# UNIVERSIDAD TÉCNICA DEL NORTE

## FACULTAD DE POSGRADO

## PROGRAMA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

### TRABAJO DE INTEGRACIÓN CURRICULAR

**TEMA:**

"GUÍA PARA EL ANÁLISIS DE GESTIÓN DE RIESGOS TECNOLÓGICOS DEL CORE FINANCIERO COMO INSUMO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO DEL SEGMENTO 2 Y 3"

Trabajo de titulación previo a la obtención del título en Magíster en Computación con Mención en Seguridad Informática

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


**AUTOR:**

Jorge Enrique Morán Andrade

**DIRECTOR:**

MSc. Xavier Mauricio Rea Peñafiel


**Ibarra – Ecuador 2026**

**APROBACIÓN DEL DIRECTOR**

Yo, Msc. Mauricio Rea, certifico que el maestrante Morán Andrade Jorge Enrique, con cédula N.º 1002825956 ha elaborado bajo mi tutoría la sustentación del Trabajo de Grado titulado: "Guía para el análisis de gestión de riesgos tecnológicos del Core financiero como insumo del sistema de gestión de seguridad de la información para una cooperativa de ahorro y crédito del segmento 2 y 3"

Este trabajo se sujeta a las normas y metodologías dispuestas en los Reglamentos de Titulación a obtener; por lo tanto, autorizo la presentación sustentación para la calificación respectiva.

Ibarra, a los 27 días del mes de agosto de 2026




Director: MSc. Xavier Mauricio Rea Peñafiel

Desarrollo, aplicación de Software y Cyber Security (Seguridad Cibernética)

**DEDICATORIA**

Va dedicado a mi madre, que con su constante apoyo ha estado pendiente de que culmine este logro académico, a mi padre que desde el cielo ha sido guía y fortaleza para cumplir este objetivo, a mis hermanos y mi amigo Julio quienes han estado pendiente de este objetivo.

Jorge Enrique Morán Andrade

Maestrante

**AGRADECIMIENTOS**

A mi madre Eugenia Andrade por su apoyo incondicional, mi padre Jorge Morán que desde el cielo siempre está pendiente y dando su bendición, mis hermanos, amigos y familia, que ha aportado en poder culminar esta etapa importante en mi vida.

Jorge Enrique Morán Andrade

Maestrante

# UNIVERSIDAD TÉCNICA DEL NORTE
## DIRECCIÓN DE BIBLIOTECA

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

### 1. IDENTIFICACIÓN DE LA OBRA

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

| DATOS DE CONTACTO | |
|---|---|
| **APELLIDOS Y NOMBRES:** | Morán Andrade Jorge Enrique |

| DATOS DE LA OBRA | |
|---|---|
| **TÍTULO:** | GUÍA PARA EL ANÁLISIS DE GESTIÓN DE RIESGOS TECNOLÓGICOS DEL CORE FINANCIERO COMO INSUMO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO DEL SEGMENTO 2 Y 3 |
| **AUTOR (ES):** | Morán Andrade Jorge Enrique |
| **FECHA: DD/MM/AAAA** | 27/08/2026 |
| SOLO PARA TRABAJOS DE GRADO | |
| **PROGRAMA:** | ☐ **PREGRADO** ■ **POSGRADO** |
| **TITULO POR EL QUE OPTA:** | Magíster en Computación con Mención en Seguridad Informática |
| **DIRECTOR /ASESOR:** | Msc. Mauricio Rea / Msc. Rolando Aguilar |

### 2. CONSTANCIAS

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

Ibarra, a los 27 días del mes de Agosto de 2026

**EL AUTOR:**

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE ENRIQUE MORAN ANDRADE

Nombre: Morán Andrade Jorge Enrique

**RESUMEN**

La investigación soluciona la vulnerabilidad ante amenazas cibernéticas en el sector financiero cooperativo ; el objetivo general propone una guía para el análisis de gestión de riesgos tecnológicos del Core financiero como insumo del Sistema de Gestión de Seguridad de la Información (SGSI) en cooperativas de ahorro y crédito de segmentos 2 y 3. El método aplica un diseño exploratorio-descriptivo mixto ; ejecuta la metodología MAGERIT v.3 en fases de catalogación de activos, valoración de amenazas, evaluación de salvaguardas y estimación de riesgo residual. Se utilizan encuestas y listas de control para el diagnóstico de infraestructura tecnológica; los resultados configuran un marco de trabajo adaptado a la resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002, ISO/IEC 27001:2024 e ISO/IEC 27003:2017. El estudio aporta una guía validada mediante prueba de concepto; genera el Mapa de Riesgos, la Declaración de Aplicabilidad y el Plan de Tratamiento. Se concluye que el instrumento permite anticipar incidentes, establecer controles de seguridad y asegurar la continuidad operativa.

***Palabras clave:*** *Gestión de Riesgos, SGSI, MAGERIT v.3, Core Financiero, Seguridad de la Información.*

**ABSTRACT**

This study develops a guide for risk management analysis of the Core Financial System as a fundamental input for the Information Security Management System (ISMS) in Credit Unions (CU) specifically within Segment 2. A framework has been designed based on internationally recognized standards and regulations, such as MAGERIT v.3 [1]The primary goal is to develop an ISMS that complies with SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 regulations, utilizing the MAGERIT v.3 [2] risk methodology and based on ISO/IEC 27003:2017 and ISO/IEC 27001:2024-02 standards. The specific objectives include conducting a comprehensive risk analysis on the technological services of the financial core of Segment 2 CU using the MAGERIT v.3 methodology[3], creating guidelines and documentation in accordance with SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 regulations, and developing an information security policy aligned with ISO/IEC 27001:2024-02. From a methodological perspective, an initial ISMS diagnosis is conducted, compliance metrics are identified, and an evaluation framework is established. This framework will be evaluated through proof of concept and analysis of the results obtained.

***Keywords:*** *Security, Information, System, Management, Savings and Credit Cooperatives, Regulations, Evaluation, Risk Management, Core Financial System, Information Security, ISMS, SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002.*

**CONTENIDO**

APROBACIÓN DEL DIRECTOR ..... 1

DEDICATORIA ..... 2

AGRADECIMIENTOS ..... 3

CONSTANCIA ..... 4

RESUMEN ..... 5

ABSTRACT ..... 7

INDICE DE TABLAS ..... 12

INDICE DE FIGURAS ..... 13

1. CAPÍTULO I ..... 15

1.1. El Problema ..... 15

1.1.1. Planteamiento del problema ..... 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 ..... 17

1.4. Justificación ..... 17

1.4.1. Justificación institucional ..... 17

1.4.2. Justificación metodológica ..... 17

1.4.3. Justificación teórica ..... 18

2. CAPITULO II ..... 19

2.1. Marco Referencial ..... 19

2.1.1. Antecedentes ..... 19

2.2. Marco Teórico ..... 21

2.2.1. Guía ISO/IEC 27001:2024-02 – Requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) ..... 22

2.2.2. Beneficios de la ISO/IEC 27001:2024-02 ..... 22

2.2.3. Guía ISO/IEC 27007:2022 - Pautas para auditorías de SGSI.....23
2.2.4. Beneficios de la ISO/IEC 27007:2020 .....23
2.2.5. Norma ISO/IEC 27004:2016 - Medición y métricas de Seguridad de la Información .....23
2.3. Metodologías de Evaluación de Seguridad.....23
2.4. Sistemas de Información en Cooperativas de Ahorro y Crédito.....26
2.5. Importancia de las TIC para la Gestión Empresarial .....26
2.5.1. Ley Orgánica de Economía Popular y Solidaria (LOEPS).....26
2.5.2. Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) 27
2.5.3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos ...27
2.5.4. Normativa del Banco Central del Ecuador (BCE).....27
2.5.5. NTE INEN-ISO/IEC 27000.....27
2.5.6. NTE INEN-ISO/IEC 27002:2013.....27
2.5.7. NTE INEN-ISO/IEC 27005: 2022.....28
2.5.8. NTE INEN-ISO/IEC 27032:2023.....28
2.5.9. Marco legal específico para las Cooperativas de Ahorro y Crédito (CAC) en Ecuador.....29
2.5.10. Roles de la SEPS .....29
3. CAPITULO III.....31
3.1. Marco Metodológico.....31
3.2. Descripción del Área de Estudio / Descripción del Grupo de Estudio. .....31
3.2.1. Evaluación de la necesidad del SGSI .....32
3.2.2. Análisis de recursos disponibles.....32
3.3. Enfoque y Tipo de Investigación .....32
3.4. Procedimiento de Análisis de Riesgos.....33
3.4.1. Paso 1: Activos. Identificación de activos.....33
3.4.2. Paso 2: Amenazas. Identificación de amenazas y vulnerabilidades .....36

3.4.3. Determinación del riesgo potencial .....41
3.4.4. Paso 3: Salvaguardas .....45
3.4.5. Paso 4: Impacto residual .....52
3.4.6. Paso 5: riesgo residual .....53
3.5. Método de Formalización de Actividades .....54
3.5.1. Método de Análisis de Riesgos (MAR) 1: Caracterización de los activos ...54
3.5.2. Método de Análisis de Riesgos (MAR) 2: Caracterización de las amenazas 55
3.5.3. Método de Análisis de Riesgos (MAR) 3: Caracterización de las salvaguardas 56
3.5.4. Método de Análisis de Riesgos (MAR) 4: Estimación del estado de riesgo 57
3.6. Documentación .....58
3.6.1. Documentación intermedia .....58
3.6.2. Documentación final .....59
3.7. Lista de Control .....61
3.8. Incorporación de Normativas al Marco Propuesto .....61
4. CAPITULO IV .....63
4.1. Guía 63
4.1.1. Introducción y Propósito .....63
4.1.2. Alcance y Marco Normativo .....64
4.1.3. Fase 1: Inventario y Valoración de Activos .....64
4.1.4. Fase 2: Identificación y Valoración de Amenazas .....65
4.1.5. Fase 3: Evaluación de Salvaguardas Existentes .....66
4.1.6. Fase 4: Estimación del Estado de Riesgo .....67
4.1.7. Fase 5: Riesgo Residual y Plan de Tratamiento .....68
4.1.8. Resultados del Diagnóstico Organizacional .....69
4.1.9. Productos de Salida del Análisis de Riesgos .....85
4.2. Hallazgos en la Provincia de Pichincha .....86

4.2.1. Análisis de la Situación Actual ..... 86
4.2.2. Resultados y Decisiones del Estudio ..... 87
4.2.3. Problemas Comunes y Necesidades ..... 87
4.2.4. Validaciones y Conclusiones del Diagnóstico ..... 88
4.2.5. Entregables Formales del Análisis ..... 89
4.3. Documentación del Análisis de Riesgos con Técnicas MAGERIT: Recomendaciones para la guía de esta tesis ..... 90
4.3.1. Principios Generales para la Documentación del Análisis de Riesgos ..... 90
4.3.2. Documentación de la Fase de Inventario y Valoración de Activos ..... 91
4.3.3. Documentación del Mapa de Riesgos y la Evaluación de Amenazas ..... 92
4.3.4. Documentación de la Evaluación de Salvaguardas y del Informe de Insuficiencias ..... 93
4.3.5. Documentación del Estado de Riesgo Residual y del Plan de Tratamiento ..... 94
5. REFERENCIAS BIBLIOGRÁFICAS ..... 99

**INDICE DE TABLAS**

Tabla I Degradación de Valor. ..... 38

Tabla II Pobabilidad de Ocurrencia. ..... 38

Tabla III Tipos de salvaguardas. ..... 50

Tabla IV Eficacia y madurez de las salvaguardas Fuente: Magerit V.3 ..... 51

Tabla V Lista de control. Fuente: Magerit V.3[1] ..... 61

Tabla VI Tabla de trazabilidad objetivos ..... 95

**INDICE DE FIGURAS**

Fig. 1. Flujo de la metodología Magerit v.3 Fuente: Magerit v.3 [1] ..... 24

Fig. 2. Normas Técnicas ISO 2022. Fuente: ISO, 2023[23] ..... 28

Fig. 3. Elementos del análisis de riesgos potenciales ..... 31

Fig. 4. Coste de la [interrupción de la] disponibilidad. Fuente: [1] ..... 36

Fig. 5. El riesgo en función del impacto y la probabilidad. Fuente: [1] ..... 42

Fig. 6. Elementos de análisis del riesgo residual ..... 47

Fig. 7. Método de Análisis de Riesgos (MAR) Fuente: Magerit V.3[1] ..... 54

Fig. 8. Segmento al que pertenece la cooperativa ..... 69

Fig. 9. Segmento al que pertenece la cooperativa ..... 70

Fig. 10. Años de experiencia en el cargo ..... 71

Fig. 11. Líder de la función de Administración del Análisis de Riesgos de TI en la Cooperativa ..... 71

Fig. 12. Cooperativa con un Marco de Gobernanza de la Información aprobado por la Alta Dirección ..... 72

Fig. 13. Cooperativa cuenta actualmente con un Sistema de Gestión de Seguridad de la Información (SGSI) implementado ..... 73

Fig. 14. Elementos gobernanza de la información ..... 74

Fig. 15. Análisis de riesgos en 24 meses ..... 75

Fig. 16. Frecuencia análisis de riesgos ..... 75

Fig. 17. Metodologías de análisis de riesgos ..... 76

Fig. 18. Existencia de documento de política de seguridad de la información. 77

Fig. 19. Razones desuso de análisis de riesgos ..... 78

Fig. 20. Evaluación de conocimientos, recursos, metodologías aplicables, y claridad normativa SEPS 2022-002 ..... 79

Fig. 21. Necesidad percibida de una guía metodológica ..... 80

Fig. 22. Modo de análisis de riesgos de TI formal en las cooperativas ..... 80

Fig. 23. Frecuencia de análisis de riesgos de TI formal en las cooperativas .... 81

Fig. 24. Evaluación de necesidad de guía, base en Magerit V.3, adaptación al sector corporativo y disposición de adoptar guía metodológica..... 82

Fig. 25. Dificultades concretas ha enfrentado la cooperativa al intentar gestionar riesgos tecnológicos..... 83

Fig. 26. Incidentes y exposición ..... 83

Fig. 27. Tipo de incidente ..... 84

Fig. 28. Comentarios o sugerencias sobre la gestión de riesgos tecnológicos. 85

# 1. CAPÍTULO I

## 1.1. El Problema

### 1.1.1. Planteamiento del problema

La Superintendencia de Economía Popular y Solidaria (SEPS), entidad que regula el sector financiero cooperativo en Ecuador, ha dictado pautas de seguridad de la información que las Cooperativas de Ahorro y Crédito (CAC) de todos los segmentos deben acatar de forma obligatoria [4]. Dentro de esas pautas, la SEPS pide poner en marcha un Sistema de Gestión de Seguridad de la Información (SGSI); este se vuelve la base principal para cuidar la información en el sector financiero cooperativo [4].

Amenazas y ataques cibernéticos:

El sector financiero es un blanco principal para los ciberdelincuentes, dado el gran número de datos delicados y operaciones que maneja; peligros como el malware, el phishing, el ransomware y los ataques DDoS intentan entrar sin permiso, robar información o frenar la operación [1].

Cumplimiento normativo y regulatorio:

El sector financiero debe seguir reglas como la Ley de Protección de Datos Personales, las normas propias del rubro y los estándares de orden mundial; cumplir todos esos marcos a la vez resulta un reto para las organizaciones [1].

Gestión de riesgos:

El manejo de riesgos es vital en el sector financiero; hallar y medir los riesgos de seguridad, tanto los de dentro como los de fuera, es el paso previo para fijar controles y decidir qué se va a aplicar [2].

El manejo de los riesgos tecnológicos, eje central del SGSI, deja hallar, medir y reducir las amenazas antes de que lleguen a ocurrir.

Al manejar los riesgos tecnológicos, las organizaciones logran prever y bajar la posibilidad de que ocurran hechos de seguridad; así cuidan tanto sus activos como su buen nombre en el medio [1]. Este trabajo supone medir de forma continua las debilidades y

las amenazas que podrían surgir; entre ellas están las fallas técnicas, los errores humanos, los hechos naturales y los ataques informáticos.

Un buen manejo de los riesgos tecnológicos da medidas que nutren el SGSI; esto permite contar con controles de seguridad más sólidos y asegura que se cumplan las normas y los estándares mundiales [2]. Actuar de forma anticipada en el manejo de riesgos ayuda, asimismo, a usar mejor los recursos; para ello se da prioridad a las áreas que quedan más expuestas al riesgo.

## 1.2. Interrogantes de la Investigación

Las preguntas asociadas a la presente investigación se relacionan con cada uno de los objetivos específicos, teniendo el siguiente resultado:

P1. ¿Cuáles son las funciones y características principales que emplea la metodología Magerit V3 para la evaluación de riesgos de tecnología de la información enfocados en sector financiero de Cooperativas de Ahorro y Crédito del segmento 2 y 3?

P2. ¿Cuáles son las principales vulnerabilidades de Seguridad de la Información en los servicios tecnológicos de una Cooperativa de Ahorro y Crédito del Segmento 2 y 3?

P3. ¿Existe una guía para evaluar y administrar los riesgos Tecnológicos que se generan en los activos de información del Core Financiero en una Cooperativa de Ahorro y Crédito del Segmento 2 y 3?

P4. ¿Cuáles son los resultados obtenidos al aplicar la guía de análisis de riesgos tecnológicos utilizando la metodología MAGERIT en el Core Financiero en una Cooperativa de Ahorro y Crédito de segmento 2 o 3?

## 1.3. Objetivos de la Investigación

### 1.3.1. Objetivo general

Proponer una guía para el análisis de gestión de riesgos tecnológicos del Core financiero como insumo del Sistema de Gestión de Seguridad de la Información para una cooperativa de ahorro y crédito del segmento 2 y 3.

### 1.3.2. Objetivos específicos

1. Detallar las funciones y características principales para la aplicación de la Metodología MAGERIT v3 en Cooperativas de Ahorro y Crédito del segmento 2 y 3.
2. Identificar las principales vulnerabilidades de Seguridad de la Información para una Cooperativa de Ahorro y Crédito del segmento 2 y 3 alineadas al cumplimiento de la Normativa de la SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002.
3. Elaborar una Guía para el Análisis de gestión de riesgos tecnológicos del Core Financiero como insumo del Sistema de Gestión de Seguridad de la Información para una Cooperativa de Ahorro y Crédito del Segmento 2 y 3.
4. Evaluar la guía elaborada mediante su aplicación en un caso práctico.

## 1.4. Justificación

### 1.4.1. Justificación institucional

Según [4] en el sector cooperativo de ahorro y crédito en Ecuador, realizar un análisis de riesgos es fundamental para asegurar la protección de la información financiera y personal de los socios [3]. Este sector maneja datos sensibles y transacciones económicas que, si llegan a ser comprometidos, afectarían la seguridad financiera y la confianza de los socios. Para establecer una adecuada metodología que se alinea a las normas de la SEPS se propone el uso de una rigurosa y exhaustiva identificación de riesgos y activos críticos a través de la metodología MAGERIT V.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) la cual permite, además, identificar sistemas de gestión de datos, plataformas digitales y bases de información; evaluando y destacando sus vulnerabilidades según su prioridad para la “Organización”. En este caso de las Cooperativas de Ahorro y Crédito (CAC).

### 1.4.2. Justificación metodológica

El diseño y desarrollo de esta guía encuentran su sustento metodológico en la aplicación rigurosa de MAGERIT V.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), un marco de trabajo de referencia internacional que destaca por su enfoque sistemático y adaptabilidad. Las cooperativas a menudo enfrentan

limitaciones de recursos técnicos y financieros, lo que hace inviable la adopción de metodologías excesivamente complejas o abstractas. MAGERIT V.3 proporciona la estructura metodológica adecuada, al desglosar el proceso en componentes sumamente claros y digeribles: la identificación y valorización de los activos del Core financiero (software, bases de datos, infraestructura), el análisis cualitativo o cuantitativo de las amenazas que los acechan, y la evaluación de las salvaguardas existentes para determinar el impacto real y el riesgo residual. Al utilizar las técnicas y el catálogo de elementos de MAGERIT, la guía se convierte en una herramienta práctica que traduce la complejidad técnica del Core financiero a matrices de riesgo claras, facilitando un camino lógico y estructurado permitiendo a los gestores de riegos puedan diseñar planes de tratamiento efectivos y realistas para la realidad cooperativa.

### 1.4.3. Justificación teórica

El análisis de riesgos es la base indispensable sobre la cual se construye un Sistema de Gestión de Seguridad de la Información (SGSI). Teóricamente, es imposible proteger un entorno tecnológico si primero no se conocen el valor de sus activos y la probabilidad de que sus vulnerabilidades sean explotadas. Esta investigación se justifica teóricamente al evaluar la relación de dependencia entre el Core financiero y la triada fundamental de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad (CID). Al identificar el análisis de riesgos como el "insumo primario", esta investigación se hace necesaria ya que abarca el conocimiento sobre la gobernanza de TI en el sector popular y solidario. Permitiendo una coyuntura conceptual que conecta las teorías generales de la gestión de riesgos tecnológicos con la práctica específica del cooperativismo de ahorro y crédito, evidenciando cómo los modelos algorítmicos y cualitativos de MAGERIT V.3 dan la base científica necesaria para la formulación de políticas de seguridad, controles de acceso y planes de continuidad del negocio que den soporte al SGSI de manera sostenible en el tiempo.

# 2. CAPITULO II

## 2.1. Marco Referencial

### 2.1.1. Antecedentes

Hoy la protección de la información llega a ser una base clave dentro de cualquier empresa del país; cuidarla obliga a seguir los mejores métodos y normas reconocidas a nivel mundial [9]. Sobre todo, el sector financiero defiende mucho esas normas; en ella se encuentran los bancos, las cooperativas de ahorro y crédito, las mutualistas, debido a la sensible información y datos que gestionan dichas entidades; por eso, ha sido uno de los primeros sectores en guiar y poner en marcha el cuidado de la seguridad de la información en las organizaciones [10].

En Ecuador, las cooperativas de ahorro y crédito están bajo el control de la Superintendencia de Economía Popular y Solidaria (SEPS)[5]. Este organismo cumple un papel fundamental: marca las pautas y vigila a las cooperativas que prestan servicios financieros, con el fin de lograr un buen manejo de los fondos de socios y clientes. Asimismo, la SEPS cuida la claridad y la firmeza del sistema financiero popular y solidario; de este modo protege tanto los derechos de los socios como la continuidad de las entidades reguladas [3].

Según las investigaciones de Rodríguez Guerra (2019) [6] ya hay modelos y métodos para poner en marcha un SGSI; sin embargo, estos no se ajustan al contexto ecuatoriano según las normas de la SEPS o la Superintendencia de Bancos (SB), y tampoco cubren todos los frentes de trabajo en la seguridad de la información ni el uso de controles de seguridad informática [4]. Junto a ello, dichos modelos no se han creado pensando en cumplir la norma que el organismo de control fijó mediante la resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.

La normativa ecuatoriana SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 marca un avance fundamental para la inclusión de un sistema de gestión de la seguridad de la información (SGSI) en las entidades del sector financiero popular y solidario; además, fija establece directrices que impulsan la protección y confidencialidad de la información dentro de sus operaciones [11]. Frente a ataques informáticos cada vez más difíciles, la norma establece aplicar controles de seguridad y

manejar los riesgos de forma ordenada. Contar con un SGSI permite identificar, evaluar y mitigar vulnerabilidades asegurando la integridad, disponibilidad y confidencialidad de la información[5]. Este marco regulatorio destaca la importancia de desarrollar políticas internas de seguridad que incluyan protocolos de acceso, resguardo de la información sensible, y estrategias de respuesta ante incidentes de seguridad.

