UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN, PARA LA COAC ACHIK INTI DEL CANTÓN CAÑAR, SEGMENTO 4 Y SU PROGRESIÓN AL SEGMENTO 3, BAJO LA REGULACIÓN DE LA SEPS

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

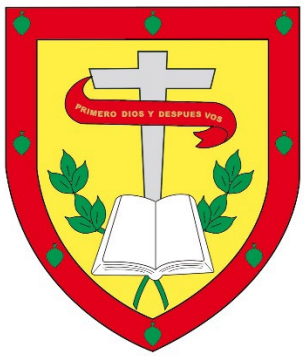
AUTORA: ISRAEL SEBASTIAN ROMERO LOJA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN, PARA LA COAC ACHIK INTI DEL CANTÓN CAÑAR, SEGMENTO 4 Y SU PROGRESIÓN AL SEGMENTO 3, BAJO LA REGULACIÓN DE LA SEPS.

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTORA: ISRAEL SEBASTIAN ROMERO LOJA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

Declaratoria de Autoría y Responsabilidad

Israel Sebastián Romero Loja, portador(a) de la cedula de ciudadanía N. **0303040125**. Declaro ser el autor de la obra : **Cumplimiento de la normativa de seguridad de La información, para la COAC Achik Inti del cantón Cañar, segmento 4 y su progresión al segmento 3, bajo la regulación de La SEPS** sobre lo cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 29 de noviembre del 2024

F: .....

Israel Sebastián Romero Loja

C.I. **0303040125**

Universidad Católica de Cuenca

CERTIFICACIÓN DEL TUTOR

El trabajo de titulación denominado **Cumplimiento de la normativa de seguridad de La información, para la COAC Achik Inti del cantón Cañar, segmento 4 y su progresión al segmento 3, bajo la regulación de La SEPS**, elaborado por **Israel Sebastián Romero Loja**, previo a la obtención del título de **Ingeniera en Sistema de Información**, ha sido asesorado, revisado y supervisado durante su ejecución bajo mi tutoría, por lo que certifico que el presente documento fue desarrollado siguiendo los parámetros del método científico, se sujeta a las normas éticas de investigación, por lo que esta expedito para su presentación y sustentación ante el respectivo tribunal.

Cañar, 29 de noviembre de 2024

Ing. ING. Cristhian Humberto Flores Urgilés.

CI: 0301638375

TUTOR

DEDICATORIA

A mis padres, **German Romero y María Loja**, por su amor incondicional, apoyo constante y por siempre creer en mí, incluso cuando las dificultades parecían insuperables. Su ejemplo de trabajo duro, sacrificio y perseverancia ha sido mi mayor fuente de inspiración en este largo camino académico.

A **mis hermanos Diego y Paulina Romero Loja**, por su paciencia, comprensión y por ser mi pilar en los momentos de duda. Gracias por estar siempre a mi lado, por motivarme cuando sentía que no podía continuar, y por compartir este viaje lleno de desafíos y logros.

A mis compañeros de carrera y amigos, con quienes compartí experiencias y aprendizaje, y que me dieron la oportunidad de crecer tanto en el ámbito académico como personal. Su confianza hizo que este proceso fuera más enriquecedor y agradable.

Este logro también es para todos aquellos que han influido en mi vida y formación como profesional de la Ingeniería Informática. Sin su apoyo y ejemplo, este proyecto no habría sido posible.

Y, por supuesto, a ti, Dios, te dedico este esfuerzo, este logro y mi vida renovada. Que siempre sea tu voluntad la que guíe mis pasos y que este trabajo sea un testimonio de que, cuando confiamos en ti, todo es posible. Gracias por salvarme y por darme el coraje para seguir adelante, por darme una nueva oportunidad de construir un futuro mejor.

AGRADECIMIENTO

A Dios, mi salvador y guía, a quien le agradezco infinitamente por haberme dado una nueva oportunidad de vida, gracias a él, hoy puedo celebrar este logro, sabiendo que es fruto no solo de mi esfuerzo, sino de su misericordia y su amor incondicional. Mi fe en tí me ha dado la fuerza para seguir adelante, incluso en los momentos de mayor incertidumbre.

Un profundo y sincero agradecimiento a todas las personas que han sido parte fundamental en la realización de esta tesis de grado. Sin su apoyo, guía y colaboración, este trabajo no habría sido posible.

En primer lugar, agradezco al Ingeniero Cristian Flores, mi director de tesis, por su valiosa orientación, paciencia y dedicación a lo largo de este proceso. Su conocimiento, consejos y disposición para ayudarme en cada etapa del proyecto han sido imprescindibles para llevar a cabo este trabajo de manera exitosa.

A **todos mis docentes**, quienes han aportado su experiencia y conocimientos en áreas claves de esta investigación, permitiéndome mejorar y enriquecer el contenido y los enfoques de este estudio.

Mi agradecimiento a todo el personal **Administrativo, docente y a la Universidad Católica**, por ofrecerme los recursos, la formación y el entorno adecuado para desarrollar mis capacidades académicas y profesionales. Este proyecto no habría sido posible sin el acceso a las instalaciones, bibliografía y herramientas de software que me proporcionaron.

A mis compañeros de carrera y amigos, quienes han sido una fuente de motivación y apoyo durante todo mi proceso académico. Gracias por los intercambios de ideas, por esas duras, sacrificadas y largas horas de trabajo conjunto y las risas que nos han permitido superar juntos los momentos más difíciles.

A mi familia, especialmente a mis padres y hermanos por su amor incondicional, por creer en mí y por brindarme el apoyo emocional necesario en cada etapa de este recorrido. Gracias por ser mi mayor fuente de motivación y por estar siempre a mi lado en los momentos de éxito y en los de dificultad.

Finalmente, a todos mis amigos y todas las personas que de alguna forma han aportado a mi formación académica, personal y profesional, ya sea mediante enseñanzas directas o a través de experiencias compartidas. Cada uno de ustedes ha dejado una huella en mi vida y ha sido fundamental en mi desarrollo como profesional de la ingeniería informática.

Gracias a todos por su apoyo y por ser parte de este logro.

RESUMEN

La presente investigación analiza el cumplimiento normativo de seguridad de la información en la Cooperativa de Ahorro y Crédito Achik Inti del cantón Cañar, en su transición del Segmento 4 al Segmento 3, según las regulaciones de la Superintendencia de Economía Popular y Solidaria (SEPS). El estudio tiene como objetivo principal identificar las brechas en la seguridad de la información y proponer soluciones que mejoren los procesos de la cooperativa. Se plantean tres objetivos específicos: realizar una revisión teórica sobre la seguridad de la información en cooperativas, levantar información exhaustiva sobre el estado actual de la cooperativa y desarrollar un plan que incluya acciones, recursos y plazos para cumplir con las normativas del Segmento 3, enfocándose en la mejora de políticas, infraestructura tecnológica, capacitación y gestión de riesgos. La metodología de enfoque mixto emplea tanto técnicas cualitativas como cuantitativas, utilizando la norma ISO/IEC 27001:2022 como marco de evaluación, con encuestas y entrevistas al personal clave. El análisis de riesgos se fundamenta en la identificación de activos críticos y amenazas, implementando controles de seguridad adecuados.

Palabras Clave: seguridad de la información, ISO/IEC 27001, SEPS, gestión de riesgos, cumplimiento normativo.

ABSTRACT

This research analyzes compliance with information security regulations in the Achik Inti Savings and Credit Cooperative in the canton of Cañar during its transition from Segment 4 to Segment 3, in accordance with the regulations of the Superintendence of Popular and Solidarity Economy (SEPS). The study's main objective is to identify gaps in information security and propose solutions to improve the cooperative's processes. Three specific objectives are outlined: to conduct a theoretical review of information security in cooperatives, collect comprehensive data on the cooperative's current state, and develop a plan that includes actions, resources and timelines to comply with Segment 3 regulations, focusing on improving policies, technological infrastructure, training and risk management. The mixed-methods approach combines qualitative and quantitative techniques, using ISO/IEC 27001:2022 as an evaluation framework, surveys and interviews with key personnel. Risk analysis centers on identifying critical assets and threats and implementing adequate security controls.

Keywords: information security, ISO/IEC 27001, SEPS, risk management, regulatory compliance.

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

A continuación, se presenta una breve descripción de los capítulos que conforman este documento:

Capítulo I: Se expone la explicación del problema de investigación, enfocándose en la evaluación y mejora de la seguridad de la información en la COAC Achik Inti. Este capítulo ofrece un análisis detallado de la situación actual de la seguridad de la información y la gestión de riesgos en la cooperativa, identificando las brechas que justifican la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Asimismo, se establecen los objetivos generales y específicos que orientan la investigación y se definen las limitaciones y delimitaciones que enmarcan el estudio.

Capítulo II: Contiene el marco teórico que sustenta la investigación. En este capítulo se exploran los conceptos fundamentales relacionados con la seguridad de la información, la gestión de riesgos, y las normativas internacionales como la ISO/IEC 27001, que rigen las mejores prácticas en estos ámbitos. Este marco teórico proporciona los conceptos clave y la base conceptual necesarios para comprender los desafíos y oportunidades en la implementación de un SGSI en la COAC Achik Inti.

Capítulo III: Presenta el marco metodológico de la investigación, describiendo la metodología utilizada para llevar a cabo el diagnóstico inicial de TI en la cooperativa. Se detalla el enfoque descriptivo y evaluativo adoptado, que combina técnicas cualitativas y cuantitativas. Este capítulo también incluye el proceso de recolección de datos, mediante una encuesta con el personal clave de la cooperativa del área tecnológica, así como el análisis de los resultados obtenidos, que sirven de base para identificar las brechas y riesgos en la seguridad de la información.

Capítulo IV: En este capítulo se desarrolla la propuesta del plan de mejora enfocado en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y un Plan de Continuidad del Negocio (PCN) para la COAC Achik Inti. Se describen las estrategias de mitigación de riesgos, la identificación de activos críticos, y la planificación de contingencias necesarias para asegurar la resiliencia operativa y el cumplimiento de los requisitos normativos. Además, se detalla el cronograma de implementación de estas medidas, priorizando las acciones en función de la criticidad de las brechas identificadas.

CAPÍTULO I

1. Planteamiento del problema

La Cooperativa de Ahorro y Crédito (COAC) Achik Inti, ubicada en el cantón Cañar, actualmente se encuentra clasificada en el segmento 4 según las regulaciones de la Superintendencia de Economía Popular y Solidaria (SEPS). Esta clasificación implica ciertas normativas de seguridad de la información que deben ser cumplidas. La cooperativa aspira a progresar al segmento 3, lo que conlleva un conjunto más riguroso de requisitos en términos de seguridad de la información.

La Cooperativa ha implementado algunas medidas de Seguridad de la Información, sin embargo enfrenta el desafío de adaptarse a las normativas más estrictas de seguridad de la información requeridas para el segmento 3. Esto implica evaluar y mejorar sus sistemas actuales, políticas y procesos para cumplir con los estándares establecidos por la SEPS. La falta de cumplimiento no solo impide la transición al segmento deseado, sino que también puede exponer a la cooperativa a riesgos de seguridad, afectando la confianza y la integridad de la institución. Es por ello que, el cumplimiento normativo es esencial para la operación segura y eficiente de las instituciones financieras como la COAC Achik Inti.

1.1. Formulación del problema

A medida que la Cooperativa Achik Inti, busca avanzar del Segmento 4 al Segmento 3 según la regulación de la Superintendencia de Economía Popular y Solidaria (SEPS), enfrenta una serie de desafíos relacionados con el cumplimiento normativo de la seguridad de la información. Puesto que el marco regulatorio exige una gestión más rigurosa de los datos y procesos informáticos para para salvaguardar la integridad, confidencialidad y disponibilidad de la información. Por ello se plantea lo siguiente:

¿Cómo puede la COAC Achik Inti del cantón Cañar, Segmento 4, mejorar su cumplimiento normativo de seguridad de la información bajo la regulación de la SEPS para progresar al Segmento 3, considerando los desafíos relacionados con la gestión de riesgos, infraestructura tecnológica, procedimientos y capacitación del personal?

1.2. Antecedentes de la Investigación

Las cooperativas de ahorro y crédito manejan información confidencial de sus socios y clientes, como datos personales, información financiera y transacciones. Esta información es susceptible a ataques cibernéticos y otras amenazas a la seguridad de la información. Las investigaciones sobre el cumplimiento normativo ayudan a identificar las brechas y riesgos en la seguridad de la información y a tomar medidas para proteger la información confidencial. Es por esto que varios autores han desarrollado proyectos que van dirigidos para el beneficio de las cooperativas sobre el cumplimiento de las normativas de la SEPS.

Freire (2024) presenta en su trabajo de titulación denominado "Aplicación del método COBIT y el control de seguridad de la información en la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda."; en el que presenta la importancia del control de seguridad de la información en las cooperativas de ahorro y crédito, y describe el método COBIT como una herramienta para la gestión de la seguridad de la información. Menciona que la evaluación del estado actual de la seguridad de la información en la Cooperativa de Ahorro y Crédito Uniblock y Servicios Ltda. se realizó utilizando como referencia la Resolución SEPS-0279. Además, indica que la aplicación del método COBIT permitió a la cooperativa cumplir con los requisitos de la Resolución SEPS-0279.

Otro de los trabajos relacionados es el de Prado (2022) en el que presenta la importancia de la gestión de riesgos operativos en las cooperativas de ahorro y crédito, y describe el contexto normativo ecuatoriano en materia de riesgos operativos, incluyendo la Resolución SEPS-0279 e ISO 31000. Este documento es una guía para la realización del trabajo de titulación, en cuanto al marco conceptual ya que presenta la gestión de riesgos operativos, incluyendo definiciones, tipologías, metodologías y herramientas.

Poaquiza (2021) presenta el contexto del sector cooperativista en Ecuador, destacando la importancia de las cooperativas de ahorro y crédito en la economía del país. El documento también describe la SEPS y sus funciones de supervisión y control del sector cooperativista. Presenta también un análisis de la eficiencia técnica de las cooperativas de ahorro y crédito del Ecuador, mismo que servirá como referencia para evaluar el desempeño de la COAC Achik Inti en términos de eficiencia técnica.

