UNIVERSIDAD CATÓLICA DE CUENCA

Maestría en Ciberseguridad

Informe de Investigación previo a la obtención del título de Magíster en Ciberseguridad

Tema: Sistema de Gestión de Seguridad de la Información (SGSI) de la COAC Fasayñan: Enfrentando Amenazas Cibernéticas en Departamentos Operativos y Administrativos.

Autor: Andrés Patricio Garnica Bueno

Asesores: Ing. Juan Pablo Cuenca. Mgs

Cuenca, 2025

Certificación de Asesores

Se certifica que:

El informe de investigación “Sistema de Gestión de Seguridad de la Información (SGSI) de la COAC Fasayñan: Enfrentando Amenazas Cibernéticas en Departamentos Operativos y Administrativos.”, de autoría de la Señor Ingeniero de Sistemas Andrés Patricio Garnica Bueno, CC: 0106111180, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católicade Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Abril, 2025.

Ing. Juan Pablo Cuenca. Mgs
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

"Sistema de Gestión de Seguridad de la Información (SGSI) de la COAC Fasayñan: Enfrentando Amenazas Cibernéticas en Departamentos Operativos y Administrativos. ", es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2019.

_____

Ing. Andrés Patricio Garnica B.

CC:0106111180

Agradecimiento

Agradezco primeramente a Dios por darme salud y de manera especial para mi familia por apoyarme en mis objetivos tanto en lo laboral y profesional, a mi tutor el Ingeniero Juan Pablo Cuenca y de igual forma al director de la Maestría al Ingeniero Juan Carlos Ortega, que gracias a sus conocimientos y aprendizajes fueron unos guías para cumplir este objetivo profesional. De igual forma a un gran amigo Jorge López que gracias a sus consejos y apoyo se cumplió este gran objetivo.

Dedicatoria

Este trabajo está dedicado para mis padres Manuel y Patricia, a mis hermanos Diego y Jonnathan “SUANDY”, siempre me han apoyado en mis proyectos. De igual forma dedicar este trabajo a Karina Cumbe que siempre ha sido un pilar fundamental en mi vida, para cumplir estos objetivos por apoyarme a superarme y continuar cumpliendo mis metas.

Resumen

Este proyecto de investigación se propuso diseñar una estrategia para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Ahorro y Crédito Fasayñan Ltda. Esto surge como respuesta a la creciente amenaza de ciberataques y a las exigencias normativas de la Superintendencia de Economía Popular y Solidaria (SEPS). El estudio se basó en los lineamientos de la norma ISO/IEC 27001 y utilizó metodologías de diagnóstico tanto cualitativas como cuantitativas, a través de entrevistas, encuestas estructuradas y análisis de activos críticos.

A partir del diagnóstico, se detectó una preocupante falta de políticas de seguridad formales, un escaso conocimiento del personal sobre riesgos como la ingeniería social, y la ausencia de protocolos de capacitación interna. Utilizando el modelo CIA (Confidencialidad, Integridad y Disponibilidad), se clasificó la información por departamentos, lo que reveló que áreas como Legal, Crédito y Cumplimiento manejan activos de alta criticidad.

La propuesta del SGSI incluye fases de implementación progresivas, el diseño de controles técnicos y administrativos, y un plan de capacitación integral que busca fomentar una cultura de ciberseguridad. Con este proyecto, se pretende no solo reducir las vulnerabilidades existentes, sino también asegurar el cumplimiento normativo y fortalecer la confianza de los socios en la institución.

Palabras claves: Seguridad de la información, amenazas cibernéticas, ISO/IEC 27001, SGSI, modelo CIA, cooperativas, activos críticos, cultura de ciberseguridad.

Abstract

This research project proposed to design a strategy to implement an Information Security Management System (ISMS) at the Fasayñan Credit Union Ltda. This arises as a response to the growing threat of cyber attacks and to the regulatory demands of the Superintendence of Popular and Solidarity Economy (SEPS). The study was based on the guidelines of the ISO/IEC 27001 standard and used both qualitative and quantitative diagnostic methodologies, through interviews, structured surveys and analysis of critical assets.

From the diagnosis, a worrying lack of formal security policies was detected, a lack of staff knowledge about risks such as social engineering, and the absence of internal training protocols. Using the CIA (Confidentiality, Integrity and Availability) model, the information was classified by departments, which revealed that areas such as Legal, Credit and Compliance handle highly critical assets.

The ISMS proposal includes progressive implementation phases, the design of technical and administrative controls, and a comprehensive training plan that seeks to foster a culture of cybersecurity. With this project, the aim is not only to reduce existing vulnerabilities, but also to ensure regulatory compliance and strengthen the trust of partners in the institution.

Keywords: Information security, cyber threats, ISO/IEC 27001, ISMS, CIA model, cooperatives, critical assets, cybersecurity culture.

Índice de contenidos

Índice de figuras

Índice de tablas

Capítulo I. Introducción

1.1 Situación problemática

Las instituciones financieras de hoy en día tienen problemas serios para proteger la información debido a la acelerada digitalización. La seguridad de los datos es uno de los problemas más importantes ya que las instituciones necesitan garantizar confianza y estabilidad. Esto es más crítico dentro del sector cooperativo, donde la administración de información sensible es el centro de operación. Sin embargo, muchas de las entidades todavía tienen brechas en su sistema de protecciones que las hace más vulnerables a sufrir ataques cibernéticos (Superintendencia de Economía popular y Solidaria, 2021).

Al igual que otras entidades del sector, la Cooperativa de Ahorro y Crédito Fasayñan Ltda. tiene en su poder información sensible de sus socios y operaciones financieras. A pesar de lo crítico que es esta información, la cooperativa tiene una gestión de seguridad de la información muy precaria lo que pone de riesgo gran parte de la organización. La falta de conocimiento por parte de los colaboradores y la falta de protocolos ha creado un entorno donde los ciberataques podrían comprometer la disponibilidad y la integridad de los datos. Entre las amenazas más comunes están la suplantación de identidad, información mal intencionada, acceso no autorizado y fraude informático (23 de Julio, 2023).

El problema se ve complicado por la falta de ciberseguridad del personal. Muchos trabajadores carecen del conocimiento sobre la forma en la que se debe proteger la organización y por consiguiente, no se lograran prevenir y/o detectar muchos incidentes. Adicionalmente, la inexistencia de una cultura organizacional en la seguridad de la información ha retrasado en gran medida la puesta en acción de medidas efectivas para contrarrestar riesgos (OEA, 2018).

Con relación a normatividad, la cooperativa también se encuentra en falta con la seguridad que exige la Superintendencia de Economía Popular y Solidaria (SEPS) así como con los lineamientos de la ISO 27001. Por no contar con un sistema definido de gestión de la seguridad de la información, resulta imposible determinar con exactitud las deficiencias existentes y establecer controles correctos (SEPS, 2022).

Los desafiantes obstáculos de infraestructura y la falta de recursos han dificultado la implementación de soluciones avanzadas dentro de los sistemas tecnológicos. La falta de controles de acceso robustos, herramientas de monitoreo continuo insuficientes y protocolos de emergencia incrementan las posibilidades de violaciones exitosas del sistema. Adicionalmente, el reciente cambio administrativo dentro del departamento de tecnología ha creado un área gris en la gestión de la seguridad de la información, lo que ha retrasado enormemente el progreso de los planes de acción efectivos.

Dadas estas circunstancias desafiantes, existe una clara necesidad de desarrollar un sistema de gestión de seguridad de la información que sea capaz de reconocer riesgos e implementar medidas preventivas, al mismo tiempo que protege los activos digitales de la cooperativa. Este estudio intenta evaluar el estado actual de las cuestiones relacionadas con la seguridad de la información y proponer medidas destinadas a mitigar las vulnerabilidades organizacionales, mejorar la gestión de riesgos y garantizar la continuidad operativa de la entidad.

1.2 Problema científico

La protección de datos es y ha sido uno de los problemas más grandes para las instituciones dentro del sistema financiero, especialmente aquellas que manejan información muy específica y confidencial sobre sus clientes y sus operaciones. Tanto datos como

operaciones. La Cooperativa de Ahorro y Crédito Fasayñan Ltda carece de un sistema de gestión de la seguridad de la información, lo cual la hace ser blanco de innumerables riesgos cibernéticos que pueden llegar a atentar contra la confidencialidad, integridad y disponibilidad de su información. Por esta razón, debería haber preocupación sobre la seguridad y capacidad de respuesta de la cooperativa frente a los incidentes de seguridad.

Una de las cosas que preocupan es la falta de enfoque y un solo especialista dirigido a la evaluación de la vulnerabilidad en la parte operativa y administrativa. No disponer de un análisis sistemático sobre los riesgos cibernéticos permite el control y la mínima seguridad a la cooperativa, lo cual la deja expuesta a diferentes ataques cuyo resultado puede poner en peligro la estabilidad operativa de la cooperativa. Esta menor capacidad y limitada instrucción sobre seguridad cibernética, de parte del personal administrativo del sistema cooperativo, aumenta la vulnerabilidad a ataques computacionales que resulten en fallos de seguridad (OEA, 2018).

Otro aspecto importante son los desafíos relacionados con el cumplimiento normativo. La normativa vigente de la Superintendencia de Economía Popular y Solidaria (SEPS) obliga a la cooperativa a establecer alguna clase de medida de protección para la información del sector financiero cooperativo. No obstante, la cooperativa ha sido incapaz de poner en práctica la normativa vigente que permite minimizar riesgos en la administración de la seguridad informática. La no adherencia a ciertos requisitos, como la norma ISO 27001, dificultan el manejo de los riesgos y la adopción de racionales de protección de la información que son aseguradas por él (SEPS, 2022).

Se requiere proteger la organización determinando el grado de vulnerabilidad que tiene la cooperativa frente a ataques cibernéticos y las deficiencias que existen en sus sistemas de

información. Para ello, se necesita una evaluación que permita clasificar los niveles de riesgo que pueden ser considerados para aumentar la seguridad de la información.

Basado en lo mencionado anteriormente, esta investigación tiene la siguiente pregunta:

¿Cuál es el nivel de vulnerabilidad de la Cooperativa de Ahorro y Crédito Fasayñan Ltda. hacia ataques cibernéticos en sus departamentos operativo y administrativo, y qué medidas se pueden tomar para proteger mejor la información?

1.3 Objeto de estudio

El punto focal de esta investigación es la Cooperativa de Ahorro y Crédito Fasayñan Ltda., una institución financiera ubicada en la cabecera parroquial de Chordeleg, cantón de Ecuador. Se inició el día 24 de mayo de 2001 bajo el nombre de Caja de Ahorro y Crédito y obtuvo su personalidad jurídica en octubre del año 2002. Actualmente, está bajo la supervisión de la Superintendencia de Economía Popular y Solidaria. A lo largo de dos décadas, la cooperativa ha crecido de manera constante y se ha convertido en un pilar de la comunidad al apoyar actividades productivas. Este progreso ha sido el resultado del esfuerzo consolidado de los gerentes y socios directivos que han mejorado la salud financiera de la región (CACF, 2025).

El análisis se centrará en los procesos internos de la cooperativa en lo que respecta al plan de la cartera de créditos y las causas de la morosidad de los créditos a los miembros de la cooperativa. Se dará un énfasis particular a las políticas de crédito, los procedimientos de evaluación y monitoreo de los créditos, y las estrategias de mitigación del riesgo de crédito. Además, se plantearon algunas preguntas sobre el bienestar de los empleados, a saber, el grado de estrés al que están sometidos estos trabajadores y cómo esto afecta su productividad (López Vera & Guamushin Tarco, 2022).

Esto proporcionará una visión integral de los factores que afectan la eficiencia operativa y la calidad del servicio proporcionado por la cooperativa. Al centrar la investigación en la Cooperativa de Ahorro y Crédito Fasayñan Ltda., el objetivo es ofrecer información pertinente que ayude a comprender su situación y sirva de base para formular acciones que mejoren su posición en el mercado financiero local.

1.4 Campo de acción

El alcance de esta investigación se enfoca en la revisión y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Ahorro y Crédito Fasayñan Ltda. El SGSI abarca la totalidad dentro del cooperativa para la protección de la información y seguridad de los datos, en especial defensa de ataques cibernéticos que puedan amenazar la confidencialidad, integridad y disponibilidad de la información vital. Esta investigación evaluara el control que tiene la cooperativa sobre los riesgos de seguridad de la información dentro de sus funciones operativas y administrativas.

La presente investigación contemplará la revisión de las actividades de la cooperativa, en especial la gestión de información, el sistema de acceso y control de datos, así como el manejo de incidentes de seguridad. También se evaluará el nivel de cumplimiento de la cooperativa con las leyes del país y otros supranacionales, en especial aquellas descritas en la norma ISO/IEC 27001, que es la norma internacional que establece la guía para la implementación y el mantenimiento de un SGSI. Para que el sistema sea aceptado necesita cumplir con las normativas que la ISO/IEC 27001 exige, y entre estas se encuentra definir absol tener políticas de resguardo de información y que los sistemas de gestión puedan enfrentar nuevos ciber riesgos (ISO/IEC 27001:2013, 2013).

El análisis se llevará a cabo definiendo primero los activos de información que son

críticos dentro de la cooperativa, y luego realizando una revisión de los riesgos para determinar a qué riesgos estos activos críticos están expuestos. Se aplicarán técnicas de evaluación de riesgos reconocidas, como MAGERIT que permite identificar la vulnerabilidad y amenaza más importante y plantear acciones para reducirla. Esta parte del estudio también se encargará de evaluar los sistemas de seguridad que se han puesto en marcha analizando las computer security incident response planning (CSIRT) buenas prácticas, proponiendo y revisando los controles de seguridad idóneas a base de la norma ISO/IEC 27002 que es una norma que da pautas a las organizaciones sobre cómo implementar controles de seguridad (ISO/IEC 27002:2013, 2013)

Para cerrar el trabajo de investigación, se dará un enfoque en la capacitación del recurso, aceptando que uno de los aspectos más relevantes en lo que respecta a la seguridad de la información es la concienciación y competencia del personal. Se planteará una propuesta de capacitación cumpliendo con disposiciones de carácter internacional como la norma ISO/IEC 27034, que propone principios para integrar la seguridad durante todo el ciclo de vida de desarrollo y uso de los sistemas de información (ISO/IEC 27034-1:2011, 2011)

Para esta investigación, las limitaciones incluyen la falta de personal y tecnología dentro de la cooperativa, lo que puede obstruir la aplicación de algunas de las acciones propuestas. Además, el estudio se limitará a la ubicación base de la cooperativa y excluirá cualquier filial o sucursal conocida.

1.5 Objetivos

Evaluar la implementación y efectividad del Sistema de Gestión de Seguridad de la Información (SGSI) en la Cooperativa de Ahorro y Crédito Fasayñan Ltda. con el fin de detectar debilidades y sugerir acciones para mitigar los riesgos cibernéticos, protegiendo así la

información crítica y asegurando la continuidad del negocio de la cooperativa.

1.6 Específicos

- Identificar y evaluar los activos de información que tienen mayor valor dentro de la cooperativa, examinando los riesgos y consecuencias de las amenazas cibernéticas expuestas con el objetivo de formular planes de acción protectores efectivos.
- Determinar el nivel de cumplimiento que tiene la cooperativa con normas de seguridad de la información como ISO/IEC 27001 y otras regulaciones relevantes, y determinar qué brechas existen en las medidas de control de seguridad que se han implementado.
- Desarrollar un plan integral que sea más constructivo al incorporar controles de seguridad adicionales, diseñar un programa de capacitación en concienciación sobre ciberseguridad para el personal de la cooperativa, y mejorar los procedimientos de gestión de incidentes para mejorar la cultura organizacional y la respuesta a los riesgos cibernéticos.

1.7 Justificación

Considerando las amenazas cibernéticas que hay hoy en día hacia las instituciones financieras, desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) en la cooperativa de ahorro y crédito Fasayñan es un tema urgente. En una economía donde la digitalización lo abarca todo, la información es uno de los activos más importantes y su confidencialidad, integridad y disponibilidad deja de ser una buena práctica para la organización y se convierte en un imperativo.

Las cooperativas financieras en Ecuador cuentan con un amplio rango de datos sensibles como información personal de los socios junto con sus transacciones financieras. Todos estos datos son vulnerables a sufrir ataques informáticos. La falta de protocolos

sistemáticos que ayuden en la gestión de tales riesgos pone en peligro el funcionamiento constante de la cooperativa, erosiona la confianza de sus usuarios y expone a la organización a multas por la falta de regulación.