Uno de los aspectos relevantes de la normativa es su enfoque en la administración de riesgos, considerado un elemento esencial para el funcionamiento adecuado de un SGSI. La administración de riesgos representa un proceso continuo de identificación y evaluación de amenazas que podrían afectar los activos de información, así como la implementación de controles para mitigar estos riesgos [12]. También señala que cada entidad debe tener un plan de gestión de riesgos actualizado y ajustado a las necesidades y recursos que dispone la organización. Dicho plan tiene que ir acorde con los mejores métodos y normas mundiales; tal es el caso de la norma ISO/IEC 27001[7], la cual fija los requisitos de un SGSI y abarca puntos clave de la seguridad de la información; estos van desde hallar los riesgos hasta poner en práctica políticas de control de acceso y auditorías de seguridad[7].

La normativa resalta la necesidad de crear una cultura organizacional que valore y promueva la seguridad en todos los niveles de las entidades Financieras y las relacionadas con el sector. Así como también considera que el personal debe recibir capacitación continua sobre los protocolos de seguridad [8] con el fin de garantizar que todos comprendan sus responsabilidades en la protección de la información. Además, la normativa sugiere la implementación de tecnologías avanzadas que permitan detectar y responder de manera oportuna a cualquier incidente de seguridad, como herramientas de monitoreo continuo, sistemas de detección de intrusos y soluciones de cifrado de datos [8]. Esto es particularmente importante en el sector financiero popular y solidario, donde las entidades manejan datos sensibles de sus clientes y deben garantizar que dicha información no sea accesible a personas no autorizadas.

En resumen, la norma se enfoca en cuidar los datos y los sistemas de información de las entidades financieras; y, fortalecer la confianza de los usuarios en el sector financiero popular y solidario [8]. Al impulsar una cultura de seguridad y fijar una forma activa de manejar los riesgos, esta regulación logra que las entidades ganen más capacidad

de respuesta ante las amenazas de hoy y futuras; de esta manera asegura un entorno firme y confiable para sus operaciones y sus usuarios[8].

## 2.2. Marco Teórico

El marco teórico fundamenta el entendimiento de la Seguridad de la Información y su aplicación en las CAC. En lo referente a la Seguridad de la Información, este entendimiento resulta clave para enfrentar de manera adecuada y resiliente los retos y las amenazas que viven las organizaciones.

La información segura es un concepto central en cualquier empresa u organización actual. Según Tipton y Krause (2017)[9], alude al resguardo de los distintos tipos de activos de información frente a un acceso no autorizado, así como ante la divulgación de a información, la interrupción o su destrucción. Este resguardo se apoya en tres bases principales, llamadas el triángulo de la información segura: confidencialidad, integridad y disponibilidad [9]. Primero, la confidencialidad se logra al dar acceso a la información solo a quienes tienen permiso. Segundo, la integridad asegura que los datos o la información no sean cambiados por personas no autorizadas. Tercero, la disponibilidad que la información sea accesible cuando se la requiera; como resultado, se mejora el manejo de riesgos [9]. Estos principios son básicos para cuidar los datos de los clientes y mantener la integridad de las operaciones en una cooperativa de ahorro y crédito.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es una estructura dentro de una organización que reúne políticas, procesos, procedimientos y recursos pensados para manejar la seguridad de la información de forma efectiva [8]. Poner en marcha un SGSI en una cooperativa de ahorro y crédito trae varios beneficios. Según Von Solms y Van Niekerk (2013)[10], entre estos beneficios sobresalen la baja de riesgos, la mayor eficiencia en las operaciones y el cumplimiento de los requisitos legales y de regulación. La guía ISO/IEC 27001[7], dentro del SGSI, fija elementos clave como definir una política de seguridad, manejar los riesgos y responder a los incidentes. Esta norma brinda un marco firme para implementar y mantener la seguridad de la información en cualquier tipo de organización [7][8].

### 2.2.1. Guía ISO/IEC 27001:2024-02 – Requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI)

La guía ISO/IEC 27001:2024-02[7] es uno de los estándares mundiales más reconocidos en el campo de la seguridad de la información. Este estándar fija los requisitos básicos para implementar y mantener un SGSI. Brinda un enfoque ordenado y sistemático que ayuda a las organizaciones a manejar los riesgos de seguridad de la información; este parte de hallarlos y medirlos [7][8]:

Política de Seguridad de la Información (SI): la norma requiere que las organizaciones fijen una política de Seguridad de la Información que muestre su compromiso con el cuidado de los activos de información (AI) y con el cumplimiento de las leyes y reglas que apliquen [4].

Evaluación de riesgos: se espera que las organizaciones midan los riesgos para hallar y entender las amenazas y debilidades que puedan poner en peligro la seguridad de la información.

Tratamiento de riesgos: cuando los riesgos ya están hallados, las organizaciones deben decidir cómo encararlos; pueden aplicar controles de seguridad, aceptar el riesgo o pasarlo a terceros.

Implementación de controles: la norma brinda varios controles que las organizaciones pueden usar para reducir los riesgos. Estos controles van desde el manejo de accesos hasta la seguridad física y la respuesta a los incidentes.

Revisión y mejora continua: se pide que las organizaciones revisen y mejoren de forma constante su SGSI para que siga siendo efectivo con el paso del tiempo.

### 2.2.2. Beneficios de la ISO/IEC 27001:2024-02

Mejora en la seguridad: ayuda a las organizaciones a reforzar sus prácticas de seguridad de la información y a bajar la posibilidad de que ocurran incidentes.

Cumplimiento legal: facilita acatar los requisitos legales y de regulación ligados a la seguridad de la información.

Confianza de los Stakeholders: eleva la confianza de los clientes y de otras partes interesadas al mostrar un compromiso firme con la seguridad de la información.

Gestión eficaz de riesgos: brinda un marco firme para manejar los riesgos de seguridad de la información.

#### 2.2.3. Guía ISO/IEC 27007:2022 - Pautas para auditorías de SGSI

La guía ISO/IEC 27007:2022 brinda pautas para hacer auditorías efectivas a los Sistemas de Gestión de Seguridad de la Información (SGSI). Esta norma es clave para asegurar que un SGSI funcione conforme a los requisitos de la ISO/IEC 27001[7] y para garantizar que cumpla con los estándares fijados.

#### 2.2.4. Beneficios de la ISO/IEC 27007:2020

a. Mejora de la efectividad de las auditorías: ayuda a lograr que las auditorías de SGSI sean más efectivas y eficientes [11].

b. Cumplimiento normativo: aporta al cumplimiento constante de los requisitos de la ISO/IEC 27001[7] y otras regulaciones aplicables [11].

c. Gestión continua de incidentes: facilita hallar y reducir los riesgos de seguridad de la información por medio de auditorías periódicas[11].

#### 2.2.5. Norma ISO/IEC 27004:2016 - Medición y métricas de Seguridad de la Información

La norma ISO/IEC 27004:2016 se enfoca en dar guía sobre cómo medir y evaluar el desempeño de un SGSI y de sus controles. Resulta básica para asegurar que un SGSI cumpla sus objetivos y que su efectividad mejore de forma continua[12]

### 2.3. Metodologías de Evaluación de Seguridad

La metodología MAGERIT v.3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es un enfoque muy reconocido para medir los riesgos en los Sistemas de Información. Esta metodología se enfoca en ordenar los activos y las debilidades; también mide la probabilidad y el impacto de los riesgos[1]. Este enfoque busca hallar activos, amenazas y debilidades; asimismo, mide tanto el impacto como la

probabilidad de que surjan riesgos [5]. Resulta muy útil para las CAC por lo particular de sus activos financieros críticos. Enseguida se muestra un resumen amplio del flujo de trabajo de la metodología MAGERIT v.3 [1]

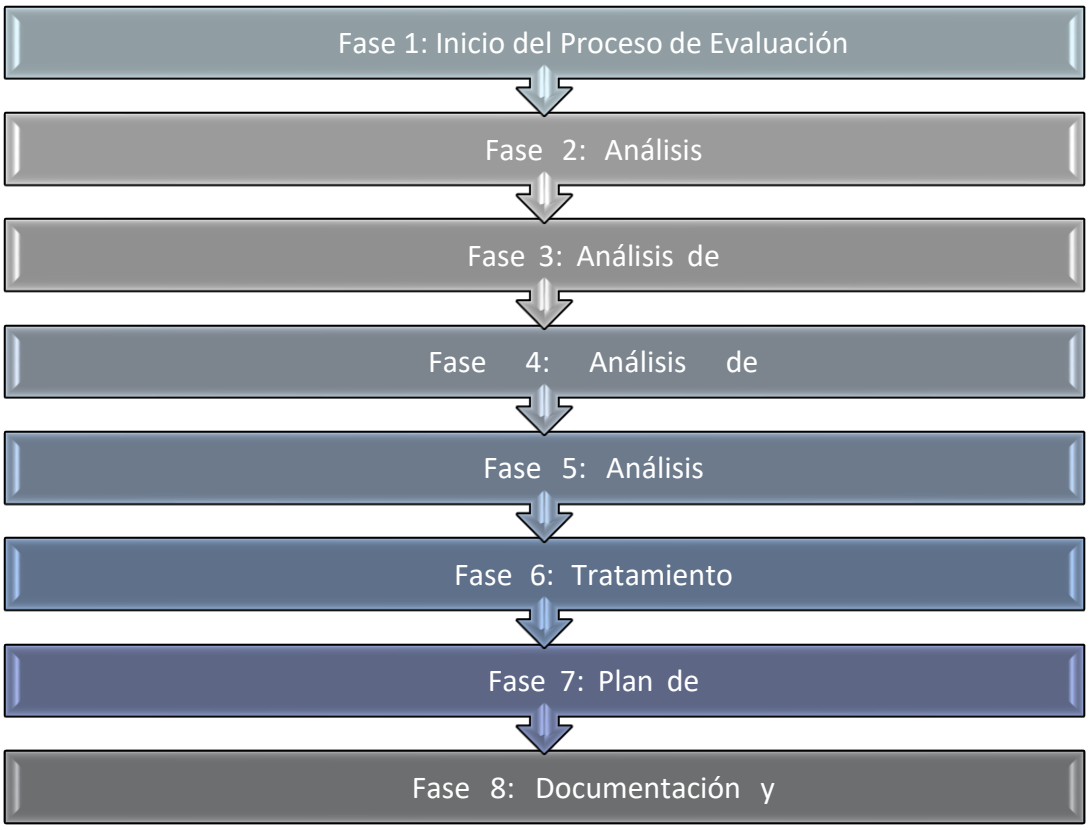



Fig. 1. Flujo de la metodología Magerit v.3 Fuente: Magerit v.3 [1]

Enseguida se explica el flujo de la metodología MAGERIT v.3 de forma amplia:

Fase 1: Inicio del Proceso de evaluación de riesgos

Preparación: en esta etapa inicial, se fijan los fines y los límites del proceso de evaluación de riesgos. Esto supone definir qué sistemas de información se van a evaluar y bajo qué criterios.

Fase 2: Análisis de activos

2.1 Identificación de Activos: se reconocen y ordenan los activos críticos de información que caen dentro del campo de estudio. Aquí entran los datos, los sistemas, el hardware, el software y cualquier otro elemento de importancia.

Fase 3: Análisis de amenazas

3.1 Tipificación de ataques: se reconocen todos los posibles ataques que suelen dañar los activos de información. Tales amenazas pueden abarcar ataques informáticos, desastres naturales, errores humanos, entre otros.

Fase 4: Análisis de vulnerabilidades

4.1 Identificación de Vulnerabilidades: se revisan las debilidades que las amenazas halladas en la fase previa podrían aprovechar. Estas debilidades pueden ligarse a la tecnología, a los procesos o a las personas [1].

Fase 5: Análisis de Riesgos

5.1 Evaluación de riesgos: en esta etapa, se valoran los riesgos hallados. Esto se hace al estimar la probabilidad de que una amenaza aproveche una debilidad y el efecto que tendría sobre los activos de información; la probabilidad y el impacto se califican en una escala[1].

5.2 Cálculo de Riesgos: el riesgo se obtiene al multiplicar la probabilidad por el impacto. Esto ayuda a ordenar los riesgos según su gravedad.

Fase 6: Tratamiento de riesgos

6.1 Identificación de protocolos o medidas de seguridad: se plantean y eligen formas de protección para tratar los riesgos hallados. Tales medidas pueden incluir controles de seguridad, políticas, procedimientos y otros enfoques.

6.2 Análisis de Costo-Beneficio: se valora el costo y el beneficio de aplicar las medidas de seguridad propuestas. Esto ayuda a tomar decisiones bien fundadas sobre qué medidas adoptar.

Fase 7: Plan de seguridad

7.1 Desarrollo del Plan de Seguridad: se elabora un plan de protección que reúne todas las medidas a aplicar, los plazos y los responsables de llevarlas a cabo. Fase 8: Documentación y seguimiento

7.2 Documentación: se registran todos los resultados del proceso de valoración de riesgos; esto abarca la tipificación de activos, ataques, debilidades, riesgos, medidas de seguridad y el plan de seguridad.

7.3 Seguimiento y Revisión: se fija un proceso continuo de seguimiento y revisión de la SI para confirmar que las medidas aplicadas sigan siendo efectivas y adecuadas con el tiempo.

La metodología MAGERIT v.3 brinda un marco ordenado y completo para valorar y manejar los riesgos en los sistemas de información; esto deja que las organizaciones hallen, analicen y traten de buena forma las amenazas que podrían dañar sus activos de información y la continuidad de sus operaciones [1].

## 2.4. Sistemas de Información en Cooperativas de Ahorro y Crédito

Las Cooperativas de Ahorro y Crédito (CAC) se apoyan en los sistemas de información para gestionar los productos, las transacciones y los servicios financieros [7]. Los datos sensibles y críticos para estas instituciones este entorno.

## 2.5. Importancia de las TIC para la Gestión Empresarial

Las Tecnologías de la Información y la Comunicación (TIC) cumplen un papel clave en el mundo empresarial de hoy, ya que [13], [14]:

En el sector financiero cooperativo, la seguridad de la información se rige por varias leyes y normas que fijan requisitos concretos para cuidar la confidencialidad, la integridad y la disponibilidad de los datos [15]. Entre las principales leyes y normas figuran las siguientes.

### 2.5.1. Ley Orgánica de Economía Popular y Solidaria (LOEPS)

Normativa de la Superintendencia de Economía Popular y Solidaria (SEPS) [5]

La SEPS dicta reglas concretas para el sector financiero cooperativo; estas cubren temas como el cuidado de los datos, el manejo de riesgos y la continuidad del negocio [5]

### 2.5.2. Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)

Si bien esta ley asegura el acceso a la información pública, también pide aplicar medidas de seguridad para cuidar la información delicada y secreta en el sector financiero cooperativo [16].

### 2.5.3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta ley regula el comercio electrónico y fija normas para asegurar la información en las transacciones electrónicas que realizan las cooperativas financieras [8]

### 2.5.4. Normativa del Banco Central del Ecuador (BCE)

El BCE dicta reglas para el sector financiero en general; algunas de ellas también valen para el sector financiero cooperativo en cuanto a la seguridad de la información. Estas normas tratan temas como el manejo de riesgos, la ciberseguridad y el cuidado de los datos [17]

Asimismo, pueden existir reglas concretas dictadas por otras instituciones internacionales que complementen estas leyes y normas generales.

### 2.5.5. NTE INEN-ISO/IEC 27000

La norma ISO/IEC 27000 fija las bases y el vocabulario del sistema de gestión de seguridad de la información (SGSI) [12]. Es una guía inicial que define los conceptos y principios básicos ligados al manejo de la seguridad de la información; además, sirve de base para todas las demás normas de la serie ISO/IEC 27000 [18]

### 2.5.6. NTE INEN-ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013 brinda un grupo de controles de seguridad de la información que se pueden aplicar dentro de un SGSI basado en la ISO/IEC 27001[7]. Esta norma da pautas para aplicar los controles que se aceptan y se usan de forma común en el manejo de la seguridad de la información.

### 2.5.7. NTE INEN-ISO/IEC 27005: 2022

La norma ISO/IEC 27005 brinda pautas para manejar los riesgos de seguridad de la información[19]. Esta norma es clave para hallar, medir y tratar los riesgos de seguridad de la información en cualquier organización; así ayuda a cuidar la confidencialidad, la integridad y la disponibilidad de la información [19].

### 2.5.8. NTE INEN-ISO/IEC 27032:2023

La norma ISO/IEC 27032 [20]se enfoca en la ciberseguridad; ofrece pautas para mejorar la seguridad de los sistemas de información en el ciberespacio. Esta norma trata las amenazas y las debilidades en las interacciones en línea; asimismo, da un marco para manejar la seguridad en el entorno cibernético [20]

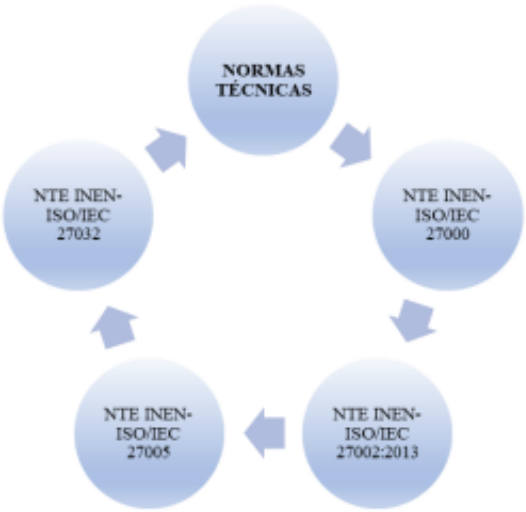



Fig. 2. Normas Técnicas ISO 2022. Fuente: ISO, 2023[20]

La Ley Orgánica de Gestión de la Identidad y Datos Civiles asegura el derecho a la identidad por medio del registro civil de la población; además, prohíbe el manejo doloso de información de interés público [17][21]

Según la Superintendencia de Economía Popular y Solidaria (2022) [4] conviene resaltar que las CAC deben cumplir reglas particulares que cambian según la jurisdicción y el país donde operan [5]. Estas reglas tratan con precisión temas ligados a la seguridad

de la información (SDI) y a los sistemas de gestión de seguridad de la información (SGSI) [5]. Por eso, hace falta hallar y medir estas reglas concretas para lograr que se cumplan bien y asegurar el cuidado de la información.

### 2.5.9. Marco legal específico para las Cooperativas de Ahorro y Crédito (CAC) en Ecuador

En Ecuador, las Cooperativas de Ahorro y Crédito (CAC) deben acatar varias reglas concretas que dicta la Superintendencia de Economía Popular y Solidaria (SEPS) [8]. Este organismo se encarga de vigilar y regular las actividades de las CAC en el país; así busca que estas organizaciones operen de forma segura y protegida.

### 2.5.10. Roles de la SEPS

- Supervisión y regulación: la SEPS tiene la tarea de vigilar y regular las operaciones de las CAC para asegurar su estabilidad financiera y cuidar los intereses de sus miembros y depositantes[5].

- Emisión de normativas: Asimismo, la SEPS dicta reglas y resoluciones que detallan los requisitos y estándares que las CAC deben seguir. Estas reglas contienen disposiciones amplias sobre seguridad de la información (SI) y manejo de riesgos (GR)[5].

Impacto de la Resolución No. SEPS 2022-002 [4]: Dentro del marco legal que rige a las CAC en Ecuador, sobresale la Resolución No. SEPS 2022-002 [4], la cual fija pautas importantes en materia de seguridad de la información y manejo de riesgos cibernéticos[4].

Algunos de los puntos clave de esta resolución son:

- Requisitos de seguridad de la información (SI): la resolución indica que las CAC deben cumplir criterios concretos ligados al cuidado de los datos delicados de socios y clientes; también deben asegurar un buen control de accesos y contar con formas de detectar y responder ante incidentes de seguridad[4].

- Evaluación y gestión de riesgos cibernéticos: se pide que las CAC midan de forma periódica los riesgos cibernéticos y tomen medidas para reducir los riesgos hallados[4].

- Notificación de incidentes de seguridad: se fijan pautas para que las CAC avisen de forma obligatoria cualquier incidente de seguridad, tanto a la SEPS como a las partes interesadas que correspondan[4].

- Cumplimiento y auditorías: las CAC deben procurar cumplir los estándares de seguridad de la información fijados y pasar por auditorías periódicas para comprobar dicho cumplimiento[4].

Legislación de defensa de datos en Ecuador: Aparte de las reglas que dicta la SEPS, las CAC en Ecuador también quedan sujetas a la ley nacional en materia de protección de datos y privacidad. Esta ley regula cómo las cooperativas deben recoger, guardar y manejar los datos personales de sus socios y clientes[4].

El marco legal que rige a las CAC en Ecuador abarca la Resolución No. SEPS 2022-002 y la ley nacional de protección de datos; ambas fijan requisitos de seguridad de la información y manejo de riesgos cibernéticos que protegen los derechos de socios y clientes [5].

# 3. CAPITULO III

## 3.1. Marco Metodológico

Para llevar a cabo el proyecto se emplea la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT v.3, junto con su uso en entidades financieras. Enseguida se muestra el esquema con el que se aplica la metodología [1].

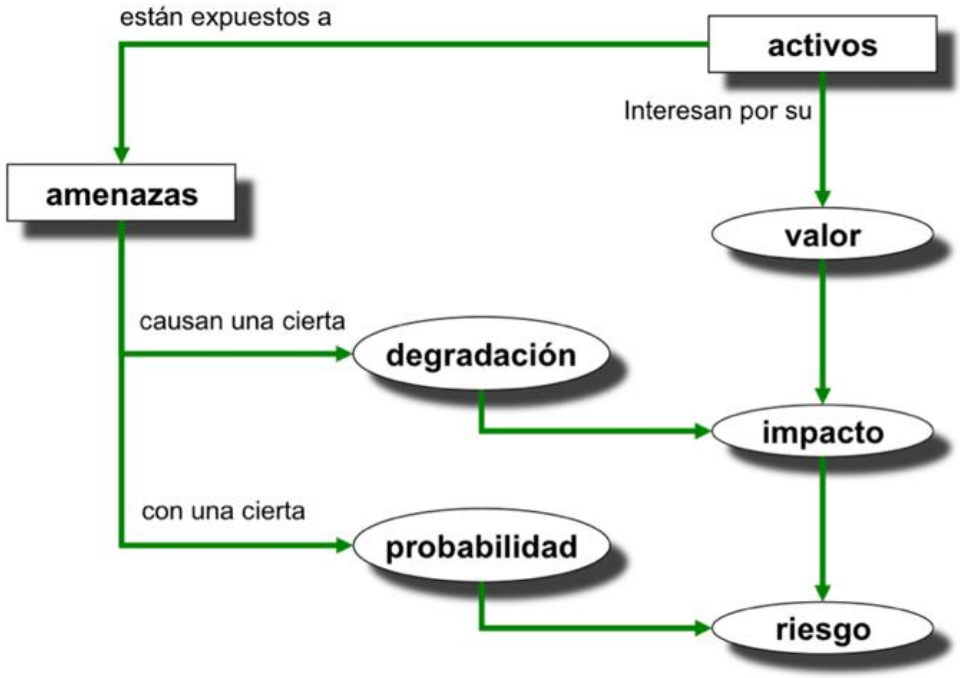



Fig. 3. Elementos del análisis de riesgos potenciales

## 3.2. Descripción del Área de Estudio / Descripción del Grupo de Estudio.

El área de estudio es el sector financiero cooperativo del Ecuador; en concreto, las Cooperativas de Ahorro y crédito del segmento 2.