Luque & Peñaherrera (2021) analizan la evolución del sector cooperativista ecuatoriano en las últimas décadas. El documento destaca el crecimiento del sector en términos de activos, cartera de créditos y número de socios. Sin embargo, el documento

también advierte sobre algunos problemas que enfrenta el sector, como la concentración del mercado, la morosidad y la falta de innovación. Este artículo proporciona una mejor comprensión del contexto en el que opera la COAC Achik Inti, ya que describe los principales desafíos que enfrentan las cooperativas de ahorro y crédito en Ecuador, incluyendo la competencia con el sector financiero privado, la falta de formación cooperativa y la debilidad en la gestión.

1.3. **Justificación de la investigación**

El cumplimiento de las normativas de seguridad de la información es crucial para cualquier entidad financiera, más aún para las cooperativas de ahorro y crédito como la COAC Achik Inti. Estas normativas no solo salvaguardan la información sensible de los socios y clientes, sino que también protegen a la institución contra riesgos legales, operativos y reputacionales. Asegurar el cumplimiento normativo no solo es una obligación legal, sino una necesidad estratégica que respalda la integridad, confiabilidad y continuidad del negocio.

La transición de la COAC Achik Inti del segmento 4 al segmento 3 es un paso significativo hacia su crecimiento y expansión. Este cambio implica no solo un mayor volumen de operaciones y una base de socios ampliada, sino también la adopción de estándares más estrictos en términos de seguridad de la información. Dicha transición conlleva una revisión y fortalecimiento del sistema actual de seguridad de la información, lo que a su vez incrementa la confianza de los socios y mejora la imagen de la cooperativa en el mercado.

En la era digital, la seguridad de la información es un pilar fundamental para el funcionamiento seguro y eficiente de las instituciones financieras. Un sistema robusto de seguridad de la información no solo previene pérdidas financieras debido a fraudes o robos de datos, sino que también garantiza la continuidad operativa ante posibles amenazas cibernéticas. La COAC Achik Inti debe adaptarse a este entorno, garantizando una gestión eficaz de los riesgos asociados a la seguridad de la información. El cumplimiento con las normativas de la SEPS es un requisito indispensable para la operatividad de la cooperativa en su nuevo segmento. La investigación y desarrollo de estrategias para alcanzar este cumplimiento no solo es una obligación regulatoria, sino que también es una oportunidad para modernizar y optimizar los procesos internos, alineándolos con las mejores prácticas del sector.

1.4. Objetivos

1.4.1. Objetivo General

- Analizar el Cumplimiento normativo de Seguridad de la Información para la COAC Achik Inti del cantón Cañar, segmento 4 y su progresión al segmento 3 bajo la regulación de la SEPS

1.4.2. Objetivos Específicos

- **Elaborar una revisión detallada del marco teórico relacionado con la seguridad de la información en el contexto de cooperativas de ahorro y crédito.**
  - Realizar un levantamiento de información exhaustivo para determinar el estado actual de la seguridad de la información en la COAC Achik Inti.
  - Elaborar un documento que detalle las acciones específicas, los recursos necesarios y los plazos para el cumplimiento de las normativas de seguridad de la información del segmento 3. Este documento debe incluir la actualización de políticas, la mejora de infraestructuras tecnológicas, la capacitación del personal, y las medidas para la gestión de riesgos y la protección de datos.

1.5. Limitaciones

La presente investigación podría verse limitada por varios puntos tales como:

- Limitación en información detallada sobre las prácticas internas de la seguridad de la información de la cooperativa.
- El estudio no profundizará en aspectos técnicos muy específicos de infraestructura de TI, centrando su análisis en la gestión y cumplimiento normativo general.
- Las respuestas y la información proporcionada por los empleados y gestores de la cooperativa durante las entrevistas pueden estar sujetas a sesgos o limitaciones en su conocimiento sobre las normativas y procedimientos de seguridad de la información.

1.6. Delimitaciones

- El estudio se delimita a las normativas impuestas por la Superintendencia de Economía Popular y Solidaria (SEPS), relacionadas con la seguridad de la información.
- La investigación se desarrollará dentro de un periodo específico (tres meses), considerando la situación actual de la cooperativa y no abordará cambios normativos futuros o pasados.

CAPÍTULO II

MARCO TEÓRICO

2.1. Seguridad de la Información

Se refiere a la protección de la información y los sistemas de información contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción, con el fin de proporcionar confidencialidad, integridad y disponibilidad. Es fundamental considerar que la seguridad de la información es importante para cualquier organización, independientemente de su tamaño o sector; sin embargo, es aún más importante para aquellas que manejan datos sensibles, como datos financieros, datos de salud o personales (Briceño, 2021).

2.1.1. Confidencialidad

De acuerdo con (Jha, 2023):

> La confidencialidad garantiza que la información sea accesible únicamente para aquellos con la autorización necesaria. Esto ayuda a proteger la privacidad y evitar la divulgación de datos a personas o entidades no autorizadas.

2.1.2. Integridad

La integridad garantiza la exactitud y completitud de la información, así como la fiabilidad de los métodos de procesamiento. Esto previene alteraciones no autorizadas, ya sean accidentales o deliberadas, asegurando que los datos sean confiables y correctos (Kumar & Bhatia, 2020).

2.2.3. Disponibilidad

Se refiere a la garantía de que la información y los recursos relacionados estén disponibles para los usuarios autorizados cuando sean necesarios. Esto incluye proteger los sistemas

y redes de ataques o fallos que puedan impedir el acceso a la información (Palacios, 2024).

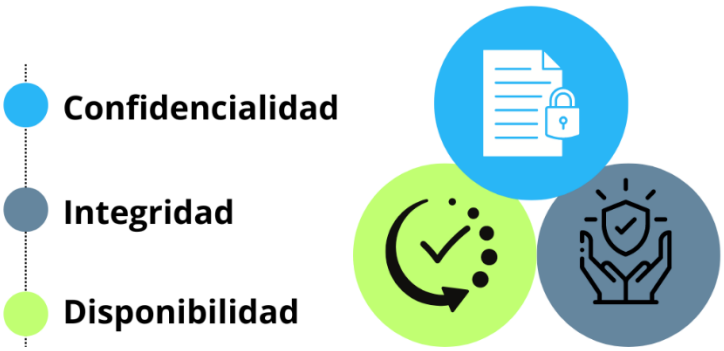


Ilustración 1. TRIADA CIA. Fuente: Autoría Propia.

2.3. Normativas y Estándares de Seguridad de la Información

Las organizaciones, independientemente de su naturaleza (cooperativas, empresas, instituciones públicas, etc.), deben implementar medidas de seguridad para proteger sus datos e información. Las normativas y estándares de seguridad de la información proporcionan un marco de referencia para establecer controles de seguridad efectivos. Estos estándares incluyen mejores prácticas y métodos para:

- **Protección de datos personales:** Garantizar la privacidad y confidencialidad de la información personal.
- **Prevención de ciberataques:** Implementar medidas para proteger los sistemas de información de amenazas externas.
- **Gestión de incidentes:** Establecer procedimientos para responder a incidentes de seguridad.
- **Cumplimiento normativo:** Asegurar el cumplimiento de las leyes y regulaciones aplicables en materia de protección de datos (Lazo & Correa, 2023).

2.3.1. ISO/IEC 27001

La norma ISO/IEC 27001 es uno de los estándares más reconocidos y adoptados a nivel mundial para la gestión de la seguridad de la información. Ofrece un marco para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de

gestión de seguridad de la información (SGSI). La norma se enfoca en la evaluación del riesgo y la gestión basada en riesgos, lo que permite a las organizaciones identificar y tratar los riesgos de seguridad de manera eficiente (Malatji, 2023).

2.3.2. Payment Card Industry Data Security Standard (PCI)

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS) es un marco de seguridad diseñado para proteger la información de las tarjetas de crédito de las principales marcas. Al prevenir, detectar y responder a amenazas, el PCI DSS no solo evita multas y daños a la reputación, sino que también salvaguarda la confianza de los clientes. El cumplimiento de este estándar es esencial para garantizar la seguridad de los datos y prevenir fraudes, asegurando así la continuidad de las operaciones de pago (Garzón Ramos, 2023).

2.3.3. NIST

Este marco proporciona un conjunto de políticas y tecnologías recomendadas destinadas a ayudar a las organizaciones a mejorar su postura de seguridad cibernética. El marco es flexible y adaptable a las necesidades de diferentes tipos de organizaciones, incluyendo sectores privados y gubernamentales. NIST CSF está estructurado por cinco funciones principales que facilitan un enfoque de alto nivel para la gestión y reducción del riesgo de ciberseguridad (NIST , 2024).

- **Identificar:** Desarrollar un entendimiento organizacional para gestionar el riesgo de sistemas, activos, datos y capacidades. Esto incluye identificar qué recursos necesitan ser protegidos y qué riesgos enfrentan.
- **Proteger:** Efectuar las salvaguardias necesarias para limitar o contener el impacto de un potencial incidente de seguridad.
- **Detectar:** Desarrollar e implementar las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad
- **Responder:** Desarrollar e implementar acciones apropiadas tras detectar un incidente de ciberseguridad.
- **Recuperar:** Desarrollar e implementar actividades para restaurar cualquier servicio o capacidad que se haya deteriorado debido a un incidente de ciberseguridad (OEA, 2019).

2.3.4. General Data Protection Regulation (GDPR)

El GDPR es una regulación que tiene como objetivo imponer requisitos fundamentales sobre cómo las organizaciones o empresas deben proteger los datos personales de los ciudadanos de la UE, incluyendo medidas de seguridad técnicas y organizativas para proteger estos datos (Intersoft, 2016).

2.3.5. Tabla comparativa de las Normativas y Estándares de Seguridad de la Información

Las normas de seguridad de la información son esenciales para garantizar la protección de los activos digitales de las organizaciones. La siguiente tabla ofrece una visión general de cuatro de las normas más relevantes, comparando sus objetivos, enfoques y requisitos, lo que facilita la selección de la norma más adecuada para cada contexto.

El proceso de cumplimiento que permite entender como las organizaciones pueden demostrar su adherencia a cada norma; beneficios de cumplimiento, destaca las ventajas de cumplir con cada estándar, que van desde la mejora de la seguridad y la resiliencia organizacional hasta el cumplimiento regulatorio y la protección contra multas y daños reputacionales.

Tabla 1. Tabla comparativa de las normativas y estándares de seguridad de la Información.

Característica	ISO/IEC 27001	NIST Cybersecurity Framework	GDPR (General Data Protection Regulation)	PCI DSS (Payment Card Industry Data Security Standard)
Objetivo Principal	Establecer, implementar y mantener un SGSI	Mejorar la ciberseguridad de la organización	Proteger los datos personales en la UE	Proteger los datos de tarjetas de crédito
Enfoque	Gestión de seguridad de la información	Marco de gestión de riesgos de ciberseguridad	Regulación de privacidad	Estándar de seguridad específico para la industria de pagos

Alcance	Global, todas las industrias	Global, todas las industrias	Organizaciones que procesan datos de ciudadanos de la UE	Cualquier entidad que maneje datos de tarjetas de crédito
Requisitos clave	Sistema de gestión de seguridad de la información (SGSI)	Identificar, Proteger, Detectar, Responder, Recuperar	Consentimiento, derechos de acceso, control y notificación de brechas	Protección de datos almacenados, cifrado de transmisiones de datos
Proceso de Cumplimiento	Auditorías externas regulares	Autoevaluación, auditorías opcionales	Auditorías, reportes obligatorios	Auditorías regulares y evaluaciones de seguridad
Beneficios de Cumplimiento	Mejora continua de la seguridad de la información	Mejora la resiliencia ante ciberataques	Cumplimiento de regulaciones de protección de datos en la UE	Evita multas y mejora la confianza del consumidor en seguridad

. En el sector financiero, donde la protección de datos sensibles es crítica, la **ISO/IEC 27001** se destaca como la norma de referencia. Su enfoque en la implementación y mantenimiento de un **Sistema de Gestión de Seguridad de la Información (SGSI)** proporciona un marco integral que abarca todos los aspectos de la seguridad, desde la política de seguridad hasta los incidentes. Al establecer un ciclo de mejora continua, la ISO 27001 permite a las instituciones financieras adaptarse a las nuevas amenazas y cumplir con los requisitos regulatorios cambiantes, como el **GDPR** y las regulaciones locales. Además, la certificación ISO 27001 aporta credibilidad y confianza a los clientes, demostrando un compromiso sólido con la seguridad de la información.

2.4. Gestión de Riesgos de Tecnologías de Información

La gestión de riesgos de TI es un componente crítico de la gestión general de una organización que implica la identificación, evaluación y tratamiento de los riesgos

asociados con las tecnologías de la información. Su objetivo es proteger los activos de TI, asegurar la continuidad del negocio y minimizar el impacto financiero y operativo de los incidentes de seguridad (Samimi, 2020).

La gestión de riesgos de TI se basa en los siguientes principios:

- **Enfoque proactivo:** La gestión de riesgos de TI debe ser un proceso proactivo que permita identificar y evaluar los riesgos antes de que se materialicen.
- **Enfoque basado en hechos:** La gestión de riesgos de TI debe basarse en una evaluación objetiva de los riesgos, utilizando datos y análisis.
- **Enfoque integrado:** La gestión de riesgos de TI debe estar integrada en todos los procesos de la organización.
- **Comunicación y colaboración:** La gestión de riesgos de TI requiere una comunicación y colaboración efectiva entre todas las partes interesadas.

La gestión de riesgos de TI es una herramienta esencial para todas las organizaciones que dependen de los sistemas de información. Al implementar un proceso de gestión de riesgos de TI efectivo, las organizaciones pueden proteger sus activos digitales, reducir las pérdidas potenciales y mejorar su capacidad para responder a las amenazas cibernéticas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020).

2.4.1. Metodologías de gestión de riesgos de TI

Las metodologías de gestión de riesgos son marcos sistemáticos y estructurados utilizados por las organizaciones para identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con sus actividades y operaciones. Estas metodologías proporcionan un enfoque coherente y repetible para manejar los riesgos de manera efectiva, asegurando que las decisiones estén basadas en la comprensión de las amenazas, vulnerabilidades y su potencial impacto (Campos Cruz & Campos Cruz, 2020).