El análisis numérico en el riesgo que enfrenta la cooperativa Fasayñan se puede cuantificar. En el apartado de Ciber Riesgo 2023 de la SEPS, se indica que más del 60% de las cooperativas del segmento 2 reportaron algún tipo de incidente de seguridad en los últimos 18 meses, siendo el phishing, acceso no autorizado y la pérdida de datos los más comunes. En el caso de la cooperativa, esta ha registrado internamente por lo menos cinco incidentes relevantes en el último año que no han sido económicamente devastadores, pero que han dañado procesos fundamentales, críticas, estrangulamiento, autenticación y gestión de cuentas institucionales, con exposición de riesgo, economía, directa. Adicionalmente, las encuestas llevadas como parte de esta investigación sugieren que más del 68% de los empleados nunca recibieron capacitación en ciberseguridad especializada, mientras que el 59% desconoce los protocolos para responder a incidentes de seguridad.

Todo esto realza profundamente el requisito de un modelo integral sistemático. Por esta razón, esta investigación plantea no solo adaptar un SGSI a las condiciones de la cooperativa, sino realizar cambios radicales a la estrategia dentro del marco de gestión de riesgos de la organización.

1.6.1. Justificación institucional.

El sector cooperativo desempeña un papel importante en el sistema financiero ecuatoriano no solo en las áreas rurales o semiurbanas donde no existe banca tradicional, sino también en las regiones con presencia bancaria. La Cooperativa Fasayñan Ltda., que ha estado operando durante más de dos décadas, es una de las instituciones locales para el desarrollo económico.

Su perdurabilidad, solvencia y reputación están condicionadas por cómo protegen los datos de sus socios y sus operaciones internas de los riesgos en el mundo digital.

En este sentido, la implementación de un SGSI abordará el problema desde un punto de vista técnico, en este caso específico, ayudará a fortalecer las estrategias de la cooperativa. Utilizar las normas internacionales ISO/IEC 27001 como base permitirá a la cooperativa consolidar sus defensas, establecer políticas efectivas y demostrar que se están realizando esfuerzos por proteger los beneficios de los socios.

1.6.2. Justificación Metodológica.

El enfoque metodológico de esta investigación tiene como objetivo detallar los procesos de seguridad de la información de la Cooperativa Fasayñan en el contexto de preparar recomendaciones viables para la mejora utilizando estándares internacionales. Se utilizará una combinación de técnicas cualitativas y cuantitativas, que incluyen revisión de documentos, entrevistas con informantes clave, encuesta de diagnóstico, categorización de activos a través de matrices de criticidad y gestión de riesgos aplicando la metodología MAGERIT.

Además, se utilizará la norma ISO/IEC 27001 para auditar el cumplimiento del sistema con el SGSI, y la norma ISO/IEC 27034 se utilizará para desarrollar un programa de concienciación sobre la seguridad de aplicaciones para su certificación. Esto no solo permite un diagnóstico situacional integral y profundo, sino que también garantiza que las soluciones propuestas se caractericen por un enfoque sólido, metodológico, práctico y riguroso.

1.6.3. Justificación teórica.

El estudio, en su enfoque teórico, considera la gestión de la seguridad de la información y el riesgo tecnológico como un todo. La literatura cibernética dentro del sector financiero señala su intención de construir modelos sistemáticos que sean capaces de enfrentar amenazas

cada vez más sofisticadas, exponenciales y SoA. Normas tales como ISO/IEC 27001 y 27002 no solamente ofrecen recomendaciones, sino que también constituyen estructuras para la planificación preventiva, los ataques a las vulnerabilidades, y las posteriores recuperaciones de incidentes.

Para facilitar la comprensión y aplicación de estos principios, se incorporarán materiales gráficos tales como mapas de conceptos, diagramas y tablas. Una comparación de tablas entre ISO 27001 e ISO 27002, por ejemplo, ayudaría a visibilizar la diferencia entre los requisitos de implementación (lo que se hará) y los controles recomendados (cómo se realizará), creando así más sustento al marco teórico del trabajo.

Tabla 1 *Normativas con su enfoque y aplicación*

Norma	Enfoque principal	Aplicación
ISO/IEC 27001	Establece los requisitos para implementar un SGSI	Define qué hacer (estructura y política)
ISO/IEC 27002	Proporciona directrices sobre controles de seguridad	Define cómo hacerlo (controles específicos)

1.8 Fundamentación teórica

La base teórica de este estudio se centra en los principios, conceptos y regulaciones que abordan la importancia de la protección de la información dentro de las instituciones financieras, particularmente hacia las cooperativas de ahorro y crédito. Se basa en áreas clave de apoyo, comenzando desde los marcos regulatorios internacionales, a través de la gestión de riesgos de la seguridad informática, y concluyendo con la implementación de controles efectivos sobre información sensible. A continuación, describimos las principales áreas que constituyen la base de la investigación.

1.7.1 *Seguridad de la Información en Organizaciones Financieras*

La seguridad de la información es un tema delicado para las organizaciones financieras y, en particular, para aquellas que trabajan con datos sensibles relacionados con clientes, socios y procesos internos. En este sentido, la seguridad significa no solo protección contra el acceso no autorizado, sino también la garantía de que hay integridad de los datos, control adecuado de acceso y disponibilidad de los datos cuando se necesiten. Las organizaciones financieras están particularmente expuestas a riesgos de seguridad debido a los frecuentes ciberataques dirigidos hacia ellas, dado el valor de la información que poseen.

1.7.1.1 La Relevancia de la Seguridad de la Información Dentro de las Organizaciones Financieras

Las instituciones financieras suelen violar datos sensibles que se relacionan directamente con la confianza y la seguridad económica de sus clientes. En este ámbito, esto puede incluir información personal sensible, detalles de cuentas bancarias e incluso información sobre transacciones financieras y sobre inversiones o préstamos. La pérdida o exposición de dicha información sensible puede tener impactos catastróficos en una organización, así como en sus clientes. Por lo tanto, deben buscarse con fervor políticas y procedimientos de seguridad que mitiguen de manera preventiva la posibilidad de violaciones de información y seguridad.

Proteger tres atributos clave de la información es un objetivo primario en el sector financiero:

- Confidencialidad: Limitar la información solo a aquellas personas y/o sistemas que estén autorizados para verlo.
- Integridad: Asegurar que no hay cambios no autorizados en la información y que esta

permanezca precisa y completa.

- Disponibilidad: Garantizar el acceso a la información cuando se necesite, proporcionándola de manera oportuna a los usuarios aprobados.

Tabla 2 *Principios clave de la Seguridad de la Información (CIA)*

Principio	Descripción
Confidencialidad	Garantiza que la información solo esté disponible para las personas o sistemas autorizados.
Integridad	Asegura que la información se mantenga exacta, completa y libre de modificaciones no autorizadas.
Disponibilidad	Permite que la información esté accesible y utilizable cuando se necesite, por los usuarios autorizados.

Fuente: Elaboración propia con base en ISO/IEC 27001.

La Confidencialidad, Integridad y Disponibilidad (principios CIA) son los pilares clave de la seguridad de la información y, para las cooperativas de ahorro y crédito que manejan información muy sensible, estos principios son muy importantes. Una gran dependencia de estos principios garantiza que la información confidencial no será revelada indiscriminadamente, será precisa y no se verá alterada, y será accesible para los usuarios cuando se necesite.

1.7.1.2 Amenazas Cibernéticas del Sector Financiero

El sector financiero está expuesto a diferentes formas de amenazas cibernéticas, desde el robo de datos hasta el sabotaje de sistemas. Algunas de las más comunes incluyen:

Tabla 3 Amenazas Cibernéticas Comunes en el Sector Financiero

Amenaza	Descripción
Phishing	Es un método empleado por cibercriminales para infiltrarse en un empleado o cliente de una organización para extraer información sensible como contraseñas y números de tarjetas de crédito.
Malware	Es un software intrusivo que está destinado a dañar el sistema informático al robar o alterar la información contenida en él. Este tipo de amenazas puede ocurrir dentro de la cooperativa (empleados) o fuera de ella (proveedores o clientes).
Ransomware	Un software malicioso que toma control de los datos de una organización al encriptarlos y mantenerlos como rehén hasta que se pague un rescate por la clave de desbloqueo.
Ataques de denegación de servicio distribuido (DDoS)	Ataques destinados a hacer que el sistema sea inaccesible al abrumarlo con una avalancha de solicitudes que incapacitan la funcionalidad del servicio.
Acceso no autorizado y fraude interno	Amenazas que resultan desde dentro de una organización, como un empleado o ex empleado que accede a los sistemas sin permiso y roba o altera información financiera sensible.

Fuente: Elaboración propia basada en informes de la OEA y la ISO/IEC 27001.

El alcance de dichos ataques puede ser catastrófico para la organización, tanto por el costo como por el daño a la imagen corporativa. En consecuencia, es fundamental que todas las cooperativas de ahorro y crédito implementen medidas de seguridad proactivas y reactivas en caso de que se efectúe un ataque a sus sistemas informáticos.

1.7.1.3 Categoría de Falencias en Ciertas Instituciones Financieras

El término financiero es amplio y abarca gran variedad de organizaciones, por lo cual las falencias que puedan existir se pueden simplificar en tres grados de categorías principales:

Tabla 4 Tipos de Falencias en la Seguridad de la Información en Entidades Financieras

Categoría	Descripción	Ejemplos comunes
Fallas tecnológicas	Deficiencias relacionadas con infraestructura, software y hardware obsoletos o mal configurados.	Falta de cifrado, sistemas sin actualizar, ausencia de firewalls o IDS, configuraciones erróneas.
Fallas humanas	Errores causados por desconocimiento, descuido o falta de formación del personal, que comprometen la seguridad.	Uso de contraseñas débiles, respuestas a correos fraudulentos, uso inadecuado de recursos tecnológicos.
Fallas administrativas	Carencia de políticas, procesos o cultura institucional en torno a la ciberseguridad.	Falta de capacitación, ausencia de normativas, desconocimiento de protocolos de acceso o monitoreo.

Fuente: Adaptado de OEA (2022) y análisis propio.

En la Tabla 4 se presenta un resumen sintetizado de los problemas más importantes asociados a la seguridad de la información que afectan a las entidades financieras. Al agruparlos en tecnología, personas y administración, se pueden reflejar de manera clara las deficiencias, así como dirigir con mayor facilidad las medidas correctivas. Esta clasificación será útil en los estudios posteriores de diagnóstico y en la elaboración de planes para el SGSI en la cooperativa.

1.7.1.4 Marco Regulatorio y de Políticas del Sector Financiero

La regulación es uno de los aspectos clave utilizados para garantizar la seguridad en una institución financiera. Al igual que otras cooperativas de crédito nacionales e

internacionales, las cooperativas están sujetas a una variedad de regulaciones destinadas a la protección de datos, la seguridad de la información y la transparencia en la gestión de la información financiera.

- ISO/IEC 27001: Define los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. En el contexto internacional, ayuda a las organizaciones a gestionar su seguridad de la información. Este estándar es central para la gestión de riesgos en organizaciones financieras y sirve para formular políticas, procedimientos y controles efectivos.
- ISO/IEC 27002: Este estándar es una descripción de un conjunto de prácticas recomendadas completas y detalladas para la implementación de controles de seguridad de la información dentro de una empresa. Está destinado a ser utilizado junto con la ISO/IEC 27001 y aborda áreas como controles de acceso, seguridad de la comunicación y confidencialidad de la información protegida.

Tabla 5 *Cuadro comparativo entre ISO/IEC 27001 e ISO/IEC 27002*

Aspecto	ISO/IEC 27001	ISO/IEC 27002
Naturaleza	Norma certificable	Norma de buenas prácticas no certificable
Propósito	Establece requisitos para implementar un SGSI	Brinda directrices para la implementación de controles
Contenido	Requisitos organizacionales (Cláusulas y Anexo A)	Controles agrupados en dominios temáticos
Aplicación	Obligatoria para certificación de un SGSI	Apoyo para personalizar controles de seguridad
Relación entre ellas	Principal marco normativo para	Complementaria: ayuda a

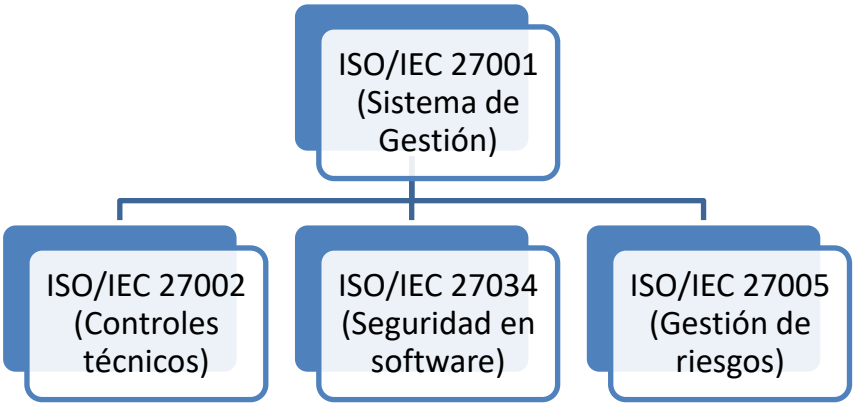
	establecer un SGSI	cumplir los controles del Anexo A

Fuente: Elaboración propia con base en ISO/IEC 27001:2013 e ISO/IEC 27002:2022.

La Tabla 5 hace más que solo mostrar las diferencias y relaciones entre las normas ISO/IEC 27001 e ISO/IEC 27002, pues en sus interacciones se denota que ambas constituyen una subestructura dentro de un sistema en la gerencia de la seguridad de la información (SGSI). ISO 27001 contiene requisitos necesarios para establecer un SGSI e incorporar una gestión de control, convirtiéndola en la principal demanda de certificaciones; en cambio, ISO 27002 brinda orientaciones al nivel de una guía configurativa, sobre cómo implementar los controles de seguridad de la primera.

Es decir, ISO 27001 responde el "qué hacer" para establecer una estructura organizacional segura y ISO 27002 el "cómo hacerlo", mediante la entrega de buenas prácticas para su implementación que son adecuadas a la realidad de cada organismo. Esta distinción resulta clave para la elección y adaptación de controles de seguridad que la cooperativa decida aplicar en su contexto particular.

Figura 1 *Relación entre normas ISO aplicables al SGSI*



Fuente: Elaboración propia.

En la figura 1 se puede apreciar de manera más sencilla la relación jerárquica y

funcional que presentan dentro de la gestión de seguridad de la información cada una de las normas ISO referidas, considerando su aplicabilidad.

- Los automóviles y otros medios de transporte pueden ser incorporados al movimiento de deportes debido a su valor para la educación física y el deporte.
- La norma base es ISO/IEC 27001, que se encuentra centralizada, norma principal que estructura todo el sistema de gestión.
- ISO/IEC 27002 proporciona dicha ayuda desde lo técnico operativo, todo lo referente a los controles de la gestión.
- ISO/IEC 27005 trata sobre los procedimientos de identificación, análisis y tratamiento de riesgos.
- ISO/IEC 27034 abarca la definición de seguridad en el diseño y aplicación de sistemas de software propietario o de terceros.

Este modelo ilustra cómo las diferentes normas se integran en un ecosistema coherente, y muestra que un Sistema de Gestión de Seguridad de la Información (SGSI) no solo se trata de políticas, sino que abarca controles, riesgos y tecnología desde una perspectiva holística.

Basilea III: En finanzas, los acuerdos de Basilea III establecen una serie de regulaciones para mejorar la supervisión, la gestión de riesgos y la transparencia del sector bancario. Si bien se centra predominantemente en la estabilidad financiera, incluye principios subyacentes que se refieren a la gestión de la seguridad de la información.

Reglamento General de Protección de Datos (GDPR): En cuanto a aquellas empresas que operan en la Unión Europea o tienen clientes europeos, cumplir con el GDPR es un imperativo. Esta regulación trata sobre la protección de datos, especialmente en lo que respecta a la información personal y las prácticas de información en Internet.