Este grupo de instituciones financieras se compone de 69 cooperativas repartidas por todo el país; la guía se usará en una cooperativa que represente al segmento, en la que se pondrá en marcha el Sistema de Gestión de Seguridad de la Información (SGSI).

Al revisar la infraestructura informática de la cooperativa, se halló una creciente dependencia de los sistemas digitales para manejar la información financiera y personal de los miembros [18]. La exposición a las amenazas cibernéticas y la necesidad de cuidar los datos secretos se han hecho más claras con el tiempo; esto explica la urgencia de reforzar la seguridad de la información [18].

Las cooperativas han enfrentado problemas para encarar de forma ordenada y efectiva los retos de seguridad de la información. Hechos anteriores, como los intentos de acceso sin permiso y la pérdida de datos, dejan ver la necesidad de adoptar un enfoque metodológico ordenado para manejar los riesgos.

La revisión de las prácticas y normas actuales mostró una brecha en la alineación con los estándares mundiales de seguridad de la información. La ausencia de un método coherente, apoyado en marcos reconocidos en la teoría, deja a la cooperativa en desventaja frente a la competencia y la norma; esto refuerza la necesidad de una base teórica firme [19].

### 3.2.1. Evaluación de la necesidad del SGSI

Poner en marcha un Sistema de Gestión de Seguridad de la Información (SGSI) en la cooperativa se justifica por el análisis de los riesgos, las debilidades y las amenazas halladas en sus procesos digitales [7]. La creciente dependencia de la tecnología y el manejo de datos delicados piden un enfoque ordenado para reducir las posibles brechas de seguridad [18]. Asimismo, cumplir las normas y los estándares mundiales en seguridad de la información resulta básico para asegurar la confianza de los socios y la estabilidad operativa de la institución[18].

### 3.2.2. Análisis de recursos disponibles

Para poner en marcha el SGSI, hace falta valorar los recursos con los que cuenta la cooperativa; entre ellos, la infraestructura tecnológica, el software, el talento humano y el presupuesto [8]. Se estudiará la capacidad del equipo de TI para manejar y mantener el sistema, así como la disponibilidad de herramientas y plataformas adecuadas para su puesta en marcha[8]. Además, se tendrá en cuenta si resulta viable, en lo financiero y lo operativo, adoptar nuevas tecnologías o mejorar las actuales; así se asegura un uso eficiente de los recursos sin poner en riesgo la estabilidad económica de la institución [8].

## 3.3. Enfoque y Tipo de Investigación

La investigación toma un enfoque exploratorio-descriptivo; este resulta adecuado para describir cómo se maneja el riesgo tecnológico en las CAC del segmento 2 y 3.

## 3.4. Procedimiento de Análisis de Riesgos

### 3.4.1. Paso 1: Activos. Identificación de activos

Un activo se identifica como "Componente o funcionalidad de un sistema de información susceptible de ser atacado…" [2]. En un sistema de información se reconocen dos activos esenciales: la información y los servicios. Asimismo, se deben hallar los activos subordinados; estos son los siguientes:

- Datos que materializan la información.
- Servicios auxiliares que se necesitan para poder organizar el sistema.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

El paso siguiente es valorar los activos según cómo se clasifican en cuanto a impacto y riesgo por dependencias, pues unos activos dependen de otros y forman una especie de árbol; allí los activos "superiores", que están más arriba, dependen de los "inferiores" (abajo) de la cadena [1] De aquí surge el concepto de "dependencia entre activos" un activo "superior" depende de un "inferior" cuando al existir una amenaza en el activo inferior tiene consecuencias en el activo superior aunque este esquema depende de la Organización en la que existan. En este caso, se puede manejar un sistema entre capas:

**Activos esenciales**

- Información que se maneja.
- Servicios prestados.

Servicios internos:

- Que estructuran ordenadamente el sistema de información.

El equipamiento informático:

- Aplicaciones (software)
- Equipos informáticos (hardware)
- Comunicaciones.
- Soportes de información: discos, cintas, etc.

El entorno: activos que se precisan para garantizar las siguientes capas

- Equipamiento y suministros: energía, climatización, etc.

Mobiliario.

Los servicios subcontratados a terceros.

Las instalaciones físicas.

El personal:

- Usuarios.
- Operadores y administradores.
- Desarrolladores.

**Valoración**

Se debe fijar el valor de los activos al medir cuánto importan para la organización. El valor puede ser acumulado o propio. “Se dice que los activos inferiores en un es quema de dependencias, acumulan el valor de los activos que se apoyan en ellos.” [2]. El valor central suele estar en la información que el sistema maneja y en los servicios que se prestan (activos esenciales); los demás activos quedan supeditados a las necesidades de uso y protección de lo esencial. Asimismo, hará falta una valoración cualitativa y cuantitativa.

**Dimensiones**

De un activo puede interesar calibrar diferentes dimensiones:

• Confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.

• Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcial mente falsos o, incluso, faltar datos.

• Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

• Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? [1]Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar) [1]

• Trazabilidad del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

• Trazabilidad del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

El valor de la interrupción del servicio

La mayoría de las dimensiones citadas antes se pueden medir de forma sencilla, ya sea cualitativa o cuantitativa. Sin embargo, hay una excepción: la disponibilidad. No es igual que un servicio se corte una hora, un día o un mes. Un corte de una hora podría no traer mayor impacto, mientras que un día sin servicio sí podría causar un daño [2] Pero si el servicio se detiene un mes, esto podría significar el fin de la actividad. Lo difícil es que no hay una relación proporcional directa entre el tiempo de corte y las consecuencias que provoca [2]. Por eso, para medir la disponibilidad de un activo, sobre todo en casos de corte, hace falta usar un enfoque más amplio y ordenado, que se puede mostrar de forma gráfica para entenderlo mejor:

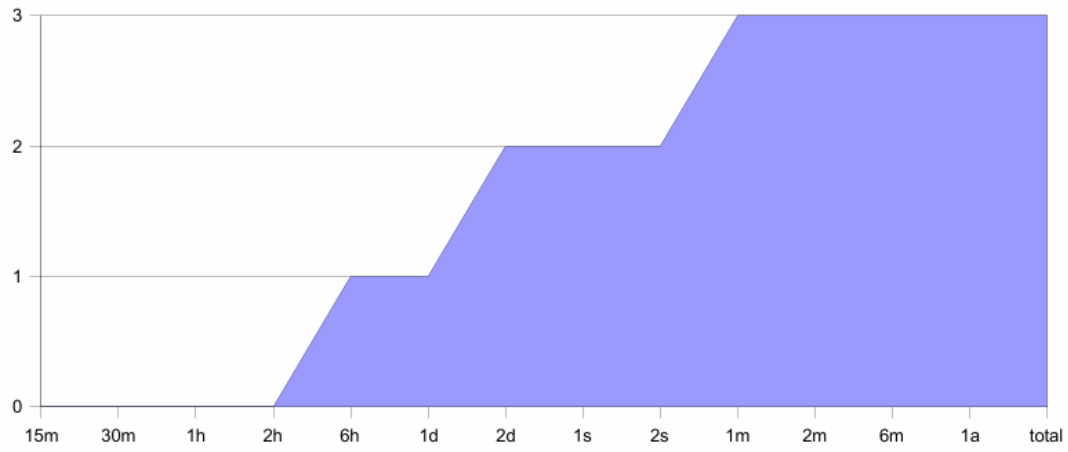



Fig. 4. Coste de la [interrupción de la] disponibilidad. Fuente: Magerit v3 [1]

Aquí se muestra una serie de niveles o "escalones" de corte, que van desde situaciones manejables hasta la pérdida total o permanente del activo [1]. Según el ejemplo citado, los cortes de hasta 6 horas se pueden tomar como sin mayores consecuencias [1]. Sin embargo, al pasar las 6 horas, se prenden alertas que crecen si la parada dura más de 2 días [1]. Y si el corte llega a durar un mes, se puede afirmar que la organización ha perdido por completo su capacidad de operar[1]. Resulta razonable poner ciertos recursos para evitar que un corte pase de 6 horas o de 2 días, pues los costos ligados a esos tiempos de parada pueden ser altos [1]. Sin embargo, al valorar lo que supone evitar que un corte dure más de un mes, hace falta pesar el valor total de la organización frente al costo de las medidas de protección [1]. En algunos casos, esa inversión podría no justificarse en lo económico, según el impacto que tendría en la organización [1].

### 3.4.2. Paso 2: Amenazas. Identificación de amenazas y vulnerabilidades

Una amenaza es una “Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización” [2]. En este apartado se analizan las posibles amenazas que podrían afectar los activos de información. Existen cinco:

De origen natural. - Existen accidentes naturales (terremotos, inundaciones, etc.). Ante esos hechos, el sistema de información es una víctima pasiva; aun así, tendremos en cuenta lo que puede pasar.

Del entorno (de origen industrial). - Existen desastres industriales (contaminación, fallas eléctricas, etc.) ante los cuales el sistema de información es una víctima pasiva; pero el hecho de ser pasivos no obliga a quedar sin defensa.

Defectos de las aplicaciones. - Existen problemas que surgen de forma directa en el propio equipamiento por fallas en su diseño o en su puesta en marcha, con efectos que podrían ser negativos para el sistema [1]. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, “vulnerabilidades”[1].

Causadas por las personas de forma accidental. - Las personas con acceso al sistema de información pueden originar problemas sin querer, por lo común por error o por descuido.

Causadas por las personas de forma deliberada. - Las personas con acceso al sistema de información pueden originar problemas a propósito: ataques deliberados; ya sea con la intención de sacar provecho indebido, ya sea con el fin de dañar a los dueños legítimos [2][2]

Estas cinco categorías forman el conjunto de amenazas que MAGERIT v3 considera para armar el mapa de riesgos de un sistema de información [1].

**Valoración de amenazas**

No todas las amenazas afectan todas las dimensiones; por ello, hay que fijar el nivel de amenaza en dos sentidos:

- Degradación: cuán perjudicado resultaría el [valor del] activo.
- Probabilidad: cuán probable o improbable es que se materialice la amenaza.

La degradación suele verse como una parte o fracción del valor total de un activo. Por eso, es común oír frases como que un activo quedó "totalmente degradado" o "degradado en una pequeña proporción" [2]. Cuando las amenazas no son intencionales, suele bastar con saber qué parte física del activo se vio afectada para calcular la pérdida de valor de forma proporcional. Sin embargo, cuando la amenaza es intencional, esa proporción no aplica, pues un atacante puede causar un daño mucho mayor y más puntual, incluso de forma selectiva.

Por otra parte, la probabilidad de que una amenaza ocurra es más difícil de fijar y de expresar. En algunos casos, se usa una escala cualitativa, como una clasificación nominal, para modelar esa probabilidad.

Tabla I Degradación de Valor.

| **Código** | Ocurrencia | Probabilidad | Fácil |
|---|---|---|---|
| **MA** | Muy alta | Casi seguro | Fácil |
| **A** | Alta | Muy alto | Medio |
| **M** | Media | Posible | Difícil |
| **B** | Baja | Poco probable | Muy difícil |
| **MB** | Muy baja | Muy raro | Extremadamente difícil |

Nota: Fuente: Magerit v.3 [1]

A veces, la probabilidad de que algo ocurra se modela en números según su frecuencia [1]. Es común tomar como referencia un lapso de un año y usar la tasa anual de ocurrencia como una forma de medir la probabilidad de que un evento pase[1]. Algunos valores comunes que se usan en este contexto son:

Tabla II Pobabilidad de Ocurrencia.

| **Código** | **Factor** | **Frecuencia** | **Periodicidad** |
|---|---|---|---|
| **MA** | 100 | Muy frecuente | A diario |
| **A** | 10 | Frecuente | Mensualmente |
| **M** | 1 | Normal | Una vez al año |
| **B** | 1/10 | Poco frecuente | Cada varios años |
| **MB** | 1/100 | Muy poco frecuente | Siglos |

Nota: Fuente: Magerit v.3 [1]

### 3.2.3. Determinación del potencial impacto

El impacto se define como la medida del daño que sufre un activo cuando una amenaza se materializa [2]. Si sabemos el valor de los activos (con sus distintas dimensiones) y el nivel de degradación que las amenazas pueden causar, se puede calcular de forma directa el impacto que estas tendrían sobre el sistema.

Sin embargo, hay un aspecto clave que no podemos pasar por alto: las dependencias entre los activos. Muchas veces, el valor del sistema se concentra en la

información que maneja y en los servicios que ofrece; sin embargo, las amenazas suelen golpear primero los medios que sostienen esos activos. Para entender cómo se enlazan estos elementos, usamos el grafo de dependencias, que deja ver y analizar las relaciones entre los distintos componentes del sistema [1].[1]

**Impacto acumulado**

- Se refiere al impacto calculado sobre un activo, considerando:
- Su valor acumulado (el propio más el acumulado de los activos que dependen de él).
- Las amenazas a que está expuesto.

Este impacto acumulado se fija para cada activo, amenaza y dimensión de valoración; depende tanto del valor acumulado como del daño que podría causarse. Cuanto mayor sea el valor del activo o su dependencia, mayor será el impacto. Del mismo modo, a mayor degradación del activo afectado, mayor será la consecuencia [1]

Al evaluar el impacto acumulado en los activos críticos que sostienen el sistema de información, se pueden identificar las medidas de protección necesarias, como:

- Protección de equipos.
- Copias de seguridad.
- Otras salvaguardas para garantizar la continuidad operativa.

Este enfoque ayuda a priorizar las acciones de seguridad más efectivas [1]

**Impacto repercutido**

- Se calcula sobre un activo considerando:
- Su valor intrínseco.
- Las amenazas que afectan a los activos de los que depende.

El impacto repercutido se evalúa para cada activo, amenaza y dimensión de valoración, en función de:

- El valor propio del activo.
- El grado de degradación sufrida.

Cuanto mayor sea el valor del activo, mayor será el impacto. A mayor daño en el activo atacado, más graves serán las consecuencias. Además, cuanto más dependan otros activos de él, más significativo será el efecto [1]

Al analizar el impacto repercutido en los activos con valor propio, se pueden fijar los efectos de las fallas técnicas sobre la misión del sistema de información. Este enfoque da una mirada gerencial y facilita una de las decisiones clave en el manejo de riesgos: aceptar cierto nivel de riesgo cuando haga falta [1]

Notas clave:

- Enfoque en dependencias y valor intrínseco.
- Relación directa entre degradación, valor e impacto.
- Herramienta para justificar decisiones estratégicas en ciberseguridad.

**Agregación de valores de impacto**

Los análisis previos fijan el impacto individual que una amenaza podría causar sobre un activo en una dimensión concreta. Estos impactos sueltos se pueden combinar bajo ciertas condiciones:

- Es posible sumar el impacto repercutido sobre distintos activos.
- Se puede agregar el impacto acumulado en activos que no dependan entre sí ni compartan un valor heredado de un mismo activo superior.
- No debe sumarse el impacto acumulado en activos interdependientes, ya que esto sobrevaloraría el impacto al contar múltiples veces el valor acumulado de activos superiores.
- Puede combinarse el impacto de varias amenazas sobre un mismo activo, aunque conviene evaluar si estas amenazas son independientes y pueden ocurrir simultáneamente.
- Es factible agregar el impacto de una misma amenaza en diferentes dimensiones de valoración.

Claves del Análisis:

- Agregación válida: Impactos no solapados (activos independientes o amenazas no concurrentes).

- Agregación no válida: Impactos con dependencias cruzadas (para evitar duplicaciones).

Precaución: Evaluar la independencia de amenazas y activos antes de consolidar impactos.

Este enfoque deja evitar distorsiones en la evaluación de riesgos y asegura una ponderación precisa al ordenar las medidas de protección [1]

### 3.4.3. Determinación del riesgo potencial

El riesgo es la medida del daño posible que puede afectar a un sistema. Para fijarlo, se valora tanto el impacto de las amenazas sobre los activos como su probabilidad de ocurrencia [1] El nivel de riesgo crece a medida que aumentan el impacto y la probabilidad; esto deja ordenarlo en distintas zonas de prioridad:

- Zona 1 (Alta Prioridad):
  - Riesgos muy probables y de impacto extremadamente alto.
  - Requieren medidas inmediatas para mitigar consecuencias graves.
- Zona 2 (Prioridad Media - Franja Amarilla):
  - Abarca desde riesgos poco probables, pero de impacto moderado, hasta situaciones muy probables, pero de bajo impacto.
  - Aquí se implementan controles de seguridad, como:
    - Controles técnicos (firewalls, cifrado).
    - Políticas y procedimientos.
    - Capacitación y concienciación del personal.
- Zona 3 (Baja Prioridad):
  - Riesgos improbables y de impacto reducido.
  - Pueden aceptarse o gestionarse con medidas básicas.
- Zona 4 (Prioridad Estratégica):
  - Riesgos poco probables, pero con impacto catastrófico (ej.: ciberataques masivos).
  - Aunque su probabilidad sea baja, exigen planes de contingencia por su gravedad potencial.

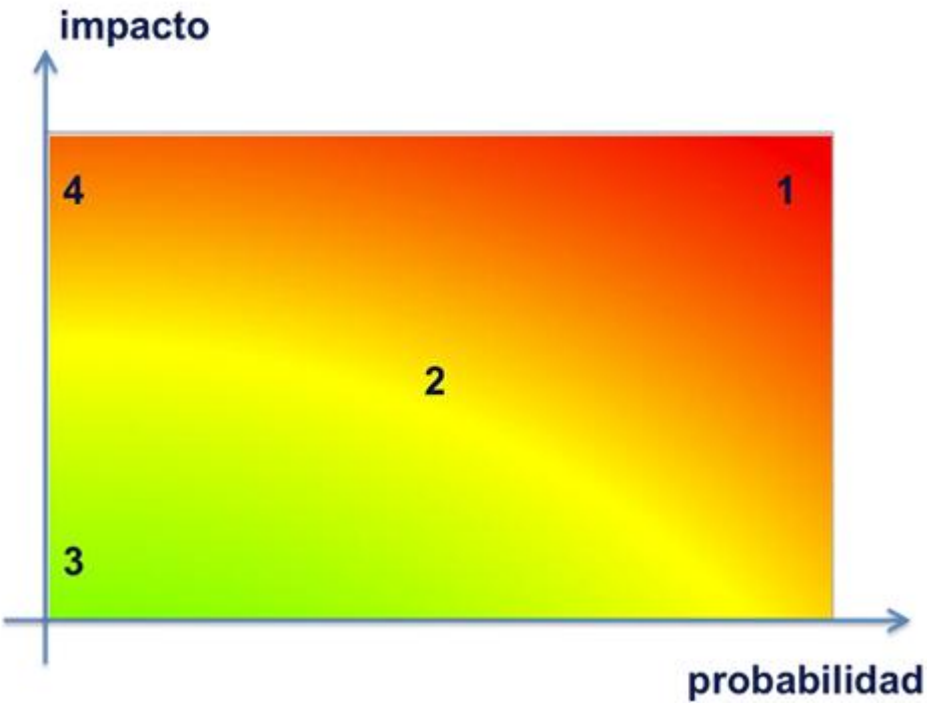



Fig. 5. El riesgo en función del impacto y la probabilidad. Fuente: Magerit V.3 [1]

**Riesgo acumulado**

El riesgo acumulado se determina evaluando un activo en función de:

- El impacto acumulado que una amenaza podría generar sobre él.
- La probabilidad de que dicha amenaza ocurra.

Este cálculo se realiza para cada activo, amenaza y dimensión de valoración, considerando:

- El valor total del activo (incluyendo su valor propio y el de los activos dependientes).
- El nivel de degradación que la amenaza podría causar.
- La probabilidad de ocurrencia de la amenaza.

Aplicación Práctica:

Al analizar el riesgo acumulado en los activos críticos que sostienen el sistema de información, se identifican las medidas de protección necesarias, tales como:

- Protección física y lógica de equipos.

- Copias de seguridad (backups).
- Otras salvaguardas para garantizar la continuidad operativa.

Este enfoque deja ordenar los recursos de seguridad y centrarse en los activos con mayor exposición a amenazas probables y de alto impacto [1]

**Riesgo repercutido**

Se refiere a la evaluación del riesgo asociado a un activo, considerando:

- El impacto repercutido que una amenaza podría generar sobre él.
- La probabilidad de que dicha amenaza se materialice.

Cálculo y Características: Este análisis se realiza para cada activo, amenaza y dimensión de valoración, y se basa en tres factores clave:

1. Valor intrínseco del activo.
2. Grado de degradación que la amenaza podría causar.
3. Probabilidad de ocurrencia de la amenaza.

Importancia Gerencial: Al centrarse en activos con valor propio, el riesgo repercutido ayuda a:

- Prever las consecuencias de fallos técnicos en la operatividad del sistema.
- Tomar decisiones estratégicas, como aceptar niveles de riesgo controlados cuando el coste de mitigación supera el beneficio.

Ejemplo Práctico: En un sistema de información, este enfoque permite justificar:

- Inversiones en redundancias (ej.: servidores de respaldo).
- Priorización de salvaguardas para activos críticos.

Mientras el riesgo acumulado toma en cuenta las dependencias entre activos, el repercutido se centra en el valor propio y en su impacto directo[1]

**Agregación de riesgos**

Los análisis hechos antes dejan medir el riesgo concreto que una amenaza particular supone para un activo en una dimensión específica [1] Estos riesgos

individuales admiten procesos de consolidación, siempre que se cumplan las siguientes condiciones básicas:

- Reglas para la Combinación de Riesgos
- Integración Horizontal de Riesgos Repercutidos
- Admiten agregación los riesgos repercutidos que afecten a distintos activos del sistema
- Suma Controlada de Impactos Acumulados
- Solo pueden combinarse impactos acumulados cuando:
  - Los activos carezcan de relaciones de dependencia mutua
  - No compartan valoración procedente de un activo superior común

Limitaciones en la Agregación de Riesgos Acumulados:

Se prohíbe expresamente la suma de riesgos acumulados en activos con interdependencias, ya que:

- Provocaría una duplicación en la contabilización

Generaría una sobrevaloración artificial al repetir el cómputo del valor de activos superiores.

Consolidación de Múltiples Amenazas: Es posible agregar riesgos derivados de distintas amenazas sobre un mismo activo, previo análisis de:

- Su grado de independencia estadística
- Su potencial concurrencia temporal
- Integración Multidimensional

Permite la combinación del riesgo asociado a una misma amenaza cuando se manifiesta en diferentes dimensiones de valoración.

Principios Rectores:

Validez: Solo cuando no existan solapamientos en dependencias o valoraciones

Precisión: Evitando toda duplicación en la contabilización de valores

Rigor Analítico: Verificando siempre la independencia real entre amenazas. Esta metodología garantiza:

- Exactitud en la evaluación global de riesgos.
- Eficiencia en la priorización de contramedidas.
- Optimización en la asignación de recursos de seguridad.

### 3.4.4. Paso 3: Salvaguardas

Los análisis previos han tomado escenarios donde no hay medidas de protección aplicadas; así se calculan los impactos y riesgos posibles a los que quedarían expuestos los activos en condiciones de vulnerabilidad total[1]. En la práctica diaria, rara vez hallamos sistemas del todo desprotegidos: estos resultados muestran lo que pasaría si se quitaran todas las defensas que existen[1].