Las metodologías de gestión de riesgos de TI son cruciales porque proporcionan un marco estandarizado y efectivo para gestionar los riesgos de manera proactiva; guían a las organizaciones en el proceso de identificación, evaluación, manejo y monitoreo de los riesgos asociados con sus sistemas y operaciones de tecnología de la información.

2.4.1.1. MAGERIT

La metodología MAGERIT es un marco de gestión de riesgos desarrollado y mantenido por el Consejo Superior de Administración Electrónica del Gobierno de España (Consejo Superior de Administración Electrónica, 2012). Su objetivo principal es ayudar a las organizaciones a analizar y gestionar los riesgos asociados con sus sistemas de información. MAGERIT es ampliamente reconocida y utilizada, especialmente dentro de las administraciones públicas en España, pero también es aplicable a cualquier organización que necesite gestionar riesgos de TI de manera sistemática.

Esta metodología se compone de las siguientes fases:

- **Identificación de activos:** La metodología MAGERIT inicia con la identificación de activos de información que son esenciales para una determinada organización.
- **Identificación de amenazas:** Una vez que se han identificado los activos, se analizan las potenciales amenazas que podrían comprometer la seguridad de dichos activos.
- **Determinación del riesgo:** Determinar la probabilidad de que ocurran las amenazas y el impacto que tendrían si se materializan. Esto permite priorizar los riesgos en función de su severidad.
- **Determinación de medidas preventivas:** Esta fase define las salvaguardas que reducen el riesgo.
- **Estimación del riesgo residual:** De acuerdo con Avila & Cuenca (2021) En esta fase:

  > "Se realiza el proceso de análisis y evaluación de riesgos inherentes, después de implementar las salvaguardias existentes en la empresa, para así determinar el riesgo residual de los activos" (pág. 369).

2.4.1.2. OCTAVE

OCTAVE es una metodología de análisis y gestión de riesgos, que tiene como objetivo garantizar la protección de los sistemas de información en una empresa, en base a los pilares de la seguridad de la información.

Se divide en tres fases:

- **Fase 1: Crear Perfiles de Activos y Amenazas**

1. **Identificación de Activos Críticos**: Se identifican los activos de información que son críticos para la misión y el negocio.
2. **Identificación de Requerimientos de Seguridad**: Se definen los requerimientos de seguridad para cada activo crítico, considerando la confidencialidad, la integridad y la disponibilidad.
3. **Identificación de Amenazas**: Identificación de amenazas potenciales que podrían afectar a esos activos.

- **Fase 2: Identificar la Infraestructura Vulnerable**

1. **Evaluación de Prácticas de Seguridad**: Se evalúan las prácticas actuales de seguridad para determinar su efectividad en la protección de los activos críticos.
2. **Identificación de Vulnerabilidades**: Se identifican las vulnerabilidades en la infraestructura que podrían ser explotadas por las amenazas identificadas.

- **Fase 3: Desarrollar Estrategias de Mitigación y Protección**

1. **Análisis de Riesgos**: Se analiza el impacto y la probabilidad de las amenazas identificadas para determinar el nivel de riesgo.
2. **Desarrollo de Estrategias de Mitigación**: Se desarrollan y priorizan estrategias para mitigar los riesgos identificados.
3. **Preparación de Planes de Protección**: Se elaboran planes para implementar las estrategias de mitigación seleccionadas (Fernández, Santamaría, & Chacón, 2021).

2.4.1.3. NTE INEN ISO/IEC 27005:2012

ISO/IEC 27005 es crucial para las organizaciones que buscan establecer, mantener y mejorar continuamente un SGSI eficaz. Proporciona un enfoque metodológico para la gestión de riesgos que ayuda a las organizaciones a identificar las áreas donde se requieren controles de seguridad y a justificar las inversiones en esos controles. Además, se utiliza en conjunto con ISO/IEC 27001, proporcionando las pautas detalladas necesarias para la evaluación y tratamiento de riesgos dentro del SGSI (INEN, 2020).

La gestión de riesgos según la ISO/IEC 27005 inicia con el **establecimiento del contexto**, donde se define el entorno interno y externo de la organización, así como el

alcance y los criterios de riesgo del proceso de gestión. Esto prepara el terreno para la **valoración de riesgos**, que incluye la identificación de activos, amenazas y vulnerabilidades, seguido por el análisis de la probabilidad e impacto de estos riesgos, y su posterior evaluación contra los criterios preestablecidos para determinar su severidad. La siguiente fase es el **tratamiento de riesgos**, donde se seleccionan y aplican opciones y controles para mitigar, transferir o aceptar los riesgos. Después de implementar estos controles, la fase de **aceptación de riesgos** implica que los riesgos residuales sean formalmente aceptados por la administración (Bezerra, Lima, Motta, & Piccolini, 2016).

Durante todo el proceso, se lleva a cabo una **comunicación y consulta continua** con las partes interesadas para mantenerlas informadas e involucradas. Finalmente, el proceso concluye con un **monitoreo y revisión regulares** del contexto de riesgo, los criterios de riesgo y la eficacia de los controles implementados, asegurando que la gestión de riesgos se mantenga relevante y efectiva frente a los cambios en el entorno operativo y de amenazas.

2.4.2. Matriz comparativa de metodologías de gestión de riesgos

Los indicadores utilizados en esta tabla sirven como criterios de evaluación para comparar las diferentes metodologías y determinar cuál se alinea mejor con las necesidades específicas de cada entidad.

Estos indicadores permiten evaluar aspectos como: el enfoque general de la metodología (cualitativo, cuantitativo o mixto), su nivel de flexibilidad para adaptarse a diferentes contextos, la complejidad de su implementación, los recursos necesarios, el grado de participación de la organización, la profundidad del análisis de riesgos, la disponibilidad de herramientas de soporte y su orientación hacia la mejora continua. Al analizar estos indicadores, las organizaciones pueden identificar cuál metodología ofrece el mejor equilibrio entre rigor, adaptabilidad y facilidad de uso, permitiéndoles seleccionar la herramienta más adecuada para gestionar sus riesgos de manera efectiva y eficiente.

Tabla 2. Matriz Comparativa de las metodologías de gestión de riesgos. Fuente: Autoría Propia

Indicadores	MAGERIT	OCTAVE	ISO/IEC 27005
Enfoque Metodológico	Mixto	Cualitativo	Mixto

Flexibilidad	Alta, adaptable a distintos entornos	Moderada, con énfasis en participación interna	Alta, muy adaptable a cualquier organización
Complejidad	Media, estructurada	Media, necesita coordinación interna	Baja a media, dependiendo de la aplicación
Recursos Necesarios	Medios a altos, dependiendo del tamaño y complejidad de la organización	Medios, requiere tiempo para talleres y entrevistas	Medios, necesita personal cualificado para evaluación de riesgos
Participación de la organización	Alta, involucra varios niveles de la organización	Alta, enfocada en involucrar a múltiples partes de la organización	Media, enfocada en el equipo de seguridad y TI
Capacidades de análisis de riesgos	Alta, análisis detallado de activos, amenazas y vulnerabilidades	Alta, análisis detallado con enfoque en activos críticos	Alta, metodología detallada para identificación y análisis
Soporte de Herramientas	Varias herramientas específicas de soporte disponibles	Algunas herramientas específicas disponibles	Se basa en herramientas genéricas de análisis de riesgos
Orientación a la mejora continua	Incluye revisiones y actualizaciones regulares del análisis	Promueve evaluaciones regulares y mejora continua	Incluye monitoreo y revisión continua del proceso de riesgos

2.5. Cooperativismo

Este término hace referencia al movimiento y modelo económico y social basado en la cooperación y la autogestión, en donde los miembros de la entidad financiera trabajan de

manera conjunta para alcanzar objetivos comunes que puedan llegar a beneficiar a todos los involucrados.

Entre los principios del cooperativismo se encuentran los siguientes:

- **Adhesión Voluntaria y Abierta**: Las cooperativas son organizaciones voluntarias, abiertas a todas las personas dispuestas a utilizar sus servicios y dispuestas a aceptar las responsabilidades de ser miembros, sin discriminación de género, raza, clase social, posición política o religiosa.

- **Control Democrático de los Miembros**: Las cooperativas son organizaciones democráticas controladas por sus miembros, quienes participan activamente en la formulación de políticas y en la toma de decisiones. Los representantes electos son responsables ante los miembros.

- **Participación Económica de los Miembros**: Los miembros contribuyen equitativamente y controlan democráticamente el capital de la cooperativa. Parte de ese capital es habitualmente propiedad común de la cooperativa. Los miembros generalmente reciben una compensación limitada, si la hay, sobre el capital suscrito como condición de membresía. Los excedentes se distribuyen entre los miembros, se destinan a mejorar la cooperativa o se usan en beneficio de la comunidad.

- **Autonomía e Independencia**: Las cooperativas son organizaciones autónomas de autoayuda controladas por sus miembros. Si entran en acuerdos con otras organizaciones, incluidos los gobiernos, o si recaudan capital de fuentes externas, lo hacen en términos que aseguren el control democrático por parte de sus miembros y mantengan su autonomía cooperativa.

- **Educación, Formación e Información**: Las cooperativas proporcionan educación y formación a sus miembros, representantes electos, gerentes y empleados para que puedan contribuir eficazmente al desarrollo de sus cooperativas. Informan al público en general, particularmente a los jóvenes y a los líderes de opinión, sobre la naturaleza y los beneficios de la cooperación.

- **Cooperación entre Cooperativas**: Las cooperativas sirven a sus miembros de la manera más eficaz y fortalecen el movimiento cooperativo trabajando juntas a través de estructuras locales, nacionales, regionales e internacionales.

- **Interés por la Comunidad**: Las cooperativas trabajan para el desarrollo sostenible de sus comunidades a través de políticas aprobadas por sus miembros

2.6. Cumplimiento Normativo en las Cooperativas Financieras

El cumplimiento normativo es un aspecto crucial para las cooperativas financieras en Ecuador, ya que deben adherirse a una serie de leyes y regulaciones diseñadas para garantizar la estabilidad y la confianza en el sistema financiero. Estas regulaciones están orientadas a proteger a los socios, garantizar la solidez financiera de las instituciones y promover la transparencia y la responsabilidad (Moreira García, 2024).

2.6.1. Superintendencia de Economía Popular y Solidaria (SEPS)

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

2.6.1.1. Clasificación de segmentos de las Cooperativas por la SEPS

La Superintendencia de Economía Popular y Solidaria (SEPS) clasifica a las cooperativas en diferentes segmentos basándose en criterios como el tamaño, la complejidad y el nivel de riesgo de sus operaciones. Esta clasificación permite a la SEPS aplicar una supervisión diferenciada y adecuada a las características específicas de cada cooperativa. En Ecuador, las cooperativas de ahorro y crédito se clasifican en cuatro segmentos principales:

Segmento 1

- Características: Incluye a las cooperativas más grandes en términos de activos, número de socios y volumen de operaciones.

- Requisitos: Estas cooperativas deben cumplir con los más altos estándares de gestión de riesgos, gobernanza y control interno. Tienen mayores obligaciones en términos de capital y liquidez.
- Supervisión: Están sujetas a un nivel de supervisión muy riguroso y frecuente por parte de la SEPS.

Segmento 2

- Características: Incluye a cooperativas de tamaño intermedio, que son más pequeñas que las del Segmento 1 pero aún tienen una presencia significativa en el mercado.
- Requisitos: Deben cumplir con normas de gestión de riesgos y control interno robustas, aunque con menos rigidez comparado con el Segmento 1.
- Supervisión: Reciben una supervisión regular por parte de la SEPS, aunque menos intensiva que las cooperativas del Segmento 1.

Segmento 3

- Características: Agrupa a cooperativas más pequeñas, con una estructura organizativa y operativa menos compleja que las de los Segmentos 1 y 2.
- Requisitos: Aunque las exigencias de capital y control interno son menos estrictas, estas cooperativas aún deben demostrar una gestión adecuada de sus riesgos y operaciones.
- Supervisión: La supervisión es menos intensiva, con un enfoque en asegurar que mantengan prácticas de gestión adecuadas y cumplan con las regulaciones básicas.

Segmento 4

- Características: Incluye a las cooperativas más pequeñas, que generalmente operan a nivel local o comunitario y tienen un volumen de operaciones relativamente bajo.
- Requisitos: Tienen los requisitos menos estrictos en términos de capital, gestión de riesgos y control interno, pero deben cumplir con las regulaciones mínimas establecidas por la SEPS.

- Supervisión: La supervisión es más básica, centrada en asegurar que estas cooperativas mantengan la solvencia y protejan los intereses de sus socios.

2.6.1.2. Importancia de la Clasificación por Segmentos

La clasificación por segmentos permite a la SEPS aplicar una supervisión y regulación proporcional al tamaño y complejidad de cada cooperativa, optimizando los recursos y enfoques regulatorios. Las cooperativas más grandes y complejas (Segmentos 1 y 2) requieren una supervisión más detallada y estricta debido al mayor impacto potencial en el sistema financiero, mientras que las cooperativas más pequeñas (Segmentos 3 y 4) reciben una supervisión más adaptada a su menor escala y riesgo.

Esta segmentación también ayuda a las cooperativas a entender mejor sus obligaciones regulatorias y a gestionar sus operaciones de manera que cumplan con los requisitos específicos de su segmento, fomentando así la estabilidad y el crecimiento sostenible del sector financiero popular y solidario en Ecuador.

2.6.2. Aspectos Clave del cumplimiento normativo de las cooperativas financieras de Ecuador

2.6.2.1. Marco Regulatorio Principal

- **Ley Orgánica de Economía Popular y Solidaria y del Sector Financiero Popular y Solidario**: Esta ley establece las normativas que rigen el funcionamiento de las cooperativas en Ecuador, incluyendo aspectos de administración, fiscalización, y controles internos (Barrezueta, 2011).
- **Superintendencia de Economía Popular y Solidaria (SEPS)**: Es el ente regulador que supervisa las actividades de las cooperativas financieras, asegurando que cumplan con las normativas vigentes y operen de manera segura y transparente. La SEPS juega un papel crucial en garantizar la transparencia, estabilidad y desarrollo de estas entidades, promoviendo prácticas responsables y sostenibles que beneficien a sus socios y al sistema financiero en general. Supervisando y controlando a las organizaciones del sector financiero popular y solidario para asegurar que operen de acuerdo a la normativa vigente, esto incluye la revisión de informes financieros, auditorías y visitas de inspección (SEPS, 2023).

