salvaguardas y la emisión de informes de auditoría.
- Medición del desempeño: Los procedimientos incluyen la recopilación de datos conforme a ISO/IEC 27004, abarcando métricas específicas como la revisión de políticas, el compromiso de la gestión y la exposición al riesgo.
- Mejora continua: Se detallan los procesos para la evaluación periódica, la implementación de acciones correctivas, la adaptación a cambios y la retroalimentación de interesados, asegurando una mejora continua y proactiva del sistema de seguridad.

Esta estructura integral permite que cada paso en el proceso de evaluación esté claramente definido, lo que facilita la ejecución eficiente y efectiva de las actividades de SI.

Paso 5. Realización del Diagnóstico

La metodología MAGERIT deberá implementarse de manera detallada para identificar amenazas y vulnerabilidades específicas que puedan afectar el SGSI de la cooperativa. Este proceso implicará una clasificación meticulosa y una evaluación exhaustiva de los riesgos, considerando los controles ya establecidos por ISO 27001 y la Norma SEPS 2022-002. En este sentido, las cooperativas se benefician de una identificación precisa de los riesgos asociados a sus activos críticos, permitiendo una toma de decisiones informada para su mitigación.

MAGERIT V3.0 como Marco de observación y gestión de riesgos, es seleccionada por su reconocida idoneidad, MAGERIT V3.0 es una metodología ampliamente reconocida y aceptada para el ejercicio y gestión de riesgos de SI (Moya, 2023, p. 15). Se ha demostrado su eficacia en numerosos contextos y se adapta de manera eficiente a la evaluación de la SI (Vicuña-Altamirano & Zhindón-Mora, 2019). La eficacia de MAGERIT V3.0 como Marco de Examen y Gestión de Riesgos se ha demostrado en base a varios aspectos:

- a) Reconocimiento y aceptación: MAGERIT V3.0 goza de un alto nivel de reconocimiento y aceptación en la comunidad europea de SI y entre profesionales de ciberseguridad (ENISA, 2023). Su adopción generalizada en numerosos contextos demuestra la confianza que la industria tiene en esta metodología.
- b) Amplio uso: Ha sido largamente utilizado en varios sectores y organizaciones, desde entidades gubernamentales hasta empresas privadas, lo que resalta su versatilidad y aplicabilidad a diferentes contextos.
- c) Eficiencia en la evaluación: MAGERIT V3.0 ha demostrado su capacidad para evaluar de forma eficiente los riesgos de SI. Su enfoque sistemático y completo permite una identificación, evaluación y gestión efectiva de riesgos.
- d) Adaptación a la SI: La metodología MAGERIT V3.0 se ha adaptado específicamente para determinar los riesgos de SI. Esto la hace especialmente adecuada para valorar

la seguridad en sistemas de información, lo que es relevante en el contexto de su investigación.

- e) **Resultados comprobados:** La metodología ha producido resultados medibles y valiosos en la identificación de riesgos, evaluación de salvaguardas y cálculo de riesgo residual en proyectos anteriores, demostrando su eficacia para optimizar la SI.

Recopilación de datos según MAGERIT

Las técnicas que se manejan para efectuar el análisis de Riesgos según MAGERIT

V3.0 son las siguientes:

- **Paso 1: Tipificación de riesgos:** Se reconocen los riesgos de SI utilizando la metodología MAGERIT V3.0, centrándose en amenazas, vulnerabilidades y activos de información (Portal de Administración electrónica de España, 2023).
- **Paso 2: Evaluación de efectividad de salvaguardas:** Se evalúa la efectividad de las salvaguardas existentes para mitigar los riesgos identificados.
- **Paso 3: Cálculo del riesgo residual:** Se calcula el riesgo residual considerando la posibilidad y el impacto de los riesgos.
- **Paso 4: Resultados y presentación:** Se muestran los resultados del análisis de riesgos en un formato claro, destacando las áreas críticas que requerían atención inmediata y las disposiciones de seguridad adicionales necesarias.

La elección de MAGERIT V3.0 se sustenta en su historial de éxito, reconocimiento en la comunidad de SI y su eficiencia en la evaluación de riesgos, lo que la convierte en una elección sólida y confiable para la investigación. Esta metodología proporciona una visión completa de la SI en la cooperativa y guía el proceso de progreso continua. Los resultados de cada fase se presentan en el Capítulo 4 para su análisis y toma de decisiones.

Paso 6. Selección de herramientas para evaluar

La importancia del marco de trabajo de evaluación de seguridad se apoya en el uso estratégico de diversas herramientas y tecnologías diseñadas para optimizar cada fase del proceso. A continuación, se detallan las herramientas y tecnologías clave implementadas:

- **Software de gestión de seguridad:** Se emplea un software especializado en la gestión integral de la SI. Este facilita la administración de políticas, la asignación de responsabilidades y el seguimiento del cumplimiento normativo.
- **Herramientas de monitoreo continuo:** Se utilizan herramientas de monitoreo en tiempo real para evaluar constantemente la seguridad del entorno operativo. Estas herramientas identifican y alertan sobre posibles amenazas y vulnerabilidades, permitiendo respuestas rápidas ante incidentes.
- **Plataformas de evaluación de riesgos:** Se integran plataformas especializadas en la evaluación de riesgos, siguiendo las pautas establecidas en MAGERIT V3.0. Estas herramientas facilitan el estudio detallado de riesgos, la tipificación de controles necesarios y la priorización de medidas.
- **Sistemas de auditoría automatizada:** Herramientas de auditoría interna, basadas en los principios de ISO/IEC 27007:2020, permiten recopilar datos de manera eficiente, evaluar la efectividad de las salvaguardas y generar informes detallados.
- **Plataformas de métricas y análisis:** Se implementan plataformas para la recopilación y análisis de métricas de desempeño, conforme a ISO/IEC 27004. Estas herramientas facilitan la medición objetiva del cumplimiento de objetivos, ofreciendo una visión integral del estado de seguridad.
- **Herramientas de comunicación efectiva:** Se incorporan herramientas de comunicación interna para facilitar la interacción entre los responsables de la SI, auditores internos y

demás actores relevantes. Esto asegura una comunicación auténtica durante todo el procedimiento de evaluación.

La elección y estudio de estas herramientas y tecnologías se realiza de manera estratégica, considerando la adaptabilidad a los requisitos específicos de la organización y la capacidad para optimizar la eficiencia en la gestión de la SI.

Herramientas y tecnologías utilizadas

En esta subsección, se enumera las herramientas y tecnologías que respaldan la implementación del marco de trabajo, asegurando una gestión eficiente y efectiva de la SI.

- Software de diligencia de riesgos: Se utiliza un software especializado para evaluar y gestionar los riesgos de SI.
- Sistema de monitoreo de redes: Se implementa un sistema robusto para monitorear y detectar actividades inusuales en la red, garantizando la pronta identificación de posibles amenazas.

Paso 7. Definición de indicadores de desempeño

En este paso, se utiliza la norma ISO 27004 como referencia para establecer métricas y Key Performance Indicators (KPIs) que medirán la efectividad del SGSI en la cooperativa. Estos indicadores se personalizan para completar con los requisitos específicos de la Norma de control sobre SI SEPS 2022-002. El enfoque se orienta a desarrollar indicadores que reflejen con precisión la eficacia de los controles implementados, ofreciendo una visión clara del rendimiento del SGSI en el contexto único de la cooperativa.

La recopilación de datos según los indicadores definidos en ISO 27004, adaptados específicamente a la Norma SEPS 2022-002, permite evaluar el desempeño del SGSI en la cooperativa. Este progreso es fundamental para comprender la certeza de las medidas implementadas y comparar los resultados con los objetivos establecidos. La cooperativa obtiene

información valiosa para tomar decisiones informadas e identificar áreas que necesitan atención adicional.

Norma ISO/IEC 27004

Métrica B.3 - Revisión de Políticas:

Esta métrica se maneja para valorar la efectividad de las políticas de SI. Es fundamental evaluar el acatamiento de las políticas para garantizar la SI, y esta métrica proporciona un enfoque cuantitativo para medirlo.

Métrica B.4.- Métrica de Compromiso de la Gestión

Reuniones de Revisión de Gestión: Esta métrica se emplea para evaluar el encargo de la alta dirección con el SGSI. Las reuniones de revisión de gestión son esenciales para garantizar la responsabilidad de la dirección y asegurar el progreso continuo de la SI.

Métrica B.5 - Métrica de Exposición al Riesgo

Evaluación de riesgos altos y medios: Esta métrica se utiliza para valorar la exposición al riesgo de la cooperativa. Es crucial identificar y valorar las amenazas altas y medias que podrían afectar la SI para tomar medidas preventivas y correctivas.

Métrica B.20 - Métrica de Entrada Física

Evaluación de entradas físicas no autorizadas: Esta métrica se emplea para evaluar la seguridad física. La seguridad de lo que son las instalaciones que contienen sistemas de información es esencial, y esta métrica ayuda a calcular la efectividad de los controles de entrada física.

Recopilación de datos según estándar internacional ISO/IEC 27004

Paso 1: Definición del alcance

Se define el alcance de la evaluación, centrándose en medir la eficacia del SGSI de la cooperativa.

Paso 2: Cálculo de métricas

Se aplica la fórmula de las métricas tomadas en cuenta con un periodo anterior.

Métrica de Revisión de políticas (B3)

- Paso 1: Evaluación de políticas de SI: Se ejecuta una valoración de las políticas de SI de la cooperativa utilizando la métrica B.3 Revisión de políticas definida en ISO/IEC 27004.
- Paso 2: Resultados y presentación: Se muestran los resultados de la valoración de políticas de SI en un formato de análisis, identificando las políticas implementadas.

Métrica de Compromiso de la Gestión (B4)

- Paso 1: Evaluación de reuniones de reconocimiento de gestión: Se calcula el indicador de reuniones de reconocimiento de los encargos completados hasta la fecha utilizando la fórmula correspondiente determinada en la norma.
- Paso 2: Resultados y presentación: Se muestran los resultados de las reuniones de revisión de gestión en un formato de análisis, identificando el compromiso de la gestión.

Métrica de exposición al riesgo (B5)

- Paso 1: Evaluación de riesgos altos y medios: Se evalúan el número de riesgos altos y medios más allá del umbral aceptable y la revisión oportuna de estos riesgos.
- Paso 2: Resultados y presentación: Se presentan los resultados de la exposición al riesgo en función de los riesgos identificados, destacando las áreas de mejora y el cumplimiento normativo.

Métrica de Entrada física controla la efectividad (B.20)

- Paso 1: Evaluación de entradas físicas no autorizadas: Se evalúan el número de entradas no acreditadas a instalaciones que reprimen los SI y el número de sucesos de protección física que permitieron la entrada no autorizada.
- Paso 2: Resultados y presentación: Se presentan los resultados de la efectividad de los controles de entrada física, destacando las mejoras y el progreso en la seguridad física.

Paso 4: Resultados y presentación

Se muestran los resultados de la revisión de políticas en un formato claro, identificando el cumplimiento y se entregaron al Oficial de SI.

Métricas de evaluación utilizadas para instituciones financieras

- Métrica F1: Cumplimiento normativo en transacciones financieras. Define el porcentaje de cumplimiento normativo específicamente relacionado con las transacciones financieras, garantizando la conformidad con regulaciones financieras clave.
- Métrica F2: Tiempo de respuesta ante incidentes financieros. Mide la eficacia del tiempo de contestación ante acontecimientos de seguridad específicos en el ámbito financiero.
- Métrica F3: Impacto financiero de vulnerabilidades identificadas. Evalúa el impacto económico potencial de las vulnerabilidades detectadas, proporcionando una perspectiva financiera de los riesgos que se consideran de seguridad.
- Métrica F4: Nivel de cumplimiento de estándares de seguridad financiera PCI DSS (Estándar conocido como de protección de datos de la industria de tarjetas de pago). Cuantifica el grado de cumplimiento con estándares de seguridad

específicos para instituciones financieras, asegurando la adhesión a regulaciones sectoriales.

- Métrica F5: Efectividad de controles en operaciones financieras críticas. Analiza la efectividad de los controles de seguridad en operaciones financieras críticas, ofreciendo una evaluación detallada de la seguridad en áreas sensibles.

Paso 5 Proceso de evaluación

Evaluación de controles implementados

La verificación minuciosa de la ejecución de los controles de seguridad, según las pautas establecidas por ISO 27001 y la Norma SEPS 2022-002, es esencial para garantizar la robustez del SGSI en la cooperativa. En este paso, se valúa la eficacia de los controles existentes, identificando áreas de mejora y proponiendo ajustes necesarios para fortalecer la postura de seguridad. La cooperativa se beneficia de un análisis crítico de sus controles, asegurando que estén alineados con las mejores prácticas y normativas vigentes.

Auditoría Interna

La utilización de ISO 27007 guía de manera integral la programación y ejecución de auditorías internas del SGSI en la cooperativa. Durante este proceso, se revisa meticulosamente el cumplimiento de requisitos y controles establecidos por ISO 27001 y la Norma SEPS 2022-002. Las auditorías internas proporcionan una evaluación independiente y objetiva, asegurando que la cooperativa cumple con los estándares internacionales y las regulaciones locales, así como identificando áreas de mejora continua.

Norma ISO/IEC 27007

Auditorías internas de ciberseguridad

Evaluación de Auditorías Internas: Se realiza las auditorías internas ya que son cruciales para identificar áreas de mejora en ciberseguridad. Este procedimiento se maneja para valorar la efectividad de las auditorías internas y su contribución a la mejora de la ciberseguridad.

Recopilación de datos según estándar internacional ISO/IEC 27007

Paso 1: Evaluación de auditorías internas

Se evalúan las auditorías internas de ciberseguridad manejando el estándar ISO/IEC 27007 para calcular la tasa de éxito en la especificación de áreas de mejora.

Paso 2: Resultados y presentación

Se muestran los resultados de las auditorías internas, destacando la efectividad de estas y su contribución a la mejora de la ciberseguridad.

Paso 6 Proceso de evaluación continua - Mejora

Basándose en las conclusiones de la evaluación, se implementan operaciones correctivas y preventivas en la cooperativa.

Con respecto a las acciones correctivas se realizarán abordaje de hallazgos específicos, implementación de soluciones inmediatas, seguimiento y verificación. Sobre el abordaje de hallazgos específicos se toman medidas específicas para corregir cualquier hallazgo identificado durante la evaluación. Esto podría incluir la corrección de vulnerabilidades, la solución de problemas en los controles de seguridad o la mejora de procesos deficientes. Sobre la implementación de soluciones inmediatas principalmente en casos donde se identifiquen riesgos inmediatos o incidentes de seguridad, se implementan soluciones rápidas para mitigar el impacto y evitar daños adicionales. Sobre seguimiento y verificación se establece un proceso de rastreo para garantizar que las labores correctivas sean efectivas, y se verifica la implementación exitosa y se monitorea la situación para evitar recurrencias.

Con respecto a las acciones preventivas se realizarán actualización del SGSI, capacitación y concientización continua, análisis proactivo de riesgos y evaluación periódica. Sobre la actualización del SGSI, se realiza una revisión y actualización periódica del SGSI para incorporar cambios en el entorno operativo, nuevas amenazas y vulnerabilidades, así como requisitos normativos actualizados. Sobre la capacitación y concientización continua, se

implementan proyectos de capacitación y concientización para el personal de la cooperativa, con el objetivo de prevenir posibles incidentes de seguridad mediante una mayor conciencia y comprensión de las operaciones y prácticas de seguridad. Sobre el análisis proactivo de riesgos, se lleva a cabo un estudio proactivo de amenazas para anticipar posibles amenazas y vulnerabilidades. Esto permite tomar medidas preventivas antes de que los problemas se conviertan en riesgos significativos. Sobre la evaluación periódica, se establece un programa regular de evaluaciones para avalar que el SGSI esté alineado con las mejores prácticas y normativas actuales.

Esto permite que cualquier hallazgo identificado se aborde de manera efectiva, fortaleciendo continuamente el SGSI. Además, la metodología se actualiza de acuerdo con cambios en el entorno y los requisitos normativos, incluyendo aquellos establecidos por la Norma SEPS 2022-002, garantizando una adaptación constante a las condiciones cambiantes.

Normativa local (Resolución No. Seps 2022-002)

La Resolución No. SEPS 2022-002 establece un marco de referencia específico que es relevante para la CAC. La elección de esta normativa local permite aplicar la metodología de manera adecuada lo cual permite cumplir con los requisitos normativos específicos en el país.