Las salvaguardas (o contramedidas) abarcan mecanismos y procedimientos pensados para reducir riesgos; se clasifican según su naturaleza: organizativas, técnicas, de seguridad física y de manejo del personal [1] Este enfoque deja medir el valor que suman las medidas actuales y hallar las brechas críticas en la protección de hoy.

**Selección de salvaguardas**

Ante la variedad de medidas que existen, hace falta elegir las salvaguardas pertinentes para cada activo crítico [2]. Este filtrado debe apoyarse en cuatro bases principales:

1. Naturaleza de los Activos: Cada categoría de activo (datos, infraestructura, personal) demanda estrategias de protección específicas y adaptadas.
2. Dimensiones de Seguridad Afectadas: Es crucial determinar si requerimos proteger confidencialidad, integridad, disponibilidad o combinaciones de estas.
3. Panorama de Amenazas Relevantes: El enfoque debe dirigirse exclusivamente a las amenazas realistas y probables para nuestro entorno.
4. Existencia de Medidas Alternativas: Se debe evaluar si otras salvaguardas ya implementadas proporcionan cobertura suficiente.

Principios Rectores para la Selección:

- Proporcionalidad: Priorizar recursos en función de:
  - Valor intrínseco o acumulado de los activos
  - Probabilidad materialización de amenazas (según zonificación de riesgo)
  - Cobertura residual de medidas existentes
- Criterios de Exclusión:
  - No aplica: Cuando la salvaguarda es técnicamente incompatible con:
    - Tipo de activo
    - Dimensión de seguridad requerida
    - Amenaza específica considerada
  - No justificada: Cuando el coste/impacto de implementación excede desproporcionadamente el riesgo a mitigar

La aplicación sistemática de estos filtros genera una "Declaración de Aplicabilidad" definitiva:

- Listado depurado de salvaguardas candidatas.
- Base objetiva para el diseño del sistema de protección.
- Eliminación de opciones redundantes o ineficientes.

**Efecto de salvaguardas**

Las salvaguardas entran en el cálculo del riesgo de dos formas:

**Reduciendo la probabilidad de las amenazas**

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

**Limitando el daño causado**

Existen tres categorías fundamentales de medidas de seguridad, diferenciadas por su forma de actuar frente a las amenazas:

1. Salvaguardas Preventivas
   - Actúan como barreras proactivas que reducen directamente la posible degradación del sistema
   - Ejemplos: firewalls, sistemas de autenticación robusta, cifrado de datos

2. Salvaguardas de Detección
   - Permiten identificar ataques en tiempo real para contener el daño
   - Ejemplos: sistemas IDS/IPS, monitorización continua, SIEMs
   - Objetivo: Minimizar el tiempo de exposición y propagación del ataque
3. Salvaguardas de Recuperación
   - Facilitan la restauración rápida tras un incidente
   - Ejemplos: backups automatizados, planes DRP, sistemas redundantes
   - Garantizan la continuidad operativa incluso tras materializarse la amenaza

Efecto común: todas buscan limitar las consecuencias, aunque actúan en momentos distintos (antes, durante o después del incidente). En algunos casos no se puede evitar que la amenaza se concrete, pero su impacto final queda muy reducido [1]

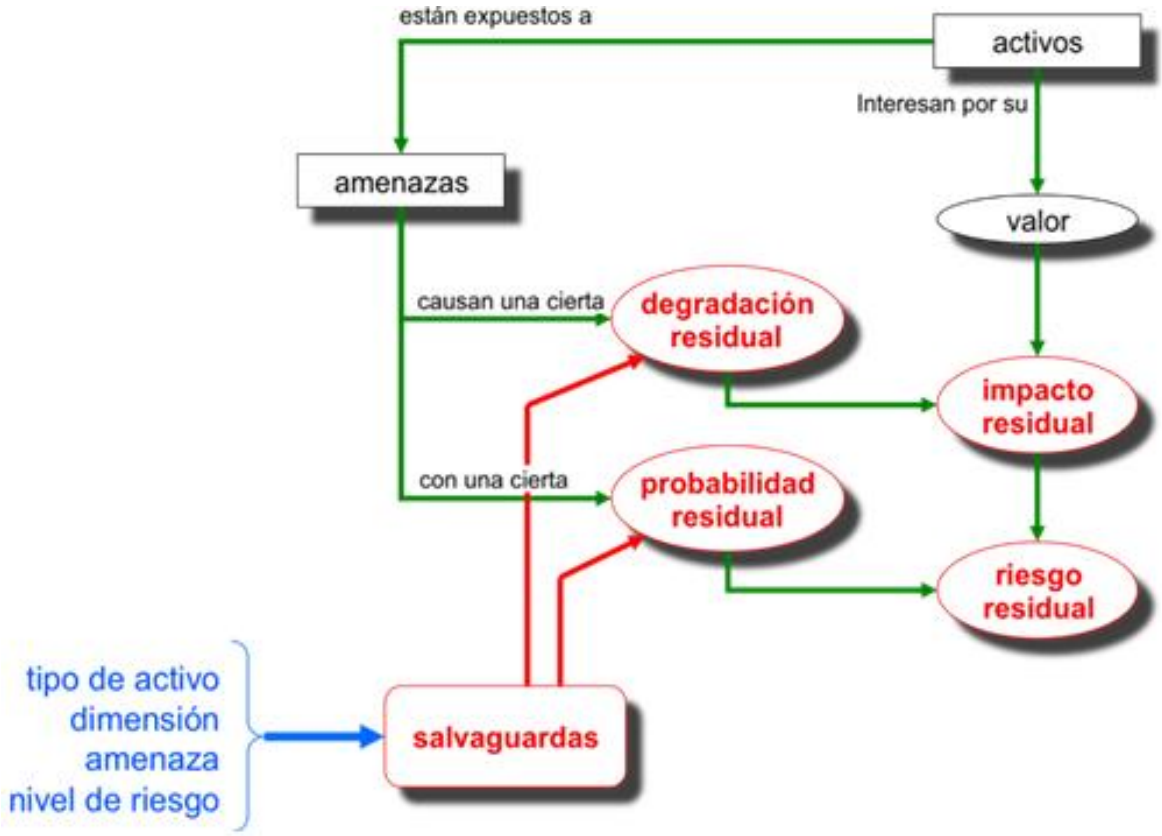



Fig. 6. Elementos de análisis del riesgo residual

**Tipo de protección**

Este enfoque tradicional puede quedar corto, pues en la práctica las salvaguardas brindan distintos tipos de protección que podemos ordenar de forma más precisa:

1. Prevención (PR)
    - Función: Disminuye las oportunidades de que ocurra un incidente
    - Limitación: Si falla, no mitiga el daño
    - Ejemplos:
    - Control de accesos y privilegios
    - Metodologías de desarrollo seguro
    - Pruebas en entornos controlados
    - Segregación de funciones
2. Disuasión (DR)
    - Función: Desanima potenciales atacantes
    - Característica: No afecta el impacto si el ataque se materializa
    - Ejemplos:
    - Barreras físicas visibles
    - Señalización de vigilancia
    - Avisos legales
3. Eliminación (EL)
    - Función: Neutraliza completamente ciertos vectores de ataque
    - Ejemplos:
    - Eliminación de cuentas por defecto
    - Desactivación de servicios innecesarios
    - Cifrado de datos sensibles
    - Medidas de bastionado
4. Minimización de Impacto (IM)
    - Función: Limita el alcance del daño
    - Ejemplos:
    - Sistemas de desconexión automática
    - Pólizas de seguros
    - Cumplimiento normativo
5. Corrección (CR)
    - Función: Repara daños ocurridos
    - Ejemplos:
    - Protocolos de respuesta a incidentes
    - Infraestructura redundante

6. Recuperación (RC)
    - Función: Restaura el estado previo al incidente
    - Ejemplo principal:
    - Sistemas de *backup*
7. Monitorización (MN)
    - Función dual:
    - Detección en tiempo real para activar contramedidas
    - Análisis post-incidente para mejora continua
    - Ejemplos:
    - Registros de actividad
    - Logs de transacciones
8. Detección (DC)
    - Función: Identifica ataques en curso
    - Ejemplos:
    - Sistemas IDS/IPS
    - Antivirus
    - Sensores ambientales
9. Concienciación (AW)
    - Impacto:
    - Reduce errores humanos (preventivo)
    - Optimiza la operación de otras salvaguardas
    - Ejemplos:
    - Programas de formación
    - Simulacros de seguridad
10. Administración (AD)
    - Función: Garantiza el conocimiento y gestión adecuada de los controles
    - Ejemplos:
    - Inventarios de activos
    - Planes de continuidad
    - Análisis periódicos de riesgo

Relación con el Modelo Básico: esta clasificación amplia se vincula con el modelo simple (prevención-detección-recuperación) de la siguiente forma:

- Reducción de probabilidad: PR, DR, EL, AW, AD
- Limitación de daños: IM, CR, RC, DC
- Detección y respuesta: MN, DC

La siguiente tabla vincula cada uno de estos tipos de protección con el modelo previo de reducción de la degradación y de la probabilidad:

Tabla III Tipos de salvaguardas.

| Efecto | Tipo |
|---|---|
| **preventivas: reducen la probabilidad** | [PR] preventivas [DR] disuasorias [EL] eliminatorias |
| **acotan la degradación** | [IM] minimizadoras [CR] correctivas [RC] recuperativas |
| **consolidan el efecto de las demás** | [MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas |

Nota: Fuente: Magerit 3. V[1]

**Eficacia de la protección**

La eficacia de una salvaguarda no solo depende de que exista, sino también de su capacidad real para reducir el riesgo que busca controlar [2]. Una salvaguarda ideal llegaría al 100% de eficacia, lo que supone cumplir dos dimensiones clave:

1. Eficacia Técnica
    - Idoneidad: La salvaguarda debe ser técnicamente adecuada para contrarrestar la amenaza específica.
    - Aplicación consistente: Debe activarse siempre cuando sea necesaria, sin fallos en su ejecución.

2. Eficacia Operativa

    - Implantación correcta: La salvaguarda debe estar correctamente desplegada, configurada y mantenida.

- Procedimientos definidos: Deben existir protocolos claros para su uso en condiciones normales y en situaciones de incidencia.
- Formación y concienciación: Los usuarios deben conocer su funcionamiento y su importancia.
- Monitoreo y alertas: Deben implementarse controles que detecten fallos en la salvaguarda.

Grado de Eficacia Real

En la práctica, pocas salvaguardas alcanzan el 100% de eficacia. Su efectividad varía entre:

- 0%: Cuando la salvaguarda no existe o es totalmente inadecuada.
- 100%: Cuando es técnicamente perfecta y operativamente impecable.

En cada caso concreto, se debe estimar un nivel de eficacia intermedio basado en:

- Factores técnicos (¿es adecuada para el riesgo?)
- Factores operativos (¿está bien implementada y gestionada?)

Esta evaluación deja ordenar las mejoras y asegurar que las salvaguardas cumplan su función de la mejor forma [1] Para medir los aspectos organizativos, se puede usar una escala de madurez que refleje, como factor corrector, la confianza que merece el proceso de gestión de la salvaguarda:

Tabla IV Eficacia y madurez de las salvaguardas Fuente: Magerit V.3

| **Factor** | **Nivel** | **Significado** |
|---|---|---|
| **0%** | **L0** | inexistente |
| | **L1** | inicial / ad hoc |
| | **L2** | reproducible, pero intuitivo |
| | **L3** | proceso definido |
| | **L4** | gestionado y medible |
| **100%** | **L5** | optimizado |

**Vulnerabilidades**

Una vulnerabilidad se define como cualquier debilidad o falla en un sistema que una amenaza pueda aprovechar para poner en riesgo la seguridad de los activos [2]. En términos más concretos, son aquellas fallas presentes tanto en los propios activos como en las medidas de protección aplicadas, que facilitan que una amenaza posible logre su fin[1] Estas debilidades funcionan como puertas de entrada para los atacantes; así les dejan saltar los controles de seguridad y causar daños.

Cuando miramos las vulnerabilidades desde la óptica de las salvaguardas, podemos verlas como aquellas situaciones en las que las medidas de protección no existen, no bastan o no sirven para asegurar el valor propio o acumulado de un activo [2]. En muchos casos, se usa el término "insuficiencia" para resaltar que, aunque haya salvaguardas aplicadas, su nivel de eficacia no alcanza para cuidar del todo el activo frente a las amenazas a las que está expuesto. Esta insuficiencia puede deberse a varios factores, como una configuración errónea, un mantenimiento pobre o la falta de actualizaciones.

Hallar y manejar las vulnerabilidades es una pieza crítica en cualquier estrategia de seguridad[1] Las organizaciones deben hacer evaluaciones periódicas para notar estas debilidades y ordenar su corrección según el nivel de riesgo que suponen. Un enfoque activo en este campo deja reducir la superficie de ataque y bajar la probabilidad de que las amenazas se concreten con éxito [1]. Asimismo, ver las vulnerabilidades como fallas en las salvaguardas ayuda a usar mejor la inversión en seguridad; así los recursos se dirigen a reforzar los puntos más críticos del sistema.

### 3.4.5. Paso 4: Impacto residual

Cuando un sistema aplica un conjunto de salvaguardas y se mide la madurez de su gestión, se llega a un estado en el que el posible daño se llama impacto residual [2]. Esta idea refleja el cambio del impacto potencial inicial, que baja a un nivel aceptable gracias a las medidas de protección aplicadas [1]. En otras palabras, el impacto residual muestra el riesgo que queda después de aplicar los controles de seguridad, según su eficacia real.

El cálculo del impacto residual es directo, pues no cambian los activos ni sus relaciones de dependencia, sino solo el grado de degradación que estos pueden sufrir.

Para fijarlo, se repiten los mismos cálculos que sirven para estimar el impacto potencial, pero se ajusta la magnitud de la degradación según la eficacia de las salvaguardas [1]. Esta degradación ajustada surge de la diferencia entre la eficacia teórica ideal (100%) y la eficacia real medida; así se mide la parte de riesgo que no se ha reducido.

El impacto residual puede analizarse desde dos perspectivas:

1. Impacto acumulado: Evalúa cómo afecta la degradación residual a los activos que dependen jerárquicamente del activo protegido.
2. Impacto repercutido: Examina las consecuencias del daño residual en los activos superiores que dependen del activo en cuestión.

### 3.4.6. Paso 5: riesgo residual

Cuando un sistema aplica cierto conjunto de salvaguardas y se fija un nivel de madurez en su gestión, se llega a un estado de exposición al riesgo llamado residual [1]. Esta idea refleja el paso del riesgo potencial inicial -el que existiría sin controles- a un nivel reducido de riesgo que queda a pesar de las medidas aplicadas [2]. El riesgo residual es entonces la parte de exposición que queda tras aplicar las protecciones disponibles; su evaluación es el insumo principal para decidir sobre la aceptación o el tratamiento del riesgo.

El cálculo del riesgo residual sigue un enfoque ordenado [1] Como los activos y sus relaciones de dependencia no cambian, el análisis se centra en dos variables clave: la degradación y la probabilidad residuales de que ocurran las amenazas. El procedimiento consiste en:

1. Recalcular el impacto considerando la degradación residual
2. Ajustar la probabilidad de ocurrencia según la efectividad de las salvaguardas

La probabilidad residual surge de forma directa de la brecha entre la eficacia teórica máxima (100%) y la eficacia real que logran las medidas de protección aplicadas.

El riesgo residual admite dos enfoques complementarios de evaluación:

1. Enfoque acumulativo: Examina cómo se propaga el riesgo residual a través de los activos que dependen jerárquicamente del activo protegido
2. Enfoque repercutido: Analiza las consecuencias del riesgo residual en los activos superiores que tienen dependencia del activo en cuestión.

## 3.5. Método de Formalización de Actividades

El análisis de los riesgos se realiza por medio de las siguientes tareas:

| MAR – Método de Análisis de Riesgos |
| --- |
| MAR.1 – Caracterización de los activos |
| MAR.11 – Identificación de los activos |
| MAR.12 – Dependencias entre activos |
| MAR.13 – Valoración de los activos |
| MAR.2 – Caracterización de las amenazas |
| MAR.21 – Identificación de las amenazas |
| MAR.22 – Valoración de las amenazas |
| MAR.3 – Caracterización de las salvaguardas |
| MAR.31 – Identificación de las salvaguardas pertinentes |
| MAR.32 – Valoración de las salvaguardas |
| MAR.4 – Estimación del estado de riesgo |
| MAR.41 – Estimación del impacto |
| MAR.42 – Estimación del riesgo |

Fig. 7. Método de Análisis de Riesgos (MAR) Fuente: Magerit V.3[1]

### 3.5.1. Método de Análisis de Riesgos (MAR) 1: Caracterización de los activos

Esta fase fundamental del análisis de riesgos tiene como propósito principal:

1. Inventariar y clasificar todos los componentes significativos del sistema sujeto a evaluación
2. Establecer relaciones jerárquicas y funcionales entre los diferentes elementos identificados
3. Determinar el valor de cada activo en las distintas dimensiones de seguridad

Metodología de Trabajo

El proceso se estructura en tres subtareas clave:

1. MAR.11: Catalogación de Activos
   - Identificación exhaustiva de:
   - Componentes físicos (equipos, infraestructura)
   - Elementos lógicos (aplicaciones, bases de datos)
   - Recursos intangibles (información, reputación)
   - Capital humano (personal clave)
2. MAR.12: Análisis de Dependencias
   - Mapeo de interrelaciones entre activos
   - Identificación de:
   - Jerarquías funcionales
   - Flujos de información críticos
   - Puntos únicos de fallo
3. MAR.13: Valoración Estratégica
   - Evaluación multidimensional considerando:
   - Confidencialidad (grado de protección requerido)
   - Integridad (precisión y consistencia necesaria)
   - Disponibilidad (tiempos de operación críticos)
   - Otros factores (cumplimiento legal, impacto económico)

### 3.5.2. Método de Análisis de Riesgos (MAR) 2: Caracterización de las amenazas

Esta etapa busca hallar y analizar las posibles amenazas que podrían afectar al sistema en estudio; para ello mide:

- Su probabilidad de ocurrencia (frecuencia estimada)
- Su potencial de daño (grado de degradación que causarían)

Producto Principal:

Como resultado de este trabajo, se elabora el “Mapa de Riesgos”, un documento que ordena y prioriza las amenazas halladas según lo crítico que sean.

Subtareas Clave:

1. Tarea MAR.21: Identificación de Amenazas
   - Inventario exhaustivo de posibles escenarios de riesgo, considerando:
   - Amenazas externas (ciberataques, desastres naturales)
   - Amenazas internas (errores humanos, fallos técnicos)
   - Amenazas del entorno (cambios regulatorios, inestabilidad económica)
2. Tarea MAR.22: Valoración de Amenazas
   - Análisis cualitativo/cuantitativo para determinar:

Probabilidad: Basada en datos históricos, estadísticas sectoriales o juicio de expertos.

Impacto: Según la vulnerabilidad de los activos afectados y la magnitud del daño potencial.

### 3.5.3. Método de Análisis de Riesgos (MAR) 3: Caracterización de las salvaguardas

Esta fase del análisis busca hallar y valorar las medidas de protección aplicadas en el sistema en estudio; así fija su grado de eficacia para hacer frente a las amenazas halladas [1]. Como resultado de este trabajo, se generan tres documentos clave:

1. Declaración de Aplicabilidad
   - Listado de salvaguardas consideradas adecuadas para la protección del sistema.
2. Evaluación de Salvaguardas
   - Análisis de la eficacia real de las medidas existentes frente a los riesgos asociados.
3. Informe de Insuficiencias
   - Identificación de vulnerabilidades o carencias en el esquema de protección actual.

Subtareas Involucradas

- Tarea MAR.31: Identificación de Salvaguardas Relevantes

Consiste en inventariar y elegir los controles de seguridad desplegados; además, se comprueba que sean pertinentes frente a las amenazas registradas.

- Tarea MAR.32: Valoración de la Efectividad

Implica la calificación de cada salvaguarda según su capacidad real para:

  - Reducir la probabilidad de materialización de amenazas
  - Minimizar el impacto potencial sobre los activos
  - Cumplir con los estándares establecidos en el marco de seguridad

### 3.5.4. Método de Análisis de Riesgos (MAR) 4: Estimación del estado de riesgo

Esta etapa consiste en analizar toda la información reunida en las fases previas del análisis de riesgos, con el fin de:

1. Generar un informe detallado del estado de riesgo, que incluya:
   - La estimación del impacto (potencial y residual) asociado a cada activo y amenaza.
   - La evaluación del nivel de riesgo, considerando tanto la probabilidad de ocurrencia como la severidad del impacto.
2. Elaborar un informe de insuficiencias, identificando:
   - Deficiencias en las salvaguardas existentes, ya sea por su ausencia, implementación inadecuada o baja eficacia.
   - Vulnerabilidades críticas que requieran atención prioritaria.

Subtareas Clave

- Tarea MAR.41: Estimación del Impacto
  - Calcula las posibles consecuencias de una amenaza materializada sobre un activo, tanto en escenarios sin controles (impacto potencial) como con las salvaguardas aplicadas (impacto residual).
- Tarea MAR.42: Estimación del Riesgo
  - Combina el impacto estimado con la probabilidad de ocurrencia de las amenazas para determinar el nivel de riesgo asociado.

Dinámica de Ejecución

En la práctica, es común que las actividades relacionadas con:

- Identificación de activos (MAR.1)
- Análisis de amenazas (MAR.2)
- Evaluación de salvaguardas (MAR.3)

…se hagan de forma simultánea y no en secuencia, sobre todo cuando los equipos a cargo trabajan de manera integrada. Esto ocurre porque los responsables suelen analizar cada activo de forma "vertical"; revisan todos los aspectos que lo afectan (amenazas, controles, dependencias) antes de pasar al siguiente [1] Este enfoque facilita un entendimiento global y evita repeticiones al reunir la información.

## 3.6. Documentación

### 3.6.1. Documentación intermedia

El proceso de evaluación se apoya en varias fuentes de datos, que incluyen:

1. Resultados de Entrevistas
   - Información recopilada mediante consultas directas a personal clave, usuarios y responsables de sistemas.
2. Documentación Complementaria
   - Datos estadísticos: Registros históricos de incidentes, tasas de ocurrencia de amenazas, etc.
   - Opiniones de expertos: Evaluaciones cualitativas de especialistas en seguridad.
   - Hallazgos de los analistas: Observaciones derivadas de revisiones técnicas y auditorías.
3. Información Institucional Disponible
   - Documentación preexistente relevante, como:
   - Inventarios de activos actualizados
   - Registros de configuración de sistemas
   - Políticas y procedimientos internos
4. Material de Soporte Técnico y Operativo

- Planos y diagramas: Infraestructura física y lógica de sistemas.
- Organigramas: Estructura organizacional y roles.
- Requisitos y especificaciones: Normativas técnicas y funcionales.
- Manuales: Guías de usuario, operación y explotación de sistemas.
- Flujos de procesos: Diagramas de intercambio de información y procedimientos críticos.
- Modelos de datos: Estructuras de bases de datos y relaciones entre sistemas.