Establece normativas y directrices que regulan las operaciones de las cooperativas y otras entidades bajo su supervisión. Esto incluye requisitos de capital, normas de gestión de riesgos y estándares de contabilidad, garantizando que operen en beneficio de los socios, protegiendo sus intereses y asegurando que reciban información clara y precisa sobre los productos y servicios ofrecidos (Torresano, y otros, 2015).

2.6.2.2. Requisitos de Capital y Liquidez

Las cooperativas deben mantener un mínimo de capital y liquidez conforme a lo que establece la SEPS, lo cual es fundamental para garantizar su estabilidad y solvencia financiera. Los requisitos específicos pueden variar dependiendo del tamaño y del riesgo de la cooperativa.

2.6.2.3. Gestión de Riesgos

Se exige a las cooperativas implementar sistemas de gestión de riesgos efectivos que incluyan la identificación, medición, monitoreo y control de los riesgos financieros, operativos, de mercado y de crédito. La implementación de una gestión de riesgos adecuada es esencial para la operación prudente de la cooperativa.

2.6.2.4. Auditoría y Control Interno

Las cooperativas financieras están obligadas a establecer sistemas de control interno robustos y realizar auditorías internas y externas regularmente. Esto ayuda a detectar y mitigar posibles deficiencias en la gestión y asegura la integridad de la información financiera.

2.6.2.5. Protección al Socio

Es fundamental que las cooperativas cumplan con las regulaciones destinadas a proteger los intereses de sus socios, incluyendo la transparencia en la información financiera y la adecuada atención a reclamos y quejas.

2.6.2.6. Cumplimiento de norma ISO 27001

Con la creciente digitalización de los servicios financieros, las cooperativas deben asegurar la protección de la información personal y financiera de sus socios, cumpliendo con normativas específicas sobre seguridad cibernética y protección de datos.

2.6.2.7. Educación y Capacitación

La normativa también incentiva a las cooperativas a realizar programas de educación financiera para sus socios y empleados, promoviendo así una mayor comprensión de los productos financieros y los derechos y obligaciones asociados.

2.6.2.8. Importancia del Cumplimiento

El cumplimiento normativo no solo es una exigencia legal sino también un componente crítico para la confianza en el sistema financiero cooperativo. Asegura la operación efectiva y eficiente de las cooperativas, minimiza los riesgos legales y financieros y protege los intereses de los socios y la comunidad en general. Las cooperativas que priorizan el cumplimiento normativo están mejor posicionadas para crecer de manera sostenible y responder de manera efectiva a las exigencias del mercado y regulaciones futuras.

2.6.3. Marco regulatorio para las cooperativas en Ecuador relacionadas con la madurez de los Sistemas de Información.

En Ecuador, la Superintendencia de Economía Popular y Solidaria (SEPS) establece normativas y marcos regulatorios que influyen en la madurez de los sistemas de información de las cooperativas.

2.6.4. Norma de control respecto a la seguridad de la información en las entidades del Sector Financiero Popular y Solidario

Esta normativa establece los niveles mínimos para la administración de la seguridad de la información de las entidades, y requiere que las empresas y la Corporación Nacional de Finanzas Populares y Solidarias (CONAFIPS) resguarden y protejan sus activos de información, preservando su confidencialidad, disponibilidad e integridad.

Esta norma establece una serie de directrices y requisitos que cuando se implementen correctamente, pueden contribuir a aumentar la madurez de los sistemas de información de una organización. La norma promueve la mejora continua a través de la evaluación periódica de riesgos, la actualización de controles y políticas, y la capacitación

constante del personal. Estos procesos son coherentes con los principios de madurez, que enfatizan la evolución constante y la optimización de los sistemas de información.

La necesidad de documentar y reportar todas las actividades relacionadas con la seguridad de la información también apoya la madurez organizacional, ya que permite un seguimiento estructurado y facilita la identificación de áreas de mejora (SEPS, 2022).

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque de la investigación

El enfoque de la investigación es de carácter mixto, combinando métodos cualitativos y cuantitativos para obtener una comprensión más profunda del cumplimiento normativo de seguridad de la información. A través de encuestas cuantitativas, se medirán indicadores clave de desempeño relacionados con la implementación de controles de seguridad.

3.2. Nivel de la investigación

El presente estudio se enmarca en un nivel descriptivo y exploratorio, combinando enfoques cuantitativos y cualitativos para obtener una comprensión integral del cumplimiento normativo de seguridad de la información en la COAC Achik Inti. A través de encuestas, se medirán objetivamente indicadores clave como el porcentaje de cumplimiento de los controles de seguridad y la frecuencia de las evaluaciones de riesgo.

3.3. Población y muestra

La población de esta investigación se centra exclusivamente en el personal de TI la Cooperativa de Ahorro y Crédito Achik Inti. Este enfoque permite un análisis exhaustivo y detallado de la percepción, prácticas y desafíos relacionados con el cumplimiento normativo de la seguridad de la información desde diferentes perspectivas dentro de la organización.

3.4. Técnicas e instrumentos de recolección

Se llevó a cabo esta investigación sobre el cumplimiento normativo de la seguridad de la información en la Cooperativa de Ahorro y Crédito Achik Inti, se utilizarán diversas técnicas e instrumentos de recolección de datos, tales como la encuesta que tiene como fin recoger datos numéricos y medibles sobre el cumplimiento normativo, el estado actual de la seguridad de la información y otros datos adicionales.

Se realizó también una entrevista para explorar las percepciones experiencias y desafíos relacionados con la implementación de las normativas de seguridad de la información.

3.5. Tratamiento de la información

El tratamiento de la información recolectada se llevará a cabo a través de un análisis general, ya que solo se realiza una encuesta al jefe de TI.

3.6. Resultados

Tabla 3. Encuesta para análisis de la situación actual de la COAC. Achik Inti. Fuente: Autoría Propia

Cooperativa de Ahorro y Crédito Achik Inti

26-06-2024

ENCUESTA	**Objetivo:** Evaluar el cumplimiento de los requisitos establecidos por la Superintendencia de Economía Popular y Solidaria (SEPS) para la progresión de la COAC Achik Inti del Segmento 4 al Segmento 3.			
Nombre del Encuestado	Diego Ojeda Cuesta			
Cargo	Departamento de Sistemas			
SECCIÓN 1	**CONOCIMIENTO Y CAPACITACIÓN SOBRE LOS REQUISITOS DE LA SEPS**			
¿Está familiarizado con los requisitos de la SEPS para la progresión de segmento?	SI	x	NO	

¿Ha recibido capacitación formal sobre los requisitos de la SEPS en los últimos 12 meses?	SI	x	NO	
SECCIÓN 2	**IMPLEMENTACIÓN DE REQUISITOS**			
¿La cooperativa cumple con los requisitos de capital mínimo establecidos por la SEPS para el Segmento 3?	SI		NO	x
¿Con qué frecuencia se revisan y actualizan las políticas de gestión de riesgos en la cooperativa?	Mensualmente Anualmente	 x	Trimestralmente Nunca	
SECCIÓN 3	**AUDITORÍA Y CONTROL INTERNO**			
¿La cooperativa ha establecido un sistema de auditoría interna para cumplir con los requisitos de la SEPS?	SI		NO	x
En una escala del 1 al 5, donde 1 es "Nada Efectivo" y 5 es "Muy Efectivo", ¿Cómo calificaría el sistema de auditoría interna de la cooperativa?	1 2	x 	3 4 5	
¿Con qué frecuencia se realizan auditorías internas en la cooperativa?	Mensualmente		Trimestralmente	

	Anualmente ☐	Nunca x
SECCIÓN 4	**CUMPLIMIENTO DE LA ISO 27001:2022**	
¿La cooperativa ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la ISO/IEC 27001:2022?	SI ☐	NO x
En una escala del 1 al 5, donde 1 es "Nada Familiarizado" y 5 es "Muy Familiarizado", ¿cómo calificaría su conocimiento sobre los requisitos específicos de la ISO/IEC 27001:2022?	1 ☐ 2 ☐	3 ☐ 4 ☐ 5 x
¿Qué controles específicos de la ISO/IEC 27001:2022 se han implementado en la cooperativa? **(Seleccione todas las que correspondan)**	Control de acceso ☐ Cifrado de datos ☐ Gestión de cambios x	Gestión de incidentes ☐ Continuidad del Negocio ☐ Gestión de activos ☐

		Otras ☐ Especifique _____
¿Con qué frecuencia se realizan auditorías internas del SGSI conforme a la ISO/IEC 27001:2022?	Mensualmente ☐ Anualmente ☐	Trimestralmente ☐ Nunca x
¿La cooperativa tiene un proceso de mejora continua para el SGSI conforme a la ISO/IEC 27001:2022?	SI x	NO ☐
¿Qué desafíos ha enfrentado la cooperativa en la implementación y mantenimiento del SGSI conforme a la ISO/IEC 27001:2022? **(Respuesta abierta)**	No se ha implementado un SGSI	
¿La cooperativa cuenta con un plan de continuidad del negocio y recuperación ante desastres?	SI ☐	NO x
¿Bajo qué norma se ha realizado el plan de continuidad de negocio y recuperación de desastres?	ISO 27031 ☐	ISO 31000 ☐

	ISO 27001 ☐	NIST SP 800-34 ☐ Otro (Especifique) _Estamos en ese proceso
¿La cooperativa tiene políticas y procedimientos documentados para la gestión de cambios en la infraestructura de TI?	SI x	NO ☐

3.7. Análisis general de la encuesta

Una vez realizada la encuesta al jefe del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito Achik Inti, los resultados proporcionan una visión integral del estado actual del cumplimiento de los requisitos establecidos por la Superintendencia de Economía Popular y Solidaria (SEPS) para la progresión de segmento, así como del cumplimiento de la norma ISO/IEC 27001:2022. A continuación, se presenta un análisis general por secciones:

Sección 1: Conocimiento y Capacitación sobre los Requisitos de la SEPS

- **Familiaridad con los Requisitos de la SEPS**: El jefe de TI está familiarizado con los requisitos de la SEPS para la progresión de segmento y ha recibido capacitación formal en los últimos 12 meses. Esto indica un buen nivel de preparación y conocimiento sobre las normativas aplicables.

Sección 2: Implementación de Requisitos

- **Cumplimiento de Requisitos de Capital Mínimo**: La cooperativa no cumple actualmente con los requisitos de capital mínimo establecidos para el Segmento 3, lo que representa una barrera significativa para la progresión de segmento.
- **Frecuencia de Revisión de Políticas de Gestión de Riesgos**: Las políticas de gestión de riesgos se revisan y actualizan anualmente. Sin embargo, una revisión más frecuente podría ser beneficiosa para mejorar la gestión de riesgos.

Sección 3: Auditoría y Control Interno

- **Sistema de Auditoría Interna**: La cooperativa no ha establecido un sistema de auditoría interna, y el sistema existente es calificado como "Nada Efectivo". Además, las auditorías internas no se realizan regularmente, lo que es una deficiencia importante que debe ser abordada.

Sección 4: Cumplimiento de la ISO/IEC 27001:2022

- **Implementación del SGSI**: La cooperativa no ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la ISO/IEC 27001:2022.
- **Conocimiento sobre ISO/IEC 27001:2022**: El jefe de TI califica su conocimiento sobre los requisitos específicos de la norma como "Muy Familiarizado" (nivel 4), lo cual es positivo.
- **Controles Implementados**: Se ha implementado la gestión de cambios, pero otros controles esenciales como el control de acceso y la gestión de incidentes no están implementados.
- **Auditorías Internas del SGSI**: Las auditorías internas del SGSI no se realizan regularmente.
- **Proceso de Mejora Continua**: No existe un proceso de mejora continua.

Sección 5: Continuidad del Negocio y Gestión de Cambios

- **Plan de Continuidad del Negocio y Recuperación ante Desastres**: La cooperativa no cuenta con un plan de continuidad del negocio y recuperación ante desastres.
- **Políticas y Procedimientos de Gestión de Cambios**: La cooperativa tiene políticas y procedimientos documentados para la gestión de cambios en la infraestructura de TI.

CAPÍTULO IV

4. PROPUESTA

4.1. Título de la propuesta

"Cumplimiento normativo de seguridad de la información para la COAC Achik Inti del cantón cañar, segmento 4 y su progresión al segmento 3 bajo la regulación de la SEPS"

4.2. Presentación

El presente proyecto de titulación tiene como objetivo analizar el cumplimiento normativo en el ámbito de TI de la cooperativa de ahorro y crédito Achik Inti Ltda., bajo la regulación de la Superintendencia de Economía Popular y Solidaria (SEPS). A través de una encuesta a los colaboradores involucrados en la gestión de TI, se identificarán las brechas existentes en los procesos de seguridad de la información, gestión de riesgos de TI y cumplimiento normativo. Basado en los resultados de esta evaluación inicial, se propondrán medidas concretas para fortalecer estos procesos y garantizar la seguridad y confidencialidad de la información financiera de los socios. La implementación de estas medidas contribuirá a aumentar la estabilidad operativa de la cooperativa y a fortalecer su posición competitiva en el sector financiero.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001:2022 es esencial para la cooperativa de ahorro y crédito Achik Inti Ltda. Al adoptar este estándar internacional, la cooperativa no solo garantiza el cumplimiento de los requisitos regulatorios establecidos por la Superintendencia de Economía Popular y Solidaria (SEPS), sino que también refuerza la protección de los datos sensibles de sus socios. Un SGSI sólido es fundamental para mitigar riesgos cibernéticos, fomentar la confianza de los socios y demás stakeholders, y asegurar la continuidad operativa de la entidad financiera..