1.7.1.5 Estrategias para Garantizar la Seguridad de la Información

La seguridad de la información en las instituciones financieras necesita la aplicación de estrategias que incorporen tecnología, procesos organizacionales y actividades de desarrollo continuo del personal. Las estrategias más importantes son:

- **Implementación de controles técnicos de seguridad física:** como cortafuegos, Sistemas de Detección de Intrusiones (IDS) y software de cifrado que protegen la infraestructura de tecnología de la información contra accesos no autorizados.
- **Monitoreo y auditoría constantes:** Tener en marcha sistemas de monitoreo continuo de la red y auditorías regulares de incidentes de seguridad para permitir la detección y reacción oportuna ante eventos de seguridad.
- **Educación y formación sobre cultura organizacional:** Crear una cultura de comportamiento de ciberseguridad donde los empleados de todos los niveles, desde el ejecutivo más alto hasta el operativo más junior, comprendan y cumplan con los procedimientos y prácticas de seguridad.
- **Planificación de respuesta a incidentes:** Equipar a la organización para posibles violaciones de seguridad de la información elaborando un plan de respuesta a incidentes que pueda mitigar el impacto de un ataque y restaurar rápidamente las operaciones.

1.7.1.6 Herramientas y Tecnologías de Seguridad

Existen muchas herramientas y tecnologías que se pueden utilizar para mantener la seguridad de la información de una cooperativa de ahorro y crédito. Las más comunes son:

- **Cortafuegos:** Filtra, permite o deniega paquetes de información dentro o fuera de la red y establece una barrera protectora contra redes externas.
- **Software antivirus y antimalware:** Programas destinados a identificar, detener y

eliminar la presencia de malware en los sistemas.

- **Sistema de autenticación multifactor (MFA):** Refuerza la seguridad para acceder a sistemas e información al usar más de un método de verificación antes de conceder acceso.
- **Cifrado de datos:** Protege información sensible al transformarla en un formato que la hace ilegible para partes no autorizadas.

1.7.2 Sistemas de Gestión de Seguridad de la Información (SGSI)

Un Sistema de Gestión de Seguridad de la Información (SGSI) se refiere a cómo una organización gestiona la seguridad de la información. Su objetivo fundamental es gestionar la confidencialidad, integridad y disponibilidad de la información a través de la implementación de mecanismos de control, políticas y prácticas. En el contexto de cooperativas de ahorro y crédito, un SGSI eficiente no solo protege los activos informativos, sino que también garantiza que la organización cumpla con las normativas y leyes de la industria financiera que establecen una cultura de resiliencia organizacional.

1.7.2.1 Definición y Propósito de un SGSI

Un SGSI es un marco documentado que combina políticas establecidas y procedimientos junto con controles técnicos y no técnicos de seguridad humana y física. Un SGSI tiene un objetivo crítico que se basa en salvaguardar con éxito la información de la organización frente a amenazas internas y externas, asegurando el cumplimiento de las legislaciones pertinentes y fomentando la mejora de la seguridad que sea proactiva ante los cambios ambientales y de nuevos riesgos.

Para lo cual, un SGSI busca desarrollar un sistema que propenda a la creación de un ambiente controlado donde la información de la cooperativa esté a salvo y los procesos

operativos se ejecuten de manera que respeten las reglas de seguridad establecidas en las políticas. Un SGSI también optimiza y facilita la identificación y evaluación de riesgos, así como su neutralización, permitiendo una reacción ágil ante incidentes y a su vez, protegiendo los intereses de los socios y de la cooperativa.

1.7.2.2 Sub unidades de un SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) es una estructura compuesta de varios elementos que se integran para asegurar y proteger la información. Estas subunidades más importantes de un SGSI son:

- *Políticas de Seguridad de la Información:* Es el conjunto de normas y directrices que ordena toda actividad en el marco de la seguridad de la información en la institución. Las políticas deben ser claras, accesibles y revisadas de manera continua.
- *Gestión de Riesgos:* Esto se refiere a un subproceso de formular, decidir qué controles de seguridad se deben establecer, evaluar los efectos posibles y proponer cambios para disminuir la inseguridad de la información. Esto también comprende la adopción de medidas para contener la probabilidad de que un riesgo se materialice y limitar sus efectos.
- *Controles de Seguridad:* Incluyen medidas técnicas, organizativas y físicas diseñadas para prevenir el acceso no autorizado, alteración o destrucción de la información. Ejemplos incluyen cortafuegos, cifrado de datos, controles de acceso y autenticación multifactorial.
- *Planes de Continuidad del Negocio:* Incluyen las políticas y procedimientos dirigidos a asegurar que la cooperativa sea capaz de continuar operaciones después de que haya ocurrido un incidente de seguridad grave, como un ciberataque o una interrupción del

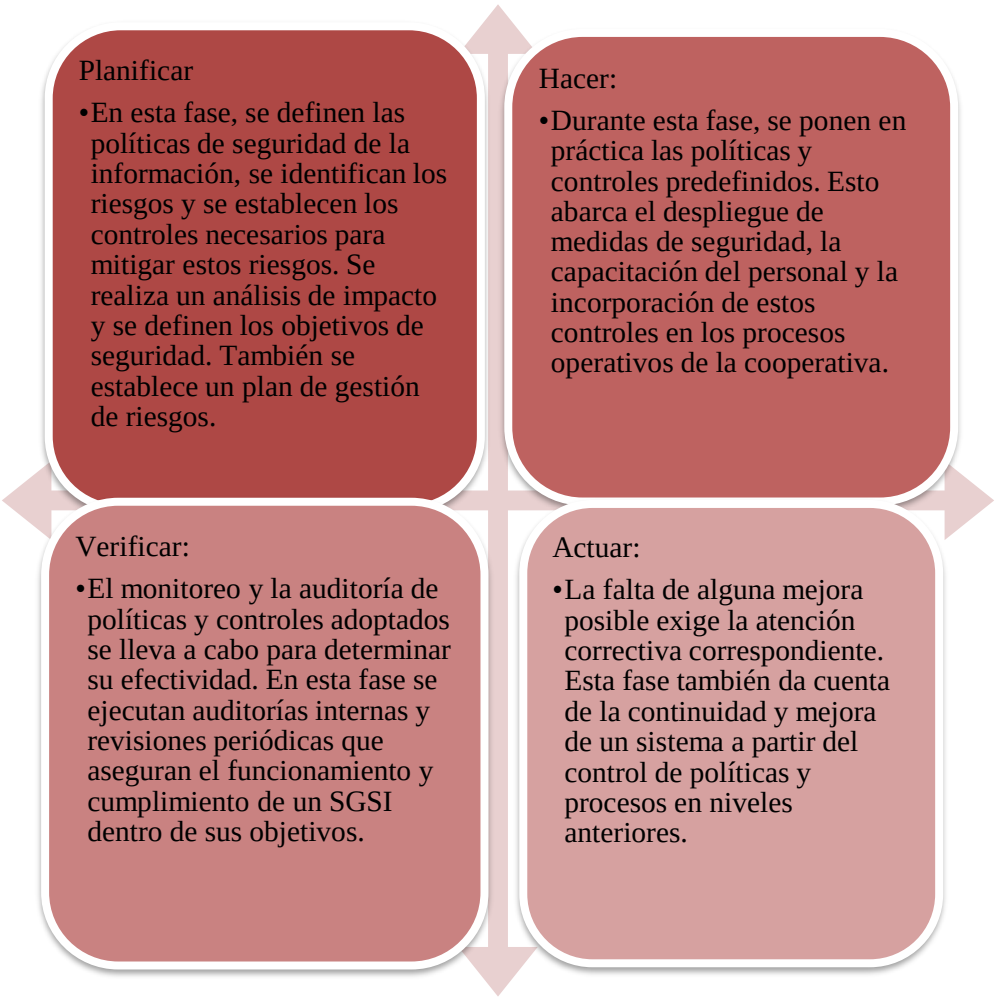
sistema. Esto implica políticas de recuperación ante desastres y respaldo de datos.

- *Monitoreo y Auditoría:* La actividad destinada a proporcionar una evaluación sistemática de, información sobre, la implementación de políticas y controles incluyendo cualquier debilidad dentro del sistema para que se tomen medidas correctivas. El monitoreo continuo también incluye la detección de incidentes y la gestión de registros.
- *Capacitación y Concienciación:* Programas destinados a la educación continua y progresiva de los empleados con el fin de asegurar el conocimiento de la fuerza laboral sobre las medidas de seguridad y las políticas internas. La educación, o más precisamente, la concienciación sobre la seguridad reduce los riesgos que surgen de errores humanos.

1.7.2.3 El Ciclo de Vida del Sistema de Gestión de Seguridad de la Información

El ciclo de vida del Sistema de Gestión de Seguridad de la Información está compuesto por un proceso interminable de planificación, operacionalización, control y mejora. Este ciclo garantiza que la seguridad de la información se controle de manera efectiva a lo largo del tiempo mientras se enfrentan nuevas amenazas y cambios organizacionales. Cada fase del ciclo de vida del sistema de gestión de seguridad de la información se describe a continuación.

Figura 2 El Ciclo de Vida del Sistema de Gestión de Seguridad de la Información



Fuente: Elaboración propia.

Este ciclo de vida sigue la metodología PHVA (Planificar, Hacer, Verificar, Actuar). Esta metodología se torna clave para la evolución y sostenimiento operacional del SGSI dentro de un contexto de ciber amenazas y cambios en la organización.

1.7.2.4 Beneficios de un SGSI en las Cooperativas de Ahorro y Crédito

Implementar un SGSI trae claramente ventaja en el gestionamiento para las cooperativas de ahorro y crédito, entre las más relevantes están:

- **Optimización de la seguridad de la información:** El sistema integral de seguridad permite a la cooperativa proteger de manera más efectiva la información de los datos

críticos, así como disminuir la probabilidad de fuga, robo o alteración de datos.

- **Cumplimiento:** Con la implementación adecuada del SGSI dentro de la cooperativa, se protege a nivel local e internacional contra violaciones de seguridad de la información que pueden llevar a multas y perjudicar la imagen de la institución.
- **Resiliencia organizacional:** Con la planificación de continuidad del negocio y recuperación ante desastres, la cooperativa puede garantizar que el servicio estará disponible incluso con incidentes severos.
- **Confianza de los miembros:** Los miembros de la cooperativa confían en que sus datos están protegidos. Un SGSI efectivo fortalece esta confianza, lo que a su vez conduce a más asociados y mayor seguridad financiera.
- **Mejora continua:** La mejora continua del SGSI asegura que la cooperativa mitigará nuevas amenazas o cambios en la tecnología mientras siempre esté altamente protegida.

1.7.2.5 Implementación de un SGSI: Desafíos y Consideraciones

Establecer un SGSI en una cooperativa de ahorro y crédito no es fácil. Algunos de los desafíos más comunes son:

- **Resistencia al cambio:** Los trabajadores estarán renuentes a adoptar nuevas políticas o herramientas si la razón para hacerlo no es convincente, especialmente si ignoran qué es un SGSI.
- **Costos de implementación:** Para cooperativas que poseen limitaciones presupuestarias, la inversión en tecnologías, recursos humanos y capacitación es un gasto que presenta una dificultad ya que se necesita para implementar el SGSI.
- **Complejidad en la integración:** Si la infraestructura tecnológica es insuficiente o no es reciente, la cooperativa puede tener problemas con la integración de los procesos de

SGSI.

- **Necesidad de capacitación continua:** Debido a la naturaleza evolutiva de la ciberseguridad, los empleados deben actualizarse completamente con respecto a nuevas amenazas y tecnologías.

1.7.2.6 Estudio de Caso: La Implementación de un Sistema SGSI en una Organización Cooperativa

Tabla 6 *Fases de Implementación de un SGSI en una Cooperativa de Ahorro y Crédito*

Fase	Acción	Resultado Esperado
Planificación	Definición de políticas y procedimientos de seguridad de la información.	Documentación de políticas de seguridad clara y estructurada.
Identificación de Riesgos	Análisis de riesgos de seguridad y de impacto en los activos de información.	Identificación de vulnerabilidades y amenazas.
Implementación	Instalación de controles técnicos y organizacionales, y capacitación del personal.	Protección adecuada de los activos de información y empleados capacitados.
Monitoreo y Auditoría	Supervisión continua del SGSI y auditorías internas.	Monitoreo efectivo de las operaciones y auditoría regular de los procesos de seguridad.
Mejora Continua	Ajustes a las políticas y controles basados en los resultados del monitoreo y auditorías.	Adaptación continua del SGSI a nuevas amenazas.

Fuente: Elaboración propia.

La tabla 6 muestra de manera sencilla las etapas más importantes en la instalación de un Sistema de Gestión de Seguridad de la Información (SGSI) en una cooperativa de ahorro y

crédito. Cabe resaltar que cada fase es planteada de modo que la gestión de la seguridad de la información se convierta en algo que no solo se hace bien, sino que se hace integralmente bien, conservando así los ahorros de la cooperativa y garantizando que las operaciones continúen sin problemas.

La fase de Planificación es de gran importancia porque se plantea el SGSI. En esta fase, la cooperativa establece sus políticas de seguridad, lleva a cabo una auditoría de sus riesgos y de los controles que deben ser establecidos para esas Auditorías de Riesgos. El producto final debe ser políticas y procedimientos que son plasmados de tal forma que se asegure que la cooperativa realmente tiene medios efectivos para la gestión de amenazas cibernéticas de una forma lógica.

La Identificación de Riesgos tiene relación con el estudio de los riesgos que constituyen para los activos de información. En este paso se encuentran amenazas y también se encuentran fallas que permiten conocer los posibles impactos. Este análisis es una parte importante que deberá ser considerado para definir las medidas de seguridad que deberán ser adoptadas.

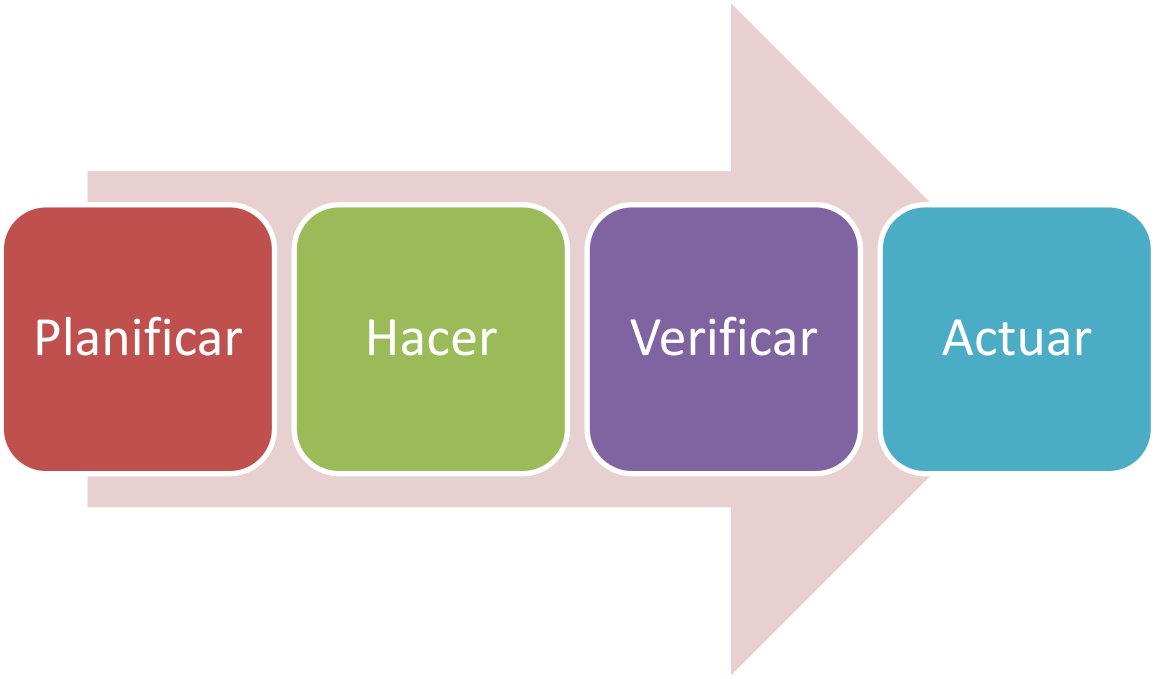
La Implementación es la fase donde se realiza el trabajo que se planificó anteriormente. Durante esta fase, se establecen controles informáticos y se brinda la capacitación pertinente al nuevo reglamento de seguridad. El objetivo es que la cooperativa cuente con la información necesaria junto con las herramientas para resguardar su información de forma adecuada.