5. Reportes Externos de Vulnerabilidades

- Alertas y evaluaciones de fallos técnicos emitidas por:
- Fabricantes de software/hardware
- Centros de Respuesta a Incidentes (CERTs)
- Entidades especializadas en ciberseguridad

### 3.6.2. Documentación final

1. Modelo de Valor

Documento que halla y describe los activos críticos del sistema; abarca:

- Sus relaciones de dependencia
- Las dimensiones de valoración (confidencialidad, integridad, disponibilidad, etc.)
- La estimación cuantitativa o cualitativa de su importancia en cada dimensión

2. Mapa de Riesgos

Reporte que ordena las amenazas importantes ligadas a cada activo y las describe mediante:

- Frecuencia estimada de ocurrencia
- Grado de degradación que generarían si se materializaran
- Priorización basada en criticidad

3. Declaración de Aplicabilidad

Inventario de contramedidas elegidas para cuidar el sistema de información; justifica:

- Su idoneidad técnica frente a las amenazas identificadas
- Su alineación con los objetivos de seguridad de la organización

4. Evaluación de Salvaguardas

Análisis que valora la eficacia real de las medidas de protección aplicadas; toma en cuenta:

- Su capacidad probada para mitigar riesgos
- Brechas entre su eficacia teórica y operativa

5. Informe de Insuficiencias

Diagnóstico que revela:

- Salvaguardas faltantes en el sistema actual
- Controles existentes con eficacia limitada
- Recomendaciones para cerrar estas brechas

6. Estado de Riesgo

Documento clave que reúne, para cada activo:

- Impacto potencial (sin controles) vs. impacto residual (con controles)
- Niveles de riesgo asociados a cada amenaza
- Justificación técnica de por qué el riesgo residual sigue siendo inaceptable

### 3.7. Lista de Control

Tabla V Lista de control. Fuente: Magerit V.3[1]

| Actividad | Tarea |
|---|---|
| Se han identificado los activos esenciales: información que se trata y servicios que se prestan | MAR. 11 |
| Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad | MAR. 13 |
| Se han identificado los demás activos del sistema | MAR. 11 |
| Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, mediante identificación de las dependencias) | MAR. 12 |
| Se han identificado las amenazas posibles sobre los activos | MAR. 21 |
| Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas | MAR. 22 |
| Se ha estimado la probabilidad de que dichas amenazas se materialicen | MAR. 23 |
| Se han estimado los impactos y riesgos potenciales, inherentes al sistema | MAR. 4 |
| Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales | MAR. 31 |
| Se ha valorado el despliegue de las salvaguardas identificadas | MAR. 32 |
| Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas | MAR. 4 |

### 3.8. Incorporación de Normativas al Marco Propuesto

El marco de trabajo aplicado se rige por un conjunto de procedimientos y estándares elegidos en el campo de la Seguridad de la Información (SI) [5]. Se ha sumado

el cumplimiento de las siguientes normas y estándares concretos para asegurar una evaluación completa y acorde con las mejores prácticas reconocidas a nivel mundial [4], [11], [12]:

- MAGERIT v.3: este marco para el manejo de riesgos de la SI, creado por el Centro Criptológico Nacional (CCN) de España, se usa para reconocer, examinar y manejar los riesgos de seguridad. Sumar MAGERIT v.3 asegura una evaluación amplia de amenazas y debilidades; así se pueden ordenar las medidas correctivas según el riesgo [1]
- Ley Orgánica de Transparencia y Acceso a la Información Pública: Esta norma concreta se suma para cumplir los requisitos particulares de la cooperativa; así se asegura la conformidad con las reglas locales y con las necesidades propias del entorno de trabajo [5], [16]

Elegir estas normas y estándares se traduce en un enfoque completo para evaluar la seguridad; este abarca temas de auditoría, medición del desempeño y manejo de riesgos [18]. Esta combinación cumple los requisitos mundiales y fomenta buenas prácticas en la Seguridad de la Información, acorde con los mandatos de supervisión de riesgos tecnológicos que fija la SEPS [18].

# 4. CAPITULO IV

## 4.1.Guía

### 4.1.1. Introducción y Propósito

Este documento técnico constituye un instrumento de referencia dirigido al responsable de seguridad de la información; cuyo propósito central es facilitar la implementación estructurada de la metodología MAGERIT v.3 en el Core financiero de las cooperativas de ahorro y crédito. Sus lineamientos guardan coherencia con los estándares internacionales vigentes y con la normativa emitida por los organismos de supervisión del sector.

El análisis formal de riesgos tecnológicos cumple tres funciones concretas: establecer el perfil de riesgo real de la infraestructura, definir el orden de prioridad para la adopción de controles de seguridad, y elaborar la Declaración de Aplicabilidad requerida por la normativa. Los resultados obtenidos durante el proceso deberán documentarse conforme a los productos de salida descritos en secciones posteriores.

El ámbito de aplicación de esta guía comprende la totalidad de los componentes del Core financiero de la cooperativa, incluyendo la información, la base técnica, los datos y los procesos asociados a las operaciones financieras esenciales. El análisis contempla los activos clasificados bajo las cinco dimensiones de seguridad del esquema CIDAN, conforme al catálogo de elementos definido por la metodología seleccionada. El marco normativo que regula esta actividad integra las resoluciones sectoriales vigentes, los estándares internacionales de gestión de seguridad de la información y las directrices de auditoría aplicables.

Asimismo, se toman como referencia los tres volúmenes que conforman la metodología MAGERIT v.3: el libro de método, el catálogo de elementos y la guía de técnicas.

- Esta guía orienta al responsable de tecnología o seguridad de la información en la aplicación sistemática de la metodología MAGERIT v.3 para el análisis de riesgos del Core financiero en CAC de segmentos 2 y 3, reguladas por la SEPS.

- La guía se alinea con los requisitos del SGSI establecidos por la norma ISO/IEC 27001:2024 [7] y la resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 [4].
- El análisis de riesgos tecnológicos producido con esta guía sirve como insumo directo para: (a) la identificación del estado de riesgo actual de la infraestructura tecnológica, (b) la priorización de controles de seguridad, y (c) la elaboración de la Declaración de Aplicabilidad requerida por la norma ISO/IEC 27001:2024.
- Los resultados obtenidos deben documentarse conforme a los productos de salida definidos en la Sección 4.1.9 de esta guía.

### 4.1.2. Alcance y Marco Normativo

El presente instrumento metodológico es aplicable a todos los componentes del Core financiero de la cooperativa, entendiendo por tales los sistemas de información, la infraestructura tecnológica, los datos y los procesos que sostienen las operaciones financieras fundamentales: captaciones, colocaciones, contabilidad, pagos y canales de atención. Su alcance comprende los activos de información categorizados en las dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (CIDAN), de acuerdo con el catálogo de elementos de MAGERIT v.3 [2].

Los instrumentos normativos y técnicos que enmarcan la aplicación de esta guía son los siguientes: la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 (regulación de gestión de riesgos tecnológicos para el sector cooperativo) [4]; la norma ISO/IEC 27001:2024 (estándares para el Sistema de Gestión de Seguridad de la Información) [19]; la norma ISO/IEC 27005:2022 (marco para la gestión de riesgos de seguridad de la información)[19] ; la norma ISO/IEC 27007:2020 (lineamientos para la auditoría del SGSI) [11]; y la metodología MAGERIT v.3, compuesta por el Libro I: Método, el Libro II: Catálogo de Elementos y el Libro III: Guía de Técnicas [1], [2], [3]

### 4.1.3. Fase 1: Inventario y Valoración de Activos

Esta fase tiene como finalidad identificar, catalogar y valorar la totalidad de los activos del Core financiero que resultan significativos para la seguridad de la información. Se entiende por activo todo componente del sistema de información que represente valor

para la cooperativa y cuya pérdida, deterioro o vulneración pueda comprometer las operaciones financieras [1].

**MAR.11 — Catalogación de activos**

Por cada categoría de activo del Core financiero se documenta: código identificador único, denominación descriptiva, tipo de activo (según catálogo MAGERIT v.3: datos/información, servicios, software, hardware, comunicaciones, instalaciones, personal), responsable a cargo y descripción del rol que desempeña dentro de las operaciones financieras. La organización de los activos es jerárquica y refleja sus relaciones de dependencia: los activos de nivel superior (procesos de negocio) dependen de activos intermedios (servicios y software) los cuales, a su vez, se sustentan en activos base (hardware, comunicaciones e instalaciones) [1]

**MAR.12 — Dependencias entre activos**

Se elabora el grafo de dependencias que modela las interrelaciones existentes entre los activos del Core financiero. Esta representación gráfica permite trazar cómo el impacto generado sobre un activo base se transmite hacia los activos que dependen de él. La regla de propagación indica que, a mayor valor del activo padre y mayor coeficiente de dependencia, mayor será el impacto acumulado sobre el activo raíz del proceso financiero comprometido [1].

**MAR.13 — Valoración de activos**

Cada activo se evalúa en las cinco dimensiones del esquema CIDAN (Confidencialidad, Integridad, Disponibilidad, Autenticidad y No repudio/Trazabilidad), aplicando la escala de 10 niveles establecida por MAGERIT v.3 (de 0 = sin valor apreciable a 10 = daño muy grave a la organización) [1]. Esta valoración debe llevarse a cabo de manera conjunta con los propietarios de cada activo y el responsable del Core financiero. Con el fin de facilitar la recopilación de esta información, se utiliza el instrumento de diagnóstico detallado en la Sección 4.1.8.

### 4.1.4. Fase 2: Identificación y Valoración de Amenazas

Esta fase tiene por objeto determinar qué amenazas pueden concretarse sobre los activos inventariados, con qué probabilidad de ocurrencia y con qué grado de degradación

potencial. En el contexto del Core financiero de una CAC regulada, se priorizan las amenazas recogidas en el catálogo MAGERIT v.3 [2] relacionadas con: averías de origen industrial o tecnológico (interrupción del suministro eléctrico, fallo de equipos, degradación de medios de almacenamiento), amenazas deliberadas (acceso no autorizado, denegación de servicio, interceptación de comunicaciones y alteración de datos), y errores no intencionados (fallos operativos, configuraciones incorrectas y eliminación accidental de información) [1].

**MAR.21 — Identificación de amenazas aplicables**

Para cada activo identificado en la Fase 1, se establece el conjunto de amenazas aplicables conforme al catálogo MAGERIT v.3 [2] De cada amenaza se documenta: código, descripción, clasificación (natural, industrial, humana no intencionada o humana deliberada), activos que afecta y dimensiones CIDAN que compromete. Las amenazas de mayor relevancia para el Core financiero de las CAC comprenden especialmente:

[N.1] Fuego, [N.2] Daños por agua, [I.5] Avería de origen físico o lógico, [I.6] Corte del suministro eléctrico, [E.1] Errores de los usuarios, [E.2] Errores del administrador, [A.5] Suplantación de identidad, [A.11] Acceso no autorizado, y [A.24] Denegación de servicio [2].

**MAR.22 — Valoración de amenazas (frecuencia y degradación)**

Cada amenaza se cuantifica en dos dimensiones: (a) Probabilidad de ocurrencia, evaluada mediante la escala cualitativo-cuantitativa de la Tabla II del presente documento (MA=muy alta, A=alta, M=media, B=baja, MB=muy baja); y (b) Degradación potencial del activo afectado, expresada como porcentaje del valor del activo en la dimensión comprometida (100%, 50%, 10%, 1% o valor intermedio). La combinación de ambos parámetros determina el nivel de riesgo potencial, conforme a la matriz presentada en la Figura 5 [1].

### 4.1.5. Fase 3: Evaluación de Salvaguardas Existentes

El objetivo de esta fase consiste en determinar qué controles de seguridad están vigentes en la cooperativa y en qué medida contribuyen a la reducción del riesgo. Las salvaguardas se agrupan de acuerdo con las categorías establecidas por MAGERIT v.3 [1]: preventivas (PR), disuasorias (DR), eliminadoras del origen de la amenaza (EL),

minimizadoras del impacto (IM), correctivas (CR), de recuperación (RC), de monitorización (MN), de detección de intrusiones (DC), de concienciación (AW) y administrativas (AD). En el contexto del Core financiero de las CAC, revisten especial importancia las salvaguardas de tipo preventivo (PR), minimizador del impacto (IM) y de recuperación (RC).

**MAR.31 — Identificación de salvaguardas**

Para cada amenaza identificada en la Fase 2, se documentan los controles que la cooperativa tiene actualmente en operación. De cada salvaguarda se registra: categoría, descripción, amenazas que mitiga, activos que protege y dimensiones CIDAN que cubre. Este inventario deberá cotejarse con la Lista de Control de la Tabla V del presente documento, la cual consolida los controles mínimos requeridos por la Resolución SEPS y los dominios de la ISO/IEC 27001:2024 [7].

**MAR.32 — Valoración de eficacia y madurez**

Cada salvaguarda se analiza en dos dimensiones: (a) Eficacia: proporción en que disminuye la degradación o la probabilidad de ocurrencia de la amenaza vinculada (0% = sin efecto, 100% = elimina completamente el riesgo); y (b) Nivel de madurez, según la escala L0–L5 de la Tabla IV: L0 = inexistente, L1 = iniciado, L2 = reproducible, L3 = definido, L4 = gestionado, L5 = optimizado [1]. Las brechas detectadas —salvaguardas con madurez L0 o L1 frente a amenazas de alta probabilidad— constituyen el insumo principal para la elaboración del plan de tratamiento de riesgos.

### 4.1.6. Fase 4: Estimación del Estado de Riesgo

A partir de la información recopilada en las fases precedentes, se determinan el impacto potencial, el riesgo potencial, el impacto residual y el riesgo residual para cada combinación activo-amenaza. La diferencia entre riesgo potencial y riesgo residual reside en si se incorporan o no las salvaguardas implementadas: el riesgo potencial parte del supuesto de ausencia total de controles, en tanto que el riesgo residual considera la eficacia de los controles relevados en la Fase 3 [1].

**MAR.41 — Cálculo del impacto**

El impacto sobre un activo se obtiene mediante la fórmula: Impacto = Valor del activo (en la dimensión afectada) × Degradación potencial de la amenaza. Cuando un activo mantiene relaciones de dependencia con otros, el impacto se propaga hacia los activos superiores del grafo elaborado en MAR.12. Se obtienen dos valores diferenciados: impacto potencial (sin considerar controles) e impacto residual (incorporando la eficacia de los controles existentes). El impacto residual sobre los procesos del Core financiero representa el indicador clave de riesgo para la cooperativa [1].

**MAR.42 — Cálculo del riesgo y zonificación**

El nivel de riesgo resulta de la combinación entre impacto y probabilidad, y se distribuye en cuatro zonas de actuación conforme a la Figura 5 del documento: Zona 1 (riesgo crítico — alta probabilidad, alto impacto): requiere tratamiento inmediato; Zona 2 (riesgo elevado — franja de atención): requiere plan de mejora a corto plazo; Zona 3 (riesgo bajo — baja probabilidad y/o bajo impacto): se puede asumir o monitorear; Zona 4 (riesgo estratégico — bajo impacto, pero alta visibilidad gerencial): tratamiento según política de la cooperativa [1]. Para el Core financiero de las CAC bajo supervisión de la SEPS, la inclusión de todos los activos en Zona 1 en el plan de tratamiento es de carácter obligatorio.

### 4.1.7. Fase 5: Riesgo Residual y Plan de Tratamiento

El riesgo residual es aquel que subsiste una vez aplicadas las salvaguardas vigentes. Cuando este riesgo supera el umbral tolerable establecido por la organización (apetito de riesgo), resulta necesario incorporar nuevas salvaguardas o fortalecer las existentes. El plan de tratamiento recoge: (a) los riesgos objeto de intervención, (b) las salvaguardas propuestas para cada uno, (c) el responsable de su implementación, (d) el plazo previsto, y (e) el riesgo residual esperado tras su aplicación [1], [11].

La elección de nuevas salvaguardas deberá atender a su coherencia con los controles del Anexo A de la ISO/IEC 27001:2024 [7] y con los requisitos específicos de la Resolución SEPS para el sector cooperativo [15]. Entre las salvaguardas prioritarias para el Core financiero se destacan: controles de acceso lógico y físico, gestión de

vulnerabilidades, cifrado de datos sensibles de los socios, monitorización continua de sistemas críticos y planes de continuidad operativa para las operaciones financieras.

### 4.1.8. Resultados del Diagnóstico Organizacional

Como base para la aplicación de esta guía, se llevó a cabo un diagnóstico sobre el estado de la gestión de riesgos tecnológicos en cooperativas de ahorro y crédito de los segmentos 1, 2 y 3 ubicadas en la provincia de Pichincha y Carchi. Para ello se empleó un instrumento de encuesta dirigido a los encargados de tecnología de la información, oficial de seguridad de la información (OSI) y auditoria informática, de siete (7) cooperativas reguladas (COAC San Francisco de Asís Ltda., Luz Cooperativa, Cooperativa Cotocollao, Cooperativa Previsión Ahorro y Desarrollo COOPAD, Cooperativa Tulcán, Cooperativa 29 de Octubre Ltda. y Cooperativa Andalucia, con la finalidad de caracterizar el estado de sus prácticas de seguridad e identificar las principales brechas respecto a los requerimientos de la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 [4].




Fig. 8. Segmento al que pertenece la cooperativa

Fuente: Elaboración propia

La Fig. 8 presenta la distribución de las cooperativas participantes según el segmento al que pertenecen. El 61.5% pertenece a cooperativas del Segmento 2.Esta caracterización resulta esencial para contextualizar los hallazgos, dado que las

obligaciones normativas en materia de gestión de riesgos tecnológicos difieren según el segmento de cada entidad.

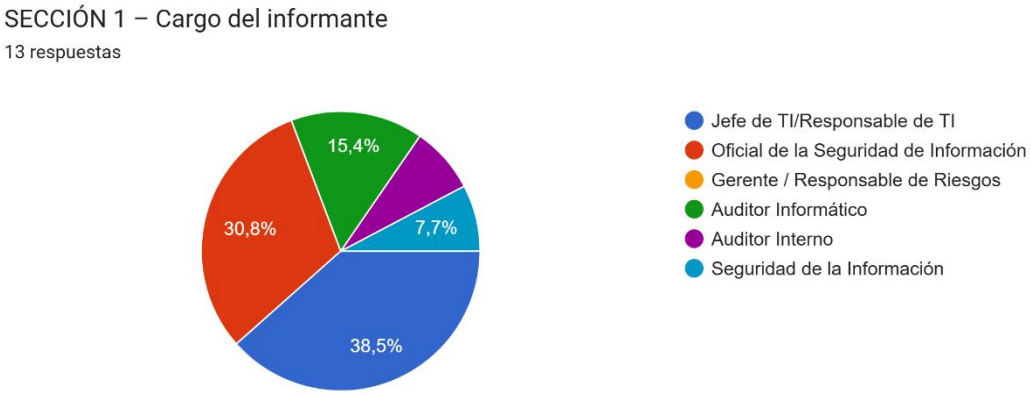



Fig. 9. Segmento al que pertenece la cooperativa

Fuente: Elaboración propia

La Fig. 9 complementa la figura anterior al mostrar la representación de los distintos segmentos en la muestra; entre los responsables generalmente es el Jefe de TI o Representante con un 38,5% después, las cooperativas tienen un Oficial de Seguridad de Información con un 30,8%, seguido de un Auditor informático con un 15,4% y encargado de Seguridad de la Información con un 7,7%. Este equilibrio refuerza la validez del diagnóstico y evidencia que las brechas en gestión de riesgos tecnológicos son comunes a los segmentos 2 y 3, lo que justifica el desarrollo de una guía metodológica única con capacidad de adaptarse a las características organizacionales y tecnológicas de cada entidad.



Fig. 10. Años de experiencia en el cargo

Fuente: Elaboración propia

La Fig. 10 refleja la experiencia acumulada de los responsables de tecnología e informática que respondieron el cuestionario. El 38.5% tienen 1 a 3 años en su cargo, el 23.1% tienen de 4 a 6 años en su cargo, el 15,4% tienen de 7 a 10 años en su cargo, el 15,4% tiene más de 10 años, y por último el 7,7% tiene menos de 1 año. Estos perfiles tienen experiencia significativa en el cargo garantiza que los hallazgos expresan una visión informada de la realidad operativa de cada institución.




Fig. 11. Líder de la función de Administración del Análisis de Riesgos de TI en la Cooperativa

Fuente: Elaboración propia

La Fig. 11 señala qué área o función asume la responsabilidad del análisis de riesgos de TI al interior de la cooperativa. El 61,5% tiene una Unidad de Seguridad de la Información/CISO, el 23,1% tiene una Oficina de Gestión de Riesgos (Enterprise Risk Management) y el 15,4% tiene Departamento de Tecnología/TI. Por lo tanto, contar con un responsable formalmente designado constituye un indicador relevante de madurez en la gobernanza tecnológica. Cuando esta función recae exclusivamente en el personal técnico de TI, aumenta la probabilidad de que el análisis se realice de manera reactiva y desvinculada de la estrategia institucional.

Los resultados de esta figura sirven de base para las recomendaciones de la guía en materia de asignación de roles y responsabilidades en el SGSI.

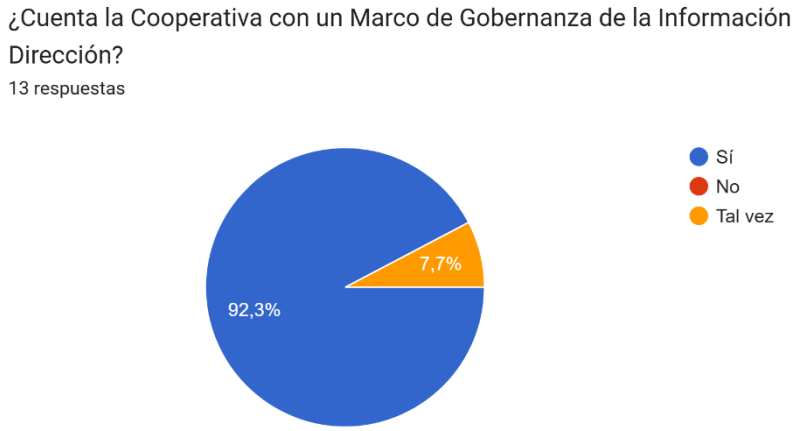



Fig. 12. Cooperativa con un Marco de Gobernanza de la Información aprobado por la Alta Dirección

Fuente: Elaboración propia

La Fig. 12 indica si la cooperativa dispone de un marco de gobernanza de la información aprobado formalmente por la alta dirección; el 92,3% tienen una respuesta afirmativa, y solo el 7,7% está en indecisión; la existencia de dicho marco es un requisito previo para la implementación efectiva del SGSI, ya que sin el compromiso explícito de la dirección los esfuerzos de seguridad suelen carecer de los recursos necesarios.

Los datos obtenidos ilustran el nivel de madurez institucional en este aspecto y fundamentan la incorporación, en la guía propuesta, de orientaciones específicas para sensibilizar a la alta dirección sobre la gestión de riesgos tecnológicos.




Fig. 13. Cooperativa cuenta actualmente con un Sistema de Gestión de Seguridad de la Información (SGSI) implementado

Fuente: Elaboración propia

La Fig. 13 muestra si la cooperativa cuenta con un Sistema de Gestión de Seguridad de la Información en funcionamiento. El 69,2% respondió que sí tienen un actual sistema de SGSI, por otor lado, el 30,8% tiene un SGSI aplicado de manera parcial. Esta variable tiene un peso determinante en el análisis, dado que la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 obliga a implementar un SGSI alineado con la norma ISO/IEC 27001:2024.

Los resultados permiten dimensionar la brecha entre el estado real de las entidades y las exigencias normativas actuales, constituyendo el argumento central que justifica la necesidad de la guía metodológica desarrollada en este trabajo.