A través de un enfoque integral que incluye la mejora de la infraestructura de TI, el fortalecimiento de la auditoría interna y la gestión de riesgos, así como la implementación de un plan de continuidad del negocio y recuperación ante desastres, esta propuesta busca establecer una base sólida para el crecimiento sostenible y la resiliencia operativa de la COAC Achik Inti. Estos esfuerzos son esenciales para alcanzar los estándares de excelencia requeridos para la progresión al Segmento 3 y asegurar la continuidad y éxito de la cooperativa en un entorno financiero cada vez más competitivo.

4.4 Evaluación Diagnóstica de la Infraestructura y Seguridad Tecnológica (Evaluación de Controles de Seguridad)

4.4.1. Alcance

El alcance de la evaluación informática realizada en la Cooperativa de Ahorro y Crédito Achik Inti abarca una revisión exhaustiva de los sistemas de información, procesos tecnológicos, y controles internos relacionados con la seguridad de la información y la gestión de TI. El propósito de definir un alcance claro es garantizar que todos los aspectos críticos para la seguridad y la operatividad de la cooperativa sean evaluados de manera integral, permitiendo así identificar posibles debilidades y áreas de mejora.

4.4.2. Objetivos

- .Revisar políticas, procedimientos y controles implementados para determinar el grado de cumplimiento de la cooperativa con las normativas vigentes, especialmente las establecidas por la SEPS y las mejores prácticas internacionales como la ISO/IEC 27001
- Identificar vulnerabilidades en los sistemas de información y la infraestructura tecnológica, mediante una evaluación integral de la gestión de accesos, la protección de datos y los procedimientos de respuesta a incidentes de seguridad, con el fin de proporcionar recomendaciones para mitigar los riesgos
- Proponer acciones para mejorar la resiliencia de la cooperativa frente a interrupciones operativas, incluyendo la propuesta de la implementación de un Plan de Continuidad del Negocio que aseguren la operatividad continua en situaciones adversas.

4.4.3. Recolección de Información

En la fase de ejecución del diagnóstico, la recolección de información es un paso crítico que sienta las bases para un análisis exhaustivo y preciso del estado de la seguridad de la información y la gestión de TI en la COAC Achik Inti. Este proceso implica la obtención de datos relevantes y verificados a través de diversas técnicas, como entrevistas, check list, revisión de documentos, observación directa, y el uso de herramientas tecnológicas especializadas.

La calidad y la integridad de la información recolectada determinan en gran medida la precisión de los hallazgos de la auditoría. Por ello, es esencial adoptar un enfoque meticuloso y sistemático durante esta fase. La información recopilada no solo servirá para evaluar la efectividad de los controles existentes y la conformidad con las

normativas vigentes, sino que también proporcionará una visión clara de las áreas donde la cooperativa puede mejorar para fortalecer su seguridad y resiliencia operativa.

Durante esta fase, se garantiza la confidencialidad de la información recolectada y se mantiene una comunicación abierta con los responsables de TI y otros miembros clave de la organización, asegurando que todos los datos relevantes sean considerados y que las observaciones realizadas sean contextualizadas adecuadamente.

A continuación, se realiza un checklist de análisis diseñada para asegurar que todas las áreas críticas de la seguridad de la información y la gestión de TI sean evaluadas de manera exhaustiva y sistemática. Este listado sirve como una guía estructurada que facilita a los auditores la revisión de controles, políticas, y procedimientos, garantizando que no se omita ningún aspecto relevante durante la auditoría.

El propósito del checklist es proporcionar una referencia clara y accesible que permita verificar el cumplimiento de los estándares y normativas aplicables, como la ISO/IEC 27001:2022 y los requisitos establecidos por la Superintendencia de Economía Popular y Solidaria (SEPS). Al utilizar este checklist, se asegura una evaluación coherente y uniforme, permitiendo identificar posibles brechas, debilidades en los controles internos, y áreas donde se pueden implementar mejoras.

Tabla A.1. Controles de seguridad de la información

La siguiente tabla presenta los resultados de una evaluación inicial de los controles de seguridad de la información implementados en la cooperativa, realizada en base a la norma ISO/IEC 27001:2022. Esta evaluación fue llevada a cabo mediante entrevistas al Jefe de TI, quien posee un conocimiento profundo de la infraestructura tecnológica de la organización.

Tabla 4. Check List de la seguridad informática conforme a la ISO 27001:2022

Número	Control Descripción	Cumplimiento (SI/NO)
5	**Controles organizacionales**	

5.1	Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización.	**SI _____ NO _____x____**
5.2	Roles y responsabilidades en la Seguridad de la Información	**Control** Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización.	**SI _____ NO _____x____**
5.3	Segregación de deberes	**Control** Los deberes y áreas de responsabilidad en conflicto deberían segregarse.	**SI _____ NO ___x_____**
5.4	Responsabilidades de la dirección	**Control** La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.	**SI _____ NO ___x_____**
5.5	Contacto con las autoridades	**Control** La organización debe establecer y mantener contacto con las autoridades pertinentes.	**SI _____ NO ___x_____**

5.6	Contacto con grupos de interés especial	**Control** La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad	**SI _____x____ NO _____**
5.7	Inteligencia de amenazas	Control La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.	**SI _____ NO __x_____**
5.8	Seguridad de la Información en la gestión de proyectos	**Control** La seguridad de la información se debe integrar en la gestión de proyectos.	**SI __x_____ NO _____**
5.9	Inventario de información y otros activos asociados	**Control** Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios.	**SI __x_____ NO _____**
5.10	Uso aceptable de la información y otros activos asociados	**Control** Se deben identificar, documentar e implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.	**SI ____x_____ NO _____**
5.11	Devolución de activos	**Control** El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.	**SI _____x____ NO _____**

5.12	Clasificación de la información	**Control** La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.	**SI ___x_____ NO _____**
5.13	Etiquetado de la información	**Control** Se debe elaborar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización	**SI _____ NO ____x_____**
5.14	Transferencia de información	**Control** Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	**SI _____ NO _____x____**
5.15	Control de acceso	**Control** Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información.	**SI ___x_____ NO _____**
5.16	Gestión de identidades	**Control** Se debe gestionar el ciclo de vida completo de las identidades.	**SI _____ NO _____x____**

5.17	Información de autenticación	**Control** La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	**SI** _____ **NO** ____x_____
5.18	Derechos de acceso	**Control** Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.	**SI** _____ **NO** _____x____
5.19	Seguridad de la información en las relaciones con proveedores	**Control** Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.	**SI** _____ **NO** ____x_____
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	**Control** Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor.	**SI** _____ **NO** __x_____
5.21	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	**Control** Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.	**SI** _____ **NO** ___x_____

5.22	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	**Control** La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios	**SI ____x_____ NO _____**
5.23	Seguridad de la información para el uso de servicios en la nube	**Control** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización.	**SI _____x____ NO _____**
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	**Control** La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.	**SI ____x_____ NO _____**
5.25	Evaluación y decisión sobre eventos de seguridad de la información	**Control** La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información.	**SI _____ NO ___x_____**
5.26	Respuesta a incidentes de seguridad de la información	**Control** Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.	**SI _____ NO ____x_____**
5.27	Aprender de los incidentes de	**Control** Los conocimientos adquiridos a partir de incidentes de seguridad de la información	

	seguridad de la información	se deben utilizar para reforzar y mejorar los controles de seguridad de la información.	**SI** _____ **NO** ____x_____
5.28	Recopilación de evidencias	**Control** La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	**SI** ____x_____ **NO** _____
5.29	Seguridad de la información durante una interrupción	**Control** La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.	**SI** _____ **NO** _____x___
5.30	Preparación de las TIC para la continuidad de negocio	**Control** La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	**SI** ____x_____ **NO** _____
5.31	Requisitos legales, reglamentarios y contractuales	**Control** Los requisitos lega les, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.	**SI** _____ **NO** _____x____
5.32	Derechos de propiedad intelectual	**Control** La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.	**SI** _____x___ **NO** _____

5.33	Protección de registros	**Control** Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados.	**SI _____x____ NO _____**
5.34	Privacidad y protección de la información de identificación personal (Pll, por sus siglas en inglés)	**Control** La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la Pll de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.	**SI _____x____ NO _____**
5.35	Revisión independiente de la seguridad de la información	**Control** El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.	**SI _____x____ NO _____**
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	**Control** El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.	**SI _____x____ NO _____**
5.37	Procedimientos operativos documentados	**Control** Los procedimientos operativos de las instalaciones de procesamiento de la información se deben documentar y poner a disposición del personal que los necesite.	**SI _____ NO ____x_____**
6	**Controles de personas**		

6.1	Selección	**Control** Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.	**SI _____x____ NO _____**
6.2	Términos y condiciones de empleo	**Control** Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.	**SI _____ NO ___x_____**
6.3	Conciencia de seguridad de la información, educación y formación	**Control** El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral.	**SI _____ NO _____x____**
6.4	Proceso disciplinario	**Control** Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.	**SI _____ NO _____x____**

6.5	Responsabilidades después de la terminación o cambio de empleo	**Control** Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.	**SI ____x_____ NO _____**
6.6	Acuerdos de confidencialidad o no divulgación	**Control** Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.	**SI ____x_____ NO _____**
6.7	Trabajo remoto	**Control** Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.	**SI _____x____ NO _____**
6.8	Informes de eventos de seguridad de la información	**Control** La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.	**SI ____x_____ NO _____**
7	**Controles físicos**		

7.1	Perímetros de seguridad física	**Control** Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.	**SI _____x____ NO _____**
7.2	Entrada física	**Control** Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.	**SI _____ NO ___x_____**
7.3	Asegurar oficinas, habitaciones e instalaciones	**Control** Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.	**SI _____ NO ____x_____**
7.4	Monitoreo de la seguridad física	**Control** Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.	**SI _____ NO _____x____**
7.5	Protección contra amenazas físicas y ambientales	**Control** Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.	**SI _____ NO ____x_____**
7.6	Trabajar en áreas seguras	**Control** Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras.	**SI _____ NO ____x_____**
7.7	Escritorio y pantalla limpios	**Control** Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento	**SI _____ NO ___x_____**

		extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.	
7.8	Emplazamiento y protección de equipos	**Control** El equipo debe estar situado de forma segura y protegida	**SI** _____ **NO** ____x_____
7.9	Seguridad de los activos fuera de las instalaciones	**Control** Los activos externos deben estar protegidos.	**SI** _____ **NO** __x_____
7.10	Medios de almacenamiento	**Control** Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	**SI** _____ **NO** ____x_____
7.11	Servicios públicos de apoyo	**Control** Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.	**SI** _____ **NO** ____x_____
7.12	Seguridad del cableado	**Control** Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.	**SI** _____ **NO** ___x_____
7.13	Mantenimiento de equipos	**Control** El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y	**SI** _____ **NO** ____x_____

		confidencialidad de la información.	
7.14	Disposición o reutilización segura de los equipos	**Control** Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.	**SI** _____ **NO** ____x_____
8	**Controles tecnológicos**		
8.1	Dispositivos de punto final de usuario	**Control** Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.	**SI** __x_____ **NO** _____
8.2	Derechos de acceso privilegiado	**Control** La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.	**SI** _____x____ **NO** _____
8.3	Restricción de acceso a la información	**Control** El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.	**SI** ____x_____ **NO** _____
8.4	Acceso al código fuente	**Control** El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente	**SI** _____ **NO** ____x_____

4.4.3.1. Análisis de Hallazgos

El checklist realizado anteriormente en la COAC. Achik Inti revela varias áreas críticas que requieren atención urgente para mejorar la seguridad de la información y asegurar el cumplimiento normativo. A continuación, se presenta un análisis detallado de los hallazgos clave identificados a partir de la encuesta:

1. Falta de Políticas y Procedimientos Formales

- **Hallazgo**: La cooperativa no tiene políticas de seguridad de la información formalmente definidas, aprobadas y comunicadas. Además, no se han asignado roles y responsabilidades claras en materia de seguridad de la información, ni se ha implementado la segregación de deberes, lo que aumenta el riesgo de errores y accesos no autorizados.
- **Impacto**: La falta de políticas y roles bien definidos debilita la estructura de control interno y aumenta la vulnerabilidad ante incidentes de seguridad. Esto también dificulta la trazabilidad y responsabilidad en caso de violaciones de seguridad.

2. Inexistencia de Controles de Gestión de Riesgos

- **Hallazgo**: No se han implementado procesos formales para la gestión de riesgos de seguridad de la información, incluida la inteligencia de amenazas y la seguridad en la gestión de proyectos.
- **Impacto**: Sin una gestión adecuada de riesgos, la cooperativa está expuesta a amenazas que podrían comprometer la confidencialidad, integridad y disponibilidad de la información. Esto también afecta la capacidad de la organización para anticipar y mitigar posibles incidentes de seguridad.

3. Deficiencias en la Gestión de Identidades y Accesos

- **Hallazgo**: La encuesta indica que no se gestionan adecuadamente las identidades y los accesos a la información. Los derechos de acceso no son revisados ni actualizados regularmente, lo que deja brechas significativas en la seguridad de los datos.
- **Impacto**: La falta de control sobre quién tiene acceso a qué información aumenta el riesgo de accesos no autorizados y posibles violaciones de seguridad.

Esto es especialmente preocupante en el manejo de información sensible de los socios de la cooperativa.

4. Ausencia de un Plan de Continuidad del Negocio y Recuperación ante Desastres

- **Hallazgo**: La cooperativa no cuenta con un plan documentado y probado de continuidad del negocio, lo que significa que no está preparada para mantener operaciones críticas en caso de interrupciones.
- **Impacto**: La falta de preparación para la continuidad del negocio podría resultar en interrupciones prolongadas en los servicios, pérdida de datos y daño a la reputación en caso de desastres o incidentes graves.

5. Inexistencia de un Proceso de Monitoreo y Revisión Continua

- **Hallazgo**: No se realizan auditorías internas regulares para revisar la efectividad de los controles de seguridad de la información. Además, la organización carece de un sistema para aprender de los incidentes de seguridad pasados y mejorar sus controles.
- **Impacto**: Sin un proceso de monitoreo y revisión continua, la cooperativa no puede garantizar que los controles de seguridad implementados sean efectivos a lo largo del tiempo. Esto impide la mejora continua y la adaptación a nuevas amenazas.