El Monitoreo y Auditoría asegura que el SGSI cumpla su función. Con las auditorías periódicas y con el constante monitoreo, la cooperativa podrá detectar y solucionar alguna vulnerabilidad de seguridad que se presente a tiempo. Esto también permite asegurar el cumplimiento de las reglas y controles que se plantearon durante las etapas anteriores.

Con la fase de Mejora Continua se aporta para que el SGSI pueda ir cambiando con el

tiempo. Conforme se detectan posibles cambios, es posible realizar modificaciones que optimizan los controles de seguridad frente a nuevas amenazas. Con esto se busca que el SGSI sea estable en todos estos nuevos riesgos.

Figura 3 Ciclo de Vida de un SGSI



Fuente: Elaboración propia.

El gráfico ilustra la vida de un SGSI. De acuerdo con el modelo PHVA (Planificar, Hacer, Verificar, Actuar) la vida de un sistema o servicio de información está en un ciclo continuo. Las cooperativas son capaces de gestionar la seguridad de la información de su cooperativa en un ciclo activo y proactivo con este enfoque.

La fase de Planificar corresponde a la etapa de análisis y definición de las políticas y controles de seguridad. Esta fase define los procesos y objetivos que se tratarán en el SGSI, por tal motivo se le considera la primera fase al momento que se decide implementar un SGSI.

La fase de Hacer corresponde a la Acción, sugiere al menos la implementación de las políticas y controles que se definieron anteriormente. Es la fase donde se comienza a poner en

marcha aquello que fue planeado. Es la fase donde se compran, instalan y configuran todas las tecnologías necesarias y se capacita a los recursos humanos.

La verificación es fundamental para poder monitorear eficientemente cada uno de los elementos que constituyen el SGSI. Esta etapa permite asegurar que las acciones y medidas establecidas están funcionando de acuerdo con los objetivos y normas fijadas.

Gradualmente, la fase Actuar muestra cómo hay una necesidad de cambios y mejoras en el sistema de gestión de seguridad de la información (SGSI). A través de la retroalimentación recibida de la fase de verificación, la cooperativa puede modificar y mejorar sus medidas de seguridad para garantizar que haya una respuesta rápida a cualquier nuevo desafío.

Este ciclo repetitivo de Planificar, Hacer, Verificar y Actuar asegura que el SGSI sea constante y pueda acomodar cualquier cambio en el entorno de seguridad, lo que permite a la cooperativa mantenerse a salvo de amenazas cibernéticas.

1.7.3 Gestión de Riesgos en Seguridad Informática

La gestión de riesgos en seguridad informática es una práctica importante destinada a salvaguardar los activos de información en cualquier organización, particularmente en aquellas del sector financiero como las cooperativas de ahorro y crédito. Poder reconocer, evaluar y abordar los riesgos relacionados con las amenazas cibernéticas es necesario para garantizar que los sistemas y/o procesos sean operativos, confiables y eficientes. Esta sección analiza los aspectos pedagógicos más importantes de la gestión de riesgos en seguridad informática, sus metodologías y su alcance dentro de las instituciones financieras, particularmente cooperativas.

1.7.3.1 Definición de Gestión de Riesgos en Seguridad Informática

La gestión de riesgos en seguridad de la información se entiende como el conjunto de

acciones llevadas a cabo por una empresa para reconocer un determinado riesgo de seguridad informática y, dependiendo de su magnitud, decidir aceptarlo, intentar eliminarlo o implementar medidas que mitiguen sus efectos. Con respecto a los sistemas de información, los ordenadores conectados a la red o aquellos de los cuales se obtiene datos tienen su propio conjunto de funciones, y su uso suele estar regido por normas y políticas diseñadas para permitir la consecución de excusas aplicables, pero no limitadas únicamente a los objetivos positivos.

El proceso de gestión de riesgos opera dentro de un ciclo interminable e iterativo que permite a las organizaciones mejorar su control y medidas de protección a lo largo del tiempo. En este sentido, la gestión de riesgos no se limita a la identificación de amenazas, sino que incluye su estimación y evaluación de impacto para proporcionar la legitimidad y eficiencia de las medidas de seguridad dentro del contexto específico de la organización.

1.7.3.2 Componentes de la Gestión de Riesgos en Seguridad Informática

La gestión de riesgos en seguridad informática tiene algunas partes constitutivas importantes que deben implementarse para garantizar la seguridad de la información. Los componentes más importantes son: Este es el primer paso en el proceso de gestión de riesgos, es decir, la identificación de los riesgos y las posibles brechas a las que los activos de información pueden estar sujetos. Las amenazas pueden provenir del exterior (como ataques cibernéticos, instalación de programas maliciosos o desastres naturales) o del interior (como errores o fallas del sistema). Las brechas son los puntos débiles en los diversos componentes del sistema que pueden ser alcanzados por la amenaza.

Una evaluación de riesgos implica asignar un valor al riesgo evaluando tanto su probabilidad de ocurrir como el daño que causaría si se presentara. Esto puede estimarse a

través de métodos cualitativos o cuantitativos, donde se da una probabilidad del riesgo y sus impactos en las operaciones de las cooperativas.

La mitigación de riesgos tiene como objetivo contrarrestar los riesgos estableciendo límites para disminuir la posibilidad de su ocurrencia o reducir su impacto. Estos pueden clasificarse en técnicos (la implementación de cortafuegos, políticas de contraseñas o autenticación de múltiples factores), organizativos (políticas de seguridad y procedimientos de respuesta ante incidentes) o físicos (seguridad de edificios y equipos).

Las cooperativas deben cambiar su percepción de la gestión de riesgos en ciberseguridad de un enfoque de evento único a un ciclo continuo, ya que siempre habrá nuevas amenazas y vulnerabilidades con el tiempo. Esto significa que debe haber una monitorización proactiva constante y evaluaciones de riesgos realizadas para garantizar que la seguridad se mantenga suficiente.

Gestión de Incidentes:

Si bien la mitigación de riesgos es un aspecto importante, aún puede ocurrir una brecha de seguridad. En estos casos, debe haber un plan de respuesta ante incidentes, que permita a la organización identificar, contener y remediar el incidente lo más rápido posible para minimizar daños y regresar a operaciones comerciales normales.

1.7.3.3 Metodologías de Gestión de Riesgos en Seguridad de Tecnologías de la Información

En seguridad de tecnologías de la información, el paso de evaluación y mitigación en la gestión de riesgos también puede realizarse en forma de escalación debido a la existencia de muchos sistemas que se utilizan. Algunas metodologías comúnmente utilizadas son las siguientes:

- ***MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información):*** es una metodología española que integra el análisis y gestión de riesgos de sistemas de información. MAGERIT se utiliza ampliamente en el campo de la seguridad informática. MAGERIT proporciona un enfoque integral en la identificación y evaluación de riesgos en los sistemas de información con la ayuda de la análisis de amenazas y la elaboración de posibles procedimientos correctivos.
- ***ISO/IEC 27005:*** Esta norma ofrece pautas para la gestión de riesgos de seguridad de la información en el contexto del Sistema de Gestión de Seguridad de la Información (SGSI). La norma ISO/IEC 27005 describe un proceso sistemático para identificar, evaluar y tratar los riesgos de seguridad de la información de acuerdo con los requisitos de ISO/IEC 27001.
- ***NIST (Instituto Nacional de Estándares y Tecnología):*** NIST ha desarrollado un marco de gestión de riesgos conocido como NIST 800-53 que define un conjunto de controles de seguridad siguiendo una evaluación continua de riesgos. Este marco es bien conocido en los Estados Unidos y se adapta perfectamente a las necesidades de las cooperativas de ahorro y crédito que manejan información sensible.
- ***OCTAVE (Evaluación de Amenazas, Activos y Vulnerabilidades Críticamente Operativos):*** OCTAVE es una metodología que proporciona un medio para que las organizaciones definan y evalúen los riesgos relacionados con sus activos críticos. Se basa en el riesgo operativo y la evaluación dentro del contexto organizacional con una evaluación cualitativa de la amenaza y la vulnerabilidad.

1.7.3.4 Herramientas y Técnicas para la Gestión de Riesgos

Las cooperativas de ahorro y crédito tienen a su disposición varias herramientas y técnicas que les permiten gestionar riesgos en ciberseguridad. Algunas de ellas son las siguientes:

Herramientas para el Análisis de Vulnerabilidades:

Software que permite escanear los sistemas de la asociación en busca de debilidades. Estas herramientas ayudan a detectar ciertas áreas riesgosas que podrían ser aprovechadas por los adversarios. Algunos de ellas son: Nessus, OpenVAS y Qualys.

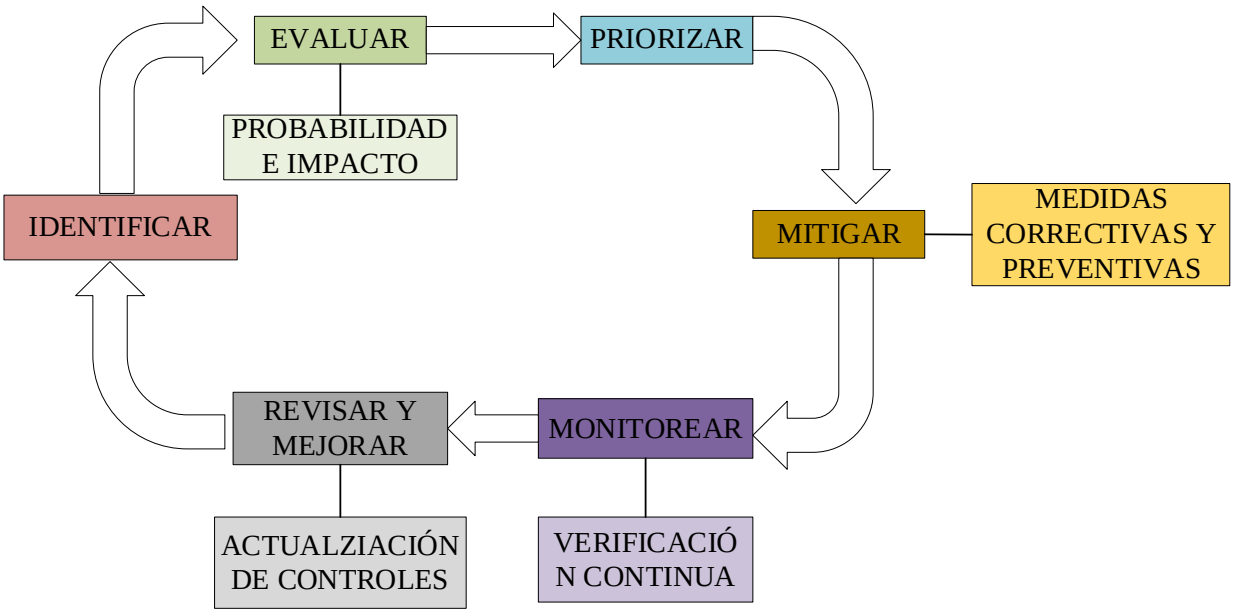
Herramientas de Monitoreo de Seguridad:

Estas herramientas son importantes para prevenir o mitigar violaciones de seguridad. Estas herramientas permiten a la organización realizar una vigilancia continua de las redes y sistemas en cuestión, reportando puntos de preocupación o actividad anómala. Algunos ejemplos son SIEM (Gestión de Información y Evento de Seguridad) como Splunk o ArcSight.

Sistemas de Gestión de Incidentes:

Estos sistemas permiten estructuralmente el esfuerzo de tratar las violaciones de seguridad cuando ocurren, facilitando la coordinación de acciones y documentando los procesos llevados a cabo. Algunos ejemplos son Remedy y ServiceNow.

Figura 4 *Ciclo de Gestión de Riesgos en Seguridad de la Información*



Fuente: Elaboración Propia - Adaptado de ISO/IEC 27005 y MAGERIT.

La Figura 4 ilustra de manera representativa el ciclo iterative de gestión de riesgos y seguridad que debe implementarse de manera variable en toda la organización. Este modelo asegura que los riesgos no solo sean identificados y tratados, sino que también sean revisados periódicamente de tal manera que la evolución constante sea posible debido a nuevas amenazas o vulnerabilidades que puedan surgir.

La retroalimentación dada hacia el final del ciclo asegura la evolución del ISMS frente al cambio tecnológico y organizacional. Es importante que las cooperativas como Fasayñan Ltda. integren este enfoque sistemático para fortalecer su resiliencia institucional.

1.7.3.5 Evaluación de Riesgos en una Cooperativa de Ahorro y Crédito

En el caso de las cooperativas de ahorro y crédito, la evaluación de riesgos es aún más importante debido a la naturaleza delicada de la información financiera que manejan. Las piezas de información más sensibles incluyen los datos personales de los miembros, sus transacciones de gestión financiera y de crédito. La evaluación de riesgos debe tener en cuenta

aspectos como el fraude interno, los ataques de phishing externos, el robo de información y también las debilidades relacionadas con la tecnología, las políticas de seguridad y los procedimientos operativos.

Tabla 7 *Evaluación de Riesgos de Seguridad de la Información en la Cooperativa Fasayñan Ltda.*

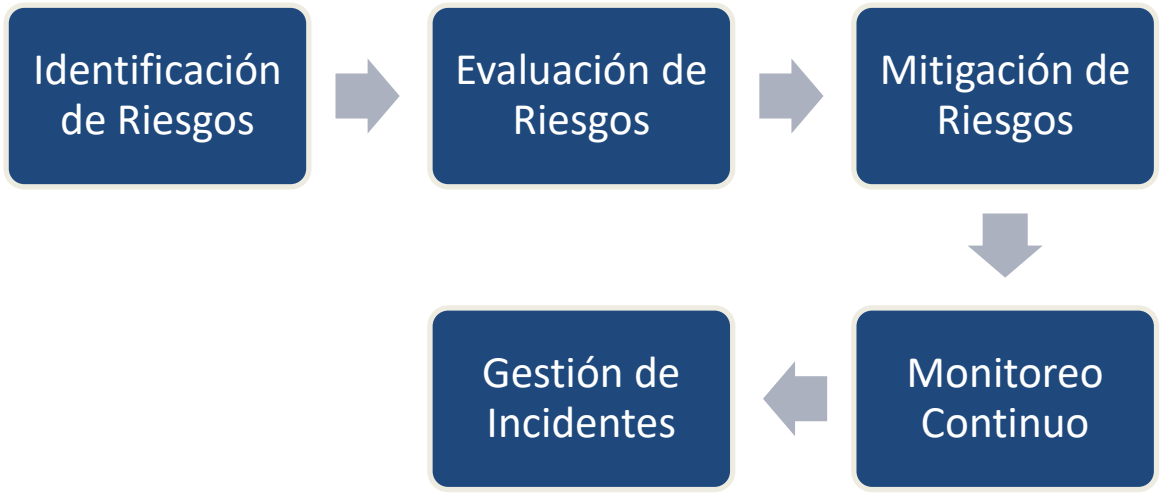
Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Medidas Mitigadoras
Acceso no autorizado a datos de socios	Alta	Crítico	Alto	Implementación de controles de acceso, autenticación multifactorial.
Phishing dirigido a empleados	Media	Alto	Medio	Capacitación en ciberseguridad, filtros de correo electrónico.
Fuga de información financiera	Baja	Alto	Medio	Encriptación de datos, monitoreo continuo.

Fuente: Elaboración propia con base en diagnóstico institucional y estándares ISO/IEC 27005.

La Tabla 7 muestra una evaluación básica de los principales riesgos cibernéticos presentes en la cooperativa, categorizados según su probabilidad de ocurrencia e impacto potencial. Este análisis permite determinar el nivel de riesgo (bajo, medio o alto) y sugerir medidas de mitigación concretas alineadas con buenas prácticas internacionales.

Este enfoque permite priorizar los riesgos más críticos —como el acceso no autorizado— y asignar recursos de seguridad de manera más eficiente. Además, sienta las bases para construir una matriz de riesgos ampliada como parte del plan de mejora del SGSI.

Figura 5 Ciclo de Gestión de Riesgos en Seguridad Informática



El manejo de riesgos en seguridad informática es un procedimiento clave en la protección de la información dentro de las cooperativas de ahorro y crédito. La adopción de métodos organizados como MAGERIT o ISO/IEC 27005, así como la utilización de sofisticadas herramientas de análisis de vulnerabilidades y monitoreo de seguridad, permite la identificación, evaluación y reducción de riesgos. Igualmente, las cooperativas deberán incorporar la posibilidad de la gestión de riesgo en el conjunto de políticas de seguridad para asegurar que los controles en un entorno hostil para la cibernética tan cambiante sean adecuados y eficientes.