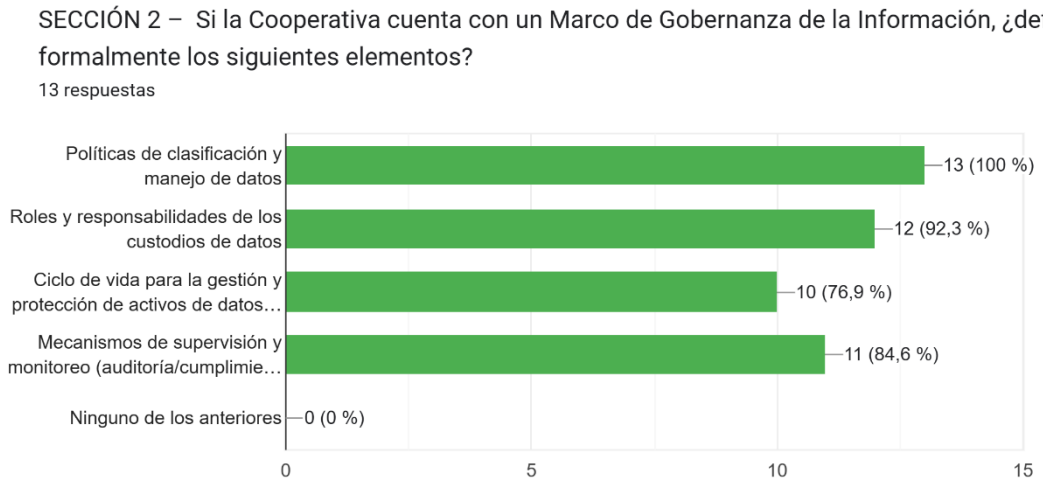



Fig. 14. Elementos gobernanza de la información

Fuente: Elaboración propia

La Fig. 14 detalla los elementos de gobernanza de la información que las cooperativas encuestadas han incorporado de manera formal. El 100% respondió que las políticas de clasificación y manejo de datos está presente formalmente en el Marco de Gobernanza de la normativa, el 92,3% tiene roles y responsabilidades de los custodios de datos, el 76,9% tiene un ciclo de vida para la gestión y protección de activos y el 84,6% tiene un mecanismo de supervisión y monitoreo.

La gobernanza de la información abarca políticas, roles, procesos y métricas que garantizan una gestión de los activos coherente con los objetivos institucionales y los requisitos regulatorios; la diversidad en la adopción de estos componentes evidencia la necesidad de una guía que defina un punto de partida claro y escalonado para la implementación de cada elemento del SGSI.

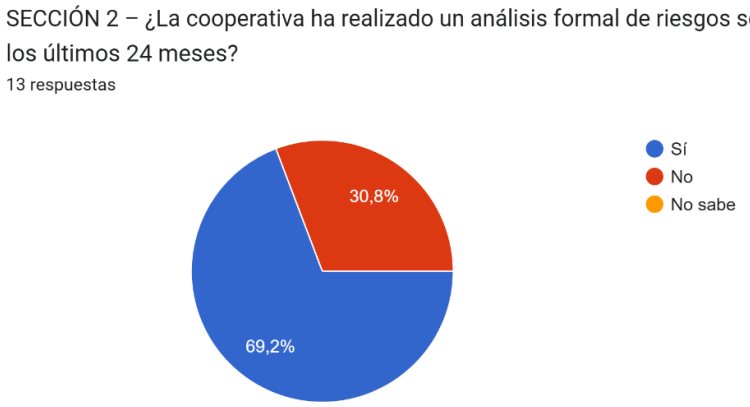



Fig. 15. Análisis de riesgos en 24 meses

Fuente: Elaboración propia

La Fig. 15 indica si la cooperativa ha realizado un análisis de riesgos tecnológicos en los últimos 24 meses, período de referencia establecido por la normativa de la SEPS. El 30,8% de los resultados muestran que no se ha realizado un análisis de riesgos en los últimos 24 meses.

La ausencia de un análisis reciente es un hecho crítico, ya que implica que la entidad desconoce su perfil de riesgo actual y no puede asegurar la protección de los activos del Core financiero ante las amenazas vigentes. Los resultados confirman la brecha diagnóstica que sustenta la propuesta de esta guía y justifican la periodicidad mínima de análisis establecida en sus fases metodológicas.

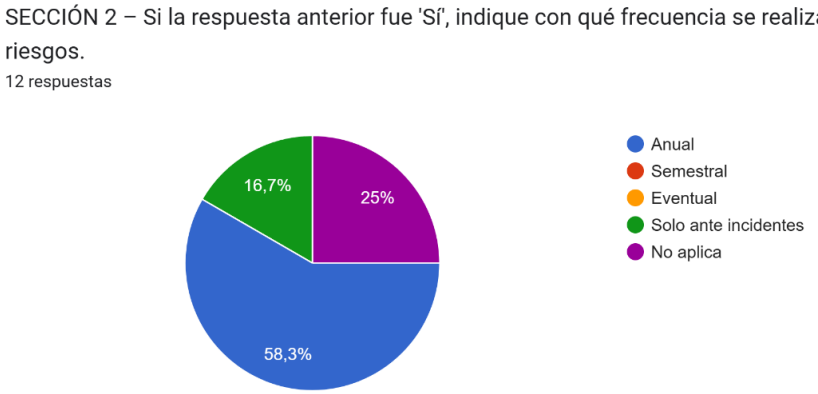



Fig. 16. Frecuencia análisis de riesgos

Fuente: Elaboración propia

La Fig. 16 muestra la periodicidad con que las cooperativas ejecutan el análisis de riesgos tecnológicos. La frecuencia con que se realiza esta actividad es un indicador directo del nivel de madurez en gestión de riesgos; entre el 69,2% que respondió que sí en la Fig. 15 tiene una periodicidad de análisis de riesgos, el 58,3% tiene un análisis anual, el 16.7% tiene un análisis en solo incidentes y el 25% dicen que no aplica, debido a que el periodo puede realizarse cada 24 meses.

La irregular información denota un enfoque reactivo, en tanto que la revisión sistemática (con una frecuencia mínima anual conforme a la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002) es expresión de una gestión proactiva y alineada con los estándares internacionales. Los datos obtenidos fundamentan las recomendaciones de la guía en cuanto a la planificación y calendarización del ciclo de análisis de riesgos en el SGSI.

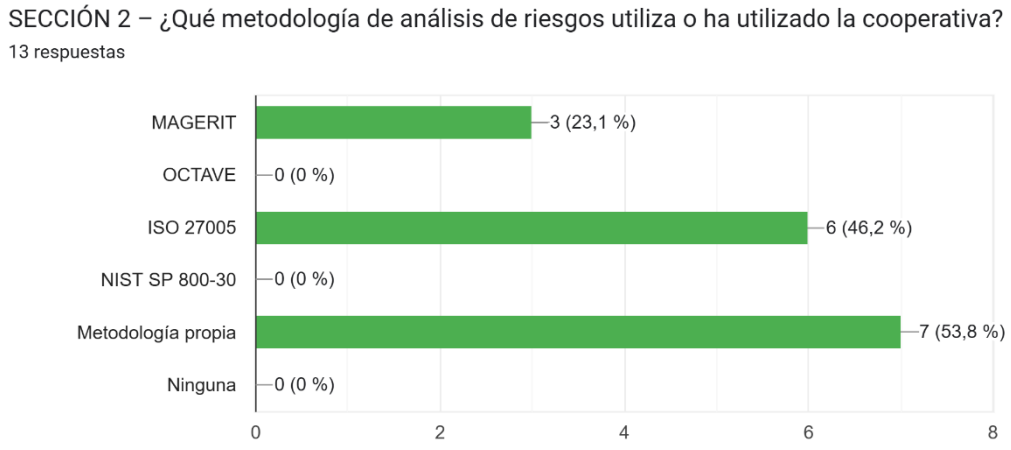



Fig. 17. Metodologías de análisis de riesgos

Fuente: Elaboración propia

La Fig. 17 revela las metodologías de análisis de riesgos que las cooperativas encuestadas emplean en la actualidad. El 23,1% respondió que usa MAGERIT, el 46,2% indicó que usa la norma ISO 27005 y el 53.8% tiene una metodología propia.

La dispersión o inexistencia de metodologías estandarizadas pone de manifiesto la falta de un enfoque uniforme en el sector; la adopción de MAGERIT v.3 como

metodología de referencia en esta guía responde precisamente a esa necesidad, por tratarse de un marco estructurado, de acceso libre y ampliamente reconocido en el contexto.

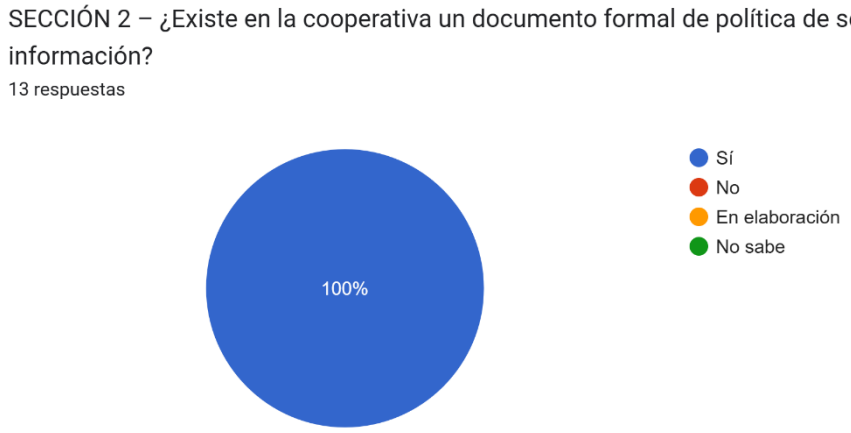



Fig. 18. Existencia de documento de política de seguridad de la información

Fuente: Elaboración propia

La Fig. 18 indica si las cooperativas cuentan con un documento formal de política de seguridad de la información. El 100% respondió que si lo tiene. La política de seguridad es el documento rector del SGSI; sin ella, los controles implementados carecen de sustento normativo interno y resultan difíciles de auditar y mantener a lo largo del tiempo. La norma ISO/IEC 27001:2024 define esta política como un requisito obligatorio en su cláusula 5.2.

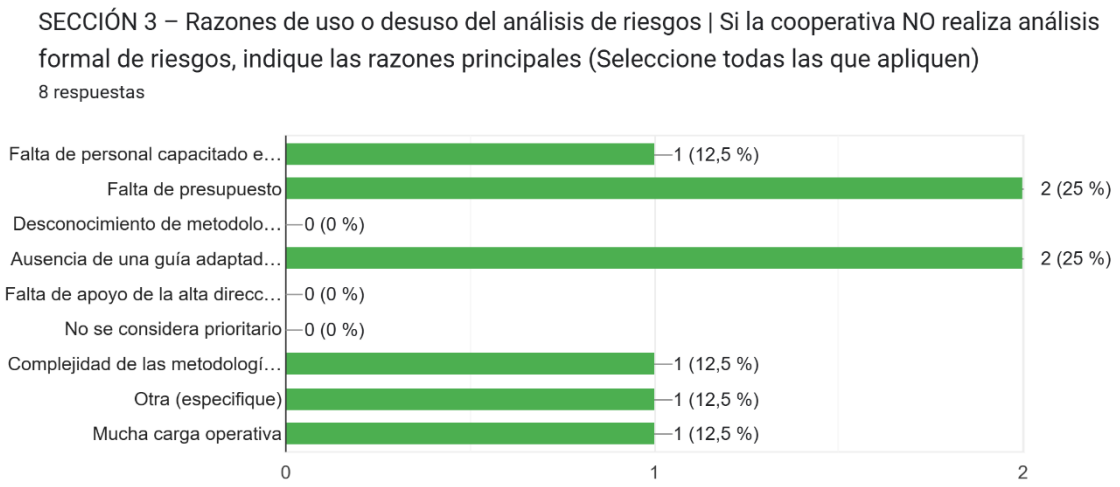



Fig. 19. Razones desuso de análisis de riesgos

Fuente: Elaboración propia

La Fig. 19 presenta los motivos por los cuales algunas cooperativas no llevan a cabo análisis de riesgos de manera sistemática. El 12,5% dijo que hay una falta de personal capacitado, el 25% respondió que existe una ausencia de una guía adaptada, el 12.5% dice que existe una complejidad de las metodologías, el 12,5% también indico que exige mucha carga operativa, entre otras razones.

Entre los factores más recurrentes se destacan la escasez de personal especializado, el desconocimiento de metodologías apropiadas, la falta de herramientas adecuadas y la percepción de que el análisis de riesgos requiere recursos que la entidad no puede destinar. Conocer estas barreras es indispensable para diseñar una guía práctica, accesible y orientada a superar los obstáculos reales que enfrentan las cooperativas de los segmentos 2 y 3 en su proceso de cumplimiento normativo.

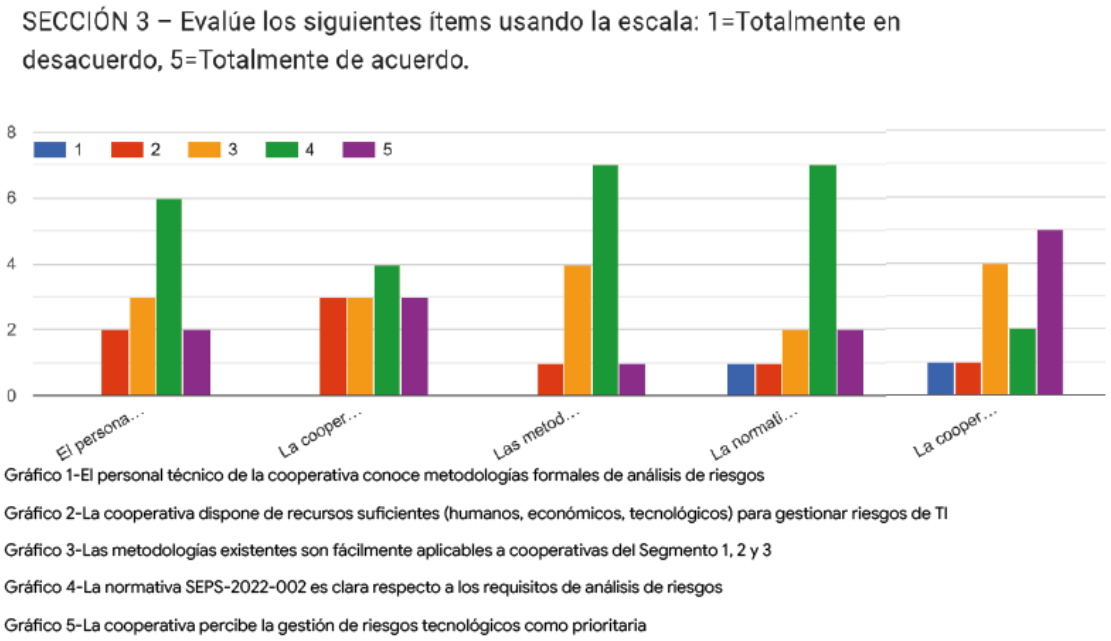



Fig. 20. Evaluación de conocimientos, recursos, metodologías aplicables, y claridad normativa SEPS 2022-002

Fuente: Elaboración propia

La Fig. 20 examina de manera conjunta el nivel de conocimiento sobre metodologías aplicables, la disponibilidad de recursos y la comprensión de los requerimientos de la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002. Existe un mutuo acuerdo de 4 en una escala de 1 a 5 de que el personal técnico de la cooperativa conoce las metodologías formales de análisis de riesgos. También en la escala de 4-Acuerdo destaca más que la cooperativa dispone de recursos suficiente, que las medidas metodológicas existentes son fácilmente aplicables y que la normativa es clara en el análisis de riesgos, a diferencia del último gráfico que, generalmente los encuestados están en la escala de 5-Muy de acuerdo con que cada cooperativa percibe la gestión prioritaria de riesgos tecnológicos

Una puntuación baja en cualquiera de estos tres ejes identifica áreas prioritarias de intervención: si el equipo desconoce la normativa, la formación es urgente; si los recursos son escasos, la guía debe ofrecer soluciones de bajo costo; y si las metodologías son desconocidas, la guía paso a paso se convierte en el principal valor agregado del instrumento propuesto.

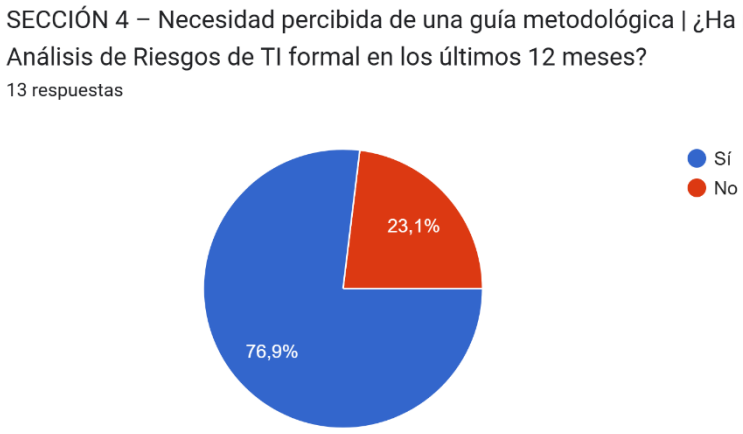



Fig. 21. Necesidad percibida de una guía metodológica

Fuente: Elaboración propia

La Fig. 21 recoge la opinión de los encuestados sobre la necesidad de disponer de una guía metodológica específica para el análisis de riesgos tecnológicos en el Core financiero cooperativo. En los últimos 12 meses sí se ha realizado un análisis de riesgos en el 76,9% de los casos, por el contrario, el 23,1% no lo ha realizado.

Un elevado nivel de acuerdo en esta variable valida directamente la pertinencia del presente trabajo: los propios actores del sector reconocen que la ausencia de un instrumento de estas características representa una de las principales limitaciones para alcanzar el nivel de madurez requerido por la SEPS.

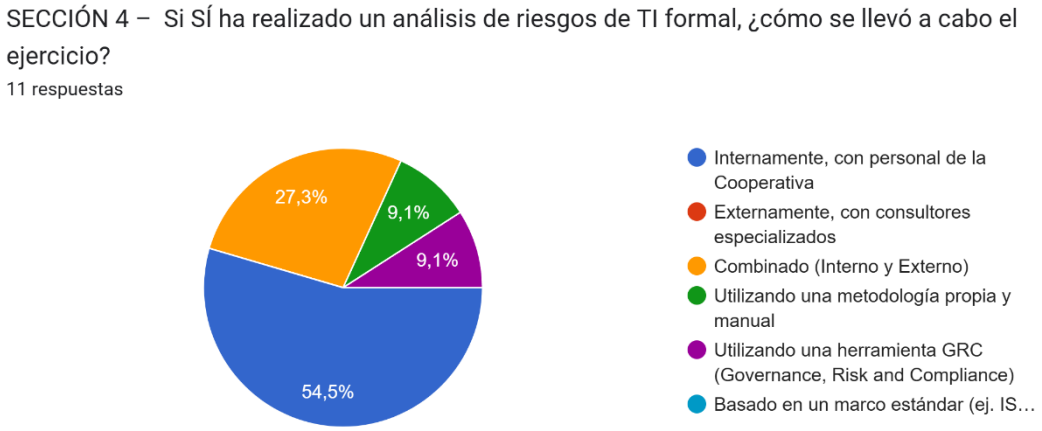



Fig. 22. Modo de análisis de riesgos de TI formal en las cooperativas

Fuente: Elaboración propia

La Fig. 22 ilustra la modalidad bajo la cual las cooperativas ejecutan el análisis de riesgos de TI (ya sea de forma interna con personal propio, mediante consultoría externa, a través de auditorías periódicas ante incidentes). Sobre cómo se llevó a cabo el ejercicio, el 54,5% dice que se lo realizó de manera interna, el 27,3% dice que fue un esfuerzo combinado (interno-externo) el 9,1% utilizaron una metodología propia y manual, y el 9,1% utilizaron una herramienta GRC (Governance, Risk and Compliance).

Identificar la modalidad predominante es relevante para valorar el nivel de apropiación institucional del proceso y para definir, en la guía, los perfiles de usuario y las responsabilidades de cada fase del análisis, con el fin de que el instrumento resulte aplicable tanto para equipos internos como con el apoyo de consultores externos.

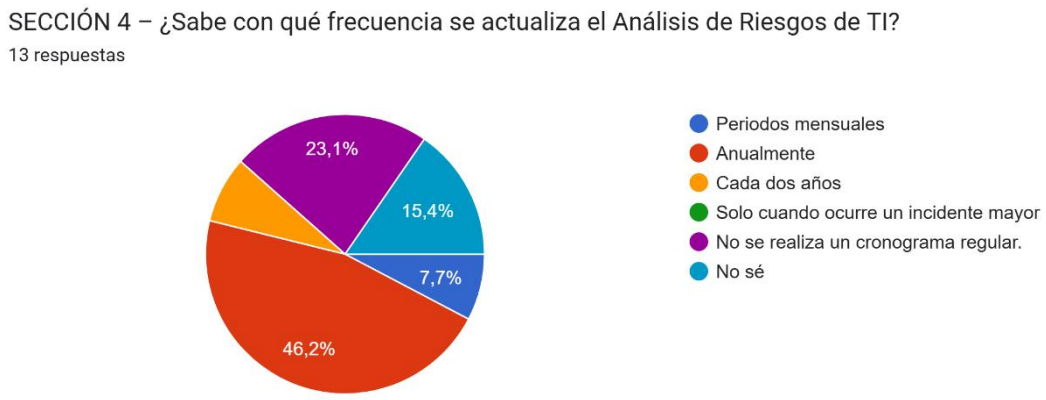



Fig. 23. Frecuencia de análisis de riesgos de TI formal en las cooperativas

Fuente: Elaboración propia

La Fig. 23 complementa la Fig. 16 al centrarse en la periodicidad con que se realiza un análisis de riesgos de TI formal, con metodología definida y productos de salida verificables; el 46,2% respondió que se lo realiza anualmente, el 23,1% que no se realiza en un cronograma regular, el 15,4% no sabe y el 7,7% respondió que en periodos mensuales. La diferencia entre análisis informal y formal es significativa.

Muchas entidades efectúan revisiones informales o puntuales que no generan evidencias auditables ni se articulan con el ciclo de mejora del SGSI. Los datos de esta

figura permiten identificar cuántas cooperativas han institucionalizado el proceso y cuántas necesitan apoyo para avanzar hacia una práctica formal y sostenida.