6. Inadecuada Seguridad Física y Ambiental

- **Hallazgo**: La encuesta muestra deficiencias en la seguridad física de las instalaciones, como la falta de controles de entrada adecuados y protección contra amenazas físicas y ambientales.
- **Impacto**: La falta de medidas de seguridad física expone a la cooperativa a riesgos de accesos no autorizados, daños a la infraestructura, y posibles pérdidas de datos debido a desastres naturales o sabotajes.

4.4.3.2. Identificación de brechas y riesgos

A continuación, se presenta una tabla que resume las principales brechas identificadas durante la evaluación diagnóstica de TI en la Cooperativa de Ahorro y Crédito Achik Inti. Esta tabla también incluye los riesgos asociados a cada brecha. La identificación y

mitigación de estas brechas son cruciales para mejorar la seguridad de la información y asegurar la continuidad operativa de la cooperativa.

Brecha	Descripción	Riesgo Asociado
Falta de Políticas y Procedimientos Formales de Seguridad de la Información	No existen políticas formalizadas y documentadas para la gestión de la seguridad de la información.	Aumento de accesos no autorizados y errores operativos debido a la falta de directrices claras.
Deficiencias en la Gestión de Riesgos	No hay un proceso formal para la identificación, evaluación y mitigación de riesgos relacionados con la seguridad de la información.	Exposición a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de datos.
Inadecuada Gestión de Identidades y Accesos	Los derechos de acceso no se revisan ni actualizan regularmente; falta de controles en la gestión de identidades.	Riesgo elevado de accesos no autorizados y posibles violaciones de datos.
Ausencia de un Plan de Continuidad del Negocio y Recuperación ante Desastres	No se dispone de un plan documentado y probado para la continuidad del negocio en caso de incidentes graves.	Posible interrupción prolongada de servicios y pérdida de datos críticos en situaciones de emergencia.
Inexistencia de un Proceso de Monitoreo y Auditoría Interna	No se realizan auditorías internas ni monitoreo continuo de los sistemas y	Dificultad para mantener la efectividad de los controles de seguridad a lo largo del tiempo.

	políticas de seguridad.	
Seguridad Física y Ambiental Insuficiente	Las instalaciones presentan deficiencias en controles de acceso físico y protección contra amenazas ambientales.	Riesgo de intrusión, sabotaje, o daños a la infraestructura y datos debido a amenazas físicas y ambientales.

4.4. Propuesta de Plan de mejora

El diagnóstico inicial realizado en la Cooperativa de Ahorro y Crédito Achik Inti ha revelado importantes brechas en la gestión de la seguridad de la información y la infraestructura tecnológica. Estas deficiencias no solo representan riesgos significativos para la protección de los activos de información, sino que también comprometen la capacidad de la cooperativa para cumplir con los requisitos regulatorios establecidos por la Superintendencia de Economía Popular y Solidaria (SEPS), necesarios para avanzar del Segmento 4 al Segmento 3.

La SEPS establece lineamientos claros para la progresión entre segmentos, los cuales incluyen, entre otros aspectos, la robustez de la infraestructura tecnológica, la gestión efectiva de riesgos, y el cumplimiento de las normativas de seguridad de la información. Para alcanzar el Segmento 3, es imprescindible que la cooperativa demuestre mejoras significativas en estas áreas, asegurando así la integridad y seguridad de los datos, así como la continuidad de las operaciones en caso de contingencias.

En respuesta a estos hallazgos y lineamientos, se presenta una propuesta de plan de mejora que tiene como objetivo no solo mitigar los riesgos identificados, sino también cumplir con los requisitos de la SEPS para avanzar al Segmento 3. El plan se basa en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, así como en el desarrollo de un Plan de Continuidad del Negocio (PCN) que garantice la resiliencia operativa de la cooperativa.

Este plan de mejora está diseñado para abordar integralmente las deficiencias detectadas, ofreciendo una hoja de ruta clara y estructurada para implementar las mejoras necesarias.

Se detallan a continuación las acciones específicas recomendadas, los recursos necesarios, y el cronograma de implementación, con el fin de cumplir con los lineamientos de la SEPS y asegurar la protección a largo plazo de los datos y operaciones de la cooperativa.

4.4.1. Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI)

El desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso fundamental para garantizar la protección de los activos de información de la COAC Achik Inti. La implementación de un SGSI conforme a la norma ISO/IEC 27001:2022 permitirá a la cooperativa gestionar de manera efectiva los riesgos de seguridad de la información, asegurar la confidencialidad, integridad y disponibilidad de los datos, y cumplir con los requisitos regulatorios establecidos por la Superintendencia de Economía Popular y Solidaria (SEPS).

4.4.1.1. Objetivos

El Sistema de Gestión de Seguridad de la Información (SGSI) tiene como principal objetivo garantizar la protección adecuada de la información de la Cooperativa de Ahorro y Crédito Achik Inti, alineándose con las mejores prácticas internacionales y cumpliendo con los requisitos establecidos por la norma ISO/IEC 27001:2022. Los objetivos clave del SGSI son:

Confidencialidad: Asegurar que la información esté disponible solo para las personas autorizadas y prevenir el acceso no autorizado a los datos sensibles.

Integridad: Garantizar la exactitud y completitud de la información y los métodos de procesamiento, asegurando que los datos no sean alterados de manera no autorizada.

Disponibilidad: Asegurar que la información y los sistemas de información estén disponibles para su uso cuando sean necesarios, minimizando las interrupciones de los servicios.

Cumplimiento Normativo: Cumplir con todas las normativas y regulaciones aplicables, incluyendo los requisitos de la Superintendencia de Economía Popular y Solidaria (SEPS) y la norma ISO/IEC 27001:2022.

Mejora Continua: Establecer un ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar) que permita ajustar y mejorar constantemente los controles de seguridad y las políticas del SGSI en respuesta a nuevas amenazas y cambios en el entorno regulatorio.

4.4.1.2. Fases de Implementación del SGSI

La implementación del SGSI se llevará a cabo en varias fases, siguiendo un enfoque sistemático y alineado con los principios de la norma ISO/IEC 27001:2022:

1. **Fase 1: Planificación**
    - **Análisis del Contexto y Definición del Alcance**: Identificación de los activos de información críticos, análisis del contexto interno y externo de la cooperativa, y definición del alcance del SGSI.
    - **Política de Seguridad de la Información**: Desarrollo y aprobación de una política de seguridad de la información que refleje los objetivos estratégicos de la cooperativa y los requisitos de la norma ISO/IEC 27001.
    - **Evaluación de Riesgos**: Realización de una evaluación de riesgos inicial para identificar y clasificar los riesgos asociados con los activos de información y establecer prioridades para su tratamiento.
2. **Fase 2: Implementación**
    - **Desarrollo de Controles y Procedimientos**: Implementación de los controles de seguridad necesarios para mitigar los riesgos identificados, incluyendo controles técnicos, organizativos y físicos.
    - **Capacitación y Concienciación**: Formación del personal sobre las políticas y procedimientos del SGSI, así como sobre las mejores prácticas de seguridad de la información.
    - **Documentación del SGSI**: Creación de la documentación requerida para el SGSI, incluyendo procedimientos operativos, planes de respuesta a incidentes, y registros de auditoría.
3. **Fase 3: Operación**

- **Monitoreo y Revisión**: Implementación de un sistema de monitoreo continuo para evaluar la efectividad de los controles de seguridad y detectar posibles incidentes de seguridad en tiempo real.
- **Gestión de Incidentes**: Establecimiento de un proceso para la gestión y respuesta a incidentes de seguridad, que incluya la identificación, contención, erradicación, y recuperación de incidentes.

4. **Fase 4: Auditoría Interna**
    - **Realización de Auditorías Internas**: Ejecución de auditorías internas periódicas para evaluar el cumplimiento del SGSI con la norma ISO/IEC 27001 y la efectividad de los controles implementados.
    - **Revisión por la Dirección**: Revisión del SGSI por parte de la alta dirección para asegurar su alineación con los objetivos estratégicos de la cooperativa y para tomar decisiones sobre la mejora continua.

5. **Fase 5: Mejora Continua**
    - **Ciclo de Mejora Continua (PDCA)**: Aplicación del ciclo Planificar-Hacer-Verificar-Actuar (PDCA) para mejorar continuamente el SGSI, ajustando los controles y políticas en función de los resultados de las auditorías, cambios en el entorno de la organización, y evolución de las amenazas.
    - **Actualización de la Evaluación de Riesgos**: Revisión y actualización periódica de la evaluación de riesgos para reflejar cambios en el entorno de la cooperativa y asegurar que los controles de seguridad sigan siendo adecuados y efectivos.

Este enfoque escalonado permite una implementación estructurada y efectiva del SGSI, asegurando que todos los aspectos críticos de la seguridad de la información sean abordados de manera integral, y que la cooperativa esté preparada para enfrentar los desafíos actuales y futuros en el ámbito de la seguridad de la información.

4.4.2. Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio (PCN) es un componente esencial para asegurar que la Cooperativa de Ahorro y Crédito Achik Inti pueda mantener sus operaciones críticas y continuar prestando servicios a sus socios en caso de interrupciones significativas, como desastres naturales, fallos tecnológicos o incidentes de seguridad. A continuación, se presenta un modelo detallado de lo que debería contener un PCN para garantizar la resiliencia operativa de la cooperativa.

1. Introducción

- **Objetivo del PCN**: Describir el propósito del PCN, que es asegurar la continuidad de las operaciones críticas de la cooperativa en caso de interrupciones graves.
- **Alcance**: Definir el alcance del PCN, especificando las áreas de la cooperativa, los procesos críticos y los sistemas que están cubiertos por el plan.
- **Contexto y Justificación**: Explicar por qué es necesario un PCN, considerando los riesgos a los que está expuesta la cooperativa y las posibles consecuencias de una interrupción prolongada.

2. Análisis de Impacto en el Negocio (BIA)

- **Identificación de Procesos Críticos**: Enumerar y describir los procesos críticos para la operatividad de la cooperativa, como la gestión de cuentas, procesamiento de transacciones y acceso a sistemas de información.
- **Evaluación del Impacto**: Evaluar el impacto financiero, operativo y reputacional que tendría la interrupción de cada proceso crítico.
- **Definición del Tiempo Objetivo de Recuperación (RTO)**: Establecer el tiempo máximo aceptable para la recuperación de cada proceso crítico después de una interrupción.
- **Definición del Punto Objetivo de Recuperación (RPO)**: Determinar la cantidad máxima de datos que la cooperativa puede permitirse perder en caso de un fallo significativo.

3. Estrategias de Continuidad del Negocio

- **Estrategias de Recuperación de Procesos Críticos**: Describir las estrategias a implementar para asegurar la continuidad de los procesos críticos identificados. Esto puede incluir la duplicación de sistemas, la implementación de centros de datos secundarios, y el almacenamiento en la nube.
- **Plan de Recuperación de Desastres (DRP)**: Establecer procedimientos específicos para la recuperación ante desastres, incluyendo el traslado a sitios alternativos, restauración de copias de seguridad, y la comunicación con proveedores de servicios críticos.
- **Gestión de Recursos**: Detallar cómo se gestionarán los recursos humanos, financieros y tecnológicos durante una interrupción para asegurar la continuidad del negocio.

4. Plan de Respuesta a Incidentes

- **Detección y Respuesta Inicial**: Describir los procedimientos para la detección temprana de incidentes que puedan causar una interrupción significativa y las acciones inmediatas a tomar.
- **Notificación y Comunicación**: Establecer un protocolo de comunicación para informar a los empleados, socios, y partes interesadas clave sobre el incidente y las acciones de respuesta.
- **Evaluación del Daño y Decisión de Activación del PCN**: Detallar el proceso para evaluar el alcance del daño y decidir cuándo activar el PCN.
- **Movilización del Equipo de Continuidad del Negocio**: Definir las funciones y responsabilidades del equipo encargado de ejecutar el PCN y coordinar las acciones de recuperación.

5. Restauración y Recuperación

- **Procedimientos de Restauración**: Describir los pasos específicos para restaurar los sistemas y procesos críticos a su estado operativo normal.
- **Prioridades de Recuperación**: Establecer el orden de prioridad en el que se restaurarán los procesos y sistemas críticos, basado en el análisis de impacto en el negocio.

- **Reintegración de Operaciones**: Detallar el proceso para reintegrar las operaciones restauradas al entorno de producción y asegurar la continuidad a largo plazo.

6. Pruebas y Mantenimiento del PCN

- **Plan de Pruebas**: Describir el programa de pruebas del PCN, incluyendo pruebas de simulación y pruebas de recuperación, para asegurar que el plan sea efectivo y que todo el personal esté familiarizado con sus roles en una emergencia.
- **Revisión y Actualización del PCN**: Establecer un cronograma regular para la revisión y actualización del PCN, asegurando que el plan se mantenga alineado con los cambios en la organización, la tecnología y el entorno de riesgo.
- **Documentación y Reportes**: Detallar cómo se documentarán los resultados de las pruebas y las revisiones, y cómo se utilizarán estos reportes para mejorar continuamente el PCN.

7. Capacitación y Concienciación

- **Programas de Capacitación**: Establecer un programa de capacitación continua para todo el personal, enfocándose en su rol dentro del PCN y las mejores prácticas para la continuidad del negocio.
- **Concienciación sobre la Continuidad del Negocio**: Implementar campañas de concienciación para asegurar que todos los empleados comprendan la importancia de la continuidad del negocio y estén preparados para actuar en caso de una interrupción.

8. Conclusiones

- **Resumen de Beneficios del PCN**: Recapitular los beneficios clave de implementar un PCN, incluyendo la mitigación de riesgos, la protección de la reputación de la cooperativa y la garantía de un servicio continuo a los socios.
- **Compromiso con la Mejora Continua**: Destacar el compromiso de la cooperativa con la mejora continua del PCN y la importancia de mantenerlo actualizado y probado regularmente.

Este modelo de Plan de Continuidad del Negocio proporciona una guía completa para asegurar que la Cooperativa de Ahorro y Crédito Achik Inti esté preparada para enfrentar interrupciones significativas, proteger sus operaciones críticas, y cumplir con las expectativas de sus socios y reguladores.