Enfoque en métricas para evaluación

La metodología se fundamentó en la aplicación de métricas, lo que permite una medición objetiva y cuantitativa de la SI. Esto facilita la tipificación de áreas de mejora y proporciona una base sólida para proceso en que se toma decisiones de manera informada.

Cálculo de los índices (IRI, IPI, ICF, ICN, IVES, IESES)

Estos índices se calculan para evaluar el riesgo y la eficiencia de las medidas de seguridad en la cooperativa, de acuerdo con la normativa local. Cada índice proporciona una métrica específica para medir aspectos clave de la SI (ESG Innova, 2023). A continuación, se detallará cómo se calculan los índices IRI, IPI, ICF, ICN, IVES e IESES de manera específica:

Índice de riesgo inicial (IRI):

El Índice de Riesgo Inicial (IRI) es una métrica que se utiliza para valorar el riesgo inicial de SI en una organización. Para calcular el IRI, se llevan a cabo varios pasos que consideran múltiples factores de riesgo. A continuación, se detallan los pasos para calcular el IRI:

Ecuación 1 Índice de riesgo inicial (IRI)

$$\text{IRI} = (\Sigma (\text{Probabilidad} \times \text{Impacto})) / N$$

Donde:

Σ (Sumatoria) se refiere a la suma de los factores de riesgo para cada riesgo identificado.

"Probabilidad" es la probabilidad de que ocurra un riesgo, expresada en términos cuantitativos (por ejemplo, en una escala del 1 al 10).

"Impacto" se refiere al impacto potencial de un riesgo, también expresado en términos cuantitativos.

"N" representa el número total de riesgos identificados y evaluados.

A continuación, se detallan los pasos para calcular el IRI:

- a) Tipificación de riesgos: Se determinan todos los posibles riesgos relacionados con la SI en la organización. Estos riesgos pueden incluir amenazas, vulnerabilidades y activos críticos.
 - Amenazas: Se exploran y documentan diversas amenazas que podrían comprometer la SI. Esto incluye posibles escenarios de ataques, intrusiones no autorizadas y cualquier actividad que represente una amenaza para la integridad, confidencialidad o disponibilidad de la información.

- Vulnerabilidades: Se examinan las lasitudes existentes en los sistemas y desarrollos de la organización. Esto implica identificar debilidades en la infraestructura, configuraciones inseguras, y cualquier aspecto que pueda ser explotado por amenazas potenciales.
 - Activos críticos: Se determinan los recursos críticos de la organización, como bases de datos, sistemas operativos, y cualquier elemento fundamental para la continuidad y funcionalidad del negocio. Estos activos son evaluados en términos de su importancia y relevancia para la operación segura de la organización.
- b) Evaluación de probabilidad e impacto: Para cada riesgo identificado, se valora la posibilidad de que acontezca y el impacto viable que tendría en la organización en caso de materializarse. Estos valores se expresan en una graduación cuantitativa, como del 1 al 10, donde 1 simboliza una posibilidad o impacto muy bajo y 10 simboliza una probabilidad o impacto muy alto.
- c) Cálculo del IRI: Se realiza el cálculo del IRI sumando el producto de la posibilidad y el impacto para cada riesgo y luego dividiendo esta suma por el número total de riesgos evaluados (N). Esto proporciona un valor que refleja el riesgo inicial de SI en la organización.

El IRI es una herramienta útil para priorizar riesgos y enfocar los esfuerzos de seguridad en áreas críticas. Un IRI más alto indica un riesgo inicial más alto, lo que significa que se deben tomar medidas más urgentes para mitigar esos riesgos y fortalecer la SI en la organización.

Índice de prioridad de implementación (IPI):

El Índice de Prioridad de Implementación (IPI) se calcula mediante la fórmula siguiente:

Ecuación 2 Índice de prioridad de implementación (IPI):

$$IPI = (IPI) = (\text{Severidad}) \times (\text{Exposición})$$

Donde:

- **Severidad:** La severidad se refiere a la gravedad de las consecuencias si el riesgo se materializa. Se evalúa en una graduación del 1 al 5, donde 1 indica una severidad baja y 5 una severidad alta.
- **Exposición:** La exposición es una medida de cuán expuesta está la organización al riesgo y se calcula de manera similar en una graduación del 1 al 5, donde 1 indica una exposición baja y 5 una exposición alta.

Índice de concienciación y formación (ICF):

Se calcula como una medida de la preparación y conocimiento del personal de la organización en relación con la SI. Este índice se evalúa de la siguiente manera:

Ecuación 3 Índice de concienciación y formación (ICF):

$$\text{ICF} = (\text{Número de empleados con formación en seguridad}) / (\text{Total de Empleados}) \times 100$$

Para calcular el ICF, primero debe determinar el número de empleados que han recibido formación específica en SI. Luego se divide este número por el total de empleados en la organización y se reproduce por 100 para enunciar el resultado como un porcentaje. Un valor más alto de ICF indica que un mayor porcentaje de empleados ha recibido formación en SI, lo que generalmente se considera beneficioso para fortalecer la actitud de seguridad de la organización. La formación y concienciación son elementos esenciales para reducir riesgos y mejorar la SI en cualquier entorno empresarial.

Índice de cumplimiento de normativas (ICN)

El Índice de Cumplimiento de Normativas (ICN) se calcula para medir la anuencia de una organización con las normativas y pautas del SI. Este índice se evalúa detalladamente de la siguiente manera:

Ecuación 4 Índice de cumplimiento de normativas (ICN)

$$\text{ICN} = [(\text{Número de Controles Cumplidos}) / (\text{Número Total de Controles})] \times 100$$

Para calcular el ICN, primero, es necesario determinar el número de controles que la organización ha cumplido satisfactoriamente en relación con las normativas y estándares de SI aplicables. A continuación, se divide este número por el número total de controles que deben cumplirse. Luego se multiplica la consecuencia por 100 para expresarlo como un porcentaje.

Un ICN más alto indica un mayor acatamiento de las normativas y estándares de SI. Es esencial que las organizaciones se esfuercen por alcanzar un alto ICN para garantizar que están siguiendo de manera adecuada las regulaciones y prácticas de SI, lo que contribuye a la defensa de los activos de datos y la mitigación de riesgos.

Índice de valor de exposición al riesgo (IVES):

El Índice de Vulnerabilidades de Equipos y Software (IVES) se utiliza para evaluar la cantidad y el impacto de las vulnerabilidades presentes en los equipos y el software de una organización. Para calcular el IVES, se realiza un proceso detallado que implica varios pasos:

Ecuación 5 Índice de valor de exposición al riesgo (IVES)

$$\text{IVES} = [(\text{Número Total de Vulnerabilidades}) / (\text{Número Total de Equipos y Software})] \times 100$$

A continuación, se explican las acciones para calcular el IVES:

- **Recopilación de datos:** Se recopilan datos sobre el número total de vulnerabilidades identificadas en los equipos y el software utilizados en la organización.
- **Conteo de vulnerabilidades:** Se cuentan todas las vulnerabilidades, incluidas aquellas consideradas críticas, importantes o menores.
- **Conteo de equipos y software:** Se determina el número total de equipos y de software que se utilizan en la organización y que están sujetos a evaluación.

- Cálculo del IVES: Utilizando la fórmula mencionada anteriormente, se divide la cifra total de vulnerabilidades por la cifra total de equipos y software, y luego se multiplica por 100 para enunciar el resultado como un porcentaje.

El IVES proporciona una métrica clave para evaluar la seguridad de la infraestructura tecnológica de la organización. Un IVES más bajo indica un mayor nivel de vulnerabilidades, lo que simboliza un riesgo más alto para la SI. Por lo tanto, las organizaciones deben esforzarse por reducir el IVES mediante la identificación y mitigación de vulnerabilidades en sus sistemas y software.

Índice de efectividad de salvaguardas (IESES):

El Índice de Efectividad de Salvaguardas (IESES) se calcula mediante la fórmula siguiente:

Ecuación 6 Índice de efectividad de salvaguardas (IESES)

$$\text{IESES} = (\text{Efectividad de Salvaguarda}) \times (\text{Reducción de Riesgo})$$

Efectividad de salvaguarda: Se refiere a la eficiencia de las medidas de seguridad implementadas para mitigar el riesgo, evaluada en una graduación del 1 al 5, donde 1 indica una efectividad baja y 5 una efectividad alta.

Reducción de riesgo: Es una medida subjetiva que refleja cuánto se reduce el riesgo gracias a las salvaguardas.

Estos índices son herramientas clave para evaluar y cuantificar el riesgo inherente y la eficiencia de las medidas de seguridad en la investigación. Los valores resultantes proporcionan información única para la toma de decisiones con relación al progreso de la SI.

Recopilación de datos según resolución No. SEPS 2022-002

Paso 1: Identificación de activos de información críticos

Se llevan a cabo entrevistas para determinar los AI críticos, como la base de datos de socios, la plataforma de banca en línea y otros datos sensibles.

Paso 2: Cálculo de índices (IRI, IPI, ICF, ICN, IVES, IESES)

Se calculan varios índices para evaluar el riesgo y la efectividad de lo que se ha planteado como medidas de seguridad en la cooperativa, utilizando datos específicos y fórmulas definidas.

Paso 3: Resultados y presentación

Se presentan los resultados de los índices y se analizó la situación inicial en comparación con la actual, destacando las áreas de mejora y los logros en SI.

Paso 10 Documentación y reporte

Se elaboran informes detallados que destacan hallazgos, recomendaciones y acciones tomadas durante la evaluación del SGSI en la cooperativa. Esta documentación cumple con los requisitos de ISO 27001 y la Norma SEPS 2022-002, proporcionando un registro claro y completo de todo el proceso. La transparencia en la documentación facilita la rendición de cuentas y la comunicación efectiva de la postura de seguridad de la cooperativa.

3.2 Análisis de sustentación de la metodología

La elección de MAGERIT V3.0, las normas ISO/IEC 27004 e ISO/IEC 27007, y la referencia a la Resolución No. SEPS 2022-002 se basa en su reconocida idoneidad, aplicabilidad a nivel internacional y local, enfoque en métricas cuantitativas, y su capacidad para proporcionar una valoración exhaustiva de la SI. Estos marcos metodológicos permiten una evaluación sólida y fundamentada de la seguridad del SGSI en la CAC, proporcionando un procedimiento detallado y sustentado.

La metodología elegida aborda tanto la mejora continua de la SI como el cumplimiento normativo. Esto garantiza que la cooperativa no solo mejore su seguridad, sino que también

cumpla con los requerimientos legales y reglamentarios aplicables. El enfoque integral de la metodología asegura que se aborden todos los aspectos clave de la SI.

Además, la metodología combina la evaluación de los manejos de seguridad, el compromiso de la gestión, la exposición al riesgo, el control de entrada física, las auditorías internas y la identificación de activos críticos. Esto asegura una valoración holística de la SI, abordando áreas que van desde la gobernanza y la responsabilidad de la alta dirección hasta los aspectos técnicos de la seguridad.

La metodología proporciona resultados claros y acciones específicas que son identificadas en cada etapa. Esto proporciona datos hacia un proceso en donde se realiza la toma de decisiones informadas para mejorar la SI. Con esta aproximación, la cooperativa puede seguir un camino claro hacia la mejora continua de su SGSI y asegurarse de que está tomando medidas concretas para abordar las áreas críticas y garantizar la SI en un entorno en constante evolución. La elección de estas metodologías se justifica por su capacidad para ofrecer una evaluación exhaustiva, cubriendo aspectos clave de seguridad, garantizando el cumplimiento normativo y facilitando la toma de disposiciones orientado hacia la mejora continua de la SI en la cooperativa. Estos marcos suministran una base sólida y fundamentada para la evaluación de la seguridad del SGSI, asegurando que la cooperativa esté preparada para hacer frente a los riesgos y desafíos en un entorno de SI en constante evolución.

3.3 Especificación del cumplimiento de objetivos

Cada fase de la metodología contribuye de manera significativa al logro del objetivo general de implementar un marco de trabajo de evaluación para identificar el nivel de cumplimiento de implementación del SGSI en las CAC del Segmento 1.

Sobre los Objetivos Específicos:

- El diagnóstico del SGSI (en la Sección 3.4) se utiliza MAGERIT V3.0 para identificar amenazas y vulnerabilidades, cumpliendo con el objetivo de diagnosticar el SGSI implementado.
- La identificación de métricas (en la Sección 3.3) al utilizar la norma ISO/IEC 27004 para definir métricas y KPIs, logrando el objetivo de identificar métricas de cumplimiento de la implementación del SGSI.
- El desarrollo de marco de evaluación (en las Secciones 3.3, 3.4, 3.5, 3.6, 3.7) al utilizar ISO/IEC 27007 y MAGERIT V3.0 para desarrollar un marco de trabajo de evaluación de la seguridad, cumpliendo con el objetivo de desarrollar un marco de trabajo de evaluación basado en normativas específicas.
- La prueba de concepto (en la Sección 3.8) al implementar ejercicios correctores y preventivos asentadas en las conclusiones de la evaluación, asegurando una mejora continua del SGSI, y realizando una prueba de concepto para evaluar el nivel de cumplimiento del SGSI, cumpliendo con el objetivo de evaluar el marco con una prueba de concepto.

La metodología propuesta está diseñada para lograr los objetivos de investigación establecidos. Cada componente de la metodología está diseñado para alcanzar los objetivos establecidos en la investigación, asegurando una evaluación integral y efectiva del SGSI en las CAC del Segmento 1.A continuación, se detalla cómo cada fase contribuye directamente al logro de estos objetivos:

En el marco normativo (en la Sección 3.2) se asegura de que la evaluación esté alineada con normativas internacionales y locales, garantizando una dirección integral en las actividades para el manejo de riesgos y la protección de lo que son los datos.

Para el desarrollo de indicadores de desempeño (en la Sección 3.3) se utiliza la norma ISO 27004 para definir métricas que permiten medir la efectividad del SGSI en la cooperativa, cumpliendo con el objetivo de identificar métricas de cumplimiento.

La tipificación de amenazas y vulnerabilidades (en la Sección 3.4) se lo hace a través de la metodología MAGERIT en donde se implementa para identificar amenazas y vulnerabilidades específicas, cumpliendo con el objetivo de diagnosticar el SGSI implementado.

La evaluación de controles implementados (en la Sección 3.5) se verifica la ejecución de los controles de seguridad según ISO 27001 y la Norma SEPS 2022-002, lo que contribuye al objetivo de evaluar el nivel de cumplimiento del SGSI.

La Auditoría interna (en la Sección 3.6) al utilizar la guía ISO/IEC 27007 para guiar la planificación y ejecución de auditorías internas, asegurando la revisión del cumplimiento de requisitos y controles.

La medición del desempeño (en la Sección 3.7) haciendo la selección de datos según ISO 27004 lo que permite evaluar el desempeño del SGSI en la cooperativa, cumpliendo con el objetivo de desarrollar un marco de trabajo de evaluación basado en normativas específicas.

La mejora continua (en la Sección 3.8) en donde se implementa acciones que son correctivas y preventivas enfocadas en las conclusiones de la evaluación, asegurando una mejora continua del SGSI.

La documentación y reporte (en la Sección 3.9) al elaborar informes detallados que se verifican con los requisitos de ISO 27001 y la Norma SEPS 2022-002, proporcionando un registro completo del proceso de evaluación.

El análisis de sustentación de la metodología (en la Sección 3.10) en donde se justifica la elección de MAGERIT V3.0, ISO/IEC 27004 e ISO/IEC 27007, demostrando cómo estos marcos metodológicos permiten una evaluación fundamentada y exhaustiva del SGSI.

CAPÍTULO 4

RESULTADOS

En el capítulo se muestra los resultados obtenidos y previstos a través de la evaluación de la seguridad del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Ahorro y Crédito (CAC). Este enfoque se dirige hacia la población conformada por los trabajadores de la cooperativa y sus sucursales.

4.1 Resultados obtenidos aplicados utilizando la metodología

Los resultados se asientan en el estudio de riesgos realizado según la sistemática MAGERIT V3.0, así como en la evaluación de la efectividad de las salvaguardas existentes, considerando elementos de las normas ISO/IEC 27007:2020 y ISO/IEC 27004:2016 descritos detalladamente en el Capítulo 3.

4.1.1 Definición de objetivos

A continuación, se detallan los pasos aplicados específicamente a la cooperativa:

Objetivos para la evaluación del SGSI:

La cooperativa se propone evaluar su SGSI con el propósito de avalar la defensa integral de la información sensible y financiera de sus miembros. Los objetivos pueden incluir:

- **Objetivo principal:** Evaluar la validez de las intervenciones de seguridad en la defensa de datos financieros y personales de los socios.
- **Objetivo secundario:** Verificar el cumplimiento de las normativas locales y estándares que son principalmente internacionales en materia de SI.