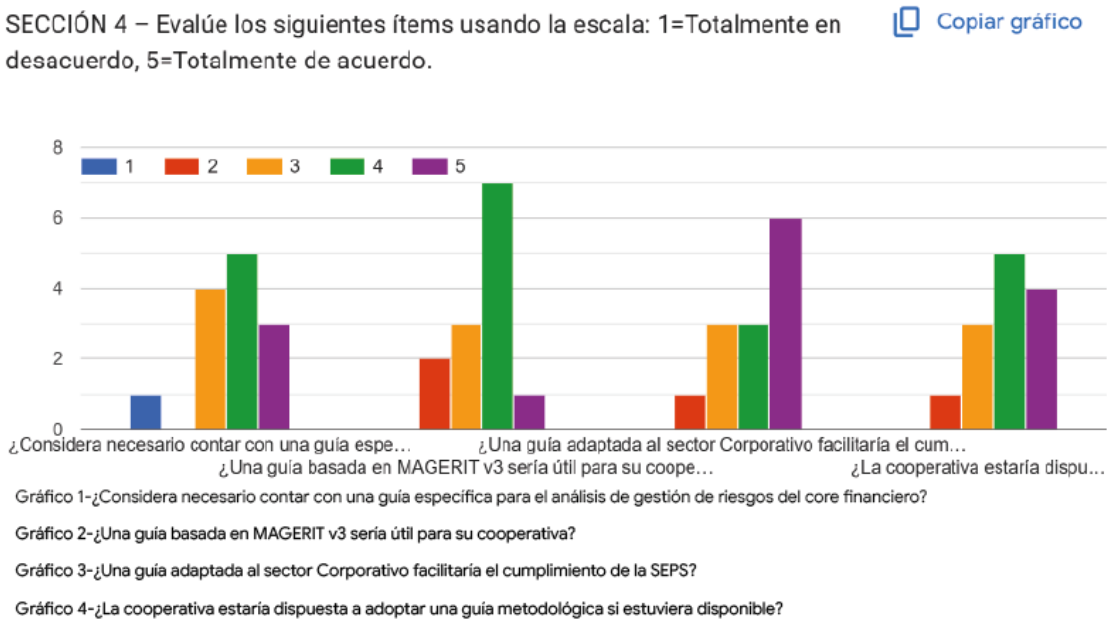



Fig. 24. Evaluación de necesidad de guía, base en Magerit V.3, adaptación al sector corporativo y disposición de adoptar guía metodológica.

Fuente: Elaboración propia

La Fig. 24 resume la valoración de los encuestados en cuatro dimensiones clave: la necesidad de una guía metodológica, la conveniencia de fundamentarla en MAGERIT v.3, la importancia de adaptar el instrumento al sector cooperativo y la predisposición institucional para adoptarlo. Generalmente se está en una escala de 4-5 Acuerdo-Muy de Acuerdo a que se considere necesario contar con una guía específica para el análisis de riesgos en el Core financiero, igualmente el considerar una guía basada en MAGERIT v.3, además de una guía adaptada al sector Corporativo para el cumplimiento de la SEPS y sus normas, y también estarían de acuerdo en adoptar una guía metodológica si estuviera disponible.

La confluencia positiva en estas cuatro variables constituye un respaldo sólido a la propuesta presentada en este trabajo, confirmando que la guía responde a necesidades reales del sector y que existe voluntad institucional favorable para su implementación.

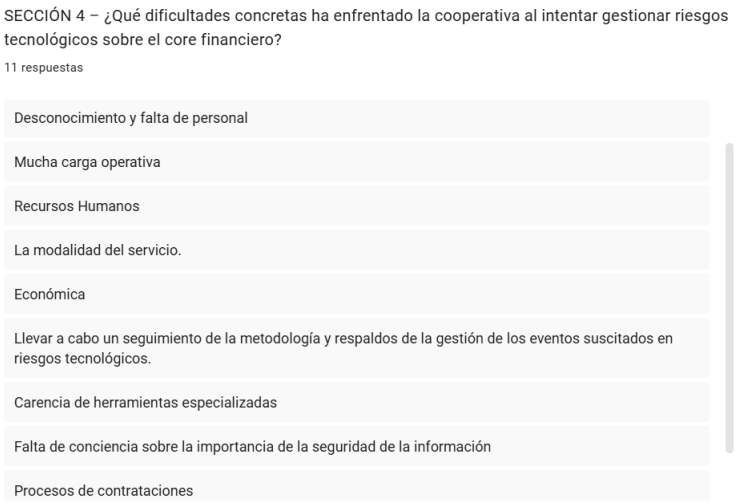



Fig. 25. Dificultades concretas ha enfrentado la cooperativa al intentar gestionar riesgos tecnológicos

Fuente: Elaboración propia

La Fig. 25 registra las dificultades específicas que las cooperativas han afrontado al gestionar los riesgos tecnológicos de su Core financiero. Los obstáculos más recurrentes incluyen la carencia de personal con formación especializada, la ausencia de herramientas tecnológicas adecuadas, la escasez de tiempo y de recursos económicos, y la falta de claridad sobre los requisitos normativos. Estos hallazgos son de especial utilidad para el diseño de la guía, ya que cada una de sus fases ha sido concebida para ofrecer respuestas prácticas a las barreras aquí identificadas.




Fig. 26. Incidentes y exposición

Fuente: Elaboración propia

La Fig. 26 refleja el nivel de exposición a incidentes de seguridad tecnológica declarado por las cooperativas encuestadas. La exposición a incidentes constituye un indicador directo del riesgo operativo de estas entidades y uno de los argumentos más sólidos para justificar la implementación inmediata de un SGSI; un alto volumen de incidentes sin un protocolo formal de gestión eleva el riesgo de pérdidas financieras, daño reputacional y sanciones regulatorias por parte de la SEPS.

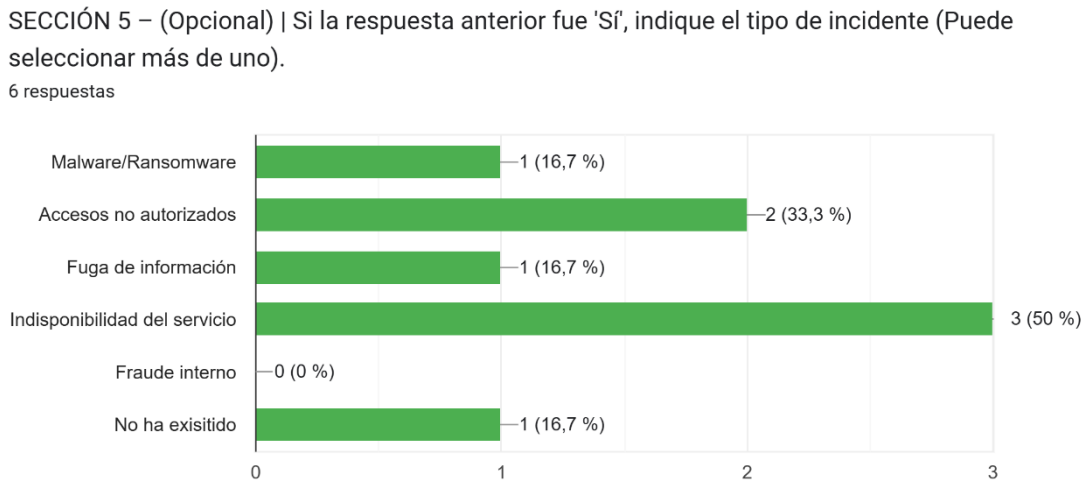



Fig. 27. Tipo de incidente

Fuente: Elaboración propia

La Fig. 27 categoriza los tipos de incidentes de seguridad tecnológica que han impactado a las cooperativas participantes. La tipología de los incidentes: fallas de disponibilidad, accesos no autorizados, pérdida de integridad de datos o amenazas externas; determina qué dimensiones del esquema CIDAN (Confidencialidad, Integridad, Disponibilidad, Autenticidad y No repudio) son más críticas para el sector y, por consiguiente, qué controles deben priorizarse en el Plan de Tratamiento de Riesgos. Estos datos refuerzan la validez del enfoque multidimensional adoptado por la guía propuesta.

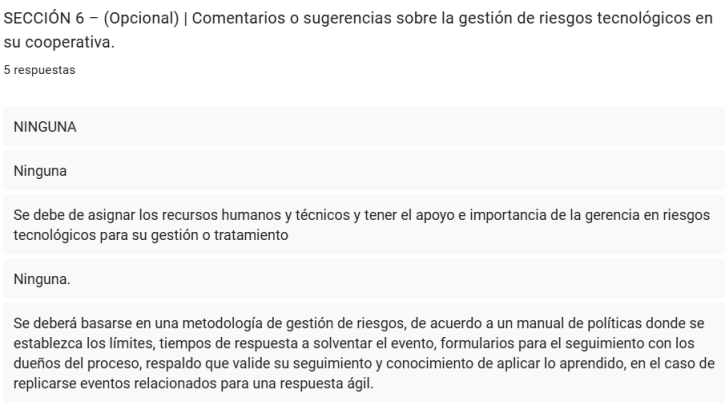



Fig. 28. Comentarios o sugerencias sobre la gestión de riesgos tecnológicos

Fuente: Elaboración propia

La Fig. 28 recopila los comentarios y sugerencias expresados por los encuestados en torno a la gestión de riesgos tecnológicos en sus cooperativas. Estas observaciones cualitativas enriquecen el diagnóstico y evidencian una necesidad transversal de orientación metodológica, respaldo de la alta dirección y recursos suficientes. Se recomienda asignar personal y apoyo en la gerencia de riesgos tecnológicos, además de que debe implementar un manual o guía donde se establezcan límites, tiempos de respuesta a solventar tras incidente, formularios de seguimiento, documentación de respaldo, en caso de aplicar lo aprendido en futuros eventos.

En conjunto, los hallazgos del diagnóstico organizacional confirman que existe una necesidad urgente y una voluntad institucional favorable para implementar una gestión de riesgos tecnológicos estructurada; lo cual valida plenamente la guía propuesta en el presente trabajo de titulación.

### 4.1.9. Productos de Salida del Análisis de Riesgos

La ejecución de las cinco fases contempladas en esta guía genera los siguientes documentos de salida, que constituyen los entregables formales del análisis de riesgos tecnológicos y alimentan directamente el SGSI de la cooperativa [1]:

Modelo de Valor: inventario de activos valorados en las cinco dimensiones CIDAN, con el grafo de dependencias del Core financiero.

Mapa de Riesgos: matriz que combina probabilidad e impacto para cada par activo-amenaza, con la zonificación de riesgo (Zonas 1 a 4).

Evaluación de Salvaguardas: inventario de controles existentes con su nivel de eficacia y madurez (L0–L5), identificando brechas respecto a los requerimientos normativos.

Informe de Insuficiencias: lista priorizada de controles faltantes o insuficientes, con estimación del riesgo residual si no se implementan.

Estado de Riesgo Residual: síntesis del nivel de riesgo que subsiste tras las salvaguardas existentes, expresado por activo, por proceso financiero y por dimensión CIDAN.

Plan de Tratamiento de Riesgos: cronograma de implementación de nuevas salvaguardas, con responsables, plazos y riesgo residual esperado, alineado con el Anexo A de ISO/IEC 27001:2024 [7] y la Resolución SEPS [4].

Declaración de Aplicabilidad (SoA): documento formal requerido por ISO/IEC 27001:2024 que enumera los controles aplicables, su justificación de inclusión o exclusión y su estado de implementación.

Estos documentos deberán archivarse y mantenerse actualizados como parte del sistema documental del SGSI. La frecuencia mínima de revisión es anual, o ante cambios significativos en la infraestructura del Core financiero, modificaciones en la normativa de la SEPS, o incidentes de seguridad que comprometan activos de la cooperativa [6], [11].

## 4.2. Hallazgos en la Provincia de Pichincha y Carchi

### 4.2.1. Análisis de la Situación Actual

Como punto de partida del estudio, se examinó el estado de la gestión de riesgos tecnológicos en siete cooperativas de la provincia de Pichincha y Carchi. Para ello se aplicó un cuestionario a los responsables de sistemas y seguridad, con el propósito de caracterizar sus prácticas e identificar las brechas respecto a la normativa vigente. Los resultados revelan el segmento al que pertenecen las entidades participantes; este dato es relevante dado que las obligaciones regulatorias varían en función del segmento. La diversidad de los participantes fortalece la validez de los resultados y confirma que las brechas en gestión de riesgos tecnológicos son comunes a distintos tipos de entidades, lo que justifica el diseño de un instrumento único adaptable a diferentes estructuras organizacionales.

El cuestionario incluyó la medición de la experiencia laboral de los responsables de sistemas que respondieron. La participación de profesionales con amplia trayectoria asegura que los datos reflejan una visión clara de la realidad operativa de las instituciones. Asimismo, se indagó qué área lidera el análisis de riesgos de TI; contar con un responsable formalmente designado es un indicador de madurez en la gobernanza institucional. Cuando esta función recae exclusivamente en el personal técnico, se incrementa el riesgo de adoptar un enfoque reactivo y desvinculado de la estrategia institucional. Estos hallazgos orientan las recomendaciones de la guía en materia de asignación de roles y responsabilidades dentro del SGSI.

### 4.2.2. Resultados y Decisiones del Estudio

Los resultados indican si la entidad dispone de un marco de gobernanza de la información aprobado formalmente por la alta dirección. El respaldo de la dirección es un prerrequisito para el funcionamiento efectivo del SGSI; sin ese compromiso, las iniciativas de seguridad suelen carecer de los recursos necesarios. Los resultados evidencian el nivel de madurez institucional y fundamentan la inclusión, en la guía, de orientaciones para sensibilizar a la alta dirección sobre la importancia de la gestión de riesgos tecnológicos. Una proporción significativa de los encuestados declara contar con un SGSI implementado total o parcialmente, lo que permite dimensionar la brecha respecto a las exigencias normativas vigentes.

Las cooperativas describen los elementos de gobernanza de la información que aplican en sus operaciones cotidianas. Este ámbito comprende políticas, roles y procesos que garantizan que la gestión de la información esté alineada con los objetivos institucionales. La heterogeneidad en la adopción de estos elementos confirma la necesidad de una guía que establezca un punto de partida claro para la implementación del SGSI. Los resultados indican si las cooperativas han realizado un análisis de riesgos en los últimos 24 meses; la ausencia de un análisis reciente implica que la entidad desconoce su perfil de riesgo actual y no puede garantizar la protección adecuada de su Core financiero.

### 4.2.3. Problemas Comunes y Necesidades

El estudio muestra la periodicidad con que las cooperativas realizan revisiones de sus riesgos tecnológicos. Una revisión frecuente refleja un nivel adecuado de madurez en

la gestión de riesgos; la normativa exige que esta actividad se realice al menos una vez al año. Los datos obtenidos orientan la planificación y calendarización del ciclo de análisis de riesgos dentro del SGSI. Adicionalmente, se identifican las metodologías que las cooperativas utilizan actualmente. La ausencia de un enfoque estandarizado evidencia la falta de homogeneidad en el sector; la adopción de MAGERIT v.3 responde a esta necesidad por ser una metodología estructurada, de acceso libre y ampliamente reconocida en el contexto hispanohablante.

La mayoría de las entidades dispone de un documento formal de política de seguridad de la información. Este instrumento es el fundamento del SGSI: sin él, los controles implementados carecen de sustento normativo interno y resultan difíciles de auditar con el tiempo. El estudio también examina los motivos por los que no se realizan estos análisis de forma sistemática. Entre las razones más frecuentes destacan la escasez de personal especializado, el desconocimiento de metodologías apropiadas y la percepción de que el proceso demanda recursos que la entidad no puede destinar. Conocer estas barreras es clave para diseñar una guía práctica y accesible que permita superar los obstáculos reales de las organizaciones.

#### 4.2.4. Validaciones y Conclusiones del Diagnóstico

El diagnóstico evalúa el nivel de conocimiento del personal, la disponibilidad de recursos y la comprensión de los requisitos normativos vigentes. Una puntuación baja en alguno de estos aspectos señala áreas de intervención prioritaria: si el conocimiento es insuficiente, la capacitación es urgente; si los recursos escasean, la guía debe ofrecer soluciones de bajo costo. Los encuestados identifican como una necesidad prioritaria contar con una guía específica para la gestión de riesgos del Core financiero. Esto respalda la pertinencia del presente trabajo; los actores del sector reconocen que la ausencia de un instrumento de este tipo limita su capacidad para alcanzar el nivel de madurez exigido por el organismo de control.

El estudio describe la modalidad bajo la cual las cooperativas llevan a cabo sus análisis de riesgos de TI. Conocer si emplean personal propio o consultoría externa permite adaptar la guía para que sea útil a ambas modalidades. Asimismo, se distingue entre un análisis informal y un análisis formal con productos de salida documentados. Numerosas entidades realizan revisiones puntuales que no generan evidencias auditables

verificables. Los resultados finales confirman la urgencia de implementar la metodología propuesta y la disposición favorable de las instituciones para adoptarla.

Las cooperativas reportan dificultades como la escasez de personal dedicado, la carga operativa diaria y la limitación de recursos económicos. La guía aborda estas dificultades ofreciendo respuestas prácticas a cada una de ellas. Finalmente, los datos revelan que varias cooperativas han sufrido incidentes de seguridad en los últimos dos años. Esta exposición a incidentes constituye un argumento contundente para implementar el SGSI de manera inmediata. Los incidentes más frecuentes son los ciberataques, los accesos no autorizados y las interrupciones del servicio; estos datos señalan qué activos y dimensiones deben priorizarse en el plan de tratamiento de riesgos.

### 4.2.5. Entregables Formales del Análisis

La aplicación de las fases contempladas en esta guía produce los siguientes documentos formales, que constituyen la base del Sistema de Gestión de Seguridad de la Información:

**Modelo de Valor:** Inventario de activos valorados en las cinco dimensiones CIDAN, acompañado del grafo de dependencias del Core financiero.

**Mapa de Riesgos:** Matriz que combina probabilidad e impacto para cada par activo-amenaza, con la zonificación de riesgo en cuatro categorías.

**Evaluación de Salvaguardas:** Inventario de los controles vigentes con su nivel de eficacia y grado de madurez (L0–L5), e identificación de brechas respecto a los requerimientos normativos.

**Informe de Insuficiencias:** Relación priorizada de controles faltantes o insuficientes, con la estimación del riesgo residual en caso de no implementarse.

**Estado de Riesgo Residual:** Síntesis del nivel de riesgo remanente en la entidad, expresado por activo y por dimensión de seguridad.

**Plan de Tratamiento:** Cronograma de implementación de nuevas salvaguardas, con responsables, plazos y riesgo residual esperado, alineado con el Anexo A de la ISO/IEC 27001:2024 y la Resolución SEPS.

**Declaración de Aplicabilidad:** Documento formal requerido por la ISO/IEC 27001:2024 que enumera los controles aplicables, su justificación de inclusión o exclusión y su estado de implementación.

Todos estos documentos deberán archivarse adecuadamente y actualizarse ante cambios significativos en la infraestructura tecnológica, en la normativa vigente o como consecuencia de incidentes de seguridad.

### 4.3. Recomendaciones para la ejecución de la guía

La formalización documental del análisis de riesgos representa uno de los pilares más importantes dentro del proceso de gestión de la seguridad de la información; sin ella, los resultados obtenidos carecen de trazabilidad, validez académica y utilidad operativa. MAGERIT v3 establece con claridad que todo proceso de análisis de riesgos debe generar productos documentales concretos: desde el Modelo de Valor y el Mapa de Riesgos hasta la Evaluación de Salvaguardas, el Informe de Insuficiencias y el Estado de Riesgo [1].

En el contexto de la guía, la documentación no cumple únicamente una función técnica; cumple además una función académica y probatoria, pues demuestra la rigurosidad del proceso aplicado, la coherencia metodológica alcanzada y la posibilidad de que el trabajo sea replicado o auditado por terceros. Este subcapítulo presenta las recomendaciones para registrar cada fase del análisis de riesgos realizado con técnicas MAGERIT en la Cooperativa de Ahorro y Crédito objeto de estudio, de forma que los documentos generados respondan tanto a los estándares normativos vigentes ISO/IEC 27001:2024 [7], ISO/IEC 27005:2022 [19] y la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002 [4].

#### 4.3.1. Principios Generales para la Documentación del Análisis de Riesgos

El Libro I de MAGERIT v3 señala que el análisis de riesgos debe quedar registrado de manera ordenada y verificable, de modo que cualquier parte interesada pueda seguir el camino que llevó de los datos de entrada hasta las conclusiones del estudio [1]. Esa exigencia se traduce en la obligación de dejar constancia escrita de cada decisión metodológica adoptada: los criterios con que se clasificaron los activos, la escala de valoración utilizada para ponderarlos, las fuentes consultadas para estimar la frecuencia de las amenazas y el procedimiento seguido para calificar la eficacia de cada salvaguarda.

Documentar estas decisiones no es un trámite burocrático; es la condición que permite que el trabajo sea sometido a escrutinio académico y que sus resultados puedan ser contrastados con estudios similares realizados en otras cooperativas del mismo segmento. Adicionalmente, la ISO/IEC 27005:2022 indica que los registros del proceso de evaluación de riesgos deben conservarse como evidencia del tratamiento aplicado, lo que otorga al documento un valor probatorio ante cualquier revisión normativa posterior [19].

Desde el punto de vista académico, la documentación del análisis de riesgos debe satisfacer al menos tres criterios fundamentales: completitud, coherencia y reproducibilidad. La completitud exige que no quede ningún activo, amenaza o control sin registro, por más que su valoración sea mínima; la coherencia demanda que los valores asignados en distintas fases del análisis sean compatibles entre sí, de modo que el riesgo potencial calculado en el MAR.2 sea directamente comparable con el riesgo residual estimado en el MAR.4 [1]; y la reproducibilidad implica que otro investigador, con acceso a los mismos datos y al mismo protocolo, llegue a resultados equivalentes.

Cumplir estos tres criterios en la tesis refuerza la validez interna del estudio y responde a las expectativas de un trabajo de titulación de maestría en seguridad informática.

### 4.3.2. Documentación de la Fase de Inventario y Valoración de Activos

La primera fase del análisis (la caracterización de activos) genera el denominado Modelo de Valor, que MAGERIT v3 describe como el documento que recoge el inventario de activos con sus relaciones de dependencia y la estimación de su importancia en cada dimensión de seguridad [1].

Se recomienda estructurar este documento en tres secciones diferenciadas: (I) el catálogo de activos, organizado según la tipología del Libro II de MAGERIT (datos, aplicaciones, servicios, equipos, instalaciones y personal [2]); (II) la matriz de dependencias que represente con claridad qué activos secundarios sostienen a cada activo primario del Core financiero; y (III) la tabla de valoración multidimensional, en la que cada activo reciba una puntuación en las cinco dimensiones CIDAN.

Para que el Modelo de Valor sea un instrumento sólido, cada fila de la tabla de valoración debe incluir: el código único del activo, su denominación técnica, la categoría MAGERIT correspondiente, la puntuación en cada dimensión con su justificación en una nota al pie o en una columna de observaciones, y el nombre del responsable custodio que validó los datos durante la entrevista o el taller de trabajo.

Esta información respalda que la valoración no se realizó de forma arbitraria, sino con base en criterios explícitos y verificables. Conviene, además, adjuntar como anexo las hojas de recolección de datos originales (con firmas digitales o sellos institucionales cuando sea posible), pues estos documentos elevan la credibilidad del trabajo ante el comité evaluador y ante la SEPS en caso de una inspección posterior [4].

### 4.3.3. Documentación del Mapa de Riesgos y la Evaluación de Amenazas

El Mapa de Riesgos es el producto central del MAR.2 y constituye el documento que ordena y prioriza las amenazas halladas sobre cada activo según su probabilidad de ocurrencia y el grado de degradación que causarían si se materializasen [1].

Se recomienda elaborar este mapa en forma de tabla de doble entrada: en las filas se ubican los activos del Core financiero identificados en la fase anterior; en las columnas [2]se registran las amenazas relevantes extraídas del catálogo del Libro II de MAGERIT, diferenciadas en accidentales y deliberadas.

Cada celda de la tabla debe contener la frecuencia estimada (expresada en la escala de cinco niveles de MAGERIT: muy frecuente, frecuente, normal, poco frecuente y muy poco frecuente) y el porcentaje de degradación correspondiente a cada dimensión CIDAN afectada. Esta presentación visual facilita la lectura del tribunal y permite identificar con rapidez los pares activo-amenaza de mayor criticidad.