4.4.3. Prioridades y Cronograma de Implementación

A continuación, se presenta una tabla que detalla las prioridades para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y el Plan de Continuidad del Negocio (PCN), junto con el cronograma propuesto para cada acción. Este cronograma está diseñado para asegurar que las áreas críticas sean abordadas primero, garantizando una mejora continua en la seguridad de la información y la resiliencia operativa de la Cooperativa de Ahorro y Crédito Achik Inti.

Prioridad	Acción	Descripción	Responsable
Alta	Definición del Alcance del SGSI y PCN	Identificación de los activos críticos y definición del alcance del SGSI y PCN.	Comité de Seguridad de la Información
Alta	Evaluación de Riesgos	Realización de la evaluación inicial de riesgos para identificar y priorizar amenazas y vulnerabilidades.	Equipo de TI y Consultores Externos
Alta	Desarrollo de Políticas y Procedimientos de Seguridad	Creación y aprobación de políticas y procedimientos de seguridad de la información conforme a la	Equipo de TI

		ISO/IEC 27001.	
Alta	Implementación de Controles de Seguridad	Implementación de controles técnicos y organizativos para mitigar riesgos identificados.	Equipo de TI
Media	Capacitación y Concienciación del Personal	Formación del personal sobre las nuevas políticas de seguridad y procedimientos del SGSI y PCN.	Recursos Humanos y Dirección de TI
Media	Desarrollo del Plan de Continuidad del Negocio (PCN)	Diseño del PCN, incluyendo estrategias de recuperación y procedimientos de respuesta a incidentes.	Equipo de Continuidad del Negocio
Media	Pruebas de Simulación del PCN	Realización de pruebas de simulación para validar la efectividad del PCN y ajustar en función de los resultados.	Equipo de Continuidad del Negocio
Baja	Auditoría Interna del SGSI	Ejecución de la primera auditoría interna del SGSI	Auditores Internos

		para evaluar el cumplimiento y efectividad de los controles.	
Baja	Revisión y Actualización del SGSI y PCN	Realizar una revisión exhaustiva del SGSI y PCN al menos una vez al año, o después de cualquier cambio significativo en la organización (como una reestructuración o la adopción de nuevas tecnologías).	Equipo de TI

CONCLUSIONES

En base al desarrollo de la presente tesis, se pueden extraer las siguientes conclusiones alineadas con los objetivos propuestos:

Se ha logrado elaborar una revisión detallada y comprensiva del marco teórico relacionado con la seguridad de la información, específicamente en el contexto de cooperativas de ahorro y crédito. Esta revisión no solo ha permitido comprender las normativas, estándares y mejores prácticas que rigen la seguridad de la información en estas instituciones, sino que también ha servido como base para el análisis específico de la situación actual en la COAC Achik Inti.

A partir de este marco teórico, se llevó a cabo un levantamiento exhaustivo de información en la COAC Achik Inti, lo que permitió determinar el estado actual de su seguridad de la información. Este diagnóstico, basado en las normativas y mejores prácticas identificadas previamente, ha revelado áreas críticas que requieren atención inmediata, como la falta de políticas de seguridad actualizadas, la necesidad de mejorar las infraestructuras tecnológicas, y la capacitación insuficiente del personal en temas de seguridad. Este análisis ha sido fundamental para identificar las brechas existentes y establecer una línea base para el desarrollo de acciones correctivas.

Como resultado del análisis previo, se ha elaborado un documento detallado que especifica las acciones necesarias para que la COAC Achik Inti cumpla con las normativas de seguridad de la información requeridas para el segmento 3. Este documento incluye la actualización de políticas de seguridad, la mejora de las infraestructuras tecnológicas, la capacitación continua del personal, y la implementación de medidas de gestión de riesgos y protección de datos. Además, se han definido los recursos necesarios y los plazos para la ejecución de estas acciones, proporcionando a la cooperativa una hoja de ruta clara y estructurada para alcanzar el cumplimiento normativo y mejorar su postura de seguridad.

RECOMENDACIONES

Se recomienda a la COAC. Achik Inti:

- Actualizar las políticas de seguridad de la información de la cooperativa para alinearlas con las normativas del segmento 3 y las mejores prácticas del sector. Además, es crucial que estas políticas sean ampliamente difundidas y comprendidas por todos los empleados para asegurar su correcta aplicación.
- Invertir en la modernización de las infraestructuras tecnológicas, asegurando que los sistemas de información sean robustos y capaces de soportar las exigencias de seguridad actuales. Esto incluye la implementación de tecnologías de cifrado, control de accesos, y medidas de protección física y lógica para los datos críticos.
- La formación regular y especializada del personal en temas de seguridad de la información es esencial para minimizar los riesgos asociados a errores humanos y garantizar una cultura de seguridad dentro de la organización. Se recomienda diseñar programas de capacitación que aborden tanto aspectos técnicos como procedimentales de la seguridad de la información.
- Implementar un sistema de monitoreo y revisión continua del Sistema de Gestión de Seguridad de la Información (SGSI) para identificar y corregir debilidades antes de que puedan ser explotadas. Este proceso debe incluir auditorías internas regulares y la actualización periódica de los procedimientos de seguridad.

A la Universidad Católica de Cuenca, extensión Cañar, Facultad de Sistemas de Información:

- Se recomienda incentivar la investigación en el área de seguridad de la información, enfocándose en estudios aplicados a cooperativas de ahorro y crédito. Esto contribuirá a desarrollar conocimientos específicos que puedan ser utilizados para mejorar la seguridad en este sector tan crucial.
- Creación de programas de capacitación o diplomados especializados en seguridad de la información para profesionales que ya se encuentran trabajando

en el sector. Esto no solo ampliaría la oferta educativa, sino que también contribuiría a elevar los estándares de seguridad en las cooperativas de la región.

REFERENCIAS

Barrezueta, H. E. (28 de 04 de 2011). *www.vicepresidencia.gob.ec*. Obtenido de www.vicepresidencia.gob.ec: https://www.vicepresidencia.gob.ec/wp-content/uploads/downloads/2018/09/Ley-Orga%CC%81nica-de-Economi%CC%81a-Popular-y-Solidaria.pdf

Bezerra, E. K., Lima, F. A., Motta, A. C., & Piccolini, J. D. (2016). *Gestión del Riesgo de las TI NTC 27005.* Colombia: RENATA. Obtenido de cedia.edu.ec: https://cedia.edu.ec/docs/efc/GTI9.pdf

Briceño, E. V. (2021). *Seguridad de la información.* 3 ciencias.

Campos Cruz, C. Y., & Campos Cruz, C. Y. (31 de 01 de 2020). *repositorio.unprg.edu.pe.* Obtenido de repositorio.unprg.edu.pe: https://repositorio.unprg.edu.pe/handle/20.500.12893/8244

Consejo Superior de Administración Electrónica. (12 de 09 de 2012). *administracionelectronica.gob.es.* Obtenido de administracionelectronica.gob.es: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Fernández, A. E., Santamaría, L. I., & Chacón, J. H. (2021). Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria. 1-13.

Garzón Ramos, L. F. (08 de 08 de 2023). *repository.unipiloto.edu.co.* Obtenido de repository.unipiloto.edu.co: https://repository.unipiloto.edu.co/handle/20.500.12277/13058

INEN. (13 de 12 de 2020). *app.virtualex.ec.* Obtenido de app.virtualex.ec: https://app.virtualex.ec/documentos/nte_inen_iso_iec_27005.pdf

Intersoft. (27 de 04 de 2016). *gdpr-info.eu*. Obtenido de gdpr-info.eu: https://gdpr-info.eu/

Jha, R. K. (2023). Ciberseguridad y confidencialidad en redes inteligentes para mejorar la sostenibilidad y la confiabilidad. *Revista de revisiones de investigaciones recientes*, 215-241.

Kumar, R., & Bhatia, M. (2020). A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability. *Conferencia Internacional IEEE sobre Tecnologías de Computación, Energía y Comunicaciones (GUCON)*, 334-337.

Lazo, C. D., & Correa, B. L. (2023). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales . *Digital Publisher*, 88-102.

Malatji, M. (2023). Gestión de la ciberseguridad empresarial: una revisión de ISO/IEC 27001:2022. *Conferencia internacional de 2023 sobre gestión e ingeniería cibernéticas (CyMaEn) , Bangkok, Tailandia*, 117-122.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (18 de 04 de 2020). *www.gobiernoelectronico.gob.ec.* Obtenido de www.gobiernoelectronico.gob.ec: https://www.gobiernoelectronico.gob.ec/wp-

content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Moreira García, G. (2024). El Obligaciones tributarias en la rentabilidad de las Cooperativas de Ahorro y Crédito. *Digital Publisher*, 405-415.

NIST . (29 de 02 de 2024). *www.nist.gov*. Obtenido de www.nist.gov: https://www.nist.gov/

OEA. (19 de 08 de 2019). *www.oas.org.* Obtenido de www.oas.org: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Palacios, A. P. (2024). *Seguridad informática (Edición 2020).* Ediciones Paraninfo, S.A.

Samimi, A. (2020). Risk Management in Information Technology . *Progress in Chemical and Biochemical Research*, 130-134. Obtenido de uvadoc.uva.es: https://uvadoc.uva.es/handle/10324/63130

SEPS. (01 de 01 de 2022). *www.seps.gob.ec.* Obtenido de www.seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

SEPS. (05 de 12 de 2023). *www.seps.gob.ec*. Obtenido de www.seps.gob.ec: https://www.seps.gob.ec/

Superintendencia de Economía Popular y Solidaria. (05 de 12 de 2023). *www.seps.gob.ec.* Obtenido de www.seps.gob.ec: https://www.seps.gob.ec/institucion/que-es-la-seps/

Torres, R. A., & Tapia, J. P. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. *Revista Científica Dominio de las Ciencias*, 363-376.

Torresano, D., Herman, E., Trávez, C., Durán, Á., Pena, A., Miño, M., . . . Bastida, O. (01 de 10 de 2015). *www.seps.gob.ec.* Obtenido de www.seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/Economia-Solidaria-Experiencias-y-Conceptos.pdf

COAC
ACHIK INTI
LTDA.

"EVALUACIÓN DIAGNÓSTICA DE LA INFRAESTRUCTURA Y SEGURIDAD DE TI EN LA COAC ACHIK INTI"

Reporte realizado por
Israel Romero Loja

CAÑAR

Diagnóstico de auditoría Informática en la Cooperativa de Ahorro y Crédito Achik Inti Ltda., agosto 2024

1. Resumen Ejecutivo

El presente diagnóstico informático se llevó a cabo para evaluar la seguridad de la información y el cumplimiento normativo de la Cooperativa de Ahorro y Crédito Achik Inti, con miras a su avance del Segmento 4 al Segmento 3 según la regulación de la Superintendencia de Economía Popular y Solidaria (SEPS). Se enfocó en la evaluación de los sistemas de información, políticas de seguridad, y controles internos implementados.

El enfoque incluyó encuestas con el personal clave, revisión de documentación, y pruebas de controles específicos. Se utilizaron estándares, como la ISO/IEC 27001:2022, para guiar la evaluación. El análisis incluyó la recolección de evidencias, la verificación de la efectividad de los controles y el cumplimiento de los requisitos regulatorios.

La auditoría identificó varias áreas críticas. Se observó que las políticas de seguridad de la información requieren actualizaciones y que el proceso de gestión de riesgos no está formalmente implementado. Además, se encontraron inconsistencias en el control de accesos y una falta de auditorías internas regulares, lo cual compromete la efectividad de los controles de seguridad. También se constató la ausencia de un plan documentado y probado para la continuidad del negocio y la recuperación ante desastres, lo cual es crucial para la resiliencia operativa de la cooperativa. Se recomienda la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la ISO/IEC 27001:2022, así como el fortalecimiento de la gestión de riesgos y la mejora de los controles de acceso. Es esencial establecer un programa de auditoría interna y desarrollar un plan de continuidad del negocio y recuperación ante desastres para garantizar la operación continua y el cumplimiento normativo.

El diagnóstico reveló áreas clave que requieren atención urgente para mejorar la seguridad de la información y asegurar el cumplimiento normativo de la COAC Achik Inti. La implementación de las recomendaciones fortalecerá la protección de los activos de información y facilitará la conformidad con los requisitos de la SEPS, permitiendo un avance seguro hacia el Segmento 3. Se destaca la prioridad de implementar un SGSI y

desarrollar un plan de continuidad del negocio para asegurar la resiliencia y sostenibilidad de las operaciones de la cooperativa.

1.1. Objetivo

El objetivo principal de la auditoría informática realizada en la COAC Achik Inti es evaluar el estado actual de la seguridad de la información, identificando las fortalezas y debilidades en los sistemas y controles internos. Se busca asegurar que la cooperativa cumpla con las normativas vigentes, especialmente en preparación para la progresión del Segmento 4 al Segmento 3 bajo la regulación de la Superintendencia de Economía Popular y Solidaria (SEPS). La auditoría también pretende proporcionar recomendaciones para mejorar la seguridad de la información y garantizar la protección adecuada de los datos sensibles y la resiliencia operativa de la organización.

1.2. Alcance

El alcance del diagnóstico incluyó una revisión exhaustiva de los sistemas de información, procesos de gestión de datos, y controles internos relacionados con la seguridad de la información. Abordando áreas clave como:

- **Políticas y Procedimientos de Seguridad de la Información**: Evaluación de la existencia, adecuación y actualización de las políticas y procedimientos de seguridad.
- **Control de Accesos y Gestión de Identidades**: Revisión de los controles de acceso físico y lógico a los sistemas y datos críticos.
- **Auditoría Interna y Cumplimiento Normativo**: Verificación de la implementación de un sistema de auditoría interna y el grado de cumplimiento con normativas internas y externas, incluyendo ISO/IEC 27001:2022 y los requisitos de la SEPS.
- **Continuidad del Negocio y Recuperación ante Desastres**: Evaluación de los planes y medidas existentes para asegurar la continuidad del negocio y la recuperación de desastres.