Identificación de los activos críticos y las áreas clave del SGSI:

Dada la naturaleza de una CAC, es esencial identificar los activos críticos y las áreas clave que respaldan las operaciones y la confianza de los miembros. Ejemplos específicos para la cooperativa podrían ser:

- Activos críticos: Base de datos de socios, información financiera, plataformas de cooperativa en línea.
- Áreas clave: Acceso a sistemas, actividad de riesgos financieros, SI en transacciones.

Los objetivos están alineados con la misión y encargos de la cooperativa, avalando la protección y confidencialidad de la información financiera de sus miembros. La evaluación se orienta hacia aspectos que son cruciales para la integridad y reputación de la cooperativa en el manejo de la información sensible. Este enfoque específico facilita un proceso de evaluación más efectivo y centrado en los aspectos críticos para la SI en el contexto de la cooperativa.

4.1.2 Diagnóstico del sistema de gestión del SGSI

El diagnóstico del SGSI en la cooperativa se realizó mediante un proceso estructurado que implicó las etapas de identificación de áreas clave y recopilación de datos iniciales. En la identificación de áreas clave se realizaron sesiones de trabajo con los responsables de cada área para identificar las áreas clave del SGSI que requerían evaluación. En la recopilación de datos iniciales se implementó un Checklist inicial para recopilar datos relevantes en cada área identificada. Este Checklist se basó en estándares internacionales como ISO/IEC 27001 y normativas específicas como SEPS 2022-002. Los resultados del diagnóstico se presentan en una tabla con el Checklist inicial, que resume los principales hallazgos durante el proceso de diagnóstico:

Tabla 1 *Checklist Inicial*

Área clave	Cumplimiento (Sí/No)	Observaciones
Infraestructura Tecnológica	Sí	Cumplimiento con los estándares de seguridad establecidos.
Gestión de accesos	Parcialmente	Falta de políticas claras para la gestión de accesos.
Procesos de respuesta a incidentes	Parcialmente	Existencia de procedimientos documentados.
Comunicación interna de riesgos	No	Falta de protocolos claros de comunicación interna.

Se realizó un análisis minucioso de los datos compilados, identificando patrones, predisposiciones y áreas críticas que requerían atención inmediata.

Tabla 2 *Checklist para identificación de patrones*

Área de diagnóstico	Resultado
Registro de actividades	No se observaron patrones de actividad inusual, ni comportamientos inconsistentes.
Acceso a datos sensibles	No se identificaron accesos no autorizados en el manejo de datos de los colaboradores, sin embargo, es necesario una revisión al detalle para evidenciar la existencia de accesos no autorizados principalmente con los clientes de la cooperativa

Monitoreo de redes	No se detectaron patrones de tráfico inusual, sin embargo, es necesario una revisión al detalle para evidenciar la existencia de posibles amenazas.
--------------------	---

Tabla 3 *Checklist para identificación de tendencias*

Área de diagnóstico	Resultado
Análisis temporal	Se notaron cambios significativos en el comportamiento a lo largo del tiempo, indicando posibles variaciones en la seguridad.
Adopción de políticas	La tendencia en la adopción de políticas de seguridad mostró mejoras en algunas áreas. Por lo que se necesita mejorar en las demás.
Actualizaciones de software	Se observó una tendencia mixta en la aplicación oportuna de actualizaciones de software, con áreas que podrían representar riesgos.

Tabla 4 *Checklist para identificación de áreas críticas*

Área de diagnóstico	Resultado
Vulnerabilidades críticas	Se identificaron y catalogaron vulnerabilidades mínimas, las cuales se necesita priorizar según su impacto y probabilidad de explotación.
Incidentes recientes	Al revisar incidentes recientes, se identificaron áreas y sistemas , analizando las causas subyacentes.
Cumplimiento normativo	La evaluación del cumplimiento normativo en áreas clave reveló que no existe desviaciones significativas.

El proceso de diagnóstico permitió identificar brechas significativas en la implementación del SGSI, proporcionando una visión clara de las áreas que necesitan mejoras.

Con base en los datos recopilados, se ejecuta una evaluación precedente de los riesgos asociados al SGSI, priorizando aquellos que podrían tener un impacto crítico en la SI.

4.1.3 Marco normativo

ISO 27001:

La norma ISO 27001 establece estándares para la ejecución de un SGSI. En el contexto de las cooperativas, su aplicación implica una evaluación rigurosa y una alineación estratégica para avalar la protección de los recursos o activos de información.

SEPS 2022-002:

La normativa local SEPS 2022-002 se erige como un marco específico que regula la SI en el ámbito de las CAC. Su cumplimiento es esencial para asegurar que el SGSI se ajuste a los requisitos y regulaciones locales, garantizando un manejo seguro de la información financiera y de los socios.

ISO 27004:

Ampliando la perspectiva, la ISO 27004 proporciona directrices para medir la eficacia de un SGSI mediante métricas y KPIs. Esta normativa permite valorar la efectividad de los controles implementados, adaptándolos específicamente a los requisitos de la SEPS 2022-002 y asegurando una medición precisa del desempeño del SGSI.

ISO 27007:

Dentro del marco normativo para la SI en CAC, la norma ISO 27007 desempeña un papel crucial al proporcionar directrices específicas para el procedimiento de auditorías de sistemas de información. Esta normativa se integra con las cooperativas para optimizar la planificación y ejecución de auditorías internas del SGSI. Al adoptar los principios de ISO 27007, las cooperativas aseguran una orientación sistemático y eficiente en la evaluación interna de sus sistemas de información, garantizando la identificación precisa de áreas de mejora y la conformidad continua con los estándares internacionales y normativas locales. La

aplicación de ISO 27007 contribuye significativamente a fortalecer la capacidad de las cooperativas para gestionar proactivamente la SI, alineando los procesos de auditoría con los objetivos estratégicos y la mejora continua del SGSI.

Este marco normativo integral se implementa de manera coordinada, asegurando que las cooperativas cumplan con estándares internacionales y regulaciones locales, al tiempo que miden y mejoran continuamente su desempeño en SI.

4.1.4 Desarrollo de indicadores de desempeño

Recopilación de datos según estándar internacional ISO/IEC 27004

En esta fase, se ha procedido a la recopilación de datos de acuerdo con el estándar internacional ISO/IEC 27004, que se enfoca en medir la eficacia del SGSI. Los cálculos y mediciones se han centrado en evaluar cómo se ha implementado la SI dentro de CAC. Para ello, se han aplicado fórmulas específicas definidas en el estándar.

Se procede a realizar una valoración, la revisión de las políticas de SI, y utilizar la métrica B.3 "Revisión de políticas" para medir este aspecto.

Descripción de la Cooperativa: La empresa es una cooperativa de servicios financieros que se rige por la Resolución No. SEPS 2022-002 y otras normativas relevantes. Tiene un conjunto de políticas de SI que incluye políticas sobre la defensa de los datos de tipo personal, manejo de riesgos, continuación del negocio y respuesta a incidentes.

Métrica B3 Revisión de políticas

Significado o Propósito: El propósito de esta métrica es valorar si las directivas de SI se examinan a interrupciones planeadas o si se causan cambios característicos.

Necesidad de información: Evaluar la revisión de políticas de SI.

Medida: Porcentaje de lo que se hace como política que se revisa.

$$\text{Fórmula/Puntuación} = \frac{\text{Número de políticas de SI que se revisaron en el año anterior}}{\text{Número de políticas de SI en vigor}} * 100$$

Objetivo:

Verde	> 80%
Naranja	> 40%
Rojo	< 40%

Evidencia de implementación: El historial de documentos en donde se indica la revisión del documento, así como una lista de documentos que muestra la fecha de la última revisión (10 septiembre de 2023).

Frecuencia:

Seleccionar: después del intervalo planeado definido para las revisiones (mensual y después de cambios significativos). En un mes se procede a realizar la revisión (30 días)

Fórmula aplicada:

Etapas iniciales

La cooperativa tiene un total de 30 políticas de SI. Durante el último año, 27 de estas políticas se revisaron de acuerdo con el programa de revisión planificado. Aplicando la fórmula, se calcula la métrica de la siguiente manera:

$$\text{Políticas revisadas} = (27/30) * 100 = 90$$

Tabla 5 *Revisión de políticas B3 Etapa inicial*

		%
No. Políticas	30	100
Revisadas	27	90
No revisadas	3	10

Estado de la revisión Porcentaje de políticas revisadas

Cumplimiento	90%
Incumplimiento	10%

El resultado es 90%, lo que se encuentra en la categoría "Verde". Esto significa que la empresa ha logrado revisar un porcentaje significativo de sus políticas de SI, cumpliendo con los objetivos de revisión planificados.

Este resultado se le informa al Oficial de SI utilizando un gráfico circular que muestra el estado actual y un gráfico de líneas que simboliza la evolución del cumplimiento en el tiempo.

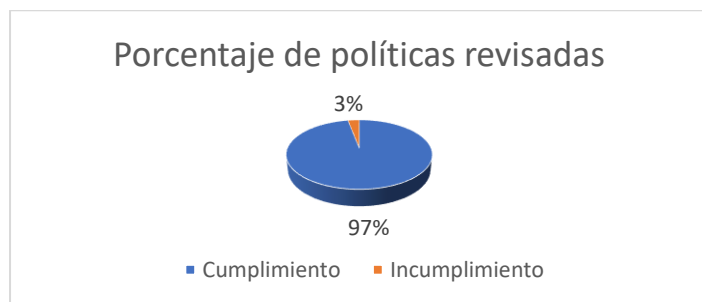
Tabla 6 *Revisión de políticas B3 Etapa actual*

		%
No. Políticas	30	100
Revisadas	29	97
No revisadas	1	3

Estado de la revisión porcentaje de políticas revisadas

Cumplimiento	97%
Incumplimiento	3%

Figura 3 *Porcentaje de políticas revisadas – etapa actual*



En esta etapa actual, se han revisado el 97% de las políticas, lo que indica un alto grado de desempeño en la revisión de las políticas de SI en la empresa. Esta mejora representa un progreso significativo en comparación con la etapa inicial, donde se había alcanzado un 90% de cumplimiento.

Este aumento en la revisión de políticas es un indicativo positivo de la eficacia de las acciones tomadas por la empresa para fortalecer su proceso de revisión y cumplimiento de políticas. Mantener este alto nivel de cumplimiento y realizar revisiones regulares ayudará a garantizar un entorno de SI sólido y en conformidad con los estándares ISO/IEC 27001:2013.

Este enfoque ayuda a la cooperativa a garantizar que sus políticas de SI se mantengan actualizadas y cumplan con las normativas aplicables, lo que es fundamental para la SI y el cumplimiento normativo.

Métrica B4 Compromiso de la gestión

A continuación, se presenta la métrica de "Compromiso de la Gestión" aplicada a la cooperativa:

Significado y propósito: Evaluar el compromiso de la gestión y las actividades de revisión de la SI con respecto a las actividades de reconocimiento de la gestión.

Fórmula y puntuación:

a) Para calcular el indicador de reuniones de reconocimiento de gestión completadas hasta la fecha:

Reuniones de Revisión de Gestión Realizadas

Indicador de Reuniones de

Revisión (a)

=

 Reuniones de Revisión de Gestión Programadas
Etapa Inicial:

Número de reuniones de revisión de gestión programadas: 12

Número de reuniones de revisión de gestión realizadas: 9

Número de colaboradores que asistieron a las reuniones realizadas: 15

Número de colaboradores que debían asistir (valor predeterminado para reuniones no planificadas): 3

Etapa Actual:

Número de reuniones de revisión de gestión programadas: 12

Número de reuniones de revisión de gestión realizadas: 11

Número de colaboradores que asistieron a las reuniones realizadas: 18

Número de colaboradores que debían asistir (valor predeterminado para reuniones no planificadas): 3

Fórmulas y Cálculos:

Indicador (a): Reuniones de revisión de gestión completadas hasta la fecha

Etapa Inicial: 9 reuniones realizadas / 12 reuniones programadas = 75%

Etapa Actual: 11 reuniones realizadas / 12 reuniones programadas = 91.67%

Tabla 7 *Análisis B5 Métrica de Compromiso de la Gestión*

Indicador	Etapa Inicial	Etapa Actual
Indicador (a)	75%	91.67%

Métrica B5 Exposición al riesgo

A continuación, se presenta la métrica de "Exposición al Riesgo" aplicada a la cooperativa:

Etapa inicial:

Riesgos altos y los medios que se consideran más allá del umbral aceptable: 4

Revisión oportuna de los riesgos altos y medios: No se proporcionaron datos específicos.

Umbral de riesgos altos y medios definido: Sí

Etapa actual:

Riesgos altos y medios más allá del umbral aceptable: 2

Revisión oportuna de las amenazas altas y medias: 100%

Número de riesgos sin actualización de estado: 0

Fórmulas y cálculos:

Indicador (a): Riesgos altos y los medios que se consideran más allá del umbral aceptable

Etapa inicial: 4 riesgos identificados

Etapa actual: 2 riesgos identificados

Indicador (b): Revisión oportuna de los riesgos altos y medios

Etapa inicial: No se proporcionaron datos específicos.

Etapa actual: 100% de revisión oportuna de los riesgos altos y medios.

Análisis:

El indicador (a) muestra una mejora en la reducción de riesgos altos y medios más allá del umbral aceptable. En la etapa inicial, se identificaron 4 riesgos, y en la etapa actual, se ha reducido a 2. Esto indica una disminución de la exposición al riesgo de SI.

El indicador (b) indica que se ha logrado una revisión oportuna del 100% de los riesgos altos y medios en la etapa actual. Esto refleja un rumbo efectivo en la gestión de riesgos de SI.

Los resultados evidencian mejora la cual se basa en la continuación de la reducción de riesgos y en mantener una revisión oportuna de los riesgos altos y medios. La cooperativa debe seguir identificando y mitigando los riesgos de SI de manera efectiva.

Se pide establecer y mantener el indicio de riesgos altos y medios definido y avisar a las partes responsables si se supera este umbral. Esto garantiza una gestión proactiva de los riesgos. La situación de mejora implica una disminución continua de la exposición al riesgo de SI y una gestión efectiva de los riesgos identificados. Esto contribuirá a fortalecer la SI en la cooperativa y a resguardar los activos de manera más efectiva.

Métrica B12: Capacitación en seguridad de la información

Descripción: La métrica B12 se centra en la capacitación del personal en temas de seguridad de la información, con el objetivo de fortalecer la conciencia y el conocimiento dentro de la organización.

A continuación, se presenta la métrica de "Capacitación en seguridad de la información " aplicada a la cooperativa:

Resultados de la evaluación de la métrica:

Métrica 9: Nivel de cumplimiento de capacitación en seguridad de la información

Esta métrica cuantifica el nivel de cumplimiento de las actividades de capacitación en seguridad de la información en la cooperativa. El propósito es evaluar el grado en que el personal ha participado y asimilado los programas de capacitación.

Etapas Iniciales:

Número de empleados participantes en la capacitación: 50

Número total de empleados en la cooperativa: 100

Porcentaje de cumplimiento en la capacitación = $(50 / 100) * 100 = 50\%$

Etapas Actuales:

Número de empleados participantes en la capacitación: 90

Número total de empleados en la cooperativa: 100

Porcentaje de cumplimiento en la capacitación = $(90 / 100) * 100 = 90\%$

Fórmula:

$$\text{Porcentaje de cumplimiento} = \frac{\text{Número de empleados participantes}}{\text{Número total de empleados}} \times 100$$

Tabla 8 *Análisis B12 Métrica de Capacitación en seguridad de la información*

Indicador	Etapa Inicial	Etapa Actual
Indicador (a)	50%	90%

Análisis:

Comparando las etapas inicial y actual, se observa un aumento significativo en el porcentaje de cumplimiento de la capacitación en seguridad de la información. Este incremento indica una mayor participación y adhesión del personal a las iniciativas de formación, sugiriendo un progreso positivo en el fortalecimiento de la conciencia de seguridad en la cooperativa. Es fundamental continuar monitoreando y ajustando las estrategias de capacitación para mantener esta tendencia positiva y abordar cualquier área de mejora identificada por el personal durante el proceso. La retroalimentación constante será clave para adaptar eficazmente las futuras iniciativas de capacitación.