Además de la tabla, la documentación de esta fase debe incluir una sección narrativa en la que se explique el procedimiento usado para estimar los valores de probabilidad: si se basaron en registros históricos de incidentes de la cooperativa, en estadísticas sectoriales del sistema financiero popular y solidario, en el juicio de expertos consultados durante los talleres o en una combinación de estas fuentes. Esta justificación es fundamental para que el tribunal de tesis y los lectores externos puedan valorar la confiabilidad de las estimaciones y para cumplir con el principio de trazabilidad que exige

la ISO/IEC 27005:2022 respecto de los datos de entrada al proceso de valoración del riesgo [19].

Se sugiere, asimismo, incluir un diagrama de calor que represente gráficamente la distribución de los pares activo-amenaza en los cuadrantes de alto, medio y bajo riesgo potencial, pues este tipo de apoyo visual enriquece la presentación de resultados y refuerza el argumento analítico de la investigación.

### 4.3.4. Documentación de la Evaluación de Salvaguardas y del Informe de Insuficiencias

La fase MAR.3 produce tres documentos estrechamente relacionados: la Declaración de Aplicabilidad, la Evaluación de Salvaguardas y el Informe de Insuficiencias [1]. Estos tres elementos pueden presentarse de manera integrada en un único capítulo de resultados o como documentos separados.

La Declaración de Aplicabilidad debe listar todos los controles del Anexo A de la ISO/IEC 27001:2024 que resultan aplicables al contexto de la cooperativa, con una columna que indique su estado de implementación (implementado, parcialmente implementado o no implementado) y otra que justifique la exclusión de los controles que no aplican al perfil tecnológico de la entidad [7], [11], [12], [19], [20]. Esta alineación entre el catálogo MAGERIT de salvaguardas y el marco de controles ISO dota al trabajo de una doble validación normativa que fortalece sus conclusiones.

La Evaluación de Salvaguardas, por su parte, debe registrar para cada control la puntuación de eficacia asignada según el modelo de madurez de cinco niveles (L0 a L5) que propone la guía, donde L0 indica la ausencia total del control y L5 su optimización plena [1]. En la documentación de la tesis, esta calificación debe acompañarse de la evidencia que la respalde: capturas de pantalla de configuraciones, actas de revisión de políticas, informes de auditorías previas o declaraciones firmadas del responsable de TI.

El Informe de Insuficiencias, que se genera como complemento de esta evaluación, debe ordenar las brechas halladas por nivel de criticidad (alta, media y baja) e indicar para cada una el riesgo residual estimado si la brecha no se cierra; este dato es el insumo directo del Plan de Tratamiento que cierra el ciclo del análisis y conecta los resultados de la tesis con las recomendaciones operativas dirigidas a la cooperativa [1].

### 4.3.5. Documentación del Estado de Riesgo Residual y del Plan de Tratamiento

El Estado de Riesgo es el documento de cierre del análisis MAGERIT; reúne, para cada activo y cada amenaza, el impacto potencial (calculado sin considerar las salvaguardas existentes) y el impacto residual (calculado después de aplicar los controles vigentes), junto con los niveles de riesgo potencial y residual correspondientes [1].

Se recomienda presentar estos valores en tablas separadas por categoría de activo (datos, aplicaciones, servicios y equipos) de modo que el lector pueda navegar los resultados con facilidad y el tribunal evalúe la profundidad del análisis por segmento tecnológico. Cada tabla debe incluir una columna de semáforo de riesgo (rojo para riesgo inaceptable, naranja para riesgo alto, amarillo para riesgo medio y verde para riesgo bajo) que comunique visualmente la gravedad de cada situación sin necesidad de que el lector interprete los valores numéricos crudos.

El Plan de Tratamiento, que la ISO/IEC 27001:2024 exige como documento obligatorio del SGSI [7], debe presentarse en la tesis como una hoja de ruta operativa que traduzca los hallazgos del análisis en acciones concretas; cada acción debe especificar: la salvaguarda propuesta o mejorada, el activo o grupo de activos que protege, el nivel de riesgo residual esperado una vez implementada, el responsable designado para su ejecución, el plazo estimado y el recurso presupuestario aproximado.

Vincular explícitamente cada acción del plan con una o más brechas del Informe de Insuficiencias (mediante un código cruzado) demuestra la coherencia interna del trabajo. Esta estructura también responde a los requisitos de la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002, que solicita a las cooperativas de ahorro y crédito de los segmentos 2 y 3 la elaboración de planes de tratamiento documentados como parte de su obligación de gestión de riesgos tecnológicos [4].

Finalmente, la documentación del análisis de riesgos en la tesis debe cerrar con una síntesis que relacione los productos documentales generados (Modelo de Valor, Mapa de Riesgos, Evaluación de Salvaguardas, Informe de Insuficiencias, Estado de Riesgo y Plan de Tratamiento) con los objetivos específicos planteados en el Capítulo I. Esta relación explícita entre evidencias, resultados y objetivos es una exigencia metodológica

básica en los trabajos de investigación aplicada [3] y constituye, al mismo tiempo, el argumento central que valida la pertinencia de haber elegido MAGERIT como metodología de análisis: la guía no solo genera datos cuantitativos y cualitativos sobre el nivel de riesgo de la cooperativa, sino que produce un conjunto articulado de documentos que pueden integrarse directamente al SGSI como insumos para el ciclo de mejora continua previsto en la ISO/IEC 27001:2024 [7].

Tabla VI Tabla de trazabilidad objetivos

| **Objetivo** | **Sección donde se cumple** | **Evidencia / producto generado** |
|---|---|---|
| **OG: Proponer una guía para el análisis de gestión de riesgos tecnológicos del Core financiero como insumo del SGSI.** | Cap. IV, 4.1 Guía; 4.1.9 Productos de salida; 4.2 Hallazgos en la Provincia de Pichincha. | Guía metodológica completa, Modelo de Valor, Mapa de Riesgos, Evaluación de Salvaguardas, Informe de Insuficiencias, Estado de Riesgo Residual, Plan de Tratamiento y Declaración de Aplicabilidad |
| **OE1: Detallar las funciones y características principales de MAGERIT v.3.** | Cap. II, Metodologías de Evaluación de Seguridad; Cap. IV, 4.1 Introducción y Propósito; 4.1.3 a 4.1.7. | Descripción del flujo MAGERIT v.3, fases de análisis, criterios CIDAN, lista de control MAR y estructura documental del método |
| **OE2: Identificar las principales vulnerabilidades de Seguridad de la Información.** | Cap. IV, 4.1.4 Fase 2; 4.1.5 Fase 3; 4.2 Resultados del Diagnóstico Organizacional. | Diagnóstico de vulnerabilidades, amenazas, brechas de salvaguardas, datos de encuesta, figuras de resultados y estimación de riesgo potencial/residual |
| **OE3: Elaborar una guía para el análisis de gestión de riesgos tecnológicos del Core financiero.** | Cap. IV, 4.1 Gua; 4.1.8 Resultados del Diagnóstico Organizacional; 4.1.9 Productos de Salida del Análisis de Riesgos. | Documento guía estructurado en 5 fases y 7 productos de salida, alineado con SEPS e ISO/IEC 27001:2024 |

| | | |
|---|---|---|
| **OE4: Evaluar la guía mediante su aplicación en un caso práctico.** | Cap. IV, 4.2 Hallazgos en la Provincia de Pichincha; 4.2.1 a 4.2.5. | Aplicación en 7 cooperativas, resultados del diagnóstico, validación de necesidades, brechas comunes y justificación de la guía |

Nota: Fuente. Elaboración Propia

# CONCLUSIONES

Se concluye que la propuesta de una guía para el análisis de gestión de riesgos tecnológicos del Core financiero constituye un insumo coherente y pertinente para fortalecer el Sistema de Gestión de Seguridad de la Información en las cooperativas de ahorro y crédito de los segmentos 2 y 3, ya que permite estructurar de forma ordenada la identificación, valoración, tratamiento y seguimiento de los riesgos tecnológicos, en correlación con la normativa vigente y las buenas prácticas internacionales.

Se determinó que la metodología MAGERIT v.3 ofrece funciones y características adecuadas para el contexto cooperativo, debido a que permite identificar activos, amenazas, vulnerabilidades, salvaguardas y riesgo residual mediante un enfoque sistemático, escalable y comprensible, facilitando la priorización de controles de seguridad según el nivel de exposición de cada activo de información.

Se evidenció la presencia de vulnerabilidades relevantes en los servicios tecnológicos del Core financiero, asociadas principalmente a debilidades en la gobernanza, controles insuficientes, falta de formalización del análisis de riesgos y brechas en la implementación de salvaguardas, lo que confirma la necesidad de un diagnóstico técnico sustentado en información cualitativa y cuantitativa para estimar con mayor precisión la probabilidad, el impacto y el riesgo residual.

Se concluye que la guía elaborada integra de manera coherente las cinco fases del análisis de riesgos y los siete productos de salida previstos, convirtiéndose en una herramienta metodológica útil para documentar el proceso, generar trazabilidad técnica y servir como base para la Declaración de Aplicabilidad, el Mapa de Riesgos, el Informe de Insuficiencias y el Plan de Tratamiento.

Se comprobó, mediante el caso práctico aplicado a siete cooperativas, que existe una necesidad real de contar con un modelo homogéneo de gestión de riesgos tecnológicos, ya que persisten dificultades comunes en la evaluación formal de riesgos, la actualización de controles y la alineación con la normativa de la SEPS, lo que valida la utilidad práctica de la guía propuesta para el sector cooperativo.

## RECOMENDACIONES

1. Se recomienda a las cooperativas de ahorro y crédito de los segmentos 2 y 3 adoptar progresivamente la guía propuesta como instrumento técnico para el análisis de riesgos del Core financiero, integrándola a sus procesos internos de seguridad de la información, continuidad operativa y gestión documental.

2. Se recomienda a los Oficiales de Seguridad de la Información, Encargados de TI, y Auditores Informáticos de las Cooperativas de Ahorro y Crédito considerar esta guía como referencia metodológica complementaria para fortalecer los lineamientos de gestión de riesgos tecnológicos en el sector cooperativo, promoviendo criterios homogéneos de evaluación, documentación y tratamiento del riesgo, acordes con la resolución vigente.

3. Se recomienda a las instituciones de educación superior incorporar esta propuesta como caso de estudio en programas de seguridad informática, gestión de riesgos y auditoría de sistemas, con el fin de vincular la teoría con escenarios reales del sector financiero cooperativo y fortalecer la formación práctica de los estudiantes.

4. Se recomienda desarrollar investigaciones futuras orientadas a automatizar la guía, ampliar su validación en otras cooperativas y segmentos, y evaluar su integración con herramientas de monitoreo, auditoría y métricas de madurez del SGSI, de modo que se profundice su aplicabilidad y mejora continua.

En conjunto, los resultados confirman que la guía propuesta constituye un aporte metodológico aplicable, adaptable y alineado con las exigencias normativas del sector cooperativo ecuatoriano.

## 5. REFERENCIAS BIBLIOGRÁFICAS


[1] GOBIERNO DE ESPAÑA, «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método», Madrid, 2012. [En línea]. Disponible en: http://administracionelectronica.gob.es/

[2] GOBIERNO DE ESPAÑA, «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos», Madrid, 2012. [En línea]. Disponible en: http://administracionelectronica.gob.es/

[3] GOBIERNO DE ESPAÑA, «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas», Madrid, 2012. [En línea]. Disponible en: http://administracionelectronica.gob.es/

[4] Superintendencia de Economía Popular y Solidaria, «Resolución Nro. SEPS-IGS-IGT-IGJ-IGDO-INGINTINTIC-INSESF-INRDNSI-2022-002», Quito, Ecuador, 2022.

[5] Superintendencia de Economía Popular y Solidaria, «Ley Orgánica de la Economía Popular Y Solidaria», n.º Registro Oficial No. 444, pp. 1-58, mayo 2011, Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://www.seps.gob.ec//wp-content/uploads/CompletosSinConcordanciaspdf92306_-_LEY_ORGA%CC%81NICA_DE_LA_ECONOMI%CC%81A_POPULAR_Y_SOLI-1.pdf

[6] J. P. Rodríguez Guerra, *Diseño de una metodología para la implementación y gestión de un sistema de seguridad para servicios transaccionales en instituciones financieras de la economía popular y solidaria basada en las buenas prácticas de la PCI DSS*. 2019.

[7] ISO/IEC, «Information security, cybersecurity and privacy protection-Information security management systems-Requirements AMENDMENT 1: Climate action changes», Vernier, Geneva, 2024. [En línea]. Disponible en: www.iso.org/iso/foreword.html.

[8] Superintendencia de Economía Popular y Solidaria, « RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116.», Quito, Ecuador, 2024

[9] H. , & K. M. Tipton, «Information Security Management Handbook», *CRC Press*, 2017.

[10] R. , & V. N. J. Von Solms, «COBIT 5 y el valor de la seguridad de la información. Informe Técnico de Seguridad de la Información.», *De políticas a principios*, 2013.

[11] ISO/IEC, *ISO/IEC 27007:2020: Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*, 3.ª ed. 2020.

[12] ISO/IEC, *ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*, 2.ª ed. 2016.

[13] «Las TIC en las empresas y su importancia - Las tic en la educación». Accedido: 1 de marzo de 2024. [En línea]. Disponible en: https://ticeducacion.com/la-importancia-de-las-tic-en-las-empresas/

[14] «¿Qué son las TIC y por qué son importantes? - Saint Leo University». Accedido: 1 de marzo de 2024. [En línea]. Disponible en: https://worldcampus.saintleo.edu/noticias/cual-es-la-importancia-de-las-tic-para-las-empresas

[15] Presidencia de la República del Ecuador, «Constitución de la República del Ecuador», vol. 30, n.º Tercer Suplemento del Registro Oficial 568, 30-V-2024, oct. 2008.

[16] Superintendencia de Economía Popular y Solidaria, «Ley Orgánica de Transparencia y Acceso a la Información Pública», vol. 29, pp. 1-25, feb. 2023, Accedido: 26 de mayo de 2026. [En línea]. Disponible en: https://www.seps.gob.ec//wp-content/uploads/CompletosSinConcordanciaspdf1177926_-_LEY_ORGA%CC%81NICA_DE_TRANSPARENCIA_Y_ACCESO_A.pdf

[17] Banco Central del Ecuador, «Estatuto Orgánico de Gestión Organizacional por Procesos del Banco Central del Ecuador», Quito, 2025.

[18] E. Túquerres, «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.», *REPOSITORIO UNIVERSIDAD TÉCNICA DEL NORTE*, 2024.

[19] ISO/IEC, «ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks», 2022.

[20] ISO/IEC, «ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security», pp. 1-28, 2023.

[21] Presidencia de la República del Ecuador, «Ley Orgánica de Gestión de la Identidad y Datos Civiles», Quito, Ecuador, 2016.

**Anexo1 Encuesta de Diagnóstico sobre la Gestión de Riesgos Tecnológicos del Core Financiero en Cooperativas de Ahorro y Crédito del Segmento 1, 2 y 3**

# Diagnóstico sobre la Gestión de Riesgos Tecnológicos del Core Financiero en Cooperativas de Ahorro y Crédito del Segmento 1, 2 y 3

Esta encuesta busca diagnosticar el estado actual de la gestión de riesgos tecnológicos sobre el core financiero en cooperativas del Segmento 1, 2 y 3 en Ecuador, bajo la regulación SEPS-2024-002.

* Indica que la pregunta es obligatoria

1. Correo *

2. SECCIÓN 1 – Nombre de la Cooperativa (Opcional)

3. SECCIÓN 1 – Segmento al que pertenece la cooperativa *

*Marca solo un óvalo.*

- ◯ Segmento 1
- ◯ Segmento 2
- ◯ Segmento 3

4. SECCIÓN 1 – Cargo del informante *

*Marca solo un óvalo.*

- Jefe de TI/Responsable de TI
- Oficial de la Seguridad de Información
- Gerente / Responsable de Riesgos
- Auditor Informático
- Auditor Interno
- Otro: _____

5. SECCIÓN 1 – Años de experiencia en el cargo *

*Marca solo un óvalo.*

- <1
- 1-3
- 4-6
- 7-10
- >10

6. SECCIÓN 2 – Estado del SGSI y de la gestión de riesgos | ¿Quién lidera actualmente la función de Administración del Análisis de Riesgos de TI en la Cooperativa? *

*Marca solo un óvalo.*

- Unidad de Seguridad de la Información/CISO
- Oficina de Gestión de Riesgos (Enterprise Risk Management)
- Departamento de Tecnología/TI
- Comité de Auditoría/Riesgos
- Otro: _____

7. ¿Cuenta la Cooperativa con un Marco de Gobernanza de la Información aprobado por la Alta Dirección? *

*Marca solo un óvalo.*

- Sí
- No
- Tal vez

8. SECCIÓN 2 – ¿La cooperativa cuenta actualmente con un Sistema de Gestión de Seguridad de la Información (SGSI) implementado? *

*Marca solo un óvalo.*

- Sí
- Parcialmente
- No
- No sabe

9. SECCIÓN 2 – Si la Cooperativa cuenta con un Marco de Gobernanza de la Información, ¿define formalmente los siguientes elementos?

*Selecciona todos los que correspondan.*

- [ ] Políticas de clasificación y manejo de datos
- [ ] Roles y responsabilidades de los custodios de datos
- [ ] Ciclo de vida para la gestión y protección de activos de datos (creación, almacenamiento, disposición)
- [ ] Mecanismos de supervisión y monitoreo (auditoría/cumplimiento)
- [ ] Ninguno de los anteriores
- [ ] Otro: _____

10. SECCIÓN 2 – ¿La cooperativa ha realizado un análisis formal de riesgos sobre el core financiero en los últimos 24 meses? *

*Marca solo un óvalo.*

- Sí
- No
- No sabe

11. SECCIÓN 2 – Si la respuesta anterior fue 'Sí', indique con qué frecuencia se realiza el análisis de riesgos.

*Marca solo un óvalo.*

- ◯ Anual
- ◯ Semestral
- ◯ Eventual
- ◯ Solo ante incidentes
- ◯ No aplica

12. SECCIÓN 2 – ¿Qué metodología de análisis de riesgos utiliza o ha utilizado la cooperativa? *

*Selecciona todos los que correspondan.*

- ☐ MAGERIT
- ☐ OCTAVE
- ☐ ISO 27005
- ☐ NIST SP 800-30
- ☐ Metodología propia
- ☐ Ninguna
- ☐ Otro: _____

13. SECCIÓN 2 – ¿Existe en la cooperativa un documento formal de política de seguridad de la información? *

*Marca solo un óvalo.*

- Sí
- No
- En elaboración
- No sabe

14. SECCIÓN 3 – Razones de uso o desuso del análisis de riesgos | Si la cooperativa NO realiza análisis formal de riesgos, indique las razones principales (Seleccione todas las que apliquen)

*Selecciona todos los que correspondan.*

- [ ] Falta de personal capacitado en metodologías de análisis de riesgos
- [ ] Falta de presupuesto
- [ ] Desconocimiento de metodologías aplicables (MAGERIT, ISO 27005, etc.)
- [ ] Ausencia de una guía adaptada al sector cooperativo
- [ ] Falta de apoyo de la alta dirección
- [ ] No se considera prioritario
- [ ] Complejidad de las metodologías existentes
- [ ] Otra (especifique)
- [ ] Otro: _____

15. SECCIÓN 3 – Evalúe los siguientes ítems usando la escala: 1=Totalmente en desacuerdo, 5=Totalmente de acuerdo. *

*Marca solo un óvalo por fila.*

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **El personal técnico de la cooperativa conoce metodologías formales de análisis de riesgos** | ◯ | ◯ | ◯ | ◯ | ◯ |
| **La cooperativa dispone de recursos suficientes (humanos, económicos, tecnológicos) para gestionar riesgos de TI** | ◯ | ◯ | ◯ | ◯ | ◯ |
| **Las metodologías existentes son fácilmente aplicables a cooperativas del Segmento 1, 2 y 3** | ◯ | ◯ | ◯ | ◯ | ◯ |
| **La normativa SEPS-2022-002 es clara respecto a los requisitos** de análisis de | ◯ | ◯ | ◯ | ◯ | ◯ |

15.

SECCIÓN 3 – Evalúe los siguientes ítems usando la escala: 1=Totalmente en desacuerdo, 5=Totalmente de acuerdo. *

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| El personal téc... | ○ | ○ | ○ | ○ | ○ |
| La cooperativa ... | ○ | ○ | ○ | ○ | ○ |
| Las metodolog... | ○ | ○ | ○ | ○ | ○ |
| La normativa S... | ○ | ○ | ○ | ○ | ○ |
| La cooperativa ... | ○ | ○ | ○ | ○ | ○ |

16. SECCIÓN 4 – Necesidad percibida de una guía metodológica | ¿Ha realizado la Cooperativa un Análisis de Riesgos de TI formal en los últimos 12 meses? *

*Marca solo un óvalo.*

- ◯ Sí
- ◯ No

17. SECCIÓN 4 – Si SÍ ha realizado un análisis de riesgos de TI formal, ¿cómo se llevó a cabo el ejercicio?

*Marca solo un óvalo.*

- Internamente, con personal de la Cooperativa
- Externamente, con consultores especializados
- Combinado (Interno y Externo)
- Utilizando una metodología propia y manual
- Utilizando una herramienta GRC (Governance, Risk and Compliance)
- Basado en un marco estándar (ej. ISO 27005, NIST SP 800-30)
- Otro: _____

18. SECCIÓN 4 – ¿Sabe con qué frecuencia se actualiza el Análisis de Riesgos de TI? *

*Marca solo un óvalo.*

- Periodos mensuales
- Anualmente
- Cada dos años
- Solo cuando ocurre un incidente mayor
- No se realiza un cronograma regular.
- No sé

19. SECCIÓN 4 – Evalúe los siguientes ítems usando la escala: 1=Totalmente en desacuerdo, 5=Totalmente de acuerdo. *

*Marca solo un óvalo por fila.*

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **¿Considera necesario contar con una guía específica para el análisis de gestión de riesgos del core financiero?** | ◯ | ◯ | ◯ | ◯ | ◯ |
| **¿Una guía basada en MAGERIT v3 sería útil para su cooperativa?** | ◯ | ◯ | ◯ | ◯ | ◯ |
| **¿Una guía adaptada al sector Corporativo facilitaría el cumplimiento de la SEPS?** | ◯ | ◯ | ◯ | ◯ | ◯ |
| **¿La cooperativa estaría dispuesta a adoptar una guía metodológica si estuviera disponible?** | ◯ | ◯ | ◯ | ◯ | ◯ |

20. SECCIÓN 4 – ¿Qué dificultades concretas ha enfrentado la cooperativa al intentar gestionar riesgos tecnológicos sobre el core financiero? *

21. SECCIÓN 5 – Incidentes y exposición (Opcional) | ¿La cooperativa ha experimentado incidentes de seguridad de la información sobre el core financiero en los últimos 24 meses?

*Marca solo un óvalo.*

- Sí
- No
- Prefiere no responder

22. SECCIÓN 5 – (Opcional) | Si la respuesta anterior fue 'Sí', indique el tipo de incidente (Puede seleccionar más de uno).

*Selecciona todos los que correspondan.*

- Malware/Ransomware
- Accesos no autorizados
- Fuga de información
- Indisponibilidad del servicio
- Fraude interno
- Otro:

23. SECCIÓN 6 – (Opcional) | Comentarios o sugerencias sobre la gestión de riesgos tecnológicos en su cooperativa.

Este contenido no ha sido creado ni aprobado por Google.

Google Formularios