1.7.4 Reglas y Normas de la Política de Seguridad de la Información

Las reglas y normas de la política de seguridad de la información son el aspecto clave para el éxito de un Sistema de Gestión de Seguridad de la Información (SGSI). Este es especialmente el caso en el sector financiero, donde la sensibilidad de la información gestionada hace que la protección de datos sea fundamental. Estos marcos sensibles garantizan

que se mantengan las leyes de tecnología de la información y las mejores prácticas de tecnología de la información por parte de las cooperativas de ahorro y crédito.

1.7.4.1 Normas y Normas Internacionales Primarias

Existen varias normas y estándares internacionales que ofrecen instrucciones sobre cómo controlar la seguridad de la información. Las más notables son las dos ISO/IEC 27001 e ISO/IEC 27002 porque son reconocidas e implementadas a nivel global. Estas normas sirven no solo como guías para la gestión de la seguridad de la información, sino también para el cumplimiento de los requisitos regulatorios locales e internacionales.

ISO/IEC 27001:

Este estándar internacional establece los requisitos para el establecimiento, implementación, mantenimiento y mejora de un SGSI. La ISO/IEC 27001 es el estándar más reconocido internacionalmente para la gestión de la seguridad de la información. Trata sobre la identificación y gestión de los riesgos de seguridad de la información, lo que ayuda a las organizaciones a proteger sus activos informáticos de amenazas internas y externas; y asegura la confidencialidad, integridad y disponibilidad de los datos (Organización Internacional de Normalización [ISO], 2013).

ISO/IEC 27002:

Además de la ISO/IEC 27001, la ISO/IEC 27002 está destinada a ofrecer orientación sobre prácticas y controles de seguridad para la protección de la información. Este estándar abarca los principales elementos de seguridad como el control de acceso, la encriptación de la información, la seguridad en las comunicaciones y la seguridad física. La ISO/IEC 27002 ofrece asistencia a las instituciones que deseen adoptar medidas de seguridad personalizadas a sus condiciones predefinidas (ISO, 2013).

ISO/IEC 27005:

Presenta directrices sobre la gestión de riesgos de seguridad de la información con un poco más de granularidad sobre cómo capturar, analizar y mitigar riesgos concernientes a la seguridad de la información y los datos. Este estándar es importante para garantizar que las Cooperativas de Ahorro y Crédito evalúen los riesgos relacionados con la información que poseen de manera razonable (ISO, 2011).

ISO/IEC 27034:

Este conjunto de estándares se centra en la seguridad de las aplicaciones. Establece algunos principios y directrices sobre los aspectos de seguridad que deben ser integrados en todo el ciclo de vida del desarrollo de sistemas de aplicaciones. Como muchas cooperativas cuentan con sistemas de aplicaciones internas para capturar datos de miembros y transacciones financieras, la ISO/IEC 27034 ayuda a garantizar que tales aplicaciones no representen riesgos indebidos para la seguridad de la información (ISO, 2011).

Tabla 8 *Comparación de Normas ISO/IEC Relacionadas con la Seguridad de la Información*

Norma	Propósito Principal	Alcance	Aplicación en el SGSI
ISO/IEC 27001	Establecer los requisitos para implementar un SGSI	Gestión organizacional de seguridad de la información	Base para certificación de un sistema de gestión
ISO/IEC 27002	Brindar directrices para implementar controles de seguridad	Controles específicos en áreas como acceso, cifrado, etc.	Apoya la implementación de controles definidos en ISO 27001
ISO/IEC 27005	Proporcionar directrices para la gestión de riesgos de	Metodología para identificar, evaluar y tratar riesgos	Sustenta el análisis de riesgos requerido por la ISO 27001

	seguridad		
ISO/IEC 27034	Integrar la seguridad en el desarrollo de aplicaciones	Seguridad en el ciclo de vida del software	Fortalece la protección de sistemas informáticos internos

Fuente: Elaboración propia basada en estándares ISO.

La Tabla 8 sintetiza las principales normas ISO que respaldan un SGSI robusto. Cada una cumple un rol específico:

- ISO 27001 actúa como el eje central para la certificación y estructura del SGSI.
- ISO 27002 ofrece una guía práctica para establecer controles detallados.
- ISO 27005 orienta en el análisis de riesgos que da sustento al diseño del SGSI.
- ISO 27034 garantiza que las aplicaciones utilizadas o desarrolladas internamente cumplan con estándares de seguridad.

Estas normas trabajan de forma integrada para asegurar que la gestión de seguridad sea proactiva, técnica, estratégica y basada en riesgos.

1.7.4.2 Normas Locales y Regionales

A nivel local, cada Cooperativa de Ahorro y Crédito también debe cumplir con un conjunto de reglas que difieren de un país o región a otro. En varias jurisdicciones, los organismos reguladores en la industria de servicios financieros han prescrito reglas y regulaciones destinadas a salvaguardar los datos financieros así como la seguridad de la información.

Reglamento General de Protección de Datos (GDPR):

Las cooperativas que operan en y tienen clientes en la Unión Europea deben cumplir con el Reglamento General de Protección de Datos (GDPR). La ley se ha establecido para

restringir la gestión de información personal y sensible a través de la implementación de medidas de protección contra el acceso no restringido, el robo o la alteración de datos (Unión Europea, 2016).

Superintendencia de Economía Popular y Solidaria (SEPS):

En Ecuador, las cooperativas de ahorro y crédito están reguladas por la SEPS, que tiene protocolos para la gestión segura de datos dentro de la industria. La SEPS exige que las cooperativas implementen Sistemas de Gestión de Seguridad de la Información (SGSI) robustos que protejan la información financiera y personal de los clientes y cumplan con estándares internacionales de seguridad de la información (Superintendencia de Economía Popular y Solidaria [SEPS], 2022).

1.7.4.3 Adherencia a las Regulaciones en Cooperativas de Ahorro y Crédito

Lograr la integración de estándares de seguridad de la información es vital para las cooperativas de ahorro y crédito. No solo asegura la protección de la información sensible, sino que también agrega valor a la imagen de la cooperativa y genera confianza entre los miembros. La implementación de un Sistema de Gestión de Seguridad de la Información, o SGSI, que cumpla con estándares internacionales como ISO/IEC 27001 y regulaciones locales emitidas por la SEPS permite a la cooperativa gestionar eficazmente los riesgos de seguridad y los cambios en el entorno de seguridad.

La integración de estas regulaciones permite la incorporación de un marco integral para la gestión de la seguridad de la información (GSI). La integridad y la vida útil de la información, desde la creación hasta el almacenamiento y destrucción, están protegidas por estas regulaciones.

1.7.4.4 Desafíos y Logros en el Cumplimiento

Lograr el cumplimiento de los estándares de seguridad de la información y otras regulaciones tiene sus desafíos y fortalezas para las cooperativas de ahorro y crédito.

Tabla 9 *Desafíos y Beneficios del Sistema de Gestión de Seguridad de la Información (SGSI)*

Desafíos	**Descripción de los Desafíos**	**Beneficios**	**Descripción de los Beneficios**
Costo de implementación	La adopción de un SGSI conforme a estándares internacionales implica una inversión en nueva infraestructura de TI, capacitación de recursos humanos y la implementación de controles de seguridad.	Mejora de la protección de datos	La adopción de un SGSI aumenta la protección de la información dentro de la organización y reduce las violaciones de seguridad, especialmente con la implementación de estándares específicos.
Resistencia al cambio	Los empleados pueden resistir el cumplimiento de políticas que protegen la seguridad organizacional si no aprecian su importancia o carecen de la capacitación adecuada.	Cumplimiento normativo	Adherirse a regulaciones internacionales y nacionales asegura que la cooperativa se mantenga dentro del marco legal, evitando sanciones y mejorando su imagen.
Monitoreo constante	El cumplimiento	Confianza de otros	La adopción de políticas

	normativo necesita un monitoreo constante y una revisión frecuente de las políticas y controles de seguridad para hacer frente a nuevos cambios.	miembros	de seguridad sólidas genera confianza entre los socios que observan que la cooperativa se preocupa por salvaguardar su información personal y financiera.

Fuente: Elaboración propia basada en estándares ISO.

La implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las entidades de ahorro y crédito presenta tanto retos como oportunidades que es necesario analizar en su total magnitud con el fin de asegurar su éxito. En relación con los retos a superar, es el costo de implementación uno de los que destaca sobremanera. Adoptar un SGSI alineado a normas internacionales exige realizar gastos de orden infraestructura tecnológica, capacitación de personas y establecimiento de controles de seguridad que son significativas. Para las cooperativas de recursos escasos, este gasto puede inicialmente aparecer como un obstáculo. No obstante, resulta necesario señalar que, a la larga, estos costos constituirán una inversión en la salvaguarda de los activos de información de la cooperativa, lo que les permitirá ahorrar y evitar gastos originados por problemas de seguridad.

Otro desafío clave es la resistencia de los empleados al cambio. La implementación de nuevas políticas de seguridad puede enfrentar oposición, particularmente cuando los empleados no entienden la importancia de tales políticas o si no se les proporcionan suficientes enseñanzas. Para superar la barrera, debe haber un enfoque claro hacia la concienciación y capacitación para que el personal aprecie la importancia de la seguridad de la información y

sea capaz de implementar las políticas de manera eficiente. Esta falta de conocimiento o subestimación de las consecuencias de las amenazas cibernéticas puede llevar a incidentes comprometidos que ponen en peligro la integridad de la información y el funcionamiento de la cooperativa.

Otro problema persistente es el monitoreo continuo de las políticas y controles de seguridad. A medida que las amenazas cibernéticas se vuelven más complejas y hay un cambio en la legislación, la cooperativa necesita mantener actualizado el nivel de seguridad de sus sistemas. Esto requiere un monitoreo continuo, auditorías regulares y cambios en las políticas con la aparición de nuevas brechas o cambios en el entorno de seguridad. Si bien este esfuerzo puede parecer irrazonablemente excesivo, es necesario para que la cooperativa mantenga un nivel razonable de protección.

A pesar de los desafíos, las ventajas de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) son significativas. Uno de los beneficios más importantes es la mejora en la salvaguarda de datos. La adopción de un SGSI aumenta enormemente la capacidad de la cooperativa para proteger la información sensible de los miembros y de la propia cooperativa contra accesos no autorizados, ciberataques y una serie de otras amenazas. Esto no solo salvaguarda los datos, sino que también minimiza las posibilidades de violaciones de seguridad que son más propensas a poner en riesgo la reputación de la cooperativa.

El cumplimiento legal es otra ventaja crítica. La implementación de un SGSI dentro de un marco internacional y local, como la ISO/IEC 27001 y las correspondientes regulaciones nacionales, asegura que la cooperativa cumpla con las obligaciones legales y regulatorias dentro de su jurisdicción. Este tipo de cumplimiento no solo ayuda a prevenir sanciones y multas, sino que también aumenta la confianza de los socios al saber que la cooperativa se

toma en serio la protección de la información.

Finalmente, la confianza de los socios es uno de los beneficios más importantes de un SGSI implementado a la perfección. Con la adopción de políticas de seguridad sólidas, hay una mayor confianza entre los socios, quienes están más dispuestos a creer que su información privada y financiera está segura. Esta confianza se traduce en una alta retención de socios, nuevos miembros que se unen y una reputación de mercado más fuerte que, a su vez, mejora el crecimiento sostenido de la cooperativa.

Aunque la implementación de un SGSI presenta desafíos significativos, los beneficios en confianza de los socios, protección de datos y cumplimiento lo justifican. Las cooperativas de crédito deben darse cuenta de la importancia de la seguridad de la información como más que un requisito técnico, sino como una estrategia cuyo impacto se siente en la sostenibilidad y el éxito a largo plazo. La parte más importante es cómo abordar estos problemas de manera sistemática, de modo que la seguridad de la información esté integrada en la cultura organizacional.

1.7.4.5 Efecto de las Normas en la Gestión de Asuntos de Seguridad de la Información

Figura 6 Relación entre las normativas de seguridad de la información y las áreas clave del SGSI

Las regulaciones internacionales como las locales interactúan con los componentes clave de un Sistema de Gestión de Seguridad de la Información (ISMS), lo que permite cubrir todos los temas relacionados con la seguridad de la información.

Las normas y estándares de seguridad de la información proporcionan un marco que permite a las cooperativas de ahorro y crédito gestionar eficazmente los riesgos cibernéticos y proteger los datos sensibles de sus miembros. La implementación de un ISMS basado en la norma ISO/IEC 27001 y en regulaciones locales como las de la SEPS, no solo ayuda a asegurar la información, sino que también mejora la confianza de los socios y garantiza que se cumplan las disposiciones legales. Estas regulaciones pueden ser difíciles de implementar, aunque las ganancias a largo plazo en protección de la información y la reputación de la cooperativa son significativas.

1.7.5 Controles de Seguridad dentro de los Sistemas de Información

Como entidad organizacional, estos controles de seguridad reconfirman que es necesario idear medios para proteger la información de los riesgos impuestos por las amenazas cibernéticas. Las medidas de seguridad son preventivas y correctivas. Su implementación debe recibir la máxima atención en una organización.

Tabla 10 Clasificación de Controles de Seguridad en los Sistemas de Información

Tipo de Control	Propósito Principal	Cooperativas de Ahorro y Crédito
Preventivo	Evitar que ocurra un incidente de seguridad	Políticas de contraseñas seguras, autenticación multifactor, control de acceso físico
Detectivo	Identificar y alertar sobre un incidente en curso o ocurrido	Sistemas de monitoreo (SIEM), registros de auditoría, sensores de intrusión
Correctivo	Restaurar el sistema o mitigar los efectos del incidente	Planes de contingencia, recuperación de respaldo, reconfiguración de sistemas comprometidos

Fuente: Elaboración propia con base en ISO/IEC 27002:2022.

La Tabla 10 organiza los controles de seguridad en función de su función dentro del ciclo de protección de la información. Esta clasificación permite a la cooperativa:

- Prevenir proactivamente incidentes con políticas y barreras técnicas.
- Detectar eventos sospechosos o anomalías mediante monitoreo.
- Corregir rápidamente cualquier daño o vulnerabilidad posterior al incidente.

Este enfoque tridimensional debe integrarse al diseño del SGSI para alcanzar una protección integral y dinámica frente a amenazas internas y externas.

Las medidas más comunes son: autenticación de usuarios, control de acceso a sistemas y datos, cifrado de información, monitoreo continuo de redes y sistemas, y el uso de cortafuegos y programas antivirus.

La seguridad de la información dentro de la organización se basa en las medidas recomendadas por la ISO/IEC 27002 y otros estándares internacionalmente aceptados relacionados con esta área. Estas recomendaciones son inclusivas en áreas clave de seguridad de la comunicación, gestión de incidentes de seguridad, seguridad física y continuidad del negocio o recuperación ante desastres. Con respecto a la información proporcionada, se busca reducir significativamente la probabilidad de ser víctima de un ataque cibernético mientras se asegura que la información requerida esté protegida.

En el caso de las cooperativas de ahorro y crédito, estas medidas deben aplicarse con flexibilidad en relación a ciertos parámetros de la organización, como la infraestructura tecnológica, los recursos disponibles y los riesgos encontrados en la evaluación de riesgos. Además, existe la necesidad de realizar exámenes que determinarán si todos los controles aún cumplen con la efectividad esperada contra nuevas amenazas emergentes.

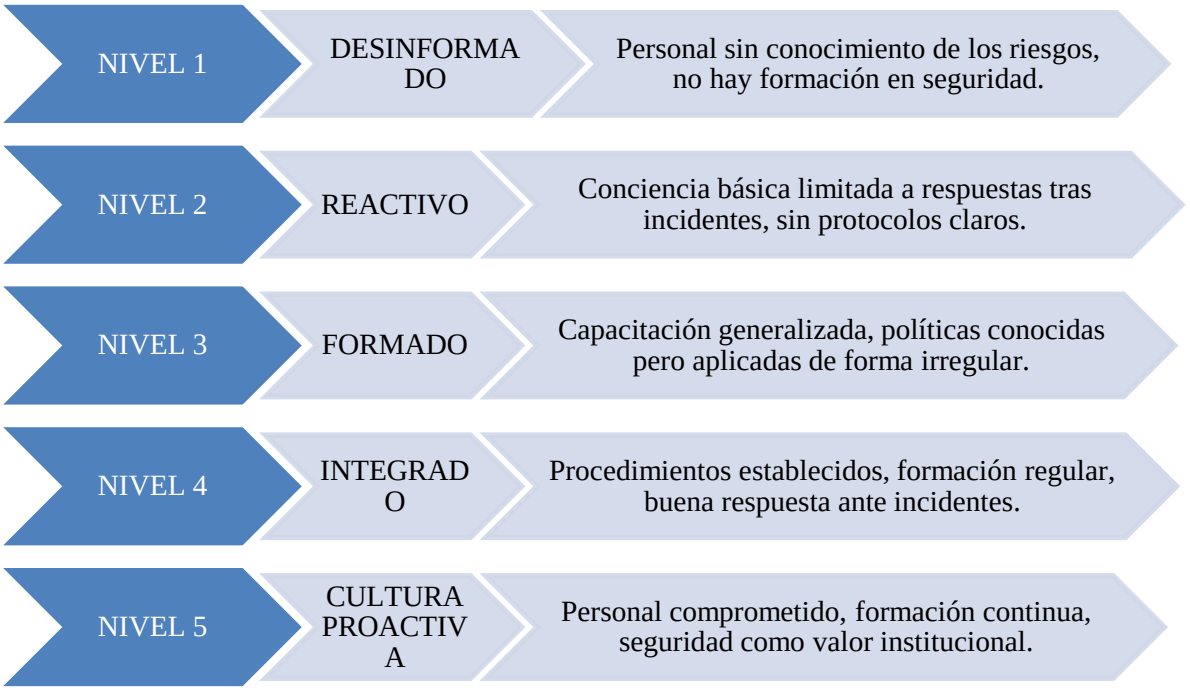
1.7.6 Cultura de Ciberseguridad y Capacitación del Personal

La capacitación del personal es un subproceso crítico dentro del ámbito de la seguridad de la información. La mayoría de los incidentes de seguridad provienen de errores humanos o de la falta de conocimiento sobre las prácticas de seguridad. Por lo tanto, es necesario que las organizaciones cuenten con programas de capacitación periódicos sobre ciberseguridad para cada miembro de la organización.

Como se enfatiza en la ISO/IEC 27034, junto con cada aspecto de la seguridad de la información, cada etapa del ciclo de vida de los sistemas de información debe incluir la

seguridad dentro de sus objetivos, lo que también abarca la educación y la capacitación. Los empleados deben conocer qué riesgos cibernéticos existen, cuáles son las amenazas básicas y qué políticas de seguridad interna se implementan. Solo así se puede esperar que tomen acciones preventivas antes de la ocurrencia de incidentes que se conviertan en problemas graves y respondan adecuadamente.

Figura 7 Niveles de Madurez en la Cultura de Ciberseguridad Organizacional



Fuente: Adaptado de ENISA (2022) y modelo de madurez NIST.

La Figura 7 muestra cómo evoluciona la madurez cultural en ciberseguridad dentro de una organización. Pasar de una etapa desinformada a una proactiva implica un cambio no solo en la formación del personal, sino en su percepción del riesgo y su participación activa en la protección de la información.

Este modelo puede ser utilizado por la Cooperativa Fasayñan Ltda. como herramienta

de diagnóstico y planificación para diseñar su programa de concienciación alineado con ISO/IEC 27034.

Adoptar una cultura organizacional de ciberseguridad no solo fortalece la protección de los activos de información, sino que también mejora la eficiencia operativa y la resiliencia cibernética de la cooperativa.

Capítulo II. Diagnóstico situacional

2.1 Metodología

El marco teórico es esencial para conocer los fundamentos de la Seguridad de la Informacióny la implementación en las Cooperativa. Como señala Johnson (2018), el marco teórico es "el conjunto de conceptos, teorías y modelos que ayudan a comprender el fenómeno bajo estudio". Enlo que se respecta a la SI, esta comprensión es fundamental para abordar eficazmente los desafíosy amenazas que enfrentan las organizaciones.

Todo el proceso del presente informe que se basa en el Análisis y Mejora del Sistema de Gestión de la Información dentro de la Coac. Fasayñan se desarrolla en faces mismas que están estructuradas y descritas en el cronograma de actividades.

Primer paso. Recabar toda la información que mantiene la cooperativa en lo referente a Seguridad de la información con la cual se podrá identificar los riesgos de activos de informacióny definir las políticas internas para hacer frente a la amenazas y todo tipo de ataque cibernético, con todo la información que se recabe se podrá hacer una selección de la información consideradacomo estratégica y útil y desechar la no valida, de igual forma se seleccionara todo el material bibliográfico base para este informe, con el fin de sustentar adecuadamente el presente trabajo.

Segundo Paso. Con la información recabada se arrancará con la ejecución del análisis y mejoradel sistema de gestión de la Información, que es fundamental para evaluar o conocer el estado de la Institución en temas se seguridad de la información.

Evaluar diversas estrategias para reducir y mitigar los ciberataques dentro de la cooperativa. Analizar los posibles riesgos a los que se enfrentan los departamentos administrativos y operativos de la COAC FASAYÑAN.

Tercer paso. Asimismo, de cada área laboral que tiene la Institución recoge la información deltodo su personal para determinar su conocimiento en temas referentes a Gestión de la Información,todo esto se realiza aplicando encuetas al personal sobre el tema.

Cuarto paso. Se procede a recopilar información de todos los activos de información, para determinas con que activos cuenta la Cooperativa y medir cueles son críticos para jerarquizarlos por su importancia por el impacto que puedan tener dentro de la Institución

Quinto paso. Identificado y definidos los activos críticos se procede a levantar el proceso de riesgos el cual a más de identificar las amenazas mide su impacto dentro de la Institución pues determina su impacto y su probabilidad de concurrencia.

Sexto paso. Definidos el tipo de riesgos, se analiza el tipo de vulneración que tiene la Cooperativa y las áreas más críticas o susceptibles a ataques y así definir la matriz para clasificar los resultados.

Séptimo paso. Con los resultados obtenidos tanto de las encuestas y las matrices se elaboró elAnálisis y Mejora del Sistema de Gestión de la Información dentro de la Coac. Fasayñan, y el planpara su aplicación todo esto enmarcado en lo norma ISO 27001 donde se asegure la confidencialidad, integridad de toda la información de la Cooperativa. Con todo esto se procede aentregar el documento final a la alta gerencia donde se detalla un informe para los directivos o miembros del comité de Seguridad de la Información con los resultados obtenidos las conclusionesy recomendaciones y el informe técnico donde se detalla todas las actividades desarrolladas y losresultados que se obtuvo.

Evaluación de Seguridad de Tecnología de la Información en la Cooperativa Fasayñan Ltda.

La evaluación es crucial para establecer qué tan bien está diseñado e implementado el sistema de seguridad de la información en la Cooperativa de Ahorro y Crédito Fasayñan Ltda. Incluye la recolección de archivos disponibles dentro de la institución, así como la realización de entrevistas técnicas, psicológicas y organizacionales, a través de las cuales fue posible evaluar el nivel de confianza relativo a las políticas corporativas y las prácticas de seguridad de la información. En la recolección de información se utilizaron entrevistas estructuradas, cuestionarios con una escala de Likert y una metodología de evaluación de riesgos basada en la norma ISO/IEC 27005.

Instrumento de Evaluación de Riesgos

El instrumento utilizado para la jerarquización de riesgos fue de enfoque mixto, combinando variables cuantitativas (probabilidad e impacto) y cualitativas (percepción del personal, análisis documental). Se empleó una matriz de riesgos basada en ISO/IEC 27005 que califica:

- Probabilidad de ocurrencia: Baja, Media o Alta
- Impacto potencial: Bajo, Medio o Alto

La combinación de ambas dimensiones permitió clasificar el nivel de riesgo global de cada activo, de acuerdo con la siguiente regla:

Tabla 11 *Matriz de riesgos basada en ISO/IEC 27005*

Probabilidad / Impacto	**Bajo**	**Medio**	**Alto**
Alta	Medio	Alto	Alto
Media	Bajo	Medio	Alto

Baja	Bajo	Bajo	Medio

Asimismo, en el caso del personal, se complementó este análisis mediante encuestas con escala tipo Likert de 5 niveles, lo que permitió cuantificar el nivel de conocimiento, percepción y prácticas asociadas a la seguridad digital.

Preguntas de Encuesta Aplicadas

Las encuestas fueron dirigidas a 38 empleados, enfocándose en evaluar la cultura organizacional sobre ciberseguridad. Se utilizaron afirmaciones cerradas, valoradas de 1 (Totalmente en desacuerdo) a 5 (Totalmente de acuerdo):

Tabla 12 *Ejemplos de Preguntas de Encuesta Aplicadas*

Nº	**Pregunta**	**Escala Likert (1–5)**
1	Conozco los protocolos establecidos en caso de incidentes de seguridad informática.	
2	He recibido capacitación en ciberseguridad en los últimos 12 meses.	
3	Considero que los sistemas de información de la cooperativa son seguros y confiables.	
4	Siento que tengo las herramientas necesarias para proteger la información de socios.	
5	Existe una política clara de gestión de contraseñas en mi área de trabajo.	

Fuente: Elaboración propia. Encuesta aplicada a colaboradores de Fasayñan Ltda., 2024.

Activos Críticos Identificados y Nivel de Riesgo Asociado

El siguiente inventario representa los activos informáticos más relevantes de la cooperativa, priorizados con base en su valor institucional y el nivel de riesgo que enfrentan:

Tabla 13 *Activos Críticos de Información y Nivel de Riesgo*

Activo de Información	Clasificación	Valor Institucional	Amenazas Identificadas	Nivel de Riesgo
Base de datos de socios	Confidencial	Crítico	Acceso no autorizado, pérdida de datos	Alto
Sistema de gestión de créditos	Confidencial	Alto	Interrupción de servicio	Alto
Correo institucional	Interno	Medio	Suplantación de identidad, phishing	Medio
Información en hojas Excel local	No clasificada	Bajo	Eliminación accidental, falta de respaldo	Bajo

Fuente: Elaboración propia a partir de entrevistas y levantamiento de activos.

Este diagnóstico hace posible no solo tener un mapa actualizado de riesgos y activos críticos, sino también identificar ausencias importantes en capacitación, cultura organizacional y lineamientos internos. Los resultados permitirán elaborar un plan de implementación para el SGSI, basado en controles relevantes y en los más apropiados para el contexto de la cooperativa.

Trazabilidad

Para mejorar la consistencia metodológica del estudio, se proporciona una matriz de trazabilidad que asocia los problemas con objetivos específicos, metodología aplicada y

resultados esperados. Este arreglo ilustra las interrelaciones lógicas y sistemáticas de los diversos componentes del diseño de investigación. Garantiza que todas las acciones tomadas estén adaptadas para satisfacer una necesidad única tal como se articula en el diagnóstico, al mismo tiempo que ayuda en el logro de los objetivos descritos.

Tabla 14 *Trazabilidad: Problema - Objetivo - Metodología - Resultado Esperado*

Problema Identificado	Objetivo Específico	Metodología / Técnica	Resultado Esperado
La cooperativa no cuenta con un SGSI, lo que la expone a riesgos cibernéticos significativos	Identificar y evaluar los activos de información que tienen mayor valor	Levantamiento de activos, entrevistas, categorización con matriz de criticidad	Inventario de activos críticos y clasificación por nivel de riesgo
Desconocimiento del personal sobre ciberseguridad y amenazas	Desarrollar un programa de capacitación en concienciación sobre ciberseguridad	Aplicación de encuestas de diagnóstico, diseño de plan de capacitación basado en ISO 27034	Programa de formación alineado con buenas prácticas que mejore la cultura organizacional en seguridad
Incumplimiento con la norma ISO/IEC 27001 y la resolución SEPS-2022-002	Determinar el nivel de cumplimiento con normas de seguridad y brechas existentes	Auditoría documental y revisión de políticas internas	Informe de cumplimiento con ISO 27001, identificación de brechas y plan de mejora
No existen procesos definidos para evaluar y mitigar riesgos	Formular un plan integral de control y mitigación de riesgos	Aplicación de MAGERIT, matriz de impacto y	Mapa de riesgos cibernéticos y plan de mitigación por área

cibernéticos	probabilidad, clasificación de riesgos

Fuente: Elaboración propia basada en el diagnóstico institucional y la normativa ISO/IEC 27001.

2.2 Análisis situacional

La cooperativa de Ahorro y Crédito Fasayñan Ltda, es una institución financiera perteneciente a la red de estructuras financieras del Astro (REFLA), supervisada por la Superintendencia de Economía Popular y Solidaria (SEPS), con presencia en el Austro ecuatoriano desde el 2002, poresta razón y al avance de la tecnología y el crecimiento de la amenazas cibernéticas, se debe evaluarla actual situación de la Institución, ya que no cuenta con un sistema acorde a la realidad en temasde seguridad de la Información y un plan estructurado sobre Riesgos de seguridad de laInformación.

2.3 Análisis comparativo

Se utilizo la norma estándar ISO 27001 que es una normativa emitida por la Organización Internacional de Normalización (ISO), misma que detalla cómo se gestiona la seguridad de la información e las empresas, asimismo, se ve la necesidad de su implementación de acuerdo a norma legal emitida para todas las Cooperativas de Ahorro y Crédito como lo determina la Resolución "SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002", de

fecha 3 de mayo del 2022 dictada por la Superintendencia de Economía Popular y Solidarias, deigual forma se aplica ISO 22301:2019 que es la GUÍA DE IMPLANTACIÓN DE LA CONTINUIDAD DE NEGOCIO.

2.4 Herramientas utilizadas

Para la ejecución de este proyecto, se han utilizado diversas herramientas:

- Hardware: Laptop.
- Software: Paquete de Office, Photoshop, software gestor de citas bibliográficas Mendeley, Navegadores de internet.
- Utilitarios de oficina: hojas A4, bolígrafos, para la elaboración de las encuestas, para la impresión de los documentos entregables.

Capítulo III. Propuesta

Alcance del S.G.S.I

Reseña Histórica de la Cooperativa

La Cooperativa, originalmente denominada Caja de Ahorro y Crédito, fue fundada el 24 de mayo de 2001 en la parroquia Principal del cantón Chordeleg, con el objetivo de apoyar las actividades productivas de la parroquia y su población. El 18 de octubre de 2002, obtuvo la personería jurídica ante la Dirección Nacional de Cooperativas, actualmente conocida como la Superintendencia de Economía Popular y Solidaria (SEPS).

Actualmente, la Cooperativa opera con cuatro agencias ubicadas en Principal, Delegsol, Chordeleg y Cuenca, clasificada en el segmento 2. Con más de 16,000 socios, ofrece una amplia gama de servicios, incluyendo inversiones y créditos. A pesar de contar con una infraestructura modesta, la Cooperativa prioriza la seguridad de la información.

Estructura de la CooperativaVisión

Al año 2023, nuestra cooperativa contará con más de 20 millones de dólares de activos, convirtiéndose en una organización ejemplo de desarrollo financiero, con transparencia, honestidad y compromiso.

Misión

Somos la entidad brinda servicios cooperativos, a nival nacional, a sus socios y clientes, demanera ágil, oportuna, con calidad y calidez, siendo una institución segura, solvente y confiable.

Organigrama de la Cooperativa

La Cooperativa esta estructurada por la asamblea general el cual segmenta tanto al consejo deadministración y vigilancia.

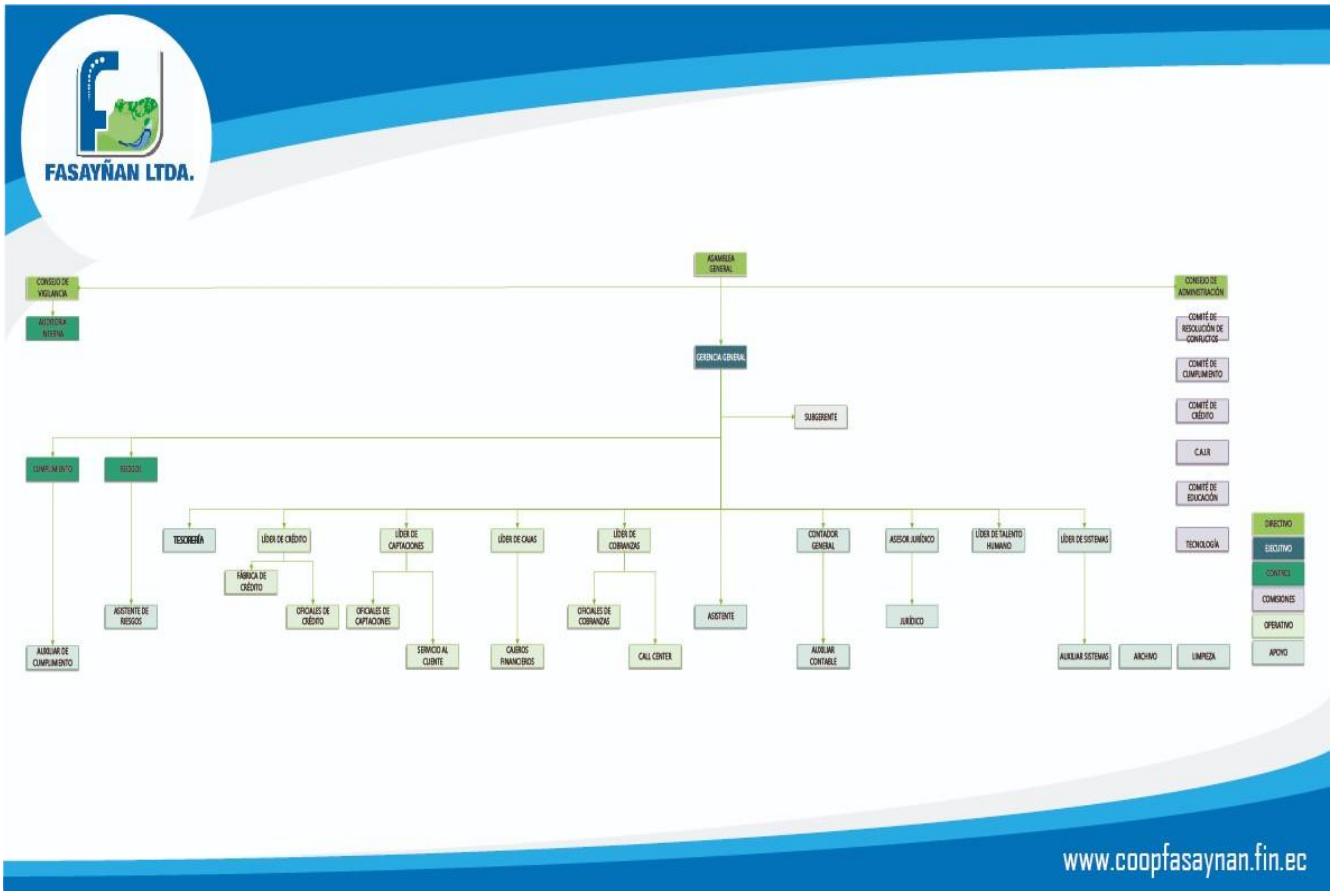


Ilustración 1. Organigrama de la Cooperativa

FODA

Para mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) frente a ataques cibernéticos, es fundamental analizar las fortalezas, oportunidades, debilidades y amenazas dentro de la institución. En consecuencia, el análisis FODA se presenta en la siguiente tabla.

Tabla 15 *FODA*

Fortalezas	**Debilidades**
Uso correcto de los recursos informáticos. Reducción de riesgos que afecten la disponibilidad integridad y confiabilidad de la	Resultados a medio o largo plazo. Ausencia de conocimiento de la normativa. Costos elevados al aplicar los controles de

información. Implementación de sistemas de seguridad avanzados como firewalls. Programas de capacitación y concientización del personal sobre prácticas seguras y protocolos de seguridad.	seguridad apropiados. Presupuesto insuficiente para invertir en nuevas tecnologías de seguridad o para ampliar el equipo de seguridad. Una infraestructura de TI compleja que dificulta la implementación y gestión de medidas de seguridad.
Oportunidades	**Amenazas**
Alinear la tecnología de lainformación con el modelo del negocio. Mejorar la calidad dentro de laorganización. Nuevas tecnologías y soluciones de seguridad que pueden ser adoptadas para mejorar la protección. Iniciativas para desarrollar y atraer talento especializado enciberseguridad. Iniciativas para desarrollar y atraer talento especializado enciberseguridad.	Oposición inter al aplicar los controles o mecanismos de laseguridad apropiadas. Amenazas cibernéticas en constante evolución, incluyendo malware, ransomware, phishing, yataques DDoS. Amenazas internas, como empleados descontentos o negligentes, que pueden causar brechas de seguridad.

Clasificación de la Información

La categorización de los niveles estándar de riesgo se realiza de acuerdo con los perfiles de información de los departamentos evaluados.

Tabla 16 *Niveles de Riesgos*

Descripción	Valor
Critico	5
Alto	4
Medio	3
Bajo	2
Muy Bajo	1

Propuesta del proyecto a alta gerencia

Luego de la reunión con gerencia se expuso el planteamiento y ejecución de este proyecto, justificando en primera instancia todo lo que se va a realizar.

Tras la reunión con la gerencia, se presentó el esquema y la planificación de este proyecto, revelando varias deficiencias en cuanto a la seguridad de la información dentro de la Cooperativa debido a la falta de políticas internas y procesos en los departamentos administrativos y operativos. Como resultado de dicha, la gerencia aprobó la ejecución de nuestro proyecto junto con el cronograma de actividades para su desarrollo.

Solicitud a gerencia

Para dar cumplimiento a los requisitos del proyecto, en primer lugar, se realizó una solicitud formal a la gerencia de la Cooperativa. Esta solicitud incluyó la presentación del tema a tratar, la justificación del proyecto y la petición de autorización para acceder a la información necesaria. La solicitud se envió el 1 de marzo de 2024 y se recibió una respuesta por parte de la gerencia el 6 de marzo de 2024, otorgando la autorización para la ejecución del proyecto según las condiciones

establecidas en el documento. Los detalles de este proceso, esenciales para el inicio de las actividades, se encuentran documentados en el ANEXO 1, que incluye ambas comunicaciones.

Situación interna sobre seguridad de la información dentro de la Cooperativa

Según el análisis llevado a cabo dentro de la Cooperativa, se ha identificado la falta de políticas, procesos y procedimientos relacionados con la seguridad de la información. Esta situación ha generado la oportunidad de emprender el presente proyecto de investigación con el objetivo de abordar estas deficiencias y contribuir de manera efectiva a fortalecer la protección de los activos de información.

Es relevante destacar que el organismo regulador de las cooperativas, la Superintendencia de Economía Popular y Solidaria (SEPS), emitió la resolución "SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002". Esta resolución fue publicada el 3 de mayo de 2022 y establece que, de acuerdo al segmento al que pertenezca la cooperativa, se deben cumplir las disposiciones contenidas en ella en un plazo de 24 meses a partir de su expedición

Dentro del plan de trabajo, se decidió llevar a cabo una evaluación integral de los departamentos administrativos y operativos de la Cooperativa en relación con conceptos fundamentales de seguridad de la información, específicamente en el área de "amenazas cibernéticas". Esta evaluación se llevó a cabo durante la tercera semana de marzo de 2024 mediante encuestas dirigidas a cada departamento.

Los resultados del análisis revelaron un gran desconocimiento considerable sobre la seguridad de la información entre los empleados. Por lo tanto, es imprescindible implementar de forma inmediata un programa de capacitación y concienciación. La mayoría de los empleados deben estar atentos a la información que manejan y procesan diariamente. Esta falta de conocimiento representa un riesgo crítico, comprometiendo la seguridad de la información dentro de la Cooperativa.

A continuación, se presentan los resultados del análisis sobre el conocimiento de la seguridad de la información ante amenazas cibernéticas.

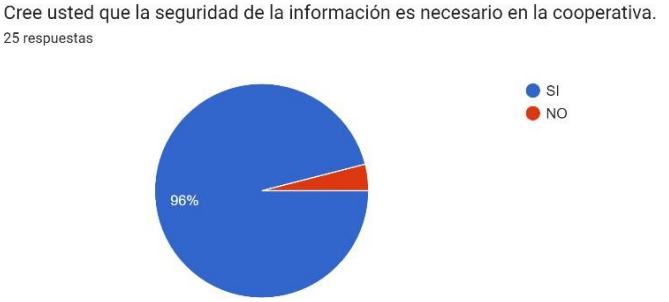


Ilustración 2. Importancia de la Seguridad de la Información

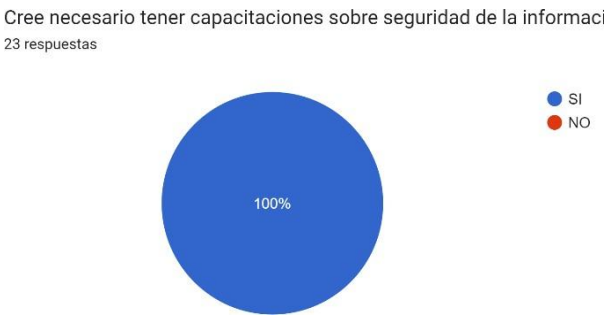


Ilustración 3. Resultado de capacitaciones sobre SI

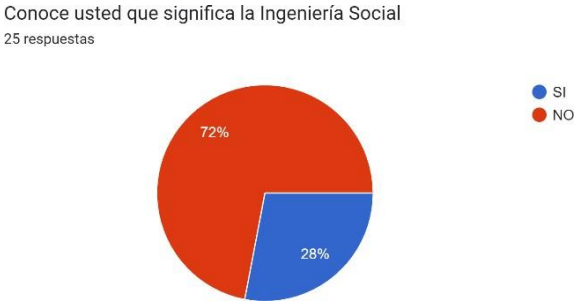


Ilustración 4. Resultado del Conocimiento de Ingeniería Social

Esquema de actividades y delimitación del proyecto

Ilustración 4. Esquema de actividades

El presente documento tiene como finalidad elaborar un plan de control y mejora de la seguridad de la información frente a amenazas cibernéticas, a las que están expuestos tanto los departamentos operativos como administrativos de la cooperativa. El cronograma de actividades se detalla en la ilustración 4 adjunta, la cual especifica las acciones a realizar.

El control y la mejora del plan se basarán en los resultados obtenidos, y se emitirá un informetécnico dirigido a la alta gerencia para informar sobre los inconvenientes detectados en lacooperativa y las medidas propuestas para mejorarlos.

Propuesta de Implementación para el SGSI en la Cooperativa Fasayñan Ltda.

Basado en el diagnóstico, se propone un modelo de implementación por fases del

Sistema de Gestión de Seguridad de la Información (SGSI) que garantiza una transición ordenada y efectiva hacia una cultura institucional de protección de la información. El proceso tiene en cuenta los recursos disponibles de la cooperativa, las prioridades institucionales y el cumplimiento normativo de SEPS, así como la norma ISO/IEC 27001.

Mapa de Ruta para la Implementación del SGSI

El siguiente roadmap presenta las fases estratégicas para el desarrollo del SGSI, junto con las principales actividades, los responsables asignados y la duración estimada por etapa:

Tabla 17 Mapa de Ruta para la Implementación del SGSI

Fase	Actividad Principal	Responsable	Tiempo Estimado
Fase 1: Diagnóstico y Planificación	Levantamiento de activos, análisis de brechas, definición de políticas iniciales	Auditor interno / Consultor externo	1 mes
Fase 2: Diseño del SGSI	Redacción del Manual SGSI, políticas de seguridad, modelo de gobernanza	Departamento de Tecnología y Gerencia General	1 mes
Fase 3: Implementación Inicial	Instalación de controles técnicos (MFA, backups, antivirus), difusión de políticas	Departamento de Sistemas / Seguridad	2 meses
Fase 4: Capacitación y Cultura	Programa de formación continua, campañas de concienciación,	RRHH + Coordinador de Seguridad	1 mes

	simulacros		
Fase 5: Evaluación y Auditoría	Auditoría interna, revisión documental, ajustes y mejoras	Comité de Seguridad / Auditoría	1 mes
Fase 6: Certificación (opcional)	Preparación y proceso de auditoría externa (si se busca ISO 27001)	Dirección + Consultoría	1 a 2 meses

Fuente: Elaboración propia según ISO/IEC 27001 e ISO/IEC 27003.

Interpretación del Roadmap

Este mapa de ruta permite establecer un cronograma estructurado para la implementación del SGSI, dividiendo el proceso en etapas comprensibles y con responsables definidos. Su enfoque escalonado facilita la gestión del cambio y permite que cada fase alimente la siguiente con insumos concretos.

Además, la inclusión de actividades de formación y evaluación periódica garantiza la sostenibilidad del sistema y su mejora continua, conforme a la metodología PHVA (Planificar - Hacer - Verificar - Actuar).

Guía de Ejecución Recolección de Datos

Para iniciar nuestro análisis de los ciberataques contra los departamentos administrativos y operativos, se procedió a la recolección de datos mediante encuestas. Posteriormente, se utilizó unanálisis FODA para evaluar el estado actual de la protección de los activos de información de la cooperativa. El objetivo de este análisis es proporcionar un diagnóstico preciso y emitir recomendaciones favorables para mejorar la seguridad de la información en la institución.

Clasificación de departamentos según gestión de información y modelo CIA

En el marco de esta investigación, se llevó a cabo un proceso sistemático de identificación y clasificación de la información manejada por cada departamento de la Cooperativa de Ahorro y Crédito Fasayñan Ltda., conforme a los principios del modelo CIA (Confidencialidad, Integridad y Disponibilidad). Este modelo, ampliamente reconocido en la normativa ISO/IEC 27001, permite evaluar la criticidad de los activos de información y definir su nivel de protección requerido.

La evaluación se realizó mediante entrevistas técnicas, encuestas aplicadas al personal, y análisis documental, lo que permitió establecer los niveles de exigencia en cuanto a la protección de datos y procesos críticos, y clasificarlos en categorías como críticos, sensibles o moderados, en función de los siguientes criterios:

- **Confidencialidad:** Grado en el que la información debe ser protegida contra accesos no autorizados.
- **Integridad:** Necesidad de que la información se mantenga precisa, sin alteraciones indebidas.
- **Disponibilidad:** Necesidad de que la información esté accesible cuando se requiera para cumplir con funciones operativas.

Como parte del análisis situacional de la Cooperativa de Ahorro y Crédito Fasayñan Ltda., se procedió a evaluar individualmente cada uno de sus departamentos funcionales. Esta evaluación consideró el tipo de información manejada, su criticidad institucional y los niveles de exigencia en cuanto a protección, tomando como base los principios del modelo CIA (Confidencialidad, Integridad y Disponibilidad). A continuación, se describe el contexto de cada área y su clasificación en la tabla correspondiente:

1. **Departamento Legal**

Este departamento gestiona documentación jurídica, procesos judiciales, oficios regulatorios y convenios institucionales. La naturaleza de su información requiere un alto nivel de reserva y control documental.

2. **Departamento de Crédito**

Encargado de la gestión y evaluación de solicitudes de crédito, historial financiero de socios, garantías y políticas crediticias. Su función es central en la operación financiera de la cooperativa.

3. **Departamento de Cobranzas**

Administra la recuperación de cartera vencida, emite notificaciones de pago y mantiene contacto con socios en mora. Aunque importante, maneja información menos crítica que el área de crédito.

4. **Departamento de Captaciones**

Procesa los productos de ahorro e inversión, apertura de cuentas y manejo de depósitos. Su operación incide directamente en la confianza de los socios y la estabilidad financiera.

5. **Departamento de Cumplimiento**

Responsable del seguimiento normativo, gestión de reportes regulatorios, y monitoreo de operaciones sospechosas. Su rol es clave en la prevención del lavado de activos y el cumplimiento de obligaciones ante la SEPS.

6. **Departamento de Caja**

Gestiona el flujo diario de efectivo, realiza pagos, retiros y mantiene interacción directa con los socios. Requiere alta disponibilidad, aunque su confidencialidad e integridad son moderadas.

7. Departamento de Contabilidad

Encargado del registro contable, generación de balances y estados financieros. Si bien no gestiona datos personales directamente, su información es esencial para la transparencia institucional.

8. Departamento de Tesorería

Administra el capital institucional, transferencias bancarias, inversiones y control del flujo financiero general. Tiene acceso a sistemas críticos y reportes de gestión de fondos.

9. Unidad de Riesgos

Vigila los riesgos financieros, operacionales y tecnológicos, realiza análisis de impacto y define políticas de mitigación. Su visión transversal le da acceso a múltiples fuentes críticas de información.

Tabla 18. Clasificación de la Información por Departamento (Modelo CIA).

Departamento	Confidencialidad	Integridad	Disponibilidad	Clasificación de la Información
Legal	Alta	Alta	Media	Crítica
Crédito	Alta	Alta	Alta	Crítica
Cobranzas	Media	Media	Media	Sensible
Captaciones	Media	Media	Alta	Sensible
Cumplimiento	Alta	Alta	Media	Crítica
Caja	Media	Media	Alta	Sensible
Contabilidad	Media	Alta	Alta	Sensible
Tesorería	Media	Alta	Alta	Sensible
Unidad de Riesgos	Alta	Alta	Media	Crítica

La información calificada como crítica corresponde a departamentos que gestionan datos sensibles con alto impacto potencial en caso de filtración, manipulación o pérdida, como es el caso de Legal, Crédito, Cumplimiento y Unidad de Riesgos. Estos requieren la

implementación de controles avanzados como cifrado robusto, autenticación multifactor y monitoreo continuo.

Por otro lado, los departamentos clasificados como sensibles mantienen una exposición intermedia y requieren medidas proporcionales de protección, como políticas de acceso basadas en roles, respaldo periódico y capacitación focalizada.

Esta clasificación no solo permite focalizar recursos y esfuerzos en función del nivel de riesgo, sino que también sustenta el diseño de controles técnicos y administrativos en el marco de la implementación del SGSI. Además, sienta las bases para la elaboración de políticas de seguridad diferenciadas por área, garantizando que cada unidad operativa actúe conforme a su perfil de riesgo real.

Mapa de calor de la clasificación CIA por departamento

Este gráfico refuerza la lectura de la tabla anterior, permitiendo visualizar de forma comparativa la intensidad del riesgo asociado a cada dimensión del modelo CIA. Se empleó una escala de tres niveles:

- 1 (bajo): riesgos controlados o con baja sensibilidad de la información.
- (medio): información operativa relevante que requiere controles estándar.
- (alto): activos críticos cuya exposición comprometería la operación o la integridad de la cooperativa.

El color más intenso en el gráfico indica mayor necesidad de controles y protección. Se observa claramente cómo departamentos como Crédito, Legal, Cumplimiento y Unidad de Riesgos concentran niveles altos en las tres dimensiones, lo que justifica su clasificación como departamentos críticos. Esta visualización servirá de base para priorizar acciones de implementación dentro del Sistema de Gestión de Seguridad de la Información (SGSI) y para

asignar controles diferenciados conforme al nivel de exposición y sensibilidad.

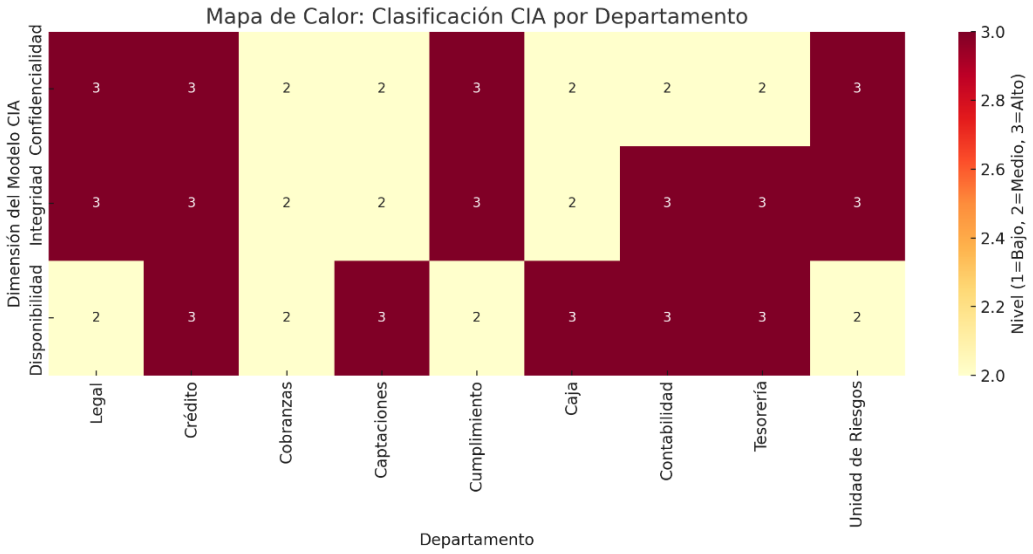


Ilustración 1 Mapa De Calor: Clasificación CIA Por Departamento

El análisis efectuado a través del modelo CIA ha permitido identificar de forma precisa los niveles de criticidad de la información manejada por cada departamento de la Cooperativa Fasayñan Ltda. La combinación de entrevistas, encuestas y clasificación técnica demuestra que existen áreas cuya exposición a amenazas cibernéticas es alta, y donde los actuales mecanismos de protección resultan insuficientes.

Departamentos como Legal, Crédito, Cumplimiento y Unidad de Riesgos destacan como los más vulnerables, debido a la sensibilidad de los datos que gestionan y a la necesidad de mantener una integridad operativa estricta. Estas unidades requieren políticas de seguridad robustas, procedimientos estandarizados y controles técnicos avanzados.

Por otra parte, áreas como Cobranzas, Captaciones, Tesorería y Contabilidad, aunque presentan un riesgo intermedio, no deben ser desatendidas, ya que una brecha en cualquiera de ellas podría comprometer la continuidad del negocio y la confianza de los socios.

Selección Bibliográfica

La selección bibliográfica permite desarrollar un marco teórico sólido y fundamentado, esencial para alcanzar los objetivos planteados en la tesis. Además, facilita la realización de comparaciones literarias que respaldan y sustentan la investigación. En este contexto, se emplearánlos controles de la norma ISO 27001, específicamente los controles A.8, A.9 y A.10. La inclusiónde estos controles permitirá una crítica adecuada de los resultados obtenidos, garantizando un análisis riguroso y una evaluación precisa de la seguridad de la información

CONTROLES	
A8	Gestión de activos
A8.1	Responsabilidad sobre los activos
A8.1.1	Inventario de activos
A8.1.2	Propiedad de los activos
A8.1.3	Uso aceptable de los activos
A8.1.4	Devolución de activos
A8.2	Clasificación de la información
A8.2.1	Clasificación de la información
A8.2.2	Etiquetado de la información
A8.2.3	Manipulado de la información
A8.3	Manipulación de los soportes
A8.3.1	Gestión de soportes extraíbles
A8.3.2	Eliminación de soportes
A8.3.3	Soportes físicos en tránsito
A9	Control de acceso
A9.1	Requisitos de negocio para el control de acceso
A9.1.1	Política de control de acceso
A9.1.2	Acceso a las redes y a los servicios de red
A9.2	Gestión de acceso de usuario
A9.2.1	Registro y baja de usuario
A9.2.2	Provisión de acceso de usuario
A9.2.3	Gestión de privilegios de acceso
A9.2.4	Gestión de la información secreta de autenticación de los usuarios
A9.2.5	Revisión de los derechos de acceso de usuario
A9.2.6	Retirada o reasignación de los derechos de acceso
A9.3	Responsabilidades del usuario
A9.3.1	Uso de la información secreta de autenticación
A9.4	Control de acceso a sistemas y aplicaciones
A9.4.1	Restricción del acceso a la información
A9.4.2	Procedimientos seguros de inicio de sesión
A9.4.3	Sistema de gestión de contraseñas
A9.4.4	Uso de utilidades con privilegios del sistema
A9.4.5	Control de acceso al código fuente de los programas
A10	Criptografía
A10.1	Controles criptográficos
A10.1.1	Política de uso de los controles criptográficos
A10.1.2	Gestión de claves

Ilustración 5. Controles ISO 27001 A8, A9 y A10

Conclusiones

Basado en la evaluación de los activos críticos de información en la Cooperativa de Ahorro y Crédito Fasayñan Ltda., se constató que la base de datos de socios, el sistema de créditos y los canales de comunicación institucional presentan un gran riesgo exponencial. Estos activos son fundamentales para la operatividad y el normal funcionamiento financiero de la cooperativa, su custodia se torna prioritaria. Las deficiencias en controles técnicos adecuados y la falta de procedimientos estandarizados, hacen que estos activos se encuentren expuestos a riesgos que comprometen la confidencialidad, integridad y disponibilidad de la información.

Con respecto al análisis de la cultura organizacional, los resultados muestran que el personal tiene poca capacitación en ciberseguridad. Un alto número de colaboradores no ha sido capacitado en años recientes y no tiene conocimiento de las políticas internas concernientes a la seguridad informática. Esta situación propicia un entorno desfavorable al control de errores humanos y el incumplimiento de procedimientos, lo que hace evidente que se debe contar con un programa de sensibilización que enseñe a los colaboradores a tratar la seguridad de la información como una cuestión natural de la organización.

En cuanto a la falta de un sistema formal, se determina que la cooperativa carece de una guía sistemática para el control de la seguridad de la información, lo que dificulta la proactividad en el tratamiento de los riesgos tecnológicos. La propuesta expuesta, fundamentada en los principios de la norma ISO/IEC 27001, crea una solución factible en la que se pueden establecer políticas, asignar responsabilidades, controles y la mejora continua. La implementación de un sistema de estas características permitirá aumentar la resistencia institucional, el cumplimiento regulatorio y la confianza de los socios.

Recomendaciones

Considerando como referencia la norma ISO/IEC 27001, se recomienda implementar un Sistema de Gestión de Seguridad de la Información a nivel de toda la cooperativa para establecer un marco organizativo que permita tanto la evaluación como el control de los riesgos derivados de los activos de información. Dicha implementación debe incluir; la creación de políticas internas adecuadas, la determinación de funciones y responsabilidades y la integración del sistema a las funciones clave de la operación. Adoptar esta estrategia alentará el fortalecimiento institucional y disminuirá las vulnerabilidades, así como también mejorará la eficacia en los procesos de toma de decisiones sobre defensas digitales.

Desde la dirección, es recomendable la creación de un comité institucional que promueva la política de seguridad de la información, compuesto de personal técnico, administrativos y un representante del nivel gerencial. Con estas funciones en su poder, el comité estará encargado de velar por el cumplimiento de las políticas operacionales, coordinar una capacitación integral para el resto de los usuarios, monitorear los indicadores de desempeño del sistema y facilitar, cuando sea necesario, la implementación de acciones correctivas. Junto a esto surge la necesidad de adoptar formalmente una política de ciberseguridad que sea divulgada en el resto de la empresa y que tenga el apoyo de un documento normativo interno que responda a las exigencias de los reguladores.

Desde el punto de vista operativo, resulta pertinente diseñar un programa permanente de sensibilización y capacitación en seguridad de la información que involucre a toda la plantilla de la cooperativa. Este programa debe incluir formación continua, simulacros de respuesta a incidentes, así como evaluaciones de saber. Por otra parte, debe establecerse el control técnico particular de autenticación multifactorial, encriptación de datos, monitoreo de

accesos y eventos críticos, así como de los ataques. Para preservar la vigencia y efectividad del sistema, se sugiere realizar auditorías internas cada seis meses con el fin de evaluar el cumplimiento de las políticas, identificar estrategias fallidas y actualizar los controles en base a nuevas amenazas.

Bibliografía

23 de Julio, C. d. (27 de Octubre de 2023). *Cooperativa en línea*. Obtenido de Cuidado de los Ciberataques: https://coop23dejulio.fin.ec/blogs/cuidado-con-los-ciberataques

CACF, C. d. (2025). *22 años Brindando Servicios Financieros de Calidad*. Obtenido de https://www.coopfasaynan.fin.ec

ISO/IEC 27001:2013, I. O. (2013). *ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements.* ISO.org.

ISO/IEC 27002:2013, I. O. (2013). *ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls.* ISO.org.

ISO/IEC 27034-1:2011, I. (2011). *ISO/IEC 27034-1:2011 - Information technology.* ISO.org.

López Vera, J. F., & Guamushin Tarco, X. P. (2022). *Prevalencia de estrés en el personal operativo v.s. el administrativo de ahorro y crédito Fasayñan LTDA. Asociado a las condiciones de trabajo en comparación con el personal administrativo, Gualaceo - Azuay Mayo - Julio 2022.* Repositorio UDLA.

OEA, O. d. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. En O. |. gente. Obtenido de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

SEPS, S. d. (2022). *Norma de control respecto a la seguridad de la Información en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria.* Obtenido de RESOLUCIÓN NO. SEPS-IGS- IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI 2022-002: https://rfd.org.ec/docs/normativa/2022/Boletin-32/Seguridad%20Informacion.pdf

Superintendencia de Economía popular y Solidaria. (Junio de 2021). SITUACIÓN DE LOS SERVICIOS FINANCIEROS DIGITALES Y SEGURIDAD DE LA INFORMACIÓN EN EL SFPS. *Intendencia Nacional de Gestión de Información y Normativa Técnica*. Dirección Nacional de Seguridad de la Información.

Anexos

ANEXO1

Cuenca 06 de marzo de 2024

Ingeniero Andrés Garnica.

De mis consideraciones:

Con un atento saludo me dirijo a usted para informarle que ha sido aceptada su solicitud para realizar su proyecto de graduación de la maestría que se encuentra cursando denominado: " Análisis y Mejora del Sistema de gestión de Seguridad de la Información (SGSI) en COAC Fasayñan: Enfrentando Amenazas Cibernéticas en Departamentos Operativos y Administrativos" tomando como caso de estudio a la COOPERATIVA DE AHORRO Y CREDITO FASAYÑAN LTDA.

Cabe resaltar que todas las actividades comprendidas en esta investigación tienen que ser estrictamente confidenciales ya que usted tendrá acceso a información muy delicada de la cooperativa.

Con seguridad su aporte para la empresa con dicha investigación será muy valioso. Espero que pueda culminar sus estudios con éxito.

Atentamente,

FASAYÑAN Ltda.

Ing. Isabel Cristina Ulloa Ulloa
GERENTE GENERAL

Gualaceo, 1 de marzo de 2024

Ing. Isabel Cristina Ulloa Ulloa

GERENTE GENERAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO FASAYÑAN LTDA.

Su despacho. -

De mis consideraciones:

Por medio de la presente, me dirijo a usted de la manera más respetuosa, con la finalidad de solicitarle su autorización para poder realizar el proyecto de graduación de la maestría que me encuentro cursando denominado: " Análisis y Mejora del Sistema de gestión de Seguridad de la Información (SGSI) en COAC Fasayñan: Enfrentando Amenazas Cibernéticas en Departamentos Operativos y Administrativos", el objetivo que me motiva a realizar dicha solicitud radica en el hecho que, actualmente la cooperativa no cuenta con un plan de esta índole, motivo por el cual he visto la oportunidad de poder realizar un trabajo de investigación que entregue un aporte de valor para la cooperativa en la cual me encuentro laborando durante este lapso de tiempo que me encuentro laborando en esta institución, es por ello que solicito su autorización para poder desarrollar todas las actividades comprendidas en esta investigación y tener acceso tanto a la información, como a la infraestructura necesaria para completar el mismo, comprometiéndome a manejar con estricta reserva la información que sea requerida durante el desarrollo de este proceso.

Por una favorable acogida a esta solicitud, anticipo mis más sinceros agradecimientos, y deseándole éxitos en sus funciones, suscribo de usted.

Atentamente,

Andrés Patricio Garnica Bueno

ENCUESTA SOBRE CONCEPTOS DE SEGURIDAD DE LA INFORMACIÓN "AMENAZAS CIBERNETICAS"

La presente encuesta, tiene como objetivo ver el conocimiento sobre amenazas cibernéticas dentro de cada departamento tanto administrativo y operativo de la Cooperativa de Ahorro y Crédito Fasayñan Ltda.

Fecha: 14- marzo - 2024

Nombre: Carolina Tello

Departamento: Tesoreria

Señale SI o NO cada respuesta

1. Conoce sobre la seguridad de la información

(SI) NO

2. Conoce usted que significa la Ingeniería Social

SI (NO)

3. Sabe qué son los riesgos informáticos

(SI) NO

4. Sabe que es un phishing

(SI) NO

5. Cree necesario tener capacitaciones sobre seguridad de la información

(SI) NO

6. Cree usted que la seguridad de la información es necesario en la Cooperativa

(SI) NO

7. A sido víctima dentro de la Cooperativa de algún ataque cibernético

SI NO

8. Cuenta sus equipos de computo con software con licencia

SI NO

9. Cuenta su equipo de cómputo con antivirus

SI NO

10. Tiene libre acceso desde su equipo de trabajo a programas, softwares ajenos a los proporcionado por la institución (redes sociales)

SI NO