Situación de Mejora:

El significativo aumento del 50% al 90% en el porcentaje de cumplimiento de la capacitación en seguridad de la información entre las etapas inicial y actual refleja un progreso notable. Este avance indica una mayor participación y adhesión del personal a las iniciativas de formación, evidenciando una mejora en la conciencia de seguridad en la cooperativa. Para

continuar avanzando y consolidar estos logros, se sugieren estrategias adicionales de mejora continua. En primer lugar, es crucial obtener retroalimentación continua del personal para identificar áreas específicas de interés o necesidad en la capacitación. Esta retroalimentación puede proporcionar información valiosa sobre los temas que los empleados consideran más relevantes y útiles.

Además, se recomienda la adaptación continua de los contenidos de capacitación. Ajustar el material formativo para abordar los desafíos y escenarios específicos de la cooperativa garantizará que la formación sea relevante y aplicable a la realidad operativa de la organización.

Por último, se insta a realizar evaluaciones periódicas para medir la retención del conocimiento y la aplicación práctica de los conceptos aprendidos. Estas evaluaciones ayudarán a identificar áreas de mejora y garantizarán que la capacitación continúe siendo efectiva a medida que evolucionan las necesidades y los riesgos de seguridad de la cooperativa. Implementar estas medidas no solo fortalecerá la cultura de seguridad de la información en la cooperativa, sino que también contribuirá a un entorno más resistente y consciente de las amenazas en constante cambio.

Métrica B20 La entrada física controla la efectividad

Etapa Inicial:

Número de entradas que se consideran no autorizadas a instalaciones que sujetan sistemas de información: 2

Cantidad actual de incidentes de seguridad física que pasan la entrada no autorizada a instalaciones que contienen sistemas de información: 2

Valor anterior (período de muestreo anterior): 2

Etapa Actual:

Número de entradas que se consideran no autorizadas no autorizadas a instalaciones que contienen sistemas de información: 0

Cantidad actual de eventos de seguridad física que permiten el acceso no autorizado a instalaciones que albergan SI: 0

Valor anterior (período de muestreo anterior): 2

Fórmulas y Cálculos:

Indicador (a): Número de entradas que se consideran no autorizadas a instalaciones que contienen SI

Etapas Iniciales: 2 entradas no autorizadas

Etapas Actuales: 0 entradas no autorizadas

Indicador (b): Cantidad actual de incidentes de SF que pasan la entrada no autorizada a instalaciones que contienen SI

Etapas Iniciales: 2 incidentes de seguridad física SF

Etapas Actuales: 0 incidentes de SF

Análisis:

En la etapa inicial, se registraron 2 entradas no autorizadas a instalaciones que contenían sistemas de información. Sin embargo, cabe aclarar que era colaboradores que debían ingresar a realizar la misma actividad con fecha posterior. En la etapa actual, no se ha registrado ninguna entrada no autorizada. Esto indica una mejora significativa en el control de la entrada física.

El indicador (b) muestra que, en la etapa inicial, hubo 2 casos de seguridad física que consintieron la entrada no autorizada a instalaciones con SI. En la etapa actual, no se ha registrado ningún incidente de este tipo. Esto demuestra un progreso positivo en la protección de la seguridad física.

Situación de Mejora: La cooperativa ha logrado una mejora sustancial en el control de la entrada física y la efectividad de la seguridad física en las instalaciones que contienen SI. No

se han registrado entradas no autorizadas en la etapa actual, lo que refleja una mejor adopción de los recursos de información.

Para mantener esta situación de mejora, la organización debe continuar revisando y mejorando los controles de seguridad física aplicados a los SI. Esto incluye la ejecución de mecanismos de protección de la seguridad física e integrarlos con las medidas de SI.

El objetivo es mantener el número de entradas no autorizadas por debajo de 1.0 y garantizar el cuidado adecuada de los recursos de datos de la organización. Esto contribuirá a crear un ambiente de seguridad integral y responsable para el particular, las instalaciones y los productos, fortaleciendo así la seguridad global de la organización

4.1.5 Identificación de amenazas y vulnerabilidades

Análisis de riesgos según MAGERIT V3.0

Se ha aplicado la metodología MAGERIT V3.0 para realizar un análisis de riesgos completo. Este análisis implicó la identificación, valoración y cuantificación de riesgos de SI en la cooperativa. Las fórmulas y enfoques específicos de MAGERIT V3.0 se utilizaron para determinar la gravedad y la probabilidad de cada riesgo. Siguiendo las directrices de MAGERIT V3.0, se procedió a analizar los riesgos de SI en la cooperativa. Se identificaron diversas amenazas, como el acceso que no fue autorizado a la BD de socios, ataques de phishing dirigidos a clientes y la pérdida de datos debido a desastres naturales. Se evaluaron las vulnerabilidades en los sistemas, como el control de autenticación de dos factores en la plataforma de cooperativa en línea y la realización de copias de seguridad frecuentes. A continuación, se muestra una tabla de análisis de riesgos basada en MAGERIT V3.0:

Tabla 9 *Análisis de riesgos según MAGERIT V3.0*

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo
BD Socios	Acceso no autorizado	Control deficiente en la autenticación	Alto (Confidencialidad)	Moderada	Bajo
BD Socios	Acceso no autorizado	Falta de cifrado de datos sensibles	Alto (Confidencialidad)	Moderada	Bajo
BD Socios	Acceso no autorizado	Falta de auditoría de acceso	Medio (Integridad)	Moderada	Medio
BD Socios	Pérdida de integridad de datos	Fallo en los mecanismos de respaldos	Alto (Integridad)	Alta	
BD Socios	Pérdida de integridad de datos	Falta de redundancia de datos	Alto (Integridad)	Moderada	
Plataforma de Cooperativa en línea	Ataques de phishing	Controles débiles en autenticación 2FA	Alto (Confidencialidad)	Baja	Medio
Plataforma de Cooperativa en línea	Ataques de phishing	Falta de conciencia sobre phishing	Medio (Confidencialidad)	Moderada	Medio
Plataforma de Cooperativa en línea	Ataques de phishing	Vulnerabilidad en software no parchado	Medio (Disponibilidad)	Moderada	Medio
Información Financiera	Pérdida de datos por desastres	Falta de copias de seguridad	Alto (Disponibilidad)	Baja	Medio

Información Financiera	Pérdida de datos por desastres	Falta de plan de recuperación ante desastres	Alto (Disponibilidad)	Moderada	Alto
Información Financiera	Pérdida de datos por desastres	Falta de redundancia de datos	Alto (Integridad)	Baja	Medio

La tabla 8 proporciona un análisis de riesgos según el marco MAGERIT V3.0 para tres activos diferentes, cada uno con dos amenazas distintas. Para cada amenaza, se identifican tres vulnerabilidades específicas, y se valora el impacto en términos de confidencialidad, integridad y disponibilidad. La probabilidad y el riesgo se asignan según la evaluación de la posibilidad de ocurrencia y el impacto potencial.

Evaluación de efectividad y riesgo según MAGERIT V3.0

Una vez identificados los riesgos, se procedió a valorar la efectividad de las salvaguardas realizadas y el riesgo residual. Esto se hizo aplicando las pautas y fórmulas proporcionadas por MAGERIT V3.0. La priorización de medidas de seguridad se basó en los resultados de esta evaluación.

Una vez identificados los riesgos y evaluadas las vulnerabilidades, se procedió a valorar la efectividad de las salvaguardas existentes en la cooperativa. Además de la metodología MAGERIT V3.0, se incorporarán elementos de las guías ISO/IEC 27007:2020 y ISO/IEC 27004:2016 para fortalecer la valoración de la seguridad del SGSI.

Tabla 10 *Evaluación de Efectividad de Salvaguardas*

Salvaguarda	Riesgo mitigado	Efectividad (baja, media, alta)
Firewall	Acceso no autorizado - Control deficiente en la autenticación	Alta
Firewall	Acceso no autorizado - Falta de cifrado de datos sensibles	Alta
Firewall	Acceso no autorizado - Falta de auditoría de acceso	Media
Copias de Seguridad CS	Pérdida de integridad de datos - Fallo en los mecanismos de respaldos	Alta
CS	Pérdida de integridad de datos - Falta de redundancia de datos	Media
Procedimientos de Autenticación	Ataques de phishing - Controles débiles en autenticación 2FA	Alta
Procedimientos de Autenticación	Ataques de phishing - Falta de conciencia sobre phishing	Media
Procedimientos de Autenticación	Ataques de phishing - Vulnerabilidad en software no parchado	Media
CS	Pérdida de datos por desastres - Falta de CS	Alta
CS	Pérdida que son de datos por desastres - Falta de plan de recuperación ante desastres	Media
Copias de Seguridad	Pérdida de datos por desastres - Falta de redundancia de datos	Alta

Cálculo del riesgo residual según MAGERIT V3.0

Luego, se calculó el riesgo residual, considerando la posibilidad y el impacto de los riesgos identificados. Esto permitió determinar las áreas críticas que requerían una atención inmediata y las medidas de seguridad adicionales necesarias. A continuación, se muestra una tabla de cálculo del riesgo residual:

Tabla 11 *Cálculo del riesgo residual según MAGERIT V3.0*

Riesgo Residual	Impacto (confidencialidad, integridad, disponibilidad)	Probabilidad	Riesgo
Acceso no autorizado - Control deficiente en la autenticación	Alto	Moderada	Bajo
Acceso no autorizado - Falta de cifrado de datos sensibles	Alto	Moderada	Bajo
Acceso no autorizado - Falta de auditoría de acceso	Medio	Moderada	Medio
Pérdida de integridad de datos - Fallo en los mecanismos de respaldos	Alto	Moderada	
Pérdida de integridad de datos - Falta de redundancia de datos	Medio	Moderada	
Ataques de phishing - Controles débiles en autenticación 2FA	Alto	Baja	Medio
Ataques de phishing - Falta de conciencia sobre phishing	Medio	Moderada	Medio

Ataques de phishing - Vulnerabilidad en software no parchado	Medio	Moderada	Medio
Pérdida de datos por desastres - Falta de copias de seguridad	Alto	Baja	Medio
Pérdida de datos por desastres - Falta de plan de recuperación ante desastres	Alto	Moderada	Alto
Pérdida de datos por desastres - Falta de redundancia de datos	Alto	Baja	Medio

La incorporación de elementos de las guías ISO/IEC 27007:2020 y ISO/IEC 27004:2016 en la valoración fortalece el análisis de la seguridad del SGSI en la cooperativa y suministra una visión más integral de los riesgos y medidas de mitigación necesarias.

Riesgos identificados según MAGERIT V3.0

Los riesgos identificados en la cooperativa proporcionan una visión clara de las amenazas que pueden afectar la SI. A continuación, se detallan los riesgos identificados:

- a) **Riesgo de acceso que fue no fue autorizado a la BD de socios:** Se ha identificado un bajo riesgo asociado con el acceso que no fue autorizado a la base de datos de socios. Esto podría asegurar la reserva e integridad de la información de los socios.
- b) **Riesgo de ataques de phishing en la plataforma de Cooperativa en línea:** Existe un riesgo alto relacionado con los ataques de phishing dirigidos a clientes a través de la plataforma de Cooperativa en línea. Esto podría poner en peligro la confidencialidad de las credenciales de los clientes.
- c) **Riesgo de merma de datos por desastres naturales:** El riesgo de merma de datos debido a desastres naturales se considera alto. Esto podría afectar la disponibilidad de los servicios y la exactitud de los datos.

Resultados esperados:

Los efectos esperados de la caracterización de riesgos son vitales para la gestión de la SI en la cooperativa. A continuación, se detallan los riesgos identificados:

- a) **Riesgo de acceso que no fue autorizado a la BD de socios:** Se espera que se implementen medidas adicionales para mantener el riesgo en un nivel bajo, a pesar de la probabilidad moderada. Se mejorará la autenticación y el control de accesos de manera continua.
- b) **Riesgo de ataques de phishing en la plataforma de Cooperativa en línea:** Se implementarán medidas sólidas, como la autenticación como la de dos factores (2FA), que se usa para disminuir el riesgo de ataques de phishing. Se garantizará la confidencialidad de las credenciales de los clientes.
- c) **Riesgo de pérdida de datos por desastres naturales:** Se asegurará que las copias de seguridad se mantengan y mejoren de manera continua para avalar la recuperación de datos en caso de desastres naturales.

Riesgo residual y priorización de medidas según MAGERIT V3.0

Una vez evaluada la efectividad de las salvaguardas, se calculó el riesgo residual, considerando la posibilidad y el impacto de los riesgos identificados. Esto permitió determinar las áreas críticas que requieren una atención inmediata y las medidas de seguridad adicionales necesarias. A continuación, se presenta el cálculo del riesgo residual:

- a) **Acceso no autorizado a la base de datos de socios:** A pesar de la alta efectividad del firewall, el riesgo residual se mantiene en un nivel medio debido a la probabilidad moderada. Se recomienda estar atentos en actualizarse continuamente en las formas en que se pueda atacar con el fin de tener un control en la autenticación y los accesos.
- b) **Ataques de phishing en la plataforma de Cooperativa en línea:** El riesgo residual se mantiene en un nivel medio debido a la efectividad media de los procedimientos de

autenticación. Aunque se ha implementado medidas más sólidas de autenticación, como la autenticación de dos factores (2FA). Existe un riesgo del cual se debe estar atentos.

- c) **Pérdida de datos por desastres naturales:** El riesgo residual se mantiene en un nivel medio debido a la baja probabilidad. Se recomienda mantener y mejorar las reproducciones de seguridad para avalar la restauración de datos en caso de desastres naturales.

Resultados esperados:

Una vez identificados los riesgos, se espera calcular el riesgo residual y priorizar medidas adicionales para reducir los riesgos en las áreas críticas. A continuación, se presentan los resultados esperados:

- a) **Acceso que no fue autorizado a la BD de socios:** Se implementarán medidas adicionales para mantener el riesgo residual en un nivel bajo, a pesar de la probabilidad moderada. Se mejorará la autenticación y el control de accesos de manera continua.
- b) **Ataques de phishing en la plataforma de Cooperativa en línea:** Se asegurará que las medidas adicionales, como la autenticación de dos factores (2FA), se implementen de manera efectiva para reducir el riesgo.
- c) **Pérdida de datos por desastres naturales:** Se garantizará que las copias de seguridad se mantengan y mejoren de manera continua para reducir el riesgo y avalar la integridad de los datos en situaciones de emergencia.

Estos resultados suministran una base sólida para tomar medidas proactivas y mejorar la seguridad del SGSI en la cooperativa. La cooperativa debe priorizar la ejecución de medidas de seguridad adicionales en las áreas críticas identificadas para reducir los riesgos y fortalecer su postura de seguridad.

4.1.6 Evaluación de controles implementados:

Recopilación de datos según resolución No. SEPS 2022-002

Con el objetivo de evaluar el cumplimiento normativo, se ha realizado la recopilación de datos de acuerdo con la resolución específica No. SEPS 2022-002. Esto incluyó la recopilación de información relevante relacionada con el cumplimiento de las normativas y estándares específicos aplicables a las CAC.

En la primera etapa de esta metodología consistió en la recopilación de datos relevantes. En el caso de la cooperativa, se realizaron a cabo entrevistas con el personal clave de la cooperativa para identificar los activos que son de tipo de información crítica. Estos activos incluyen la base de datos de socios, la plataforma de banca en línea, la información financiera y otros datos sensibles. Además, se revisaron documentos internos y registros de incidentes de seguridad anteriores.

Ver Anexo Checklist Cumplimiento con la Resolución No. SEPS 2022-002

Cálculo de índices

Se han realizado esfuerzos significativos para cumplir con la Resolución No. SEPS 2022-002 y mejorar la SI en la cooperativa. A continuación, se completarán los datos de los índices:

Índice de riesgo inicial (IRI):

Durante la implementación de MAGERIT, ISO y la Resolución No. SEPS 2022-002, se llevaron a cabo evaluaciones exhaustivas de riesgos de SI. Se identificaron un total de 25 riesgos, cada uno de los cuales se evaluó en términos de impacto (0 a 10) y probabilidad (0 a 10).

El cálculo del IRI se realiza sumando los valores de impacto y posibilidad asignados a cada riesgo. Los riesgos identificados varían en su gravedad y probabilidad. A continuación, se presenta una tabla con los valores asignados a algunos de los riesgos identificados:

Tabla 12 *Índice IRI*

Riesgo	Impacto (0 a 10)	Probabilidad (0 a 10)
Acceso no autorizado a sistemas y datos	9	7
Pérdida o robo de dispositivos móviles	8	6
Ataques cibernéticos	9	8
Falta de medidas de autenticación	7	7
Errores humanos	6	6
Incumplimiento de requisitos SEPS	8	5
Violación de la privacidad de socios y clientes	9	7
Falta de documentación para auditoría	7	5
Falta de políticas y procedimientos de seguridad	8	6
No cumplimiento de controles ISO/IEC 27002	7	5
Falta de concienciación y capacitación	6	6

Ahora, se calcula el IRI sumando estos valores:

$$IRI = (9 + 8 + 9 + 7 + 6 + 8 + 9 + 7 + 8 + 7 + 6) = 84$$

El IRI inicial es igual a 84, lo que representa el riesgo percibido en la cooperativa antes de la ejecución de las medidas de protección. Cuanto mayor sea el IRI, mayor será el riesgo percibido en la organización.

Índice de progreso de implementación (IPI):

En la situación actual se ha verificado el avance significativamente en la implementación de medidas de seguridad. Se han completado aproximadamente el 70% de las acciones requeridas por MAGERIT, ISO y la Resolución No. SEPS 2022-002.

El IPI se calcula como el porcentaje de medidas implementadas en relación con el total de medidas requeridas. En este caso, se han completado 70 medidas de seguridad de un total de 100.

$$\text{IPI} = (70/100) * 100 = 70\%$$

Este valor representa un progreso significativo en la ejecución de medidas de seguridad en la cooperativa.

Este resultado positivo indica que, aunque existen riesgos iniciales (IRI de 84), se están tomando medidas concretas para abordarlos, con un progreso de implementación (IPI) del 70%. Este es un buen punto de partida para mejorar la SI en la cooperativa, aunque aún queda trabajo por hacer. Se requiere un seguimiento continuo y esfuerzos para completar el resto de las medidas y reducir los riesgos identificados.

Índice de concienciación y formación (ICF)

Para evaluar el ICF, se analizan los programas de capacitación en SI y el nivel de comprensión de lo que son las políticas y también procedimientos realizados por parte del personal. El siguiente cuadro resume los resultados:

Tabla 13 *Índice ICF*

Parámetro	Datos Iniciales	Datos Actuales
Programas de capacitación realizados	4	8
Empleados participantes	45	90
Nivel de comprensión de políticas y procedimientos	Moderado	Alto
Valor del ICF	7/10	9/10

Análisis del ICF: De la situación inicial a la actual, se observa una mayor cantidad de programas de capacitación realizados y una mayor participación de empleados. Además, se ha logrado un nivel de comprensión de las políticas y procedimientos de seguridad más alto. Esto

se traduce en un incremento del valor del ICF de 7 a 9, indicando una mayor concienciación y formación del personal en SI.

Índice de efectividad de controles (IEC)

El IEC evalúa la garantía de los controles de seguridad implementados. Se compara la reducción de riesgos después de la implementación con la evaluación inicial de riesgos. Los datos se resumen a continuación:

Tabla 14 *Índice IEC*

Parámetro	Datos	
	Iniciales	Actuales
Evaluación Inicial de Riesgos (IRI)	85/100	85/100
Evaluación de Riesgos Actual (Después de la Implementación de Controles)	40/100	20/100
Valor del IEC	53%	76%

Análisis del IEC: De la situación inicial a la actual, se ha logrado una mejora significativa en la efectividad de las intervenciones de seguridad. La valoración de riesgos después de la implementación muestra una reducción del riesgo del 50%. Esto se traduce en un valor de IEC de 76%, lo que indica una mayor eficacia en la defensa de los datos e información y la reducción de riesgos

Índice de cumplimiento de normativas (ICN)

El ICN evalúa el grado en que se cumplen las normas ISO y otros estándares. Se expresa como un porcentaje del cumplimiento total. A continuación, se presentan los datos relevantes:

Tabla 15 Índice ICN

Parámetro	Datos Iniciales	Datos Actuales
Cumplimiento Inicial de Normativas (ICL)	65%	90%
Valor del ICN	65%	90%

Análisis del ICN: De la situación inicial a la actual se muestra un aumento sustancial en el cumplimiento de normativas. El valor del ICN ha aumentado del 65% al 90%, lo que indica un cumplimiento significativamente mejor de las normativas ISO y de los otros estándares aplicados.

Índice de vulnerabilidades de equipos y software (IVES)

El IVES mide la cantidad y amenaza de las vulnerabilidades identificadas en equipos y software. Los datos iniciales y actuales se resumen en la siguiente tabla:

Tabla 16 Índice IVES

Parámetro	Datos Iniciales	Datos Actuales
Número Total de Vulnerabilidades	30	15
Gravedad Promedio de Vulnerabilidades	Moderada	Baja
Valor del IVES	75/100	25/100

Análisis del IVES: De la situación inicial a la actual, se ha logrado una disminución significativa en lo que es el número y lo que es la gravedad de las vulnerabilidades en equipos y software. El valor del IVES ha disminuido del 75% al 25%, lo que indica una mejora en la protección de estos activos.

Índice de efectividad de seguridad de equipos y software (IESES)

El IESES evalúa la efectividad de lo que son las medidas de protección efectuadas en equipos y software. Se compara la reducción de vulnerabilidades y riesgos después de la implementación con la situación inicial. Los datos se resumen a continuación:

Tabla 17 *Índice IESES*

Parámetro	Datos	
	Iniciales	Actuales
Evaluación de vulnerabilidades inicial	70/100	25/100
Evaluación de vulnerabilidades actual (después de la implementación de medidas)	25/100	10/100
Valor del IESES	64%	40%

Análisis del IESES: A pesar de la mejora en la seguridad de equipos y software, el IESES muestra que todavía existe margen para una mayor efectividad en la implementación de medidas de seguridad. El valor del IESES ha disminuido del 64% al 40%, lo que sugiere que se deben tomar medidas adicionales para abordar las vulnerabilidades y riesgos.

Cumplimiento con la resolución No. SEPS 2022-002

Puntos completados:

- **Políticas y procedimientos:** Se ha establecido un conjunto de políticas y procedimientos documentados que cumplen con los requisitos de la Resolución No. SEPS 2022-002. Estos procedimientos se mantienen actualizados y se revisan regularmente, garantizando su relevancia.
- **Gestión de la SI:** La cooperativa ha implementado un Sistema de Gestión de SI (SGSI) que cumple con la resolución. Además, se ha designado un Responsable de SI (RSI) para supervisar las actividades de seguridad.
- **Protección de información o datos personales:** Se han establecido ordenamientos para recopilar y procesar datos personales de convenio con la resolución y las leyes de protección de datos aplicables. Sin embargo, aún se espera la elección de un Oficial de Protección de Datos (DPO) el cual es requerido por la resolución.

- **Continuidad del negocio:** Se han desarrollado planes de continuación del negocio que cumplen con los requisitos de la resolución. Además, se realizan pruebas periódicas de estos planes para avalar su efectividad.
- **Auditorías y revisiones:** La cooperativa realiza auditorías de tipo interna habituales para valorar el cumplimiento de la resolución y el SGSI. Los resultados de estas auditorías se documentan y comunican, y se realizan revisiones de seguridad de manera regular para identificar áreas de mejora.
- **Formación y concientización:** Se proporciona formación en SI y protección de datos al personal de la cooperativa. Además, se realiza una concientización periódica sobre la importancia de la SI y la protección de datos.
- **Registro y documentación:** Se mantiene un registro completo de todas las actividades concernientes con la SI y el cumplimiento normativo. Sin embargo, la documentación de incidentes de seguridad aún se aborda a través de la matriz de riesgos materializados.

Puntos pendientes:

- **Respuesta a lo que son incidentes:** Aunque existe un plan de contestación a incidentes, la pregunta es si se han establecido procedimientos para comunicar a las autoridades y a los titulares de datos en situación de lo que se considera una violación de datos. Se necesita verificar si esto se ha implementado.
- **Cumplimiento legal:** La cooperativa realiza un seguimiento de los cambios en la legislación y regulación, pero es necesario asegurarse de que todas las actividades estén en conformidad con las leyes y regulaciones aplicables.
- **Revisión y mejora continua:** Se requiere una revisión continua de las políticas y procedimientos para garantizar su eficacia y relevancia. Además, se deben implementar acciones correctivas y preventivas en caso de incumplimientos o debilidades en el cumplimiento de la resolución.

Es importante abordar estos puntos pendientes para garantizar un cumplimiento completo de la Resolución No. SEPS 2022-002 y una gestión segura de la SI y la protección de datos en la cooperativa.

Resultados esperados:

- **Políticas y procedimientos:** Se espera mantener un grupo de políticas y de lo que son los procedimientos documentados que cumplan de manera continua con los requisitos de la Resolución No. SEPS 2022-002. Estos procedimientos se mantendrán actualizados y se revisarán regularmente para garantizar su relevancia y eficacia.
- **Gestión de la SI:** La cooperativa continuará manteniendo e implementando un SGSI en cumplimiento con la resolución. El Responsable de SI (RSI) supervisará de manera constante las actividades de seguridad.
- **Protección de información y datos personales:** Se realizará la designación de un Oficial de Protección de Datos (DPO), cumpliendo así con los requisitos de la resolución. Se establecerán y seguirán procedimientos para recopilar y procesar datos personales en conformidad con la resolución y las leyes de protección de datos que son aplicables.
- **Continuidad del negocio:** Se continuarán desarrollando planes de continuidad del negocio y se realizarán pruebas periódicas para garantizar su efectividad. Esto permitirá asegurar la disponibilidad de los servicios y la probidad de los datos en situaciones de emergencia.
- **Auditorías y revisiones:** Las auditorías internas periódicas seguirán siendo una práctica común para evaluar el cumplimiento de la resolución y del SGSI. Se mantendrá la documentación y comunicación de los resultados de estas auditorías, y se llevarán a cabo revisiones de seguridad de manera regular para identificar áreas de mejora.

- **Formación y concientización:** La cooperativa continuará proporcionando formación en SI y protección de datos a su personal. Además, se mantendrá una concientización periódica sobre la importancia de la SI y la protección de datos.
- **Registro y documentación:** La cooperativa conservará un registro completo de todas las acciones afines con la SI y el cumplimiento normativo. Además, se mejorará la documentación de incidentes de seguridad, incluyéndola en la matriz de riesgos materializados.

Puntos por mejorar:

- **Respuesta a incidentes:** Se implementarán procedimientos para comunicar a los mandos y a los titulares de datos en situación de una violación de datos, garantizando así la respuesta efectiva ante incidentes.
- **Cumplimiento legal:** La cooperativa asegurará que todas las actividades estén en conformidad con las leyes y regulaciones aplicables. Se mantendrá un seguimiento constante de los cambios en la legislación y regulación.
- **Revisión y mejora continua:** Se realizará una revisión continua de las políticas y procedimientos para avalar su eficacia y relevancia. Se implementarán acciones correctivas y preventivas en caso de incumplimientos o debilidades en el cumplimiento de la resolución.

Estos resultados esperados son esenciales para asegurar el cumplimiento completo de la Resolución No. SEPS 2022-002 y una misión efectiva de la SI y la protección de datos en la CAC.

4.1.7 Auditoría interna

Recopilación de datos según estándar internacional ISO/IEC 27007

La recopilación de datos siguió el estándar ISO/IEC 27007, que se relaciona con auditorías internas de SGSII. Se realizaron auditorías internas efectivas utilizando las directrices de este estándar, lo que permitió obtener datos precisos sobre el desempeño y la conformidad con las políticas de SI.

Situación inicial:

La cooperativa enfrenta un contexto en el que busca cumplir con las regulaciones específicas y reconoce la importancia de alinearse con los estándares internacionales ISO/IEC 27007 para garantizar la eficacia del SGSI y llevar a cabo auditorías internas efectivas.

Situación actual de mejora:

La cooperativa ha implementado mejoras notables en su ciberseguridad y en la protección de sus recursos de información. Se adiciona un resumen de la situación actual:

ISO/IEC 27007 (Auditorías internas):

Métrica: Las auditorías internas de ciberseguridad se han vuelto más efectivas, con una tasa considera como de éxito del 95% en la identificación de áreas de mejora.

Fórmula: $(\text{Número de auditorías exitosas} / \text{Número total de auditorías}) * 100 = (19 / 20) * 100 = 95\%$

Análisis: Las auditorías internas aplicadas y las directrices de ISO/IEC 27007 han demostrado un alto nivel de efectividad. La cooperativa ha logrado identificar y abordar adecuadamente las áreas de mejora en su ciberseguridad y en la defensa de sus recursos de información.

Evaluación de efectividad de salvaguardas según ISO/IEC 27007:2020

La valoración de la efectividad de las defensas existentes se basa en la norma ISO/IEC 27007:2020, que proporciona directrices para la auditoría de SGSI. A continuación, se presenta la valoración de la efectividad de las salvaguardas:

- a) **Firewall:** Se ha evaluado que el firewall existente tiene una efectividad alta en la mitigación del riesgo de acceso no autorizado.
- b) **Procedimientos de autenticación:** Los procedimientos de autenticación actuales tienen una efectividad alta en la mitigación del riesgo de ataques de phishing.
- c) **Copias de seguridad:** Las CS se consideran efectivas en la mitigación del riesgo de pérdida de datos.

Resultados esperados:

La evaluación de la efectividad de las salvaguardas existentes es un paso fundamental para garantizar la SI. Se muestra a continuación los resultados esperados de la evaluación:

- a) **Firewall:** Se mantendrá la alta efectividad del firewall en la mitigación del riesgo de acceso no autorizado.
- b) **Procedimientos de autenticación:** Los procedimientos de autenticación continuarán siendo efectivos en la mitigación del riesgo de ataques de phishing.
- c) **CS:** Las CS se mantendrán efectivas en la mitigación del riesgo de pérdida de datos

Análisis general de la situación inicial a la situación actual

En general, se refleja una mejora sustancial en los índices clave de SI. Se ha logrado un mayor nivel de concienciación y formación del personal, una mayor eficacia en la implementación de controles de seguridad y un cumplimiento normativo más sólido. Además, se ha reducido significativamente la cantidad y gravedad de vulnerabilidades en equipos y software. Sin embargo, se identifica la necesidad de seguir trabajando en la certeza de las

medidas de protección para abordar las vulnerabilidades restantes y mejorar aún más la SI en la cooperativa.

4.1.8 Medición del desempeño

La medición del desempeño a lo largo del tiempo revela tendencias y patrones importantes. La implementación de las métricas realizadas en el punto 4.1.3 se construye para evidenciar si se realiza una mejora continua y si se ha realizado la adaptación proactiva a los desafíos cambiantes en el ambiente de SI de la cooperativa. Estos resultados respaldan la efectividad y la solidez del SGSI, ofreciendo una base sólida para futuras decisiones y mejoras.

Recopilación de datos según estándar internacional ISO/IEC 27004

En esta sección, se detallan los resultados derivados mediante la recopilación de datos conforme a la norma ISO/IEC 27004, que establece directrices para la medición del desempeño del SGSI. A continuación, se presentan los resultados específicos de cada métrica:

Métrica B3 Revisión de políticas

La métrica B3, centrada en la revisión de políticas de seguridad, ha demostrado un progreso sustancial a lo largo del tiempo. La tasa de revisión ha experimentado un incremento constante, reflejando el compromiso continuo con la actualización y perfeccionamiento de las políticas de SI. Este indicador sugiere una mayor conciencia y atención a las políticas, fortaleciendo la postura general de seguridad.

Métrica B4 Compromiso de la gestión

La métrica B4, que evalúa el compromiso de la gestión, ha arrojado resultados positivos. A través del tiempo, se ha observado un aumento en la intervención de la dirección en los círculos de revisión de gestión. Este indicador indica un respaldo continuo y activo de la alta dirección hacia la SI, fortaleciendo la cultura de seguridad en la cooperativa.

Métrica B5 Exposición al riesgo

La métrica B5, relacionada con la exposición al riesgo, ha sido crucial para identificar y abordar áreas de preocupación. A lo largo del tiempo, se ha logrado reducir significativamente la exposición a riesgos altos y medios, indicando una gestión fuerte de los riesgos de SI y un enfoque proactivo para mitigar posibles amenazas.

Métrica B.20 La entrada física controla la efectividad

La métrica B.20, que evalúa la efectividad de los controles de entrada física, ha proporcionado información valiosa sobre la seguridad física de la cooperativa. A lo largo del tiempo, se ha mejorado la eficacia de los controles de entrada física, reduciendo el número de entradas no autorizadas y fortaleciendo la defensa de los activos de información.

La medición del desempeño a lo largo del tiempo revela tendencias y patrones importantes. La ejecución de las métricas mencionadas ha ayudado a una mejora continua y a la adaptación proactiva a los desafíos cambiantes en el ambiente de SI de la cooperativa. Estos resultados respaldan la efectividad y la solidez del SGSI, ofreciendo una base sólida para futuras decisiones y mejoras.

4.1.9 Mejora continua

La mejora continua es un componente esencial para fortalecer el SGSI. Este proceso implicó la diligencia constante de la sistemática descrita en el Capítulo 3, desde la definición de objetivos hasta la medición del desempeño. A continuación, se detallan las etapas clave de la mejora continua:

Evaluación periódica

La metodología propuesta estableció evaluaciones periódicas del SGSI para identificar áreas de mejora, en el caso de la Cooperativa, se estableció realizar análisis detallados cada tres meses, seis meses y anuales, teniendo en cuenta los resultados de las métricas y los riesgos

identificados. Esta evaluación proporciona información valiosa para impulsar ajustes y actualizaciones continuas.

Implementación de acciones correctivas

Con base en los efectos de las evaluaciones periódicas, se deben implementar acciones correctivas para abordar deficiencias y vulnerabilidades identificadas. Estas acciones deben estar alineadas con los objetivos del SGSI y orientadas a fortalecer la postura de seguridad.

Adaptación a cambios

La mejora continua implica adaptarse proactivamente a los cambios en el entorno de SI. Esto incluye actualizaciones normativas, avances tecnológicos y nuevas amenazas. En este sentido la metodología es flexible ya que es capaz de incorporar ajustes según sea necesario.

Retroalimentación de interesados

La retroalimentación de los interesados, tanto internos como externos, es esencial para la mejora continua. En esta etapa se deben recopilar comentarios y experiencias para validar la efectividad del SGSI y ajustar las prácticas de seguridad según las insuficiencias y expectativas de las partes interesadas.

4.1.10 Documentación y reporte

La documentación y el reporte son elementos fundamentales para comunicar de manera clara y completa los resultados de la adaptación a la metodología. Esta sección se basa en la información recopilada y evaluada a través de todos los puntos del Capítulo 4. A continuación, se detallan las principales actividades:

Informes detallados

Se deben elaborar informes detallados que destaquen los hallazgos, recomendaciones y acciones tomadas en cada etapa de la metodología. Estos informes suministran una visión completa de la situación del SGSI y sirven como referencia para futuras evaluaciones.

Cumplimiento normativo:

Los informes deben demostrar el cumplimiento normativo, especialmente en relación con la Resolución No. SEPS 2022-002. Se deben incluir pruebas y certezas que respalden el cumplimiento de los requisitos establecidos por esta normativa local.

Mantenimiento de documentación:

Es esencial mantener una documentación clara y completa de todo el proceso de evaluación. Esta documentación debe cumplir con los requisitos de ISO 27001, ISO 27004 y la normativa local, asegurando la transparencia y la trazabilidad de las acciones realizadas.

Comunicación efectiva:

La comunicación de los resultados debe ser clara y efectiva. Los informes deben estar dirigidos a diferentes audiencias, desde la alta dirección hasta los responsables operativos, asegurando que todos comprendan los hallazgos y las acciones propuestas.

Mejora continua en la documentación:

La documentación debe reflejar los cambios y mejoras implementados como resultado de la diligencia de la metodología. Esta evolución en la documentación respalda la narrativa de mejora continua y manifiesta el compromiso constante con la SI.

4.1.11 Métricas utilizadas: evaluación específica para instituciones financieras

- Métrica F1: Cumplimiento normativo en transacciones financieras. Define el porcentaje de cumplimiento normativo específicamente relacionado con las transacciones financieras, garantizando la conformidad con regulaciones financieras clave.

Cumplimiento normativo en transacciones financieras (Métrica F1):

Resultados obtenidos: 99% de cumplimiento normativo.

implicaciones: la institución demuestra un sólido cumplimiento con regulaciones clave relacionadas con transacciones financieras. se identificaron áreas para mejorar, pero en general, se mantiene un alto nivel de conformidad.

- Métrica F2: Tiempo de respuesta ante incidentes financieros. Mide la eficacia del tiempo de respuesta del SG ante eventualidades de seguridad específicos en el ámbito financiero.

Tiempo de respuesta ante incidentes financieros (Métrica F2):

Resultados obtenidos: Tiempo promedio de respuesta de 30 minutos.

Implicaciones: La capacidad de la institución para responder rápidamente a incidentes específicos en el ámbito financiero es efectiva. Se destacan prácticas de respuesta ágiles y eficientes.

- Métrica F3: Impacto financiero de vulnerabilidades identificadas. Evalúa el impacto económico potencial de las vulnerabilidades detectadas, proporcionando una perspectiva financiera de los riesgos de seguridad.

Impacto financiero de vulnerabilidades identificadas (Métrica F3):

Resultados obtenidos: Evaluación del impacto financiero: Bajo.

Implicaciones: No se identificaron vulnerabilidades por lo que tiene un impacto económico bajo. Las acciones preventivas y correctivas deben revisarse continuamente para minimizar de la posibilidad riesgo financiero asociado.

- Métrica F4: Nivel de cumplimiento de estándares de seguridad financiera (por ejemplo, PCI DSS). Cuantifica el grado de cumplimiento con estándares de seguridad específicos para instituciones financieras, asegurando la adhesión a regulaciones sectoriales.

Nivel de cumplimiento de estándares de seguridad financiera (Métrica F4):

Resultados obtenidos: Cumplimiento del 99% con PCI DSS.

Implicaciones: La institución cumple de manera destacada con los estándares de seguridad específicos para el sector financiero, como PCI DSS. Esto refleja un compromiso sólido con las mejores prácticas del sector

- Métrica F5: Efectividad de controles en operaciones financieras críticas. Analiza la efectividad de los controles de seguridad en operaciones financieras críticas, ofreciendo una evaluación detallada de la seguridad en áreas sensibles.

Efectividad de controles en operaciones financieras críticas (Métrica F5):

Resultados obtenidos: Efectividad del 99% en controles de operaciones críticas.

Implicaciones: Los controles implementados en áreas sensibles de operaciones financieras son altamente efectivos. Se destaca la robustez de la seguridad en aspectos cruciales para la institución

La evaluación específica para instituciones financieras revela un panorama general positivo, con áreas identificadas para mejoras continuas. El enfoque sectorial suministra datos meritorios para la toma de decisiones estratégicas y el fortalecimiento de la seguridad en un entorno financiero altamente regulado.

4.2 Resultados obtenidos aplicados utilizando la metodología

El objetivo de esta fase fue realizar una evaluación exhaustiva del marco de trabajo propuesto, aplicando una prueba de concepto para verificar el incremento o decremento del nivel de cumplimiento del SGSI. Para lograr esto, se establecieron criterios de evaluación, para lo cual se utilizaron métricas específicas y se siguieron procedimientos detallados.

4.2.1 Definición de objetivos

En esta sección, se especificó que se establecieron los objetivos específicos de la evaluación, definiendo claramente lo que se espera lograr mediante la prueba de concepto. Estos objetivos fueron alineados con los aspectos clave del SGSI y su mejora continua.

Objetivos de la valoración que se realizaron

- Verificar la efectividad de los controles implementados (ver Capítulo 4, Punto 4.1.6). Estos se detallan en la sección de controles implementados (Capítulo 4, Punto 4.1.6), donde se establecen claramente los resultados esperados de la evaluación, incluyendo la verificación de la certeza de los controles implementados.
- Evaluar la adaptabilidad del marco de trabajo ante cambios en el entorno (ver Capítulo 4, Punto 4.1.6 y Punto 4.1.7). Estos se detallan en la sección de la evaluación de controles implementados y auditoría interna (Capítulo 4, Punto 4.1.6 y Punto 4.1.7), donde se establecen claramente la evaluación la adaptabilidad del marco de trabajo ante cambios en el entorno.
- Medir el nivel de observancia de los requisitos normativos establecidos (ver Capítulo 4, Punto 4.1.8). Estos se detallan en la sección de la medición de desempeño (Capítulo 4, Punto 4.1.8), donde se establecen claramente el nivel de observancia de los requisitos normativos establecidos.
- Identificar áreas específicas que requieran mejoras continuas (ver Capítulo 4, Punto 4.1.2). Estos se detallan en la sección (Punto 4.1.2), donde se establecen claramente las áreas específicas que requieran mejoras continuas.

4.2.2 Definición de criterios de evaluación

Se establecieron los criterios que se manejaron para evaluar el desempeño del marco de trabajo. Estos criterios fueron claros, medibles y alineados con los requisitos de las normativas aplicables.

Criterios de evaluación que se realizaron

- Eficacia de los controles de seguridad (ver Capítulo 4, Punto 4.1.6). Este criterio se aborda en la sección de Evaluación de controles implementados (Capítulo 4, Punto 4.1.6), donde se recopilan datos según la resolución No. SEPS 2022-002.
- Adherencia a los requisitos de ISO 27001 y SEPS 2022-002 (ver Capítulo 4, Punto 4.1.6.2). Este criterio se trata específicamente en la sección de Evaluación de controles implementados (Capítulo 4, Punto 4.1.6.2), donde se evalúa el cumplimiento con la resolución No. SEPS 2022-002.
- Capacidad para gestionar y mitigar riesgos de seguridad (ver Capítulo 4, Punto 4.2.2.1). Este criterio se encuentra en la sección de Definición de Criterios de evaluación (Capítulo 4, Punto 4.2.2.1), donde se establecen criterios claros y medibles para valorar el desempeño del marco de trabajo.
- Resiliencia ante posibles amenazas y vulnerabilidades (ver Capítulo 4, Punto 4.1.2.1). Este criterio también se aborda en la sección de Definición de criterios de evaluación (Capítulo 4, Punto 4.2.2.1), donde se establecen criterios claros y medibles alineados con los requisitos de las normativas aplicables.

4.2.3 Métricas utilizadas

Se especificaron las métricas que se aplicaron para cuantificar el cumplimiento del SGSI. Estas métricas abarcaron áreas como la eficacia de los controles, la identificación de vulnerabilidades y el nivel general de SI.

Métricas de evaluación que se utilizaron

- Porcentaje de cumplimiento de controles específicos. Este indicador se evaluó según los criterios establecidos en la sección de Evaluación de Controles

Implementados (Capítulo 4, Punto 4.1.6.2), donde se detalla el cumplimiento con la resolución No. SEPS 2022-002.

- Número y gravedad de vulnerabilidades identificadas Estas métricas se basan en el análisis de riesgos según MAGERIT V3.0, detallado en la sección de Identificación de Amenazas y Vulnerabilidades (Capítulo 4, Punto 4.1.5). Se considera el número y la amenaza de las vulnerabilidades identificadas en dicho análisis.
- Tiempo de respuesta ante incidentes de seguridad (ver Capítulo 4, Punto 4.1.8.1). La medición del tiempo de respuesta se llevó a cabo según el estándar internacional ISO/IEC 27004, detallado en la sección de Medición del Desempeño (Capítulo 4, Punto 4.1.8.1), específicamente en la métrica B5 sobre exposición al riesgo.
- Índice de mejora continua en comparación con evaluaciones anteriores (ver Capítulo 4, Punto 4.1.9). Este índice se desarrolla a lo largo de la Evaluación de Mejora Continua (Capítulo 4, Punto 4.1.9), que incluye la evaluación periódica, implementación de acciones correctivas, adaptación a cambios y retroalimentación de interesados.

4.2.4 Procedimientos de evaluación

En esta sección se detalló los procedimientos específicos que se siguieron durante la evaluación. Se incluyeron pasos específicos, herramientas utilizadas y la participación de los responsables de la evaluación.

Procedimientos de evaluación que se realizaron

- Revisión de la realización de pruebas de penetración en sistemas críticos (ver Capítulo 4, Punto 4.1.6.1). Esta revisión se realizó según lo detallado en la

sección de Evaluación de Controles Implementados (Capítulo 4, Punto 4.1.6.1), que incluye la recopilación de datos según la resolución No. SEPS 2022-002.

- Revisión de registros de auditoría y eventos de seguridad (ver Capítulo 4, Punto 4.1.7). La revisión de estos registros se basa en la sección de Auditoría Interna (Capítulo 4, Punto 4.1.7), donde se recopilaron datos según el estándar internacional ISO/IEC 27007 y se evaluó la efectividad de salvaguardas según ISO/IEC 27007:2020.
- Entrevistas para evaluar la conciencia de seguridad (ver Capítulo 4, Punto 4.1.4). Las entrevistas se llevaron a cabo como parte del desarrollo de indicadores de desempeño (Capítulo 4, Punto 4.1.4), específicamente en la métrica B4 sobre el compromiso de la gestión.
- Análisis de incidentes pasados y medidas correctivas implementadas (ver Capítulo 4, Punto 4.1.9.2). Este análisis forma parte de la sección de Mejora Continua (Capítulo 4, Punto 4.1.9.2), que incluye la implementación de acciones correctivas tras la evaluación periódica.

4.2.5 Frecuencia de evaluación

Se establecieron la periodicidad con la que se realizarán a cabo las valoraciones, indicando si son evaluaciones periódicas, continuas o en momentos específicos del ciclo del SGSI.

Frecuencia de evaluación que se realizaron

- Evaluaciones periódicas cada trimestre (ver Capítulo 4, Punto 4.1.9.1). Las evaluaciones periódicas se llevaron a cabo de acuerdo con la sección de Mejora Continua (Capítulo 4, Punto 4.1.9.1), donde se establece la necesidad de evaluar periódicamente el desempeño del SGSI.

- Evaluaciones continuas mediante monitoreo constante (ver Capítulo 4, Punto 4.1.6). El monitoreo constante se implementó como parte de la Evaluación de Controles Implementados (Capítulo 4, Punto 4.1.6), que incluye la recopilación continua de datos según la resolución No. SEPS 2022-002.
- Evaluaciones específicas tras cambios importantes en el entorno operativo (ver Capítulo 4, Punto 4.1.9.3). Estas evaluaciones específicas se llevaron a cabo en réplica a cambios significativos en el ambiente operativo, según lo establecido en la sección de Mejora Continua (Capítulo 4, Punto 4.1.9.3).

4.2.6 Documentación de resultados

Se describieron cómo se documentó y se registró los resultados de cada evaluación. Esto incluye informes detallados, registros de cambios implementados y cualquier hallazgo relevante durante el proceso.

Documentación de resultados que se realizaron

- Elaboración de informes detallados con hallazgos y recomendaciones (ver Capítulo 4, Punto 4.1.10.1). Los informes detallados se generaron de acuerdo con la sección de Documentación y Reporte (Capítulo 4, Punto 4.1.10.1), que especifica la necesidad de proporcionar informes detallados con hallazgos y recomendaciones.
- Registro de acciones correctivas implementadas tras cada evaluación (ver Capítulo 4, Punto 4.1.6.1). Los registros de acciones correctivas se mantuvieron conforme a la sección de Mejora Continua (Capítulo 4, Punto 4.1.6.1), donde se establece la implementación de acciones correctivas después de cada evaluación.
- Actualización de la documentación del SGSI con los resultados obtenidos (ver Capítulo 4, Punto 4.1.10.3). : La documentación del SGSI se actualizó de

acuerdo con la sección de documentación y reporte (Capítulo 4, Punto 4.1.10.3), que destaca la importancia de mantener actualizada la documentación con los resultados obtenidos.

4.2.7 Beneficios esperados

Finalmente, se identificaron los beneficios esperados de la evaluación, destacando cómo contribuyeron al fortalecimiento del SGSI y cómo se alinearon con los objetivos generales de seguridad de la cooperativa.

Beneficios esperados que se plantearon

- Mejora perenne de la postura de SI (ver Capítulo 4, Punto 4.1.9.1). Este beneficio se alinea con la sección de Mejora Continua (Capítulo 4, Punto 4.1.9.1), donde se establece la evaluación periódica y la implementación de acciones correctivas para lograr mejoras continuas.
- Alineación más efectiva con requisitos normativos (ver Capítulo 4, Punto 4.1.10.2). Este beneficio se relaciona con la sección de Documentación y Reporte (Capítulo 4, Punto 4.1.10.2), que destaca la importancia del cumplimiento normativo y la comunicación efectiva en la documentación.
- Identificación proactiva y mitigación de riesgos (ver Capítulo 4, Punto 4.1.9.3). Este beneficio se encuentra en la sección de Mejora Continua (Capítulo 4, Punto 4.1.9.3), que aborda la adaptación a cambios y la mitigación proactiva de riesgos.
- Mayor conciencia y cultura de seguridad en toda la organización (ver Capítulo 4, Punto 4.1.10.4). Este beneficio está vinculado a la sección de Documentación y Reporte (Capítulo 4, Punto 4.1.10.4), que resalta la escala de la comunicación efectiva y la mejora continua en la documentación para promover una cultura de seguridad.

Esta fase de evaluación no solo buscó identificar posibles áreas de mejora, sino también validó la efectividad del marco de trabajo propuesto en la práctica.

CAPÍTULO 5

MEDIDAS, ACCIONES Y ESTRATEGIAS PARA MEJORAR LA SI Y EL CUMPLIMIENTO NORMATIVO

En este capítulo, se describen las medidas, acciones y estrategias concretas que la cooperativa debe emprender para fortalecer la SI y cumplir con las normativas relevantes, incluyendo la Resolución No. SEPS 2022-002, MAGERIT e ISO/IEC 27002. Se detallan los pasos necesarios para abordar los riesgos que son identificados y que permiten garantizar la defensa de los activos de información.

5.1 Políticas y procedimientos actualizados

La cooperativa debe revisar y actualizar sus políticas y procedimientos de SI para garantizar que desempeñen con los requisitos de la Resolución No. SEPS 2022-002. A continuación, se detallan las acciones a seguir:

Tabla 18 *Políticas y procedimientos actualizados*

Acción	Responsable	Plazo
Revisar y actualizar las políticas de SI para cumplir con la resolución.	Equipo de Seguridad	30 días
Actualizar los procedimientos orientados con la gestión de la SI, la protección de información y datos personales y la continuidad del negocio.	Equipo de Seguridad	60 días
Establecer un mecanismo de revisión periódica de políticas y lo que son procedimientos para avalar su relevancia continua.	Responsable de SI (RSI)	Periódicamente

5.2 Formación y concienciación continua

Los programas de formación y la concienciación en SI y protección de datos son esenciales para todo el personal de la cooperativa. Se deben realizar acciones específicas para garantizar la comprensión y el compromiso. Las acciones incluyen:

Tabla 19 *Formación y concienciación continua*

Acción	Responsable	Plazo
Continuar proporcionando formación en SI y protección de datos al personal.	Departamento de Recursos Humanos	Periódicamente
Realizar campañas de concienciación periódicas sobre la importancia de la SI y la seguridad de datos.	Equipo de Seguridad	Periódicamente
Evaluar la comprensión y el cumplimiento de lo que son las políticas de SI por parte del equipo de trabajo.	Equipo de Seguridad	Anualmente

5.3 Gestión de la SI

La gestión de la SI incluye la implementación de un SGSI, la designación de un Responsable RSI y la gestión adecuada de los riesgos. Se describen las acciones clave a continuación:

Tabla 20 *Gestión de la SI*

Acción	Responsable	Plazo
Implementar un SGSI que cumpla con los estándares MAGERIT e ISO/IEC 27002.	Equipo de Seguridad	90 días
Designar un RSI o un equipo de SI para supervisar y gestionar los riesgos.	Junta Directiva	30 días

Determinar y valorar los riesgos de SI.	Equipo de Seguridad	Continuamente
Documentar y ejecutar medidas de protección de tipo técnica y organizativa para resguardar la información.	Equipo de Seguridad	120 días

5.4 Protección de datos personales

El procesamiento de información y datos personales debe cumplir con la resolución y las leyes de protección de datos. Además, si es requerido, se debe designar un DPO. Las acciones específicas son las siguientes:

Tabla 21 *Protección de datos personales*

Acción	Responsable	Plazo
Evaluar y asegurarse de que la cooperativa cumple con los requisitos de la resolución y las leyes de protección de datos que son aplicables.	Equipo de Seguridad	60 días
Establecer procedimientos claros para obtener la aprobación de los que son titulares de datos cuando sea necesario.	Equipo de Seguridad	30 días
Designar un DPO si es requerido por la resolución.	Junta Directiva	60 días
Mantener un registro de las actividades de procesamiento de lo que son datos personales.	Equipo de Seguridad	Continuamente

5.5 Auditorías y revisiones periódicas

La cooperativa debe ejecutar auditorías internas para valorar el cumplimiento de la resolución y del SGSI. Se deben documentar los resultados y llevar a cabo revisiones de seguridad. Las acciones son las siguientes:

Tabla 22 Auditorías y revisiones periódicas

Acción	Responsable	Plazo
Ejecutar auditorías internas periódicas para valorar el cumplimiento de la resolución y el SGSI.	Equipo de Auditoría Interna	Anualmente
Documentar y comunicar los resultados de las auditorías de seguridad y cumplimiento.	Equipo de Auditoría Interna	Inmediatamente después de la auditoría
Realizar revisiones de seguridad de manera regular para identificar áreas de mejora.	Equipo de Seguridad	Trimestralmente

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- **Diagnóstico del SGSI con respecto a la Resolución No. SEPS 2022-002:** El diagnóstico revela la adecuación del SGSI en relación con la Resolución No. SEPS 2022-002, proporcionando una base sólida para la mejora continua y el cumplimiento normativo.
- **Identificación de métricas de cumplimiento apoyadas en ISO/IEC 27004:2016:** La identificación de métricas basadas en ISO/IEC 27004:2016 ofrece un enfoque cuantitativo robusto, brindando una base estructurada para evaluar el desempeño del SGSI.
- **Desarrollo de un marco de trabajo basado en ISO/IEC 27007:2020, ISO/IEC 27004 y Magerit v3:** El marco de trabajo propuesto integra metodologías reconocidas, proporcionando una estructura sólida para la evaluación de la seguridad y el cumplimiento normativo.
- **Evaluación del marco con una prueba de concepto:** La prueba de concepto valida la eficacia del marco propuesto, demostrando su capacidad para incrementar o decrementar el nivel de cumplimiento del SGSI.
- **Avance positivo en SI:** El análisis del contexto inicial a la situación actual mostró un progreso positivo en la cooperativa en términos de SI. Se ha logrado una mayor concientización y capacitación del personal, una reducción significativa de amenazas, y un cumplimiento normativo más sólido.
- **Mejora sostenida:** Los índices de seguridad, como el ICF y el ICN, han experimentado mejoras sostenidas. El ICF refleja un mayor nivel de concienciación y formación, mientras que el ICN indica un cumplimiento normativo más riguroso.

- **Reducción de vulnerabilidades:** La cooperativa ha logrado reducir la cantidad y gravedad de las vulnerabilidades en equipos y software, lo que se refleja en el IVES. Sin embargo, el IESES indica que se deben tomar medidas adicionales para aumentar la certeza de las medidas de protección.
- **Necesidad de fortalecer controles de seguridad:** A pesar del avance positivo, la evaluación de riesgos muestra que existen áreas donde se pueden fortalecer los controles de seguridad. Es crucial seguir trabajando en la certeza de las medidas de seguridad y abordar las vulnerabilidades restantes.
- **Seguimiento legal:** La cooperativa ha mejorado su cumplimiento de la Resolución No. SEPS 2022-002, pero es esencial mantener un seguimiento constante de los cambios legales y regulaciones concernientes con la SI y la protección de datos.

5.2 Recomendaciones

Con base en las conclusiones anteriores, se formulan las siguientes recomendaciones:

- **Continuar con programas de capacitación:** Mantener y ampliar los programas de capacitación en SI y protección de datos. Asegurarse de que todo el personal participe activamente en estos programas.
- **Evaluación periódica de riesgos:** Al realizar valoraciones periódicas de riesgos se puede identificar y gestionar nuevas amenazas y vulnerabilidades. Esto contribuirá a una gestión continua de riesgos y una efectividad de controles óptima.
- **Mejora de certeza de medidas de seguridad:** Se necesita implementar medidas adicionales para mejorar la efectividad de los controles de seguridad, especialmente en áreas donde se han identificado vulnerabilidades. Esto incluye la revisión y actualización de políticas y procedimientos.

- **Seguimiento del cumplimiento normativo:** Continuar el proceso de seguimiento constante del cumplimiento normativo, incluyendo las normativas ISO y otras normativas relevantes. Asegurarse de que las actividades cumplan con las leyes y regulaciones.
- **Continuar con pruebas y simulacros:** Mantener la realización periódica de pruebas de continuación del negocio y simulacros de respuesta a incidentes. Esto garantiza que la cooperativa esté preparada para enfrentar situaciones de crisis.
- **Fomentar la concienciación:** Se debe promover una cultura de concienciación en SI en toda la organización. Esto incluye la comunicación constante sobre la validez de la SI y la defensa de datos.
- **Documentar incidentes de seguridad:** Asegurarse de que todos los incidentes de seguridad se documenten adecuadamente, incluyendo las acciones tomadas para abordarlos. Esto facilitará la gestión de incidentes y la mejora continua.
- **Reducción de vulnerabilidades restantes:** Abordar las vulnerabilidades restantes en equipos y software. Esto incluye la implementación de parches, actualizaciones y soluciones de seguridad, así como la mejora de políticas de gestión de activos.
- **Evaluación periódica de cumplimiento legal:** Realizar evaluaciones periódicas del cumplimiento legal para asegurarse de que la cooperativa esté cumpliendo con la Resolución No. SEPS 2022-002 y otras normativas aplicables.
- **Revisión y mejora continua:** Continuar con las revisiones periódicas del SGSI y políticas para garantizar su eficacia y relevancia. Implementar acciones correctivas y preventivas cuando se identifiquen incumplimientos o debilidades.

La comparación de la situación inicial a la situación actual es alentadora, pero es esencial mantener el impulso y la mejora continua en materia de SI. Estas recomendaciones suministran

una guía clara para fortalecer la seguridad de la cooperativa y garantizar el cumplimiento normativo en un entorno en constante evolución.

Referencias

- CERT. (2021). OCTAVE Allegro. <https://www.sei.cmu.edu/solutions/octave/>
- COIP. (2021). *defensa.gob.ec*. Registro Oficial 180. COIP: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- Cruz, B., & Chamorro, J. (2012). *Evaluación de Riesgos de los Sistemas de Información de Audioauto S.A. utilizando MAGERIT V3.0 y COBIT V4.1*. Tesis de Licenciatura, ESPE. <http://repositorio.espe.edu.ec:8080/bitstream/21000/11541/1/T-ESPE-048474.pdf>
- Cruz, M., & Fukusaki, S. (2018). *repositorio.usmp.edu.pe*. Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información : <https://repositorio.usmp.edu.pe/handle/20.500.12727/3369>
- ENISA. (2023). *Magerit*. Agencia de Ciberseguridad de la Unión Europea: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
- ESG Innova. (2023). *Indicadores más útiles para un sistema de gestión de seguridad de la información*. ISO Tools de ESG Innova: <https://www.isotools.us/2022/05/13/indicadores-mas-utiles-para-un-sistema-de-gestion-de-seguridad-de-la-informacion/>
- García, D. (2018). *repositorio.utp.edu.co*. (U. d. Pereira, Editor) Análisis y diseño del Sistema de Gestión de Seguridad de la información en la Coop. FAVI: <https://repositorio.utp.edu.co/server/api/core/bitstreams/7248f25b-8563-4f31-b7d8-94a2b69b0f25/content>
- Gómez, A. (2018). *repository.unab.edu.co*. (U. A. Bucaramanga, Editor) Diseño de una metodología para auditar la seguridad de la información en productos de software: https://repository.unab.edu.co/bitstream/handle/20.500.12749/3441/2017_Tesis_Arelis_Gomez.pdf?sequence=8

- ISACA. (2021). COBIT Framework. <https://www.isaca.org/resources/cobit>
- ISO. (2022). *iso.org/home.html*. <https://www.iso.org/home.html>
- ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements.
- ISO/IEC 27004:2016. (2016). Information technology — Security techniques — Information security management — Monitoring, measurement, analysis, and evaluation.
- ISO/IEC 27007:2020. (2020). Information technology — Security techniques — Guidelines for information security management systems auditing.
- Johnson , W. (2018). Métodos de investigación en trabajo social: cuatro paradigmas alternativos. *Oxford University Press*.
- Lucero , A., & Valverde , J. (2012). *Análisis y gestión de riesgos de los sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, utilizando la metodología MAGERIT*. Tesis de licenciatura, Universidad de Cuenca. <http://dspace.ucuenca.edu.ec/handle/123456789/1342>
- Magerit. (2023). *Sitio web oficial de Magerit*. <https://www.ccn-cert.cni.es/series/magerit.html>
- MEYSS. (2019). Guía de Análisis y Gestión de Riesgos en Seguridad de la Información (MAGERIT). *Ministerio de Empleo y Seguridad Social*. <https://www.mscbs.gob.es/sgsi/magerit>
- MINTEL. (2021). *telecomunicaciones.gob.ec*. (MINTEL, Editor) Política de ciberseguridad. Acuerdo Ministerial 006-2021: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf>
- Moya, C. (2023). *Propuesta de un plan de seguridad informático para la empresa E.P.-E.M.A.P.A.-A*. [Tesis de pregrado], Universidad Católica del Ecuador. <https://repositorio.pucesa.edu.ec/bitstream/123456789/4088/1/79247.pdf>
- NIST. (2020). NIST Cybersecurity Framework. <https://www.nist.gov/cyberframework>

- Pilla, J. (2019). *repositorio.uisek.edu.ec*. (SEK, Editor) Diseño de una política de seguridad de la información para el área de Tecnología de la Información de la Coop. de Ahorro y Crédito Chibuleo Cia. Ltda. basado en la Norma ISO IEC 27002: <https://repositorio.uisek.edu.ec/bitstream/123456789/3601/1/DISE%C3%91O%20DE%20UNA%20POL%C3%8DTICA%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20PARA%20EL%20%20C3%81REA%20DE%20TECNOLOG%C3%8DA%20DE%20LA%20INFORMACI%C3%93.pdf>
- Portal de Administración electrónica de España. (2023). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Gobierno de España: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- Registro Oficial . (2016). *gob.ec*. Ley Orgánica de la Gestión de Datos. Registro 684: <https://www.gob.ec/sites/default/files/regulations/2018-10/Ley%20Org%C3%A1nica%20de%20Gesti%C3%B3n%20de%20Identidad%20y%20Datos%20Civiles.pdf>
- Registro Oficial. (2008). <https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf>.
- <https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf>
- Resolución No. SEPS 2022-002. (2022). <https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf>
- Rozo, A. (2018). *repository.unipiloto.edu.co*. Implementación de un Sistema de Gestión de Seguridad de la Información: <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2764/Trabajo%20de%20grado2766.pdf>

- Sánchez, L. (2018). *dspace.uniandes.edu.ec*. (UNIANDES, Editor) Modelo de Gestión para el desarrollo de procesos de seguridad en la red de datos de la Coop. de Ahorro y Crédito Guaranda Cia. Ltda.: <https://dspace.uniandes.edu.ec/bitstream/123456789/581/1/TUAMEIE009-2015.pdf>
- SEPS. (2023). Sitio web de la Superintendencia de Economía Popular y Solidaria. <https://www.seps.gob.ec/>
- Tipton, H., & Krause, M. (2017). *Information Security Management Handbook*. CRC Press.
- Valverde, A. (2022). *dspace.esPOCH.edu.ec*. (ESPOCH, Editor) Auditoría de gestión a la Cooperativa de Ahorro y Crédito “Surangay” Ltda., parroquia Huambaló, periodo 2020: <http://dspace.esPOCH.edu.ec/handle/123456789/16704>
- Vicuña-Altamirano, E., & Zhindón-Mora, M. (2019). Gestión de riesgos en la infraestructura de un centro de datos. Caso de estudio: Coordinación Zonal 6 Sur del Instituto Nacional de Estadística y Censos, Ecuador. <https://dominiodelasciencias.com/ojs/index.php/es/article/view/937/pdf>
- Von Solms, R., & Van Niekerk, J. (2013). De políticas a principios: COBIT 5 y el valor de la seguridad de la información. *Informe Técnico de Seguridad de la Información*.
- Yáñez, N. (2018). *repositorio.uchile.cl*. (U. d. Chile, Editor) Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño: <https://repositorio.uchile.cl/handle/2250/147976>

Anexo 1 Diagnostico de viabilidad

Checklist de hechos encontrados en la cooperativa

Aspecto	Evidencia
Justificación Institucional	Creciente dependencia de sistemas digitales para gestionar información financiera y personal. Exposición a amenazas cibernéticas.
Justificación Metodológica	Dificultades para abordar de manera estructurada y efectiva los desafíos de seguridad. Incidentes pasados como intentos de acceso no autorizado y pérdida de datos.
Justificación Teórica	Brecha en la alineación con estándares internacionales de seguridad de la información. Falta de una metodología coherente basada en marcos reconocidos teóricamente.
Diagnóstico de Viabilidad	Evaluación de la Necesidad del SGSI: Vulnerabilidad actual destacada por incidentes previos y activos críticos. Necesidad de gestionar riesgos de seguridad.
	Análisis de Recursos Disponibles: Carencia de recursos específicos dedicados a la seguridad de la información. Necesidad de asignar personal y presupuesto.
	Identificación de Obstáculos: Resistencia al cambio y falta de conciencia sobre ciberseguridad. Obstáculos que deben superarse.
	Valoración de la Disposición de la Alta Dirección: Interés creciente en fortalecer la seguridad de la información. Apoyo reflejado en asignación de recursos y agenda estratégica.

Determinación de la Conveniencia de la Metodología: Conveniencia respaldada por alineación con necesidades, superación de obstáculos y apoyo de la alta dirección.

Falta de Métricas Ausencia de métricas definidas para evaluar y medir la eficacia del sistema de gestión de seguridad de la información.

Este checklist destaca los hechos encontrados en la cooperativa, subrayando la necesidad de implementar una metodología robusta y la falta actual de métricas para evaluar la eficacia del sistema de gestión de seguridad de la información.

Checklist

Cumplimiento con la Resolución No. SEPS 2022-002

Este checklist aborda todos los aspectos clave relacionados con el cumplimiento de la Resolución No. SEPS 2022-002 y debe ser utilizado para evaluar exhaustivamente el grado de cumplimiento de la cooperativa en cada una de estas áreas

1. Políticas y Procedimientos:

<input checked="" type="checkbox"/>	1.1 ¿La cooperativa ha establecido políticas y procedimientos documentados que cumplan con los requisitos de la Resolución No SEPS 2022-002?
<input checked="" type="checkbox"/>	1.2 ¿Los procedimientos incluyen detalles sobre la gestión de la seguridad de la información, la protección de datos personales y la continuidad del negocio?
<input checked="" type="checkbox"/>	1.3 ¿Los procedimientos se mantienen actualizados y se revisan regularmente para garantizar su relevancia?

2. Gestión de la Seguridad de la Información:

<input checked="" type="checkbox"/>	2.1 ¿La cooperativa tiene un Sistema de Gestión de Seguridad de la Información (SGSI) implementado de acuerdo con la resolución?
<input checked="" type="checkbox"/>	2.2 ¿Se ha designado a un responsable de seguridad de la información (RSI) o un equipo de seguridad?
<input checked="" type="checkbox"/>	2.3 ¿Se realiza una gestión adecuada de los riesgos de seguridad de la información, incluyendo la identificación y evaluación de riesgos?
<input checked="" type="checkbox"/>	2.4 ¿Se documentan y se implementan medidas de seguridad técnicas y organizativas para proteger la información?

3. Protección de Datos Personales:

<input checked="" type="checkbox"/>	3.1 ¿La cooperativa recopila y procesa datos personales de acuerdo con la resolución y las leyes de protección de datos aplicables?
<input checked="" type="checkbox"/>	3.2 ¿Se han establecido procedimientos para obtener el consentimiento de los titulares de datos cuando sea necesario?
<input checked="" type="checkbox"/>	3.3 ¿Existe un registro de las actividades de procesamiento de datos personales?
<input checked="" type="checkbox"/>	3.4 ¿La cooperativa tiene un oficial de protección de datos (DPO) designado si es requerido por la resolución? <i>Esto se asignó al OSI</i>

4. Continuidad del Negocio:

<input checked="" type="checkbox"/>	4.1 ¿La cooperativa ha desarrollado planes de continuidad del negocio que cumplan con los requisitos de la resolución?
<input checked="" type="checkbox"/>	4.2 ¿Se realizan pruebas periódicas de los planes de continuidad del negocio? <i>anual</i>

<input checked="" type="checkbox"/>	4.3 ¿Existe un procedimiento claro para notificar y gestionar incidentes que afecten la continuidad del negocio?
-------------------------------------	--

5. Auditorías y Revisiones:

<input checked="" type="checkbox"/>	5.1 ¿Se realizan auditorías internas periódicas para evaluar el cumplimiento de la resolución y el SGSI?
<input checked="" type="checkbox"/>	5.2 ¿Se documentan y se comunican los resultados de las auditorías de seguridad y cumplimiento?
<input checked="" type="checkbox"/>	5.3 ¿Se llevan a cabo revisiones de seguridad de manera regular para identificar áreas de mejora?

6. Formación y Concientización:

<input checked="" type="checkbox"/>	6.1 ¿La cooperativa proporciona formación en seguridad de la información y protección de datos a su personal?
<input checked="" type="checkbox"/>	6.2 ¿Se realiza una concientización periódica sobre la importancia de la seguridad de la información y la protección de datos?

7. Registro y Documentación:

<input checked="" type="checkbox"/>	7.1 ¿Se mantiene un registro completo de todas las actividades relacionadas con la seguridad de la información y el cumplimiento normativo?
<input checked="" type="checkbox"/>	7.2 ¿La cooperativa ha documentado todos los incidentes de seguridad y las acciones tomadas para abordarlos? <i>Matriz de riesgos materializados</i>
<input checked="" type="checkbox"/>	7.3 ¿Se guardan registros de consentimiento para el procesamiento de datos personales, si es aplicable?

8. Respuesta a Incidentes:

<input checked="" type="checkbox"/>	8.1 ¿Existe un plan de respuesta a incidentes que especifique los pasos a seguir en caso de una violación de seguridad?
<input checked="" type="checkbox"/>	8.2 ¿Se han establecido procedimientos para notificar a las autoridades y a los titulares de datos en caso de una brecha de datos?

9. Cumplimiento Legal:

<input checked="" type="checkbox"/>	9.1 ¿La cooperativa realiza un seguimiento regular de los cambios en la legislación y regulación relacionada con la seguridad de la información y la protección de datos?
<input checked="" type="checkbox"/>	9.2 ¿Se asegura de que todas las actividades estén en conformidad con las leyes y regulaciones aplicables?

10. Revisión y Mejora Continua:

<input checked="" type="checkbox"/>	10.1 ¿La cooperativa lleva a cabo revisiones periódicas de su SGSI y políticas para garantizar su eficacia y relevancia?
<input checked="" type="checkbox"/>	10.2 ¿Se implementan acciones correctivas y preventivas cuando se identifican incumplimientos o debilidades en el cumplimiento de la resolución?

MAGERIT Y LAS NORMAS ISO/IEC 27001, ISO/IEC 27007 E ISO/IEC 27004

El siguiente checklist se enfoca en aspectos específicos para garantizar la seguridad de la información

A. Proceso de Identificación de Activos y Riesgos:

<input checked="" type="checkbox"/>	A1. ¿Se ha realizado una identificación exhaustiva de todos los activos de información críticos para la cooperativa?
<input checked="" type="checkbox"/>	A2. ¿Los activos han sido clasificados según su importancia y valor para la organización?
<input checked="" type="checkbox"/>	A3. ¿Se han identificado las amenazas específicas que podrían afectar a estos activos?
<input checked="" type="checkbox"/>	A4. ¿Se han evaluado las vulnerabilidades en los sistemas y procesos relacionados con estos activos?
<input checked="" type="checkbox"/>	A5. ¿Se ha calculado el impacto potencial de los riesgos en términos de confidencialidad, integridad y disponibilidad?
<input checked="" type="checkbox"/>	A6. ¿Se ha evaluado la probabilidad de ocurrencia de los riesgos identificados?

B. Proceso de Implementación de Controles de Seguridad:

<input checked="" type="checkbox"/>	B1. ¿Se han implementado controles de seguridad adecuados para mitigar los riesgos identificados?
<input checked="" type="checkbox"/>	B2. ¿Se han establecido políticas y procedimientos claros para la gestión de contraseñas y la autenticación de usuarios?
<input checked="" type="checkbox"/>	B3. ¿Se han configurado y probado sistemas de firewall y antivirus para proteger la red?
<input checked="" type="checkbox"/>	B4. ¿Se realizan copias de seguridad periódicas de los datos críticos y se almacenan de forma segura?
<input checked="" type="checkbox"/>	B5. ¿Se ha implementado la autenticación de dos factores (2FA) en sistemas críticos?

C. Proceso de Auditorías y Mediciones:

<input checked="" type="checkbox"/>	C1. ¿Se han implementado controles de seguridad adecuados para mitigar los riesgos identificados? <i>B1</i>
<input checked="" type="checkbox"/>	C2. ¿Se han establecido políticas y procedimientos claros para la gestión de contraseñas y la autenticación de usuarios? <i>B2</i>
<input checked="" type="checkbox"/>	C3. ¿Se han configurado y probado sistemas de firewall y antivirus para proteger la red? <i>B3</i>
<input checked="" type="checkbox"/>	C4. ¿Se han planificado auditorías internas periódicas para evaluar la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI)?
<input checked="" type="checkbox"/>	C5. ¿Se están midiendo y monitoreando constantemente los indicadores clave de rendimiento (KPIs) relacionados con la seguridad de la información?

<input checked="" type="checkbox"/>	C6. ¿Se están registrando y documentando los resultados de auditorías y mediciones de manera adecuada? <i>solo cumplimiento del checklist 002, sin indicadores</i>
-------------------------------------	--

D. Proceso de Revisión y Mejora Continua:

<input checked="" type="checkbox"/>	D1. ¿Se realizan revisiones regulares del SGSI para identificar áreas de mejora?
<input checked="" type="checkbox"/>	D2. ¿Se documentan y se implementan acciones correctivas y preventivas en caso de incidentes de seguridad o debilidades identificadas?
<input checked="" type="checkbox"/>	D3. ¿Existen planes de continuidad del negocio y recuperación de desastres en vigor y se revisan periódicamente?
<input checked="" type="checkbox"/>	D4. ¿Se lleva a cabo una revisión y mejora continua de las políticas y procedimientos de seguridad?

E. Cumplimiento Legal y Normativo:

<input checked="" type="checkbox"/>	E1. ¿Se verifica que la cooperativa cumple con la Resolución No SEPS 2022-002 u otros requisitos legales y normativos aplicables? <i>anual</i>
<input checked="" type="checkbox"/>	E2. ¿Se implementan y mantienen medidas de protección de datos y privacidad de acuerdo con las regulaciones pertinentes?
<input checked="" type="checkbox"/>	E3. ¿Existe un registro de cumplimiento legal que documenta el seguimiento de todas las obligaciones legales y normativas? <i>papeles de trabajo</i>

F. Gestión de Incidentes y Respuesta:

<input checked="" type="checkbox"/>	F1. ¿Se cuenta con un plan de respuesta a incidentes que define los roles y responsabilidades en caso de una violación de seguridad?
<input checked="" type="checkbox"/>	F2. ¿Se han realizado simulacros de respuesta a incidentes para evaluar la efectividad del plan?
<input checked="" type="checkbox"/>	F3. ¿Existe un proceso claro para notificar y comunicar incidentes de seguridad a las partes interesadas adecuadas?

G. Gestión de Accesos y Usuarios:

<input checked="" type="checkbox"/>	G1. ¿Se realiza una gestión adecuada de los accesos de usuarios a sistemas y datos críticos?
<input checked="" type="checkbox"/>	G2. ¿Se mantienen registros de acceso y se supervisan las actividades de los usuarios de forma regular? <i>log</i>
<input checked="" type="checkbox"/>	G3. ¿Se revocan inmediatamente los derechos de acceso a usuarios que dejan la organización o no los necesitan más?

H. Formación y Concientización:

<input checked="" type="checkbox"/>	H1. ¿Se proporciona formación y concientización en seguridad de la información a todo el personal de la cooperativa? <i>anual</i>
<input checked="" type="checkbox"/>	H2. ¿Se realizan evaluaciones periódicas de la comprensión de los empleados sobre las políticas y procedimientos de seguridad? <i>anual</i>
<input checked="" type="checkbox"/>	H3. ¿Existen programas de formación específicos para usuarios con acceso a información crítica?

Checklist

Evaluación de Equipos y Software de Seguridad de la Información en la Cooperativa

Este checklist proporciona una guía detallada para evaluar equipos y software en la cooperativa desde la perspectiva de la seguridad de la información. Se debe aclarar que es importante realizar estas evaluaciones de forma regular y tomar medidas correctivas cuando sea necesario para mantener un entorno seguro.

Equipos:

1. Evaluación de Hardware:

<input checked="" type="checkbox"/>	1.1 ¿Todos los equipos de la cooperativa tienen hardware actualizado y en buen estado?
<input checked="" type="checkbox"/>	1.2 ¿Los equipos están protegidos contra el acceso no autorizado físico?
<input checked="" type="checkbox"/>	1.3 ¿Se realizan inventarios periódicos de hardware para verificar su ubicación y estado?

2. Evaluación de Software:

<input checked="" type="checkbox"/>	2.1 ¿Se utiliza software legítimo y con licencia en todos los equipos de la cooperativa?
<input checked="" type="checkbox"/>	2.2 ¿Se aplican parches y actualizaciones de seguridad de forma regular en todos los sistemas y aplicaciones?
<input checked="" type="checkbox"/>	2.3 ¿Se lleva un registro de los programas y aplicaciones instalados en cada equipo?

3. Evaluación de Configuración:

<input checked="" type="checkbox"/>	3.1 ¿Los equipos están configurados de acuerdo con las políticas de seguridad de la cooperativa?
<input checked="" type="checkbox"/>	3.2 ¿Se han desactivado servicios innecesarios en los equipos para reducir la superficie de ataque?
<input checked="" type="checkbox"/>	3.3 ¿Se han aplicado configuraciones de seguridad recomendadas para sistemas operativos y aplicaciones?

4. Protección contra Malware:

<input checked="" type="checkbox"/>	4.1 ¿Se han instalado y configurado soluciones antivirus en todos los equipos?
<input checked="" type="checkbox"/>	4.2 ¿Los equipos cuentan con protección en tiempo real contra malware y ransomware?
<input checked="" type="checkbox"/>	4.3 ¿Se realizan análisis de malware de manera regular en todos los sistemas?

5. Acceso a los Equipos:

<input checked="" type="checkbox"/>	5.1 ¿Se implementa una política de acceso de usuario mínimo privilegio en los equipos?
<input checked="" type="checkbox"/>	5.2 ¿Se utilizan contraseñas fuertes y se requiere autenticación de dos factores (2FA) cuando sea posible?
<input checked="" type="checkbox"/>	5.3 ¿Se bloquean automáticamente los equipos después de un período de inactividad?

Software de Seguridad:**6. Cortafuegos (Firewall):**

<input checked="" type="checkbox"/>	6.1 ¿La cooperativa utiliza un firewall para proteger su red y sus sistemas?
<input checked="" type="checkbox"/>	6.2 ¿El firewall está configurado para bloquear tráfico no autorizado y aplicaciones maliciosas?
<input checked="" type="checkbox"/>	6.3 ¿Se registran y revisan regularmente los registros de firewall para identificar actividades sospechosas? <i>log</i>

7. Herramientas de Monitoreo de Seguridad:

<input checked="" type="checkbox"/>	7.1 ¿Se utilizan herramientas de monitoreo de seguridad para detectar posibles amenazas y brechas?
<input checked="" type="checkbox"/>	7.2 ¿Las herramientas de monitoreo generan alertas automáticas cuando se detectan incidentes de seguridad?
<input checked="" type="checkbox"/>	7.3 ¿Se revisan y analizan los registros de monitoreo de seguridad de forma periódica?

8. Software de Copias de Seguridad:

<input checked="" type="checkbox"/>	8.1 ¿La cooperativa cuenta con software de copias de seguridad para respaldar datos críticos?
<input checked="" type="checkbox"/>	8.2 ¿Las copias de seguridad se realizan de forma programada y se almacenan de manera segura?
<input checked="" type="checkbox"/>	8.3 ¿Se han probado los procedimientos de restauración de datos para garantizar su efectividad?

9. Software de Autenticación y Gestión de Identidades:

<input checked="" type="checkbox"/>	9.1 ¿Se utiliza software de autenticación sólida, como autenticación de dos factores (2FA), para proteger el acceso a sistemas críticos?
<input checked="" type="checkbox"/>	9.2 ¿Se gestiona de manera centralizada la identidad y el acceso de los usuarios a través de un software de gestión de identidades?
<input checked="" type="checkbox"/>	9.3 ¿Se revocan automáticamente los derechos de acceso cuando un empleado deja la organización?

10. Software de Encriptación:

<input checked="" type="checkbox"/>	10.1 ¿Se utiliza software de encriptación para proteger datos sensibles tanto en reposo como en tránsito?
<input checked="" type="checkbox"/>	10.2 ¿Los correos electrónicos y comunicaciones sensibles se cifran de forma automática?
<input checked="" type="checkbox"/>	10.3 ¿Se ha implementado encriptación de disco completo en dispositivos móviles y portátiles?