1.3. Metodología

La metodología utilizada para realizar el diagnóstico informático en la COAC Achik Inti fue diseñado para proporcionar una evaluación exhaustiva de la seguridad de la información y el cumplimiento normativo. Se adoptó un enfoque sistemático y

estructurado, basado en las mejores prácticas de la industria y marcos normativos reconocidos, como la ISO/IEC 27001:2022.

2. Hallazgos

El análisis realizado mediante el checklist reveló varios hallazgos clave en la COAC Achik Inti en relación con la implementación de la norma ISO 27001 y los requisitos del segmento superior.

Área	Fortalezas	Áreas de Mejora
Políticas de Seguridad	Documento de políticas de seguridad existente y revisado periódicamente.	Difusión y conocimiento insuficientes entre el personal.
Aspectos Organizativos	Roles y responsabilidades claramente definidos; comité de seguridad establecido.	Revisión periódica del estado de la seguridad mediante reuniones formales necesita fortalecerse.
Seguridad de Recursos Humanos	Verificación de la integridad de empleados antes de la contratación; procedimientos para incidentes.	Formación regular en seguridad insuficiente; evaluaciones de desempeño no incluyen criterios de seguridad.
Gestión de Activos	Inventarios actualizados; responsables asignados para cada activo.	Categorización de activos según su importancia no completamente implementada.
Control de Accesos	Proceso formal de gestión de acceso; autenticación robusta implementada.	Monitorización de accesos privilegiados en proceso de implementación.

Cifrado	Uso de algoritmos de cifrado fuertes; gestión de claves implementada.	Revisión periódica de políticas y procedimientos de cifrado aún en proceso.
Seguridad Física y Ambiental	Protección adecuada de instalaciones; medidas contra desastres naturales implementadas.	Sistemas de monitoreo y alarmas, y simulacros de emergencia requieren fortalecimiento.
Seguridad en la Operativa	Monitorización regular de registros; gestión adecuada de copias de seguridad.	Pruebas regulares del plan de continuidad del negocio necesitan ser implementadas.
Seguridad en Telecomunicaciones	Mecanismos seguros de transmisión de información; protección de redes implementada.	Segmentación de redes en proceso para limitar acceso a recursos críticos.
Adquisición y Mantenimiento	Requisitos de seguridad incluidos en sistemas; auditorías de seguridad realizadas.	Refuerzo necesario en pruebas de seguridad durante el desarrollo de sistemas.
Relaciones con Suministradores	Auditorías de seguridad para nuevos sistemas; revisiones de actualizaciones implementadas.	Controles de seguridad en el ciclo de vida del desarrollo de software requieren atención adicional.
Gestión de Incidentes	Procedimientos documentados y medidas correctivas implementadas.	Revisión post-incidente para identificar mejoras necesita fortalecerse.
Cumplimiento	Cumplimiento con leyes y regulaciones; auditorías	Revisiones periódicas y actualizaciones de políticas para

	externas realizadas regularmente.	asegurar cumplimiento continuo son necesarias.

Identificación de brechas en el cumplimiento y posibles causas

Levantamiento de activos y procesos

Auditoría interna de lo que debería tener en base a la SEPS

3. Requisitos del Segmento Superior

Se deben considerar los siguientes lineamientos para que la COAC. Achik Inti suba de segmento:

- **Cumplimiento Normativo:** La COAC Achik Inti debe cumplir con las normativas específicas establecidas por la SEPS para el segmento 3. Esto incluye la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO 27001.
- **Políticas de Seguridad:** Las políticas de seguridad deben ser revisadas y actualizadas para cumplir con los estándares exigidos, asegurando su difusión entre todo el personal.
- **Evaluación y Gestión de Riesgos:** Es fundamental realizar una evaluación exhaustiva de riesgos de seguridad y documentar medidas de mitigación según lo requerido por la SEPS.
- **Capacitación del Personal:** El personal debe recibir formación adecuada en seguridad de la información para cumplir con los estándares del segmento superior.
- **Infraestructura Tecnológica:** Debes garantizar que la infraestructura tecnológica de la cooperativa esté adecuada para soportar las exigencias de seguridad del segmento 3, incluyendo la protección de datos, cifrado y control de accesos.
- **Auditorías y Monitoreo:** Implementa procesos de auditoría y monitoreo continuo para asegurar el cumplimiento constante de las normativas y ajustar las estrategias de seguridad según sea necesario.

4. Plan de Acción

El plan de acción para la progresión al segmento superior debe ser integral y abordar todas las áreas clave de seguridad de la información. Aquí se detalla un plan estructurado para la COAC Achik Inti:

1. Actualización de Políticas de Seguridad

- **Acción**: Revisar y actualizar las políticas de seguridad de la información para alinearlas con la normativa ISO 27001 y los requisitos del segmento 3 de la SEPS.
- **Recursos**: Equipo de seguridad de la información, consultores especializados.
- **Plazo**: 3 meses.
- **Responsable**: Comité de Seguridad de la Información.

2. Mejora de Infraestructuras Tecnológicas

- **Acción**: Modernizar la infraestructura tecnológica para cumplir con los requisitos de seguridad, incluyendo la implementación de sistemas de control de acceso, cifrado de datos, y protección contra amenazas cibernéticas.
- **Recursos**: Presupuesto para adquisición de tecnología, equipo de TI, proveedores de tecnología.
- **Plazo**: 6 meses.
- **Responsable**: Departamento de TI.

3. Capacitación del Personal

- **Acción**: Desarrollar un programa de capacitación continua en seguridad de la información para todos los empleados, con especial énfasis en las mejores prácticas y cumplimiento normativo.
- **Recursos**: Material de capacitación, formadores especializados, plataforma de e-learning.
- **Plazo**: 4 meses (inicio y luego formación continua).

- **Responsable**: Recursos Humanos en colaboración con el equipo de seguridad de la información.

4. Gestión de Riesgos y Protección de Datos

- **Acción**: Implementar un proceso de gestión de riesgos que incluya la identificación, evaluación y mitigación de riesgos relacionados con la seguridad de la información, con especial atención a la protección de datos sensibles.
- **Recursos**: Software de gestión de riesgos, consultoría externa.
- **Plazo**: 3 meses.
- **Responsable**: Comité de Riesgos y Seguridad.

5. Monitoreo y Auditoría Continua

- **Acción**: Establecer un sistema de monitoreo continuo del SGSI, incluyendo auditorías internas regulares para asegurar el cumplimiento constante con las normativas y la efectividad de las políticas implementadas.
- **Recursos**: Software de auditoría, equipo de auditoría interna.
- **Plazo**: Implementación en 2 meses, luego revisiones trimestrales.
- **Responsable**: Departamento de Auditoría Interna.

6. Comunicación y Difusión

- **Acción**: Asegurar que todas las políticas y medidas implementadas sean comunicadas de manera efectiva a todos los niveles de la organización, fomentando una cultura de seguridad de la información.
- **Recursos**: Campañas internas de comunicación, reuniones informativas.
- **Plazo**: Inmediato y continuo.
- **Responsable**: Comité de Comunicación Interna.

Este plan de acción debe ser ejecutado de manera rigurosa, con una supervisión constante y ajustes según sea necesario para asegurar que la COAC Achik Inti cumpla con los requisitos del segmento superior y fortalezca su postura en seguridad de la información.

5. Recursos Necesarios

En este apartado se detallan los recursos esenciales para llevar a cabo el plan de acción orientado a la progresión de la COAC Achik Inti al segmento superior, conforme a los requisitos establecidos por la SEPS y las normativas de seguridad de la información. La implementación exitosa de este plan requiere la asignación adecuada de recursos humanos, tecnológicos y financieros, así como la colaboración de equipos especializados. A continuación, se presenta una tabla que desglosa cada recurso necesario, su descripción, los responsables de su gestión y los plazos correspondientes.

Área	Recursos	Descripción	Responsable	Plazo
Actualización de Políticas de Seguridad	Equipo de Seguridad de la Información	Personal encargado de revisar y actualizar políticas	Comité de Seguridad de la Información	3 meses
	Consultores Especializados	Asesoría externa en normativas ISO 27001 y SEPS	Comité de Seguridad de la Información	3 meses
Mejora de Infraestructuras Tecnológicas	Presupuesto para Tecnología	Fondos para adquirir y actualizar sistemas de TI	Departamento de TI	6 meses
	Equipo de TI	Personal técnico para la implementación de nuevas tecnologías	Departamento de TI	6 meses
Capacitación del Personal	Proveedores de Tecnología	Empresas que suministren tecnología adecuada	Departamento de TI	6 meses
	Material de Capacitación	Contenido formativo en seguridad de la información	Recursos Humanos	4 meses

	Formadores Especializados	Instructores o plataformas de formación en seguridad	Recursos Humanos	4 meses
	Plataforma de E-learning	Herramientas para formación continua online	Recursos Humanos	4 meses
Gestión de Riesgos y Protección de Datos	Software de Gestión de Riesgos	Herramienta para identificar, evaluar y mitigar riesgos	Departamento de TI	3 meses
	Consultoría Externa	Asesoría para la implementación de medidas de protección de datos	Departamento de TI	3 meses
Monitoreo y Auditoría Continua	Software de Auditoría	Herramienta para monitorear y auditar el SGSI	Departamento de Auditoría Interna	2 meses
	Equipo de Auditoría Interna	Personal encargado de realizar auditorías regulares	Departamento de Auditoría Interna	2 meses
Comunicación y Difusión	Campañas Internas de Comunicación	Estrategias para comunicar políticas y medidas de seguridad	Comité de Comunicación Interna	Inmediato
	Reuniones Informativas	Sesiones para informar y sensibilizar al personal sobre nuevas políticas	Comité de Comunicación Interna	Inmediato

6. Indicadores de Progreso

Para garantizar que el plan de acción sea implementado de manera efectiva y que la COAC Achik Inti avance hacia el cumplimiento de los requisitos del segmento superior, se han definido una serie de Indicadores Clave de Desempeño (KPI) que permitirán monitorear el progreso y hacer ajustes oportunos si es necesario. Estos indicadores están diseñados para medir el éxito de las actividades en cada área clave y asegurar que se cumplan los objetivos dentro de los plazos establecidos.

Área	Indicador de Progreso (KPI)	Meta	Frecuencia de Monitoreo	Responsable
Actualización de Políticas de Seguridad	Porcentaje de políticas actualizadas	100% de políticas actualizadas	Mensual	Comité de Seguridad
	Nivel de difusión entre el personal	90% del personal informado	Trimestral	Recursos Humanos
Mejora de Infraestructuras Tecnológicas	Porcentaje de sistemas tecnológicos actualizados	100% de los sistemas necesarios	Bimensual	Departamento de TI
	Tasa de incidentes de seguridad detectados	Reducción del 50% en incidentes	Trimestral	Departamento de TI
	Porcentaje de empleados	95% del personal	Trimestral	Recursos Humanos

Capacitación del Personal	capacitados en seguridad	capacitado		
	Nivel de competencia en seguridad según evaluaciones	85% de aprobación en evaluaciones	Trimestral	Recursos Humanos
Gestión de Riesgos y Protección de Datos	Número de riesgos identificados y mitigados	100% de riesgos críticos mitigados	Trimestral	Comité de Riesgos y Seguridad
	Tasa de cumplimiento de protección de datos	100% de cumplimiento normativo	Semestral	Comité de Riesgos y Seguridad
Monitoreo y Auditoría Continua	Número de auditorías realizadas	4 auditorías anuales	Trimestral	Auditoría Interna
	Porcentaje de acciones correctivas implementadas	90% de acciones correctivas completadas	Trimestral	Auditoría Interna
Comunicación y Difusión	Nivel de conocimiento del personal sobre políticas	90% del personal comprende las políticas	Trimestral	Comunicación Interna

	Tasa de participación en campañas de concienciación	80% de participación del personal	Trimestral	Comunicación Interna

7. Monitoreo y Revisión Continua

El éxito de la implementación del plan de acción para la progresión al segmento superior depende de un monitoreo y revisión continua del avance y cumplimiento de los objetivos establecidos. Este proceso incluye las siguientes actividades clave:

1. **Monitoreo Regular:**
    - Implementar un sistema de seguimiento continuo de los Indicadores Clave de Desempeño (KPI) definidos, asegurando que cada área cumpla con sus metas dentro de los plazos estipulados.
    - Realizar revisiones mensuales de los avances en la actualización de políticas, mejoras tecnológicas, capacitación del personal y gestión de riesgos.
2. **Auditorías Internas:**
    - Programar auditorías trimestrales para evaluar la efectividad de las medidas implementadas y el cumplimiento de las normativas de seguridad.
    - Las auditorías deben identificar cualquier desviación o área de mejora, asegurando que las acciones correctivas se implementen oportunamente.
3. **Revisión de Políticas y Procedimientos:**
    - Realizar una revisión semestral de las políticas y procedimientos de seguridad de la información para garantizar que se mantengan alineados con las regulaciones actuales y los requisitos del segmento superior.

- Ajustar las políticas según los resultados del monitoreo y auditorías para responder a cambios en el entorno de amenazas o en las normativas aplicables.

4. **Informes de Progreso:**
    - Generar informes trimestrales que documenten el progreso en la implementación del plan de acción, destacando los logros, desafíos y cualquier ajuste necesario.
    - Presentar estos informes a la alta dirección y al comité de seguridad para asegurar un alineamiento continuo con los objetivos estratégicos de la COAC Achik Inti.
5. **Ajuste y Mejora Continua:**
    - Basado en los resultados del monitoreo y las auditorías, realizar ajustes en las estrategias y tácticas implementadas para asegurar la efectividad del plan.
    - Fomentar una cultura de mejora continua en todos los niveles de la organización, asegurando que el SGSI evolucione para enfrentar nuevos desafíos y oportunidades..

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Israel Sebastián Romero Loja portador(a) de la cédula de ciudadanía Nº **0303040125** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **Cumplimiento de la normativa de seguridad de La información, para la COAC Achik Inti del cantón Cañar, segmento 4 y su progresión al segmento 3, bajo la regulación de La SEPS,** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **29 de noviembre de 2024**

F: .....

Israel Sebastián Romero Loja

C.I. **0303